A TECHNIQUE FOR DETERMINING THE INVERSE OF A MATRIX WITH ELEMENTS IN CERTAIN GALOIS FIELDS

by

EDWARD PHIL FABRICIUS

B. S., Kansas State University, 1960

A REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1963

Approved by:

Leonard E. Fuller

Major Professor

TABLE OF CONTENTS

FUNDAMENTAL CONCEPTS

This report is concerned only with square, nonsingular matrices whose elements are in a Galois Field. The cases GF(p), GF(p^2), and GF(p^3) are considered separately as the author is unaware of any general method covering these three cases.

The method of inversion used is the Gaussian Elimination method. This technique is based on three types of elementary row operations defined as follows:

Type I: interchange of corresponding elements in rows i and r;

Type II: multiplication of the elements of a row by a nonzero constant;

Type III: adding k times each element of row r to the corresponding element of row i.

To invert a matrix, M, these operations are employed in a specific order to transform M into the identity matrix I_n. Then, these same operations are applied to I_n, in the exact order that they were applied to M. This transforms I_n into the inverse of M, which is denoted by M^{-1}.

In practice one usually augments the matrix with the identity matrix, which results in an augmented matrix having n rows and 2n columns. This enables one to perform the operations on both the given matrix and the identity matrix at the same time. To avoid changing notation every time a new matrix is obtained, the symbol m_{ij} is used in this report to refer to the elements of the matrix currently under consideration. When the process is completed, the augmented matrix will have the original matrix transformed into the identity and the identity matrix transformed into the inverse matrix.

To invert a matrix by the method of Gaussian Elimination, one first augments the matrix on the right with the identity matrix. Then, if m_{11} is not zero, each element of the first row is multiplied by m_{11}^{-1}. If m_{11} is zero, there will exist an element m_{r1} in the first column that is nonzero, for if all m_{r1} were zero, the matrix would be singular. The type I operation is now applied to rows 1 and r. After multiplying the elements of the first row by m_{11}^{-1}, multiply the first row by m_{k1} and subtract the product from row k where k = 2, 3, ..., n.

Next, one tests m_{22}. In general, if m_{kk} is zero, select an $m_{rk} \neq 0$ for some $r = k+1, k+2, \cdots, n$ and apply the type I operation to rows r and k. Then one multiplies the elements of row k by m_{kk}^{-1}. The other rows are transformed by replacing each m_{ij} with $m_{ij}-m_{ik}m_{kj}$ where $i = 1,2,\cdots,k-1,k+1,\cdots,n$, $j = k,k+1,\cdots,2n$. By repeating this process n times, one will transform the given matrix M into I_n and I_n into M^{-1}.

Before describing how this method is modified for use on an electronic computer, some of the basic theory of Galois Fields will be discussed. The general Galois Field, denoted by $GF(p^t)$, consists of p^t elements of the form

$$a_0 + a_1L + \cdots + a_{t-1}L^{t-1}$$

where each a_i is a residue of the prime modulus, p. The modulus of the field is an irreducible polynomial of the type just described and, for $L = 1, 2, \ldots, p-1$, the equation

$$L^t = a_0 + a_1 L + \ldots + a_{t-1} L^{t-1}$$

has no solution in the field.

Since a field has the property of closure, the product of any two elements $b(L)$ and $c(L)$ is the unique polynomial $r(L)$ given by the division algorithm

$$b(L) \cdot c(L) = q(L) \cdot m(L) + r(L);$$

the degree of $r(L)$ is less than or equal to $n-1$, and $m(L)$ is the irreducible polynomial chosen as the modulus of the field. A field also has the property that the inverse of each element, except the zero element, is in the field. Therefore, if $c(L)$ is the inverse of $b(L)$, then $r(L) = 1$.

It is shown that if $m_1(L)$ and $m_2(L)$ are two irreducible polynomials of the same degree over $GF(p^t)$, the fields $GF(p, m_1(L))$ and $GF(p, m_2(L))$ are isomorphic. This means that the $GF(p^t)$ depends only upon the prime p and the integer t and not upon the irreducible polynomial chosen as the modulus. Hence, one need determine only one irreducible equation for the field as the fields determined by the other irreducible polynomials are isomorphic to it.[1]

---

[1]Cyrus C. MacDuffee, Introduction to Abstract Algebra, pp. 174-175.

