PACIFIC JOURNAL OF MATHEMATICS
Vol. 70, No. 2, 1977

A GENERALIZATION OF THE CHINESE REMAINDER THEOREM

B. ARAZI

Let X be a set of r nonnegative integers, and let B_i, $i = 1, 2, 3, \cdots, t$ be the unordered sets of residues of the elements of X modulo m_i, where it is not known which element in X produces a given element inB_i.

For the case where $r = 1$, the Chinese Remainder Theorem introduces necessary and sufficient conditions on the values of m_i in order that X may have a unique solution mod $\Pi_{i=1}^{t} m_i$.

This paper introduces such conditions for the case where $r \geqq 1$.

Introduction. The Chinese Remainder Theorem states that the system of congruences $x \equiv b_i \pmod{m_i}$, $i = 1, 2, 3, \cdots, t$ has a unique solution mod $\Pi_{i=1}^{t} m_i$, iff $(m_i, m_j) = 1$ for $i \neq j$.

This leads to the folloing question: Let $X = \{X_1, X_2, \cdots, X_r\}$ be a set of nonnegative integers (not necessarily distinct) and let B_i, $i = 1, 2, 3, \cdots, t$, be the sets of residues of the elements of X modulo m_i, where it is not known which element in X produces a given element in B_i. If $0 \leqq X_i < \Pi_{i=1}^{t} m_i$ for $1 \leqq j \leqq r$, and $(m_i, m_j) = 1$ for $i \neq j$, is it possible to determine the elements of X uniquely, knowing the B_i's?

If a certain value C appears in X for n times then $C \pmod{i}$ appears n times in B_i. If there is only one value which appears in X for n times then in view of the Chinese Remainder Theorem it is possible to determine it uniquely and from it, the whole set X. This paper will therefore treat the most general case where every value appears for the same number of times and without loss of generality it can be assumed that all the elements of X are distinct.

Before any attempt is made at answering the question which was posed, there are two facts which have to be taken into account.

(a) If for some m_i, $X_i \equiv X_j \pmod{m_i}$ then there is no sufficient information for determining X_i and X_j uniquely.

(b) If for some m_i, the set X contains m_i successive integers, which are the only elements in the set, then the set B_i contains all integers from 0 to $m_i - 1$, and X cannot be determined uniquely.

Let X_r and X_1 be the largest and smallest elements of X respectively, and let $m_1 < m_i$ for $i > 1$. In order to take into account the two above-mentioned facts when finding an answer to our question, it is enough to require that $X_r - X_1 < m_1$ and that the number of distinct elements in X will not exceed $m_1 - 1$. With these restrictions, the answer to our question is negative (X cannot be determined uniquely). This can be demonstrated as follows:

Let $X_r > X_{r-1} > \cdots > X_1$. Let p be a divisor of some m_k, $1 \leqq k \leqq t$, and let $X_i - X_{i-1} = p$ for $i = 2, 3, \cdots, r$. Let $s \overset{\Delta}{=} \Pi_{j \neq k} m_j$, and let $q = s \cdot p$. It can be shown that the set $Y = \{X_1 + q, X_2 + q, \cdots, X_r + q\}$ and the set X have the same B_i, $i = 1, 2, \cdots, t$.

In fact, it is always possible to construct such a set Y, if X has a periodic structure with periodicity p.

A necessary and sufficient condition that there should be no periodic set Y, is that $(r, m_i) = 1$ for $i = 1, 2, 3, \cdots, t$. (In the original form of the Chinese Remainder Theorem this condition is always fulfilled, since $r = 1$.)

Interestingly enough, even this condition is not sufficient to determine X uniquely. The following demonstrates a case where two different sets X and Y have the same residue sets B_1 and B_2 ($t = 2$) although m_1 and m_2 are both primes.

$$X = \{11, 12, 14, 15, 19, 20\}$$

$$Y = \{58, 59, 63, 64, 66, 67\}$$

$$m_1 = 11,\ m_2 = 13. \quad (r = 6 < m_1 < m_2)$$

$$B_1 = \{1, 3, 4, 8, 9, 11\}$$

$$B_2 = \{1, 2, 6, 7, 11, 12\}.$$

This paper shows which are the conditions imposed on the values of m_i and r, under which X is determined uniquely.

