INFORMATION AND CONTROL 46, 16–25 (1980)

Error Codes Constructed in Residue Number Systems with Non-Pairwise-Prime Moduli

FERRUCCIO BARSI AND PIERO MAESTRINI

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

Codes constructed in a Residue Number System (RNS) of moduli $m_1, m_2, \ldots, m_n$ are non-binary, arithmetic codes whose codewords are vectors where the ith component is m_i-valued ($1 \leqslant i \leqslant n$). A new class of codes in RNS is described, where redundancy is introduced by removing the constraint that the moduli of the RNS be pairwise prime. The error-detecting and correcting capabilities of such codes are discussed and a simple approach to error detection, localization and correction is presented. Although the codes under consideration are quite inefficient in some respects, it is shown that they may provide a wide coverage of "random" errors. A subclass of these codes is examined in more detail. Codes in this subclass, besides correcting all single errors, also correct almost all of double errors and localize some errors of higher multiplicity, with less redundancy than required to construct optimal 2-correcting codes in RNS.

1. INTRODUCTION

Non-binary, multiple-error-correcting arithmetic codes constructed in Residue Number Systems (RNS) have been described in a number of previous papers. Two important classes of such codes, namely systematic codes in RNS and AN codes in RNS, have been investigated in depth and efficient decoding algorithms have been reported (Mandelbaum 1976, Barsi and Maestrini 1978a). In both classes codewords coincide with residue representations of integers in RNS with pairwise-prime moduli $m_1, m_2, \ldots, m_n$ (Szabo and Tanaka, 1967). This implies that codewords are vectors where the ith component is m_i-valued ($1 \leqslant i \leqslant n$). In Systematic codes redundancy has the form of some redundant residue digits, while in AN codes integers to be represented as codewords are multiplied by a factor A, called the generator. It has been proved that both Systematic and AN codes in RNS are optimal codes (Barsi and Maestrini, 1978b).

Other classes of codes may be constructed in RNS by using different techniques. For example, a class of 1-correcting codes displaying some interesting properties is constructed by appending a *magnitude index* to the residue representation of integers (Barsi and Maestrini, 1978c). This paper describes a new class of residue codes, where redundancy is introduced by removing the hypo-

0019-9958/80/070016-10$02.00/0

thesis that the moduli of the RNS be pairwise prime. The error-detecting and correcting capabilities of such codes are investigated and a simple approach to error detection, localization and correction is presented. Although the codes under consideration exhibit some awkward characteristics and redundancy must attain or exceed duplication in order to ensure single residue digit detection or correction, they may prove quite effective in providing a wide coverage of "random" errors. A subclass of codes constructed in RNS with non-pairwise-prime moduli, where redundancy equals duplication and each modulus shares a factor with each of the remaining moduli, is examined in more detail and it is shown that some codes in this subclass, besides correcting all single errors, also correct almost 100 % of double errors and identify all wrong digits ensuing from most errors up to multiplicity $[(n-1)/2]$[1], where n is the number of moduli, with less redundancy than required to construct optimal 2-correcting codes in RNS.

2. Residue Number Systems with Non-Pairwise-Prime Moduli

Let $m_1, m_2, \dots, m_n$ be a set of positive integers, called the *moduli*, $P = \prod_{i=1}^{n} m_i$ and $M = \text{l.c.m.}\ (m_1, m_2, \dots, m_n)$ the least common multiple of the moduli. For any integer X, $x_i = |X|_{m_i}$ denotes the *residue* of X modulo m_i and the n-tuple $(x_1, x_2, \dots, x_n)$ is called the *residue representation* of X with the moduli m_1, $m_2, \dots, m_n$, where x_i is the ith *residue digit*. If $d_{ij} = \text{g.c.d.}\ (m_i, m_j)$ is the greatest common divisor of the moduli m_i and m_j, from $X \equiv x_i \bmod m_i$, $X \equiv x_j \bmod m_j$ the following congruences are immediate (Vinogradov, 1954):

$$X \equiv x_i \bmod d_{ij}$$

$$X \equiv x_j \bmod d_{ij}$$

and also

$$x_i \equiv x_j \bmod d_{ij}. \tag{1}$$

Conversely, every n-tuple satisfying congruence (1) is the residue representation of an integer X in $[0, M)$. This result is immediate from the following theorem (Ore, 1952), which is a general form of the well-known Chinese Remainder Theorem.