These basic facts will enable one to determine the inverse of a matrix with elements in a Galois Field. However, prior to the actual inversion of such a matrix, an adaptation of the Gaussian Elimination process for a computer will be discussed.

AN ADAPTATION OF THE GAUSSIAN ELIMINATION METHOD FOR USE ON AN ELECTRONIC COMPUTER

An adaptation of the Gaussian Elimination process for use on an electronic computer is based upon the fact that when the process is to be applied to row r, the first r-1 columns are in their final form and hence need never be referred to. This enables one to shift the matrix so that when commencing with row r, the diagonal element m_{rr} is the element m_{11} and the $r^{\underline{th}}$ row is row 1.

To show the adaptation in detail, assume that the process has just been applied to row 1. Before commencing with row 2, relocate row 1 into row n+1, an extra row that has been reserved. Each element is now shifted into the row immediately above it by replacing each m_{ij} with $m_{i+1,j}$, $i = 1,2,\cdots,n$, $j = 1,2,\cdots,2n$. In essence, this is the same as applying the type I operation to rows 1 and 2, then to rows 2 and 3, ..., and finally to rows n-1 and n. As column 1 has been transformed into its final form and is not referred to later, it is erased by moving each element into the column to its left. This is accomplished by replacing each m_{ij} with $m_{i,j+1}$, $i = 1,2,\cdots,n$, $j = 1,2,\cdots,2n-1$. On the computer, both shifting operations are performed at the same time by replacing each m_{ij} with $m_{i+1,j+1}$. At this point, note that row 2 is the new row 1, element m_{22} is now m_{11}, and that there are only 2n-1 columns remaining in the augmented matrix. Also, since the first column was erased, one will note that there was no need to transform it into standard form. This is a savings in machine time.

One is now ready to perform the process on the new row 1. However, if m_{11} is zero, the nonzero m_{r1} will have to be among the first n-1 elements of the first column since the last row is the original row 1 and cannot be used again. After multiplying each element of row 1 by m_{11}^{-1}, transform the other rows by replacing each m_{ij} with $m_{ij}-m_{i1}m_{1j}$ where $i = 2, 3, \cdots, n$, $j = 2, 3, \cdots, 2n$. Relocate row 1 into row n+1 and replace each m_{ij} with $m_{i+1,j+1}$. There are now 2n-2 columns remaining in the augmented matrix.

In general, performing the k^{th} iteration, if m_{11} is zero, the nonzero m_{k1} will have to be among the first n-k+1 elements of the first column. After multiplying the elements of row 1 by m_{11}^{-1}, replace each m_{ij} with $m_{ij}-m_{i1}m_{1j}$. Now relocate row 1 into row n+1 and shift by replacing each m_{ij} with $m_{i+1,j+1}$. These five operations:

(1) obtaining nonzero m_{11},

(2) multiplying the elements of row 1 by m_{11}^{-1},

(3) transforming the other rows by replacing each m_{ij} with the difference $m_{ij}-m_{i1}m_{1j}$,

(4) relocating the first row into row n+1, and

(5) shifting the matrix by replacing each m_{ij} with $m_{i+1,j+1}$

constitute the inversion cycle. Although the process has been increased from three to five steps, the method is much easier to program for a computer. As one is interested in the inverse matrix, the process is terminated after n iterations, where n is the number of rows of the matrix. The inverse matrix will be in the locations originally occupied by the given matrix and the identity matrix does not appear.

The Number of Storage Locations Required for Storing a Matrix with Elements in GF(p^t)

For the general Galois Field, GF(p^t), each element is of the form

$$a_0 + a_1L + \ldots + a_{t-1}L^{t-1}.$$

Since one cannot store more than one coefficient in a given location, each element will require t locations. This means that each row of an n X n matrix will require nt locations. Therefore, the matrix will have to be thought of, for storage purposes, as consisting of n rows and nt columns.