Theory.

THEOREM. *Let $X = \{X_1, X_2, \cdots, X_r\}$ be a set of distinct nonnegative integers. Let X_r and X_1 be the largest and smallest elements of X respectively, and let m_1 be an integer such that $r \leqq X_r - X_1 < m_1$.*

Let m_k, $k = 2, 3, \cdots, t$ be integers such that $m_t > m_{t-1} > \cdots > m_2 > m_1$ and $(m_i, m_j) = 1$ for $i \neq j$, and let $X_r < \Pi_{i=1}^{t} m_i$.

Let B_i be the sets of residues of the elements of X modulo m_i for $i = 1, 2, 3, \cdots, t$, where it is not known which element in X produces a given element in B. Let $s_{ij} \overset{\Delta}{=} m_i - m_j$.

The set X can be determined uniquely knowing the residue sets B_i iff $(r, m_i) = 1$ and $(r, m_i - n \cdot s_{ij}) < n + 1$ for $n = 1, 2, \cdots, h - 1$ where h is the smallest integer such that $r > m_i - h \cdot s_{ij}$. This applies to $i = 1, 2, 3, \cdots, t - 1$, and all $j < i$.

Before proving the theorem it is worth while showing some corollaries.

COROLLARY 1. *If r is a power of 2, a sufficient condition that X may be determined uniquely is that m_i should be odd for $i = 1, 2, 3, \cdots, t$.*

COROLLARY 2. *X can be determined uniquely if $(r, m_i) = 1$ for $i = 1, 2, 3, \cdots, t$, and $m_i > 2m_{i-1}$ for $i = 2, 3, \cdots, t$.*

COROLLARY 3. *X can be determined uniquely for all possible values of r (as long as $r < m_1 < m_i$, $i = 2, 3, \cdots, t$) if m_i, $i = 1, 2, 3, \cdots, t$ are all primes and $m_i > 2m_{i-1}$, $i = 2, 3, \cdots, t$.*

Proof. Notations: (1) The number of elements in a sequence A is denoted by $l(A)$.

(2) Let A and B be sequences of numbers. The sequence A is a 'sub-sequence' of B iff A consists of $l(A)$ elements which appear successively in B.

Step 1. Interpretation of the theorem in terms of cyclic shifts of binary sequences.

One way of interpreting the Chinese Remainder Theorem for the case where only two congruences are considered ($t = 2$), is as follows. Let P and Q be binary sequences with only one element of value 1, which is also the first element in both sequences. Let $p \overset{\Delta}{=} l(P)$ and $q \overset{\Delta}{=} l(Q)$ (this definition of p and q holds also for the rest of the text) where $(p, q) = 1$. Let P and Q be shifted cyclically through k places until the sequences P' and Q' respectively are obtained, where the first element of both P' and Q' is 1. Then $k = n \cdot p \cdot q$ for some integer n.

In the same way, the following lemma is an interpretation of the proposed theorem for the case $t = 2$.

LEMMA 1. *Let P and Q be binary sequences with r elements of value 1, where $q > p > r$ and $(p, q) = 1$. The first p elements of Q are identical with the elements of P whose first element is 1. Let P and Q be shifted cyclically through k places until the sequences P' and Q' respectively are obtained such that the first p elements of Q' are identical with the elements of P' and this has 1 as the first element. Then k is only of the form $m \cdot p \cdot q$ for some integer m iff $(r, p) = 1$ and $(r, p - n(q - p)) < n + 1$ for $n = 1, 2, \cdots, h - 1$ where h is the smallest integer such that $r > p - h(q - p)$.*

Steps 2 to 7 of this proof deal with the proof of Lemma 1, and the general theorem will be proved only at Step 8.

Step 2. The case of a periodic P. If P has a periodic structure, i.e. it consists of repetition of a sub-sequence A, where $l(A) = k < p$, then P can repeat itself after $m \cdot k$ shifts, where $0 < m \cdot k < p$, and m is an integer. Since P contains at least one element of value 0 (this follows from the fact that $p > r$) it follows that $k \geqq 2$.