Theorem 1. *The solution of the simultaneous congruences* $X \equiv x_1 \bmod m_1$, $X \equiv x_2 \bmod m_2, \dots, X \equiv x_n \bmod m_n$ *can be expressed in the form*

$$X \equiv x_1 c_1 \frac{M}{m_1} + \cdots + x_n c_n \frac{M}{m_n} \bmod M, \tag{2}$$

[1] $[a]$ means the greatest integer smaller than, or equal to, a.

where $c_1, c_2, \ldots, c_n$ are integers satisfying

$$c_1 \frac{M}{m_1} + c_2 \frac{M}{m_2} + \cdots + c_n \frac{M}{m_n} \equiv 1 \bmod M. \tag{2'}$$

In order to determine a set of integers $c_1, c_2, \ldots, c_n$ satisfying congruence (2') let $\mu_1, \mu_2, \ldots, \mu_n$ be pairwise-prime integers such that μ_i divides m_i and $\prod_{i=1}^{n} \mu_i = M$.

Define $c_i = (m_i/\mu_i) \cdot (M/\mu_i)'$, where $(M/\mu_i)'$ denotes the multiplicative inverse of (M/μ_i) modulo μ_i, if $\mu_i > 1$, else $c_i = 0$. It is easily seen that $c_1(M/m_1) + c_2(M/m_2) + \cdots + c_n(M/m_n) \equiv 1 \bmod \mu_i$ for every i such that $\mu_i > 1$, whence congruence (2') immediately follows.

Theorem 1 provides a means to reconstruct the integers in $[0, M)$ represented by n-tuples satisfying (1), as shown in the following example.

EXAMPLE. In the residue system of moduli $m_1 = 12$, $m_2 = 15$, $m_3 = 16$ and $m_4 = 21$, consider the 4-tuple (4, 7, 8, 19) satisfying congruence (1); here $M = 1680$ and $M/m_1 = 140$, $M/m_2 = 112$, $M/m_3 = 105$, $M/m_4 = 80$. The integers $c_1 = 8$, $c_2 = 3$, $c_3 = 9$, $c_4 = 12$ satisfy congruence (2'). The number in the range $[0, M)$ satisfying congruence (2) is $X = 712$. In fact it is easily verified that the residue representation of X is (4, 7, 8, 19).

From the preceding discussion it is clear that the set of the residue representations of integers with the moduli $m_1, m_2, \ldots, m_n$ defines a RNS of range M. Such RNS is redundant since in the set of the n-tuples $(x_1, x_2, \ldots, x_n)$ with $x_i \in [0, m_i)$, $1 \leqslant i \leqslant n$, whose cardinality is P, only those n-tuples which satisfy congruence (1) are valid representations. From Theorem 1, the number of valid representations is equal to M. The set of valid representations can be regarded as a code $\mathscr{C}$, whose codewords are vectors of n components and the ith component is m_i-valued. This code has redundancy $R = P/M$. The error-detecting and correcting properties of such a code will be investigated in the following sections.

3. Error Detection and Localization

Let $(x_1, x_2, \ldots, x_n)$ be a codeword representing an integer X in $[0, M)$ and assume that an arbitrary error $E \equiv (e_1, e_2, \ldots, e_n)$, with $e_i \in [0, m_i)$ for $1 \leqslant i \leqslant n$, alters the residue digits, thus yielding the n-tuple $(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)$, where $\bar{x}_i = | x_i + e_i |_{m_i}$. The number of non-zero elements in the n-tuple $(e_1, e_2, \ldots, e_n)$ is the *error multiplicity*. Error E is detectable if and only if the resulting n-tuple is not a codeword or, from Theorem 1, if congruence

$$\bar{x}_i \equiv \bar{x}_j \bmod d_{ij} \tag{1'}$$

does not hold for at least one pair (i,j) with $i \neq j$, $1 \leqslant i, j \leqslant n$. Letting $\delta_i = $ l.c.m. $(d_{i1}, d_{i2}, \ldots, d_{in})$, it is clear that most single residue digit errors and many errors of higher multiplicity will be detected if $\delta_i \geqslant 2$ for every i, $1 \leqslant i \leqslant n$. However, the following Theorem shows that redundancy must equal or exceed duplication in order to ensure detection of all single residue digit errors.