Each element of the identity is zero except the diagonal elements which are 1. In this field, zero is represented as a polynomial of the form described above where each $a_i = 0$. The number 1 is represented in the same form except $a_0 = 1$, and all other $a_i = 0$. Hence each element of the inverse is composed of t terms. This means the identity matrix will require n rows and nt columns. Therefore, the augmented matrix will be of dimension n X 2nt.

A Method for Generating the Identity Matrix for the GF(p^t)

In practice, one usually stores the matrix in the computer and then has the computer generate the identity matrix, as it is a much faster process than to read in both matrices. To generate the identity matrix for a Galois Field, note that in the augmented matrix, the 1's in the diagonal elements appear in columns $nt+1$, $(n+1)t+1, \cdots, (n+r-1)t+1$, where r is the row in which the 1 appears. Hence, let $r = 1,2,\cdots,n$, $j = 1,2,\cdots,nt$ and define I1 to be $(r-1)t+1$ and j1 to be $nt+j$. If I1-j is zero, the location $m_{r,j1}$ is 1; if I1-j is not zero, location $m_{r,j1} = 0$. By continuing in this manner, one will generate the identity matrix for the augmented matrix with elements in GF(p^t).

INVERSION OF A MATRIX WITH ELEMENTS IN GF(p)

In this field, one must determine the multiplicative inverses of the diagonal elements. Also, each product and sum must be reduced to an element in the field.

The inverse of m_{11} will be an integer I such that $I \cdot m_{11}$ is congruent to 1 modulo p. From elementary congruence relations, this means that the product $I \cdot m_{11}$ leaves a remainder of 1 when divided by the prime p, or, in symbols,

$$I \cdot m_{11} = kp + 1.$$

This is the euclidean algorithm with $r = 1$. Since m_{11} is a residue of p, I will have to be greater than k since $I \cdot m_{11} - 1 = kp$.

Therefore, to determine I, form the expression

$$(1) \qquad I \cdot m_{11} - kp - 1$$

where $I = 1, 2, \cdots, p-1$ and $k = 1, 2, \cdots, I$. As the integers modulo a prime constitute a field, one will always be able to determine an I and a k so that the expression will equal zero. Note that if $m_{11} = 1$, the first row will be in standard form, so one will not have to determine an I and a k. When the expression (1) does equal zero, I will be the inverse of m_{11}. The first row is then transformed by replacing each m_{1j} with $(I \cdot m_{1j})_p$, where $j = 1, 2, \cdots, 2n$. The expression in parentheses is read as I times m_{1j}, then reduced modulo p.

The other rows are transformed by letting $i = 2, 3, \ldots, n$, $j = 2, 3, \ldots, 2n$ and forming the product $(m_{i1}m_{1j})_p$. If $m_{ij} - (m_{i1}m_{1j})_p$ is negative, add p to the difference to make it nonnegative and then replace m_{ij} with this difference. If the difference is nonnegative, it is in the field so one would replace m_{ij} with it. Now relocate row 1 into row n+1 and shift by replacing each m_{ij} with $m_{i+1,j+1}$.

This process is performed n times with n being the number of rows. One will then have the inverse in the locations originally occupied by the matrix, and the identity matrix will not appear.

One use of this program is for the coding and decoding of messages. Such a program, with another program for matrix - vector multiplication over this field, has been submitted to the National Security Agency.

INVERSION OF A MATRIX WITH ELEMENTS IN GF(p^2)

Before one is able to invert a matrix over this field, an irreducible equation must be determined which will be the modulus for the field. To determine such an equation, let $a_1 = 1, 2, \ldots, p$, $a_0 = 1, 2, \ldots, p-1$, and $L = 1, 2, \ldots, p-1$. Form the expression

$$(L^2)_p-(a_0+a_1L)_p.$$

If, for a fixed a_1 and a_0, this is not zero for all values of L, the equation

$$L^2 = a_0+a_1L$$

is irreducible and determines the field. If it does equal zero for some value of L, the equation determined by a_0 and a_1 is reducible and does not determine the GF(p^2). As noted previously, one need determine only one irreducible equation. However, if one were interested in determining all irreducible equations, one would let the a_i range over all the values indicated and note those for which the equation is irreducible.