If $s \overset{\Delta}{=} p/k$ (s is the number of sequences A) then s must be a divisor of r (since r elements of value 1 must be equally shared among all sub-sequences), which means that $(p, r) > 1$. It follows that the condition stated in Lemma 1 is sufficient for P to be nonperiodic.

Step 3. The case of a periodic Q. By applying to Q the considerations applied above to P, it can be shown that the periodicity of Q implies that $(q, r) > 1$, where Q consists of s sub-sequences A, with $l(A) = k$. Let b denote the number of elements of value 1 in A, then this means that A contains $k - b$ elements of value 0. On the other hand, Q has at least $q - p$ elements of value 0, which appear successively at its end (this follows from the definition of Q in Lemma 1).

Postulate. If $(r, p) = 1$ and $(r, p - n(q - p)) < n + 1$ for $n = 1, 2, \cdots, h - 1$ then Q is nonperiodic. (h was defined in Lemma 1).

Proof. Assume that Q is periodic. Then in view of the preceding discussion, $q = s \cdot k$ and $r = s \cdot b$.

Let $d = q - p$. Since $(p, r) = 1$, this means that $(q - d, r) = 1$ and it follows that $(d, s) = 1$.

It follows that one of the elements of the arithmetic progression $p, p - d, p - 2d, \cdots, p - (s - 1)d$ is divisible by s. Let this element be denoted by a_n. It follows that $(r, a_n) \geqq s$. In order to show that the conditions $(r, p) = 1$ and $(r, p - n(q - p)) < n + 1$ (for $n = 1, 2, \cdots, h - 1$) are sufficient for Q to be nonperiodic it should be shown that $s - 1 \leqq h - 1$. Let $a_1 = p - (h - 1)d$.

$$q = a_1 + hd = a_1 - d + (h + 1)d$$

but $a_1 - d < r$ (follows from the definition of h).

$$\Rightarrow q < r + (h + 1)d,$$

but $q = s \cdot k$, $r = s \cdot b$

$$\Rightarrow s(k - b) < (h + 1)d = (h + 1)(q - p).$$

It was shown before that the sub-sequence A contains $k - b$ elements of value 0, where the minimum number of these elements is $q - p$. Since $k - b \geqq q - p$ it follows that $s < h + 1$, which means that $s - 1 \leqq h - 1$.

This completes the proof of the postulate and it can be concluded that the conditions stated in Lemma 1 are sufficient for Q to be nonperiodic.

However, even for nonperiodic P and Q, it is possible to find the sequences P' and Q' described in Lemma 1 where $0 < k < p \cdot q$, as shown by the following example.

$P = 1100001$, $Q = 11000010000$ ($p = 7$, $q = 11$). If both P and Q are shifted cyclically to the left for 50 places, the following sequences are obtained, $P' = 1000011$, $Q' = 10000110000$.

Step 4. Analysing P, P', Q and Q' assuming their existence for $0 < k < p \cdot q$. Let it be assumed that the sequences P, P', Q and Q' introduced in Lemma 1 exist for $0 < k < p \cdot q$. This Step and the following one will show that this assumption is not valid under the conditions introduced later in the Lemma.

Let $i \equiv k \pmod{p}$ and $j \equiv k \pmod{q}$. It is clear that $i \neq 0$ and $j \neq 0$, otherwise $P = P'$ or $Q = Q'$. The case where $i = j$ is analysed at this Step.

In order that Q' may be obtained from Q by a cyclic shift, Q must have somewhere in it $q - p$ successive zeros (which are transferred to its end by the cyclic shift that produces Q'). These zeros are followed by a 1 (which is transferred to the beginning of Q') and therefore they cannot be part of the last $q - p$ zeros at the end of Q. It follows that Q has in it $q - p$ successive zeros confined to the first p places, which consist of the sequence P.

The sequences Q, P, Q' and P' thus have the following form.

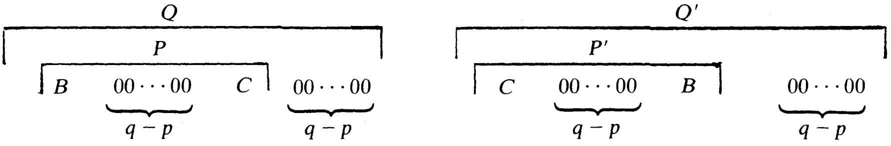

FIGURE 1

where B and C are sequences starting with a 1 (which might be their only element).