THEOREM 2. *A residue code with non-pairwise-prime moduli will detect all single errors if and only if* $\delta_i = m_i$ *for every* i, $1 \leqslant i \leqslant n$.

Proof. If error E affects the ith residue digit, then $\bar{x}_i = |x_i + e_i|_{m_i}$ and $\bar{x}_j = x_j$ for $i \neq j$. From congruence (1) error detection will occur unless $x_i + e_i \equiv x_j \bmod d_{ij}$, or equivalently $e_i \equiv 0 \bmod d_{ij}$, for every $j \neq i$. This implies that error e_i is not detectable if and only if $e_i \equiv 0 \bmod \delta_i$ (Vinogradov, 1954). Since $e_i = |\bar{x}_i - x_i|_{m_i}$, $e_i < m_i$, this congruence will never hold for $e_i \neq 0$ if and only if $\delta_i = m_i$. Q.E.D.

As a consequence of Theorem 2, every prime factor of M must be common to at least two moduli, that is $R \geqslant M$. Although Theorem 2 makes it clear that

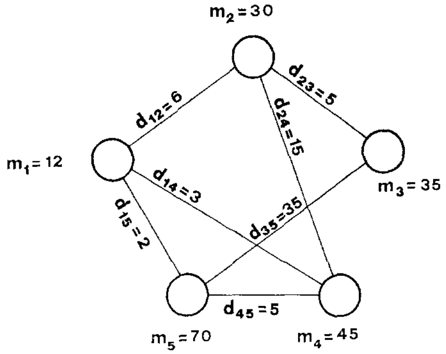

FIGURE 1. Example of an RNS whose corresponding code is more than duplicated.

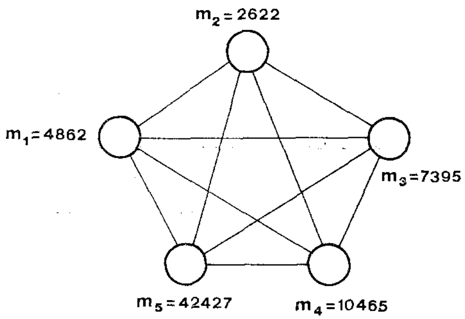

FIGURE 2. Example of an RNS whose corresponding code is exactly duplicated.

Residue Number Systems with non-pairwise-prime moduli are poor codes as far as single-error detection is concerned, a deeper investigation is in order. A graph representation is useful to this purpose. This representation consists of an undirected graph $G = (V, E)$, where to modulus m_i there corresponds vertex v_i and an edge e_{ij} connects vertices v_i and v_j if and only if $d_{ij} =$ g.c.d. $(m_i, m_j) \geqslant 2$. For example, it is easily verified that the RNS represented in Fig. 1 satisfies the condition of Theorem 2 and that the corresponding code will detect all single errors; here $P = 39690000$, $M = 210$, $R = 189000$ and the code is more than duplicated. The code corresponding to the RNS represented in Fig. 2 will also detect single errors; however, in this case $M = R = 6469693230$ and the code is exactly duplicated. The code represented in Fig. 2 is a member of a class, denoted $\mathscr{D}$, of exactly duplicated codes; codes in $\mathscr{D}$ are constructed with a set of n moduli, such that every modulus m_i has $n - 1$ pairwise-prime factors d_{ij} $(d_{ij} > 1)$ and every such factor is also a divisor of one modulus m_j other than m_i. The graph representation of every code in $\mathscr{D}$ is a complete graph of n vertices, where the edges correspond to factors d_{ij}.

Let $\bar{X} = (\bar{x}_1, \bar{x}_2, ..., \bar{x}_n)$ be an n-tuple deriving from an error E altering a codeword and assume that edge e_{ij} in the graph representation is labeled with 0 if congruence (1′) holds, and otherwise labeled with 1. It follows from the preceding analysis that error E is detected if and only if at least one edge is labeled with 1 in the graph representation.