The next step is to determine a method for reducing all products to an element in the field. To do this denote the modulus as a_0+a_1L and consider the product,

$$(b_0+b_1L)(c_0+c_1L) = (b_0c_0)_p + (b_0c_1+b_1c_0)_pL + (b_1c_1)_pL^2.$$

Each element in this field consists of only two terms, a constant term and a term involving L. Hence, to reduce the L^2 term, replace L^2 with the modulus, $a_0 + a_1L$. The product is equal to

$$(b_0c_0)_p + (b_0c_1+b_1c_0)_pL + (a_0b_1c_1)_p + (a_1b_1c_1)_pL.$$

By collecting terms, one has the desired form for the product, namely

$$(b_0c_0+a_0b_1c_1)_p + (b_0c_1+b_1(c_0+a_1c_1))_pL.$$

For the remainder of this section, the first term of this expression will be referred to as the constant term and the second as the coefficient of L.

To commence the inversion process, note that the even numbered columns contain the coefficients of L, while the odd numbered columns contain the constant coefficients. If the coefficient of L in the first element, m_{12}, is zero the inverse will be an integer I. If m_{12} is not zero, the inverse will be of the form $k_0 + k_1L$ where each k_i is a residue of the prime modulus p. Therefore, first test if m_{12} is zero. If so, and $m_{11} \neq 1$, the inverse is determined in the same manner as for GF(p). If $m_{11} = 1$, $m_{12} = 0$, the row is in standard form. If m_{12} is not zero, set $k_1 = 1,2,\cdots,p-1$, $k_0 = 1,2,\cdots,p$ and form the coefficient of L in the products:

$$(m_{11}+m_{12}L)(k_0+k_1L).$$

Values will exist for the k_i such that the coefficient of L is congruent to zero, modulo p. When they have been determined, evaluate the constant coefficient and reduce it modulo p. If the constant coefficient is 1, then k_0+k_1L is the inverse; if it is not 1 (note that it cannot be zero since a field does not have divisors of zero), determine the inverse, I, as for GF(p) and replace each k_i by $(I\cdot k_i)_p$.

If the inverse consists of a single term, I, the first row is transformed by letting $j = 1, 2, \ldots, 4n$ and replacing each m_{1j} by $(I\cdot m_{1j})_p$. If the inverse is of the form k_0+k_1L, let $j = 1, 3, 5, \ldots, 4n-1$ and form the product

$$(m_{1j}+m_{1,j+1}L)(k_0+k_1L).$$

The element m_{1j} is in an odd numbered column, so is replaced by the constant term; $m_{1,j+1}$ is in an even numbered column and is therefore replaced by the coefficient of L. Both coefficients of the product are reduced modulo p prior to replacement.

To transform the other rows, form the product

$$(m_{i1}+m_{i2}L)(m_{1j}+m_{1,j+1}L)$$

and reduce each coefficient modulo p where $i = 2, 3, \ldots, n$, $j = 3, 5, 7, \ldots, 4n-1$. This element is subtracted from the element

$$m_{ij} + m_{i,j+1}L.$$

As the difference must consist of nonnegative terms, one would first test the expression

$$m_{ij} - (\text{constant term}).$$

If this difference is nonnegative, m_{ij} is replaced by it. If the difference is negative, one would add p to it to make the difference nonnegative before replacement. This same test is now applied to

$$m_{i,j+1} - (\text{coefficient of } L).$$

Now relocate row 1 into the (n+1)th row and replace each m_{ij} by $m_{i+1,j+2}$. This erases the first two columns. The reason for this is that each element requires two locations; hence, the first column contains the constant coefficients and the second column, the coefficients of L for the first column of elements.

After repeating this process n times, the inverse will be in the first n rows and 2n columns. It will consist entirely of elements in the field and will be exact.

INVERSION OF A MATRIX WITH ELEMENTS IN $GF(p^3)$

In this field, the irreducible equations are of the form

$$L^3 = a_0 + a_1L + a_2L^2.$$

They are determined by letting L and $a_0 = 1,2,\cdots,p-1$, a_1 and $a_2 = 1,2,\cdots,p$ and noting those combinations of the a_i for which the expression

$$(L^3)_p - (a_0 + a_1L + a_2L^2)_p$$

is not zero for all values of L.