Since Q' is obtained from Q by a cyclic shift for j places this means that $l(B) + q - p = j$. Since P' is obtained from P by a cyclic shift for i places and $i = j$ it follows that P' has the following two representations.

$$(1) \quad C \quad \underbrace{00\cdots00}_{q-p}B \quad \text{and}$$

$$(2) \quad CB \quad \underbrace{00\cdots00}_{q-p}$$

These two representations cannot exist simultaneously since C is followed once with a 1 and once with a 0. It follows that the case $i = j$ is impossible.

Step 5. The case where $i \neq j$. Let D_1 denote the block of $q - p$ successive zeros starting at the $(p + 1)$th place in Q. This gives rise to a corresponding block D_2 in the $(p + 1 - j) \bmod q$ place in Q'. (Without loss of generality it can be assumed that Q' is obtained by a left cyclic shift of Q. The same applies to P' and P respectively.) Since both Q and Q' start with a 1 and end with $q - p$ successive zeros it follows that $j > q - p$ and D_2 is therefore confined to the first p places of Q'. Since the first p elements of Q' consist of P' this gives rise to a block D_3 in P' with the same location as D_2 in Q' and this gives rise to a block D_4 in the $[(p + 1 - j) \bmod q + i] \bmod p$ place in P. A block D_5 therefore exists in the same place in Q. Starting the same process all over again, another block D_6 is obtained in Q'. If this block is in the $(p + 1)$th place, the process terminates. Otherwise it goes on following the above procedure. Two blocks D_s and D_t located in the same sequence Q, Q', P or P' do not overlap or abut because they are all followed by a 1. (The first element of a sequence is considered to follow the last one.) Since q is finite this process must finally terminate by obtaining a block D_m in the $(p + 1)$th place in Q'.

It is obvious that if D_u is in Q, Q', P or P' for some u, then $u = 1 \pmod 4$, $2 \pmod 4$, $0 \pmod 4$ or $3 \pmod 4$, respectively.

Postulate. Let D_m be the block which terminates the process. Let the blocks D_{4V+1}, $V = 0, 1, \cdots, (m - 2)/4$ be deleted from Q. Then the remaining sequence consists of repetitions of a sub-sequence A, where A repeats itself at least twice.

Proof. Let all the blocks D_u, $u = 1, 2, \cdots, m$ be deleted from their corresponding sequences Q, Q', P and P' and let the remainders of the sequences be denoted by $\bar{Q}$, $\bar{Q}'$, $\bar{P}$ and $\bar{P}'$, respectively. If the tth element of an original sequence still remains after the deleting process, let its new location be denoted by $\bar{t}$.

Q' is obtained from Q by a left cyclic shift for j places. For every deleted D_{4V+1} in Q which starts at the uth place, there is a deleted D_{4V+2} in Q' which starts at the $(u - j) \bmod q$ place. It follows that $\bar{Q}'$ is obtained from $\bar{Q}$ by shifting $\bar{Q}$ cyclically to the left for $\bar{j}$ places.

P' is obtained from P by a left cyclic shift for i places. For every deleted D_{4V+3} in P' which starts at the uth place, there is a deleted $D_{4(V+1)}$ in P which starts at the $(u + i) \bmod p$ place. It follows that $\bar{P}'$ is obtained from $\bar{P}$ by shifting P cyclically to the left for $\bar{i}$ places.

It is also obvious that $\bar{P} = \bar{Q}$ and $\bar{P}' = \bar{Q}'$ and since $i \neq j$ it follows that $\bar{i} \neq \bar{j}$.

It can be concluded that $\bar{Q}$ *equals some cyclic permutation of itself*, and it therefore consists of repetitions of a sub-sequence A, whose length is $|\bar{i} - \bar{j}|$.