The graph representation shown in Fig. 1 and 2 is closely connected to the diagnostic model of Preparata *et al.* (1967). This model consists of a directed graph, where each vertex v_i represents a unit u_i of a system and there exists an arc a_{ij} from vertex v_i to vertex v_j if unit u_i tests unit v_j. Arcs are given binary labels coinciding with the test outcomes. The test outcomes will result from the state of the testing and the tested unit, as defined in Table I, where F means faulty and $\bar{F}$ means non-faulty and an x entry for the test outcome means that both test outcomes are possible. It is known (Preparata *et al.*, 1967) that the set of test outcomes contains the information necessary to identify all faulty units provided their number does not exceed the *one-step-diagnosability* of

TABLE I

Test Outcomes in the Diagnostic Model of Preparata, Metze and Chien

u_i	u_j	Outcome
$\bar{F}$	$\bar{F}$	0
$\bar{F}$	F	1
F	$\bar{F}$	x
F	F	x

the system, which is bounded above by $[(n-1)/2]$, where n is the number of units. The actual value of one-step diagnosability of a given system can be determined by analysing the diagnostic graph, and diagnostic graphs of systems of n units whose one-step diagnosability equals any given value not exceeding $[(n-1)/2]$ are easily determined (Preparata *et al.*, 1967). In particular, the one-step diagnosability of systems whose diagnostic graph is the complete graph of n nodes is equal to $[(n-1)/2]$.

Returning to the graph representation of Residue Number Systems, consider the set of errors $\mathscr{E} \equiv \{e_1', e_2', \ldots, e_n'\}$ such that e_i' is not a multiple of any factor d_{ij} common to moduli m_i and m_j such that $d_{ij} > 1$. It is easily verified that the edge labels in the graph representation, resulting from any error in $\mathscr{E}$, are those defined in Table II, where the entries F or $\bar{F}$ for m_i (or m_j) mean that the residue digit modulo m_i (or m_j) is altered or not altered, respectively, by the error under consideration, and entry x for the arc label means that both labels may occur.[2] Since Table II is a further specification of Table I it is clear that whenever the graph representation of a RNS and the diagnostic model of a system are isomorphic (it is assumed that a nonoriented edge be equivalent to a pair of arcs with both orientations), then the set of edge labels in the graph representation corresponding to any error in $\mathscr{E}$ contains the information necessary to identify all of the residue digit in error, provided that the error multiplicity does not exceed the one-step diagnosability t of the system. Although it cannot be excluded that identification of all wrong digits is possible even if the error multiplicity exceeds t, a simple reasoning shows that this is not the case if $t = [(n-1)/2]$. In fact, for any $2 \leqslant k \leqslant ((n-1)/2)$ there exist errors $E \in \mathscr{E}$ of multiplicity k such that $e_i \equiv e_j \bmod d_{ij}$ for every pair (e_i, e_j) with $e_i \neq 0$, $e_j \neq 0$. Such errors cause the edge (m_i, m_j) to be labeled with 0 in the graph representation. For each such error, there exists at least one error E' of multiplicy $n-k$, such that every wrong digit in E is correct in E' and vice-versa, and the same edge labeling results from E and E'.

TABLE II

Edge Labels Resulting from Errors in $\mathscr{E}$

m_i	m_j	Label
$\bar{F}$	$\bar{F}$	0
$\bar{F}$	F	1
F	$\bar{F}$	1
F	F	x

[2] Actually if both x_i and x_j are wrong and e_i, e_j are the corresponding error components, the label e_{ij} will be 0 if $e_i \equiv e_j \bmod d_{ij}$, and 1 otherwise.

Since errors E and E' are indistinguishable, the error-localization capability cannot extend beyond multiplicity $[(n - 1)/2]$. For example, the duplicate code (Fig. 2) has the capability of identifying all of the wrong digits resulting from double errors in $\mathscr{E}$ since the graph representation is the complete graph of 5 vertices, for which $t = [(n - 1)/2] = 2$.

The preceding discussion shows that codes constructed in Residue Number Systems with non-pairwise-prime moduli are better suited for control of "random" errors. For example, any duplicated code in the class $\mathscr{D}$ defined above, besides detecting any single error, will also detect and localize all errors of multiplicity not exceeding $[(n - 1)/2]$ which are in the set $\mathscr{E}$, that is, almost 100 % of errors of such multiplicity. A trivial error-detecting procedure consists in determining if there exists at least one edge in the graph representation which is labeled with one.