Each element in this field is of the general form

$$b_0 + b_1L + b_2L^2$$

where the b_i are elements of GF(p). One must next consider how the product of two elements is transformed into an element of this field. To show how one does transform the product, denote the modulus by

$$a_0 + a_1 L + a_2 L^2,$$

and consider the product:

$$(b_0+b_1L+b_2L^2)(c_0+c_1L+c_2L^2) = (b_0c_0)_p + (b_0c_1 + b_1c_0)_pL$$

$$+ (b_0c_2+b_1c_1+b_2c_0)_pL^2 + (b_1c_2+b_2c_1)_pL^3 + (b_2c_2)_pL^4.$$

The L^3 term is reduced by replacing L^3 with the modulus. This yields, by denoting the coefficient of L^3 with C_3,

$$C_3(a_0+a_1L+a_2L^2) = (a_0C_3)_p + (a_1C_3)_pL + (a_2C_3)_pL^2.$$

The L^4 term is transformed by replacing L^4 with L times the modulus. By denoting the coefficient of L^4 as C_4, the term is seen to be

$$C_4(a_0+a_1L+a_2L^2)L = (a_0C_4)_pL + (a_1C_4)_pL^2 + (a_2C_4)_pL^3.$$

Again, replace L^3 with the modulus in the last term to obtain

$$(a_2C_4)_p(a_0+a_1L+a_2L^2) = (a_0a_2C_4)_p + (a_1a_2C_4)_pL + (a_2^2C_4)_pL^2.$$

After collecting terms and simplifying, the product of two elements in this field is

$$(b_0c_0 + a_0(b_1c_2 + b_2(c_1 + a_2c_2)))_p +$$

$$(b_0c_1 + b_1c_0 + a_1(b_1c_2 + b_2c_1) + b_2c_2(a_0 + a_1a_2))_pL +$$

$$(b_0c_2 + b_1c_1 + b_2c_0 + a_2(b_1c_2 + b_2c_1) + b_2c_2(a_1 + a_2^2))_pL^2.$$

Hereafter, these coefficients will be referred to as the constant coefficient, the coefficient of L, and the coefficient of L^2, respectively, to avoid writing them out each time they are used.

To determine the inverse of the first element of the matrix, it will be noted that the columns numbered 3c+1 contain the constant coefficients. Those numbered 3c+2 contain the coefficients of L, and those numbered 3c+3 contain the coefficients of L^2. If the coefficients of L and L^2, m_{12} and m_{13} respectively, are zero, the inverse will be an integer I. If at least one of m_{12} and m_{13} is nonzero, the inverse of the element will be of the form

$$k_0 + k_1L + k_2L^2.$$

Therefore, test m_{12} and m_{13}. If both are zero, and $m_{11} \neq 1$, I is determined as it was for GF(p). If $m_{11} = 1$, and m_{12} and m_{13} both equal zero, the first row is in standard form. If at least one of m_{12} and m_{13} is not zero, let $k_2 = 1,2,\cdots,p$, $k_1 = 1,2,\cdots,p$, $k_0 = 1,2,\cdots,p$ and form the coefficient of L^2 in the product

$$(m_{11}+m_{12}L+m_{13}L^2)(k_0+k_1L+k_2L^2).$$

When values of the k_i are determined such that this coefficient is congruent to zero modulo p, evaluate the coefficient of L. If it is not congruent to zero modulo p, repeat the process until values of the k_i are determined so that both of these coefficients are congruent to zero. Now form the constant coefficient and reduce it modulo p. If it is 1, these values of the k_i form the inverse

$$k_0 + k_1L + k_2L^2.$$

If the constant coefficient is not 1, determine its inverse I in the manner described for GF(p) and replace each k_i by $(I \cdot k_i)_p$.

If the inverse of the first element was a constant I, each element of the first row is replaced by

$$(I \cdot m_{1j})_p$$

where $j = 1,2,\cdots,6n$. If the inverse was a polynomial of the type described above, form the product

$$(m_{1j}+m_{1,j+1}L+m_{1,j+2}L^2)(k_0+k_1L+k_2L^2)$$

where $j = 1,4,7,\cdots,6n-2$, and reduce each coefficient modulo p. The element

$$m_{1j} + m_{1,j+1}L + m_{1,j+2}L^2$$

is now replaced by this product.