Step 6. The sufficiency of the condition stated in Lemma 1. The length of $\bar{Q}$ is $p - n(q - p)$ for some n. There were n blocks D_u deleted from P with at least one sub-sequence A between any two such blocks. P also starts and ends with A which means that there are at least $n + 1$ sub-sequences A in $\bar{Q}$. Since the r elements of value 1 must be equally shared among the sub-sequences it follows that P' and Q' cannot exist for $k < p \cdot q$ if $(r, p - n(q - p)) < n + 1$ for $n = 1, 2, \cdots, [p/(q - p)]$, unless they are periodic. It was shown in Steps 2 and 3 that this condition together with $(r, p) = 1$ are sufficient for preventing P and Q from being periodic.

If $r > p - n(q - p)$ for some n, the sequence P' cannot exist for $k < p \cdot q$, since the number of elements of value 1 exceeds the number of available places. *This means that if h is the smallest integer such that* $r > p - h(q - p)$ it is not necessary to stipulate that $(r, p - n(q - p)) < n + 1$ for $n \geqq h$.

Step 7. The necessity of the condition stated in Lemma 1. It should be shown *that if* $(p, r) > 1$ or $(r, p - n(q - p)) \geqq n + 1$ for any n, $1 \leqq n \leqq h - 1$, then it is always possible to find P' or Q' for $k < p \cdot q$.

If $(p, r) > 1$ it was shown in Step 2 that P can be periodic and P' can be obtained for $k < p$.

If $(r, p - n(q - p)) = n + 1$ this means that $(r, (n + 1)p - nq) = n + 1$ and it follows that $(r, nq) = n + 1$. Since $(n, n + 1) = 1$ it follows that $(r, q) = n + 1$ and Q is therefore periodic.

If $t_n \overset{\Delta}{=} (r, p - n(q - p)) > n + 1$, let $r = b \cdot t_n$ and $p - n(q - p) = g \cdot t_n$. The values of n are always such that $g \geqq b$. Let A be a sequence of length g starting with a 1 and having b elements of value 1 in it. The *rest of its elements (if exist) are zeros. Let B be a sequence constructed* by attaching consecutively $t_n - n$ sequences A, and let D denote a sequence of $q - p$ zeros.

The sequences Q and Q' are constructed by attaching consecutively A, B and D in the following way. $Q = B, D, A, D, A, D, \cdots, A, D$; $Q' = A, D, A, D, \cdots, A, D, B, D$; where A and D are written n and $n + 1$ times, respectively. It is clear that the sequences P and P' obtained from Q and Q' by dropping the last D, are also obtained each from the other by a cyclic shift.

This completes the proof of Lemma 1.

Step 8. Conclusion. Lemma 1 was identical to the Theorem for the case $t = 2$. The following Lemma is identical to the Theorem in its general form.

LEMMA 2. *Let B_i, $i = 1, 2, 3, \cdots, t$, be binary sequences with r elements of value* 1, *where $l(B_i) \overset{\Delta}{=} m_i$. Let $m_t > m_{t-1} > \cdots > m_2 > m_1 > r$, and $(m_i, m_j) = 1$ for $i \neq j$. The first m_1 elements of all B_i consist of the sequence B_1, with their first element* 1. *Let all B_i be shifted cyclically through k places, until the sequences B'_i are obtained, respectively, where the first m_1 elements of all sequences consist of the sequence B'_1, their first element being* 1. *Let $s_{ij} \overset{\Delta}{=} m_i - m_j$.*

Then k is only of the form $m \cdot \Pi_{i=1}^{t} m_i$, for some integer m, iff $(r, m_i) = 1$ and $(r, m_i - n \cdot s_{ij}) < n + 1$ for $n = 1, 2, \cdots, h - 1$ where h is the smallest integer such that $r > m_i - h \cdot s_{ij}$. This applies to $i = 1, 2, 3, \cdots, t - 1$ and all $j < i$.

The proof of Lemma 2 follows directly by the application of the Chinese Remainder Theorem to Lemma 1, and the proof of the Theorem is thus complete.

ACKNOWLEDGEMENT. The author is thankful to a Referee for making constructive suggestions which enabled a considerable simplification of the proof of the Theorem.

Received August 23, 1976 and in revised form February 8, 1977.

NATIONAL ELECTRICAL ENGINEERING RESEARCH INSTITUTE
P. O. BOX 395
PRETORIA 0001, SOUTH AFRICA