4. Error Correction

Although it was proved that single-error detecting codes in the class $\mathscr{D}$ are also capable of localizing most errors up to multiplicity $[(n - 1)/2]$, error correction is generally impossible unless further redundancy is introduced. The reason for this is that there exist a few errors of multiplicity 2 or more which are not detectable. For example, any single error $E = (0, 0,..., e_i ,..., 0, 0)$ such that $e_i \not\equiv 0 \bmod d_{ij}$ and $e_i \equiv 0 \bmod d_{ik}$ for $k \neq j$ cannot be corrected since it is indistinguishable from error $E' = (0, 0,..., e_j ,..., 0, 0)$ such that $e_i \equiv e_j \bmod d_{ij}$ and $e_j \equiv 0 \bmod d_{jk}$ for $k \neq j$. In fact, the double error $E'' = (0, 0,..., e_i,..., e_j,..., 0)$ is not detectable since it results in a labeling with 0's in all edges of the graph representation. However, all single errors can be corrected if legitimate numbers in the RNS are limited to an appropriate range $[0, N)$, with $N < M$, as stated by the following Theorem, which uses the notation of Theorem 2.

Theorem 3. *A RNS with non-pairwise-prime moduli and $\delta_i = m_i$ for every i, will correct all single errors if the legitimate range of representation is limited to $[0, N)$, with $N \leqslant (M/\max(d_{ij}))$, $i \neq j$; $1 \leqslant i, j \leqslant n$.*

Proof. Let X be any integer in the legitimate range $[0, N)$ and let E be an arbitrary error affecting the single residue digit x_i $(1 \leqslant i \leqslant n)$; that is, $0 < e_i < m_i$ and $e_j = 0$ for $j \neq i$. If there exist at least two factors, say d_{ij} and d_{ik}, common to m_i and other moduli such that $e_i \not\equiv 0 \bmod d_{ij}$ and $e_i \not\equiv 0 \bmod d_{ik}$, it is easily seen that the error is unambiguously localized in the residue digit modulo m_i in the hypothesis of single errors. Since $\delta_i = m_i$, then l.c.m. $(m_1, m_2 ,..., m_{i-1}, m_{i+1} ,..., m_n) = M$ and the $(n - 1)$ tuples of residues modulo $m_1, m_2 ,..., m_{i-1}, m_{i+1} ,..., m_n$ are unique representations of integers in $[0, M)$. It follows that no information is lost by dropping the residue digit modulo m_i in the residue representation and error correction is achieved by recomputing x_i (e.g., by base extension (Szabo and Tanaka, 1967)) from the remaining residue digits.

If there exists a unique factor of m_i, say d_{ij}, such that $e_i \not\equiv 0 \bmod d_{ij}$, then $\bar{x}_i - x_j \equiv e_i \bmod d_{ij}$, where $\bar{x}_i$ is the wrong digit, and any n-tuple X' obtained from the wrong n-tuple by altering the ith or the jth residue digit such that $x'_i - x'_k \equiv 0 \bmod d_{ik}$ for every $k \neq i$ and $x'_j - x'_k \equiv 0 \bmod d_{jk}$ for every $k \neq j$ yields the given n-tuple by effect of a single residue digit error and might be assumed as the correct n-tuple provided it falls in the legitimate range for codewords. However, since $X' - X \equiv 0 \bmod d_{pq}$ for every $p \neq i$, $q \neq j$, $1 \leqslant p, q \leqslant n$, then $X' - X = k(M/d_{ij})$ (Vinogradov, 1954), where k is some non-zero integer. This implies that X' cannot be an integer in the legitimate range $[0, N)$, since X falls in this range and $N \leqslant (M/d_{ij})$ by hypothesis. It is concluded that error correction is unambiguous and X will be found to be the correct number. Q.E.D.