To transform the other rows, form the product

$$(m_{i1}+m_{i2}L+m_{i3}L^2)(m_{1j}+m_{1,j+1}L+m_{1,j+2}L^2),$$

for $i = 2,3,\cdots,n$, $j = 4,7,10,\cdots,6n-2$, and reduce each coefficient to an integer modulo p. This product is now subtracted from the element

$$m_{ij} + m_{i,j+1}L + m_{i,j+2}L^2.$$

Since each term of the difference must be nonnegative, one first tests

$$m_{ij} - \text{(constant coefficient)}.$$

If this difference is nonnegative, m_{ij} is replaced by it. If the difference is negative, add p to it to make the difference nonnegative before replacement. In like manner, test

$$m_{i,j+1} - \text{(coefficient of } L)$$

and

$$m_{i,j+2} - \text{(coefficient of } L^2).$$

After all rows have been transformed, relocate row 1 into row n+1 and shift each element by replacing each m_{ij} with $m_{i+1,j+3}$. This erases the first three columns since each element of the field requires three storage locations.

After the entire process has been performed n times, the inverse matrix will be located in the first n rows and 3n columns. The inverse will be exact and will consist entirely of elements in $GF(p^3)$.

INVERSION OF A MATRIX WITH ELEMENTS IN THE GENERAL GALOIS FIELD $GF(p^t)$

The general Galois Field $GF(p^t)$ is described by an irreducible equation of the form

$$L^t = a_0 + a_1 L + \cdots + a_{t-1} L^{t-1}.$$

There may be more than one irreducible equation over the field.[2] A method of determining all such equations is to form the expression

$$(L^t)_p - (a_0 + a_1L + \cdots + a_{t-1}L^{t-1})_p$$

and note those combinations of the a_i for which the expression does not equal zero for all values of L. For this, a_0 and L assume the values $1, 2, \cdots, p-1$, the other a_i assuming the values $1, 2, \cdots, p$. One of the irreducible equations is now selected as the modulus. Let it be expressed as

$$a_0 + a_1L + \cdots + a_{t-1}L^{t-1}.$$

The product of two elements in $GF(p^t)$

$$(b_0+b_1L+\cdots+b_{t-1}L^{t-1})(c_0+c_1L+\cdots+c_{t-1}L^{t-1})$$

will be considered by noting the terms of

$$(b_iL^i)(c_0+c_1L+\cdots+c_{t-1}L^{t-1}).$$

When $i = 0$, the maximum exponent of L is $t-1$. Therefore, each term will be in the field. For $i>0$, the maximum exponent of L is $t-1+i$. Thus there are at most i terms that will involve L with an exponent $> (t-1)$. This means that there will be at most $t-1$ terms in the product that involve L to a degree greater than $t-1$. Each of these terms must be transformed into new elements that are in the field. They are transformed by replacing each

---

[2] Ibid., p. 179.

$C_{t-1+i}L^{t-1+i}$ with the expression

$$C_{t-1+i}L^{i+1}(a_0+a_1L+\cdots+a_{t-1}L^{t-1}).$$

This process is continued until there is no term involving L to a degree greater than t-1. Here, C_{t-1+i} is the coefficient of L^{t-1+i} for $i = 1,2,\cdots,t-1$. After transforming each of these terms into elements that are in the field, one collects terms and reduces their coefficients modulo p.

Before determining the inverse, one will note that the augmented matrix is of dimension n X 2nt. The columns numbered tk+1 contain the constant coefficients, $k = 0,1,2,\cdots,2n-1$. Those numbered tk+2 contain coefficients of L, those numbered tk+3 contain the coefficients of L^2, . . . , and those numbered tk+t contain the coefficients of L^{t-1}. To determine the inverse of the first element of row 1, one tests first if the coefficients of L, L^2, . . . , and L^{t-1}, which are m_{12}, m_{13}, . . . , and m_{1t} respectively, are zero. If they are all zero, test if m_{11}, the constant coefficient, is 1. If so, the first row is in standard form. If m_{11} is not 1, and the other coefficients are zero, the inverse I will be determined in the manner described for GF(p). If any combination of the coefficients of the powers of L is nonzero, the inverse will be a polynomial of the form

$$k_0 + k_1L + \cdots + k_{t-1}L^{t-1}.$$

It is determined by locating those values of the k_i for which the product

$$(m_{11}+m_{12}L+\cdots+m_{1t}L^{t-1})(k_0+k_1L+\cdots+k_{t-1}L^{t-1})$$

is congruent to the element

$$1 + 0\cdot L + \cdots + 0\cdot L^{t-1}$$

where each k_i ranges over the values $1, 2, \cdots, p$.

To transform the elements of the first row, if the inverse is a constant I, let $j = 1, 2, \cdots, 2nt$ and replace each m_{1j} by

$$(I\cdot m_{1j})_p.$$

If the inverse is a polynomial $k(L)$, one forms the product of the two elements

$$(m_{1j}+m_{1,j+1}L+\cdots+m_{1,j+t}L^{t-1})(k_0+k_1L+\cdots+k_{t-1}L^{t-1})$$

and reduces the coefficients modulo p. The element

$$m_{1j} + m_{1,j+1}L + \cdots + m_{1,j+t}L^{t-1}$$

is then replaced by this product where j assumes the values $1,\ t+1,\ \cdots,\ 2nt-(t-1)$.

The other rows are now transformed by first forming the product

$$(m_{i1}+m_{i2}L+\cdots+m_{it}L^{t-1})(m_{1j}+m_{1,j+1}L+\cdots+m_{1,j+t-1}L^{t-1})$$

and reducing the coefficients modulo p. This product is now subtracted from the element

$$m_{ij} + m_{i,j+1}L + \cdots + m_{1,j+t-1}L^{t-1}.$$

Since each term of the difference must be nonnegative, test first if

$$m_{ij} - \text{(constant coefficient)}$$

is nonnegative. If it is, m_{ij} is replaced by this difference. If the difference is negative, one would add p to it to make the difference nonnegative prior to replacement. In like manner, test each

$$m_{i,j+r} - \text{(coefficient of } L^r\text{)},$$

$r = 1,2,\cdots,t-1$. When transforming the other rows, $i = 2,3,\cdots;n$ and $j = t+1, 2t+1, \cdots, 2nt-(t-1)$.

The first row is now relocated into row $n+1$, and each m_{ij} is replaced by

$$m_{i+1,j+t}.$$

This causes row 2 to become the new row 1, the constant term of the second diagonal element is now in location m_{11}, and the first t columns of the matrix have been erased.

This process is performed n times where n is the number of rows in the matrix. The inverse matrix is located in the first n rows and nt columns. The inverse matrix is exact and each element of the inverse is in the field $GF(p^t)$.

CONCLUSION

The appendix contains the flow charts and a listing of the actual FORTRAN programs for inverting a matrix with elements in the Galois Fields GF(p), GF(p^2), and GF(p^3). It should be noted that the variable L, in the report, is denoted by the Greek letter Lamda in the flow charts and by LAM in the machine listing.

The actual program is written so that if there is more than one matrix to invert, the program will not have to be read in for each one. Also, if the matrix being inverted happens to be singular, the computer will print SINGULAR and then call for a new matrix.

From the cases considered in this report, one notices that the formation of the product is a very vital part of the inversion process. For the GF(p^t), one notices that there are t-1 terms that have to be transformed into new elements that are in the field. As there does not seem to be any method of predicting, for a given GF(p^t), what the coefficients of the transformed product will consist of, it is doubtful if there can exist a program for inverting a matrix with elements in the general Galois Field. It had been the author's original intention to write such a program, but that idea has been abandoned. Even if such a program is possible, it would probably be so complex as to be impractical.

ACKNOWLEDGEMENT

The author wishes to express his appreciation and sincere thanks to his major professor, Dr. Leonard E. Fuller, for his assistance and valuable insights which he so patiently rendered; it is doubtful that the author could have written this report without this valuable assistance.

BIBLIOGRAPHY