Consider a single error-correcting code in the class $\mathscr{D}$. Although assuming $[0, N)$ as the legitimate range of representation cannot ensure correction of double errors, this further result is achieved by limiting consideration to errors in the class $\mathscr{E}$ defined in the preceding section. In fact, given the n-tuple representing any letigimate number X, assume that a double error alters the residue digits x_i and x_j, which become $\bar{x}_i = |x_i + e_i|_{m_i}$ and $\bar{x}_j = |x_j + e_j|_{m_j}$. If the error under consideration belongs to $\mathscr{E}$, the wrong digits can be identified, provided the number of moduli is at least equal to 5. By dropping the digits modulo m_i and m_j, the residue representation with the remaining moduli has the capability of representing all integers in the range $[0, M/d_{ij})$ since, as it is seen from Fig. 2, all of the factors dividing the moduli in the set $\{m_1, m_2, \ldots, m_n\}$, except d_{ij}, are retained in the subset of moduli $\{m_1, m_2, \ldots, m_n\} - \{m_i, m_j\}$. From inequality $X < N \leqslant M/d_{ij}$ it follows that no information is lost by dropping the wrong digits and error correction simply consists of recomputing x_i and x_j from the remaining residue digits; e.g., by using base extension.

As already pointed out in Section 3, the preceding result seems to indicate that some codes constructed in RNS with non-pairwise-prime moduli may prove quite efficient in providing protection against random errors, while ensuring correction of single errors. For example, Table III contains an evaluation of the percentage of double errors which are correctable in a single error-correcting code of the class represented in Fig. 2, where n is the number of moduli. The results displayed in Table III are approximate, the approximation consisting in the assumption that each modulus is made up of $n - 1$ factors d_{ij} very close in magnitude and denoting by d the average of these factors. Besides correcting all single errors and almost all of double errors, it should be remembered that the codes under consideration also enable identification of the wrong digits up to multiplicity $[(n - 1)/2]$ under the condition clarified in Section 3. The occurrence of a double error which is not correctable may result in a decoding failure (that

TABLE III

Percentage of Double Errors which Are Corrected by a 1-Correcting Code

n	d	%
5	30	99.35
5	60	99.84
5	120	99.96
7	60	99.99
7	120	99.9999

TABLE IV

Percentage of Double Errors which Result in Decoder Errors in a 1-Correcting Code

n	d	%
5	30	$0.716.10^{-2}$
5	60	$0.910.10^{-3}$
5	120	$0.114.10^{-3}$
7	60	$2.75.10^{-7}$
7	120	$7.97.10^{-9}$

is, the received vector cannot be decoded) or a decoding error (that is, the received vector is decoded into a codeword different from the original one). The percentage of double errors which result in decoding errors is shown in Table IV, which has been constructed by assuming the same approximation used for Table III.

Since Table III shows that almost all double errors are correctable, it seems interesting to provide some comparison between the codes under consideration and optimal 2-correcting codes in RNS (Barsi and Maestrini, 1978–2). A rough comparison can be obtained by assuming that both codes are made up with n moduli, each equal to the product of $n - 1$ factors very close in magnitude and denoting by d the average of these factors. It is easily seen that the number of codewords is equal to d^{n^2-5n+4} in 2-correcting optimal codes constructed in RNS and $d^{((n(n-1))/2)-1}$ in the 1-correcting codes of the class represented in Fig. 2. Since the code length is the same in both cases, it is concluded that the code constructed in RNS with non-pairwise-prime moduli has less redundancy than 2-correcting optimal codes as far as the number of moduli does not exceed seven, yet ensuring correction of almost all of double errors.

RECEIVED: June 22, 1979; REVISED: December 15, 1979

References

Barsi, F., and Maestrini, P. (1978a), A class of multiple-error-correcting arithmetic residue codes, *Inform. Contr.* **36**, 28–41.

Barsi, F., and Maestrini, P. (1978b), Arithmetic codes in residue number systems, *Digital Processes* **4**, 121–135.

Barsi, F., and Maestrini, P. (1978c), Arithmetic codes in residue number systems with magnitude index, *IEEE Trans. Computers C*-**27**, 1185–1188.

Mandelbaum, D. (1976), On a class of arithmetic codes and a decoding algorithm, *IEEE Trans. Information Theory IT*-**12**, 85–88.

Ore, O. (1952), The general chinese remainder theorem, *Amer. Math. Monthly*, 365–370.

Preparata, F. P., Metze, G., and Chien, R. T. (1967), On the connection assignment problem of diagnosable systems, *IEEE Trans. Computers EC*-**16**, 848–854.

Szabo, N. S., and Tanaka, R. I. (1967), "Residue Arithmetic and Its Application to Computer Technology," Sect. 2.3., McGraw–Hill, New York.

Vinogradov, I. M. (1954), "Elements of Number Theory," Chap. 3, Dover, New York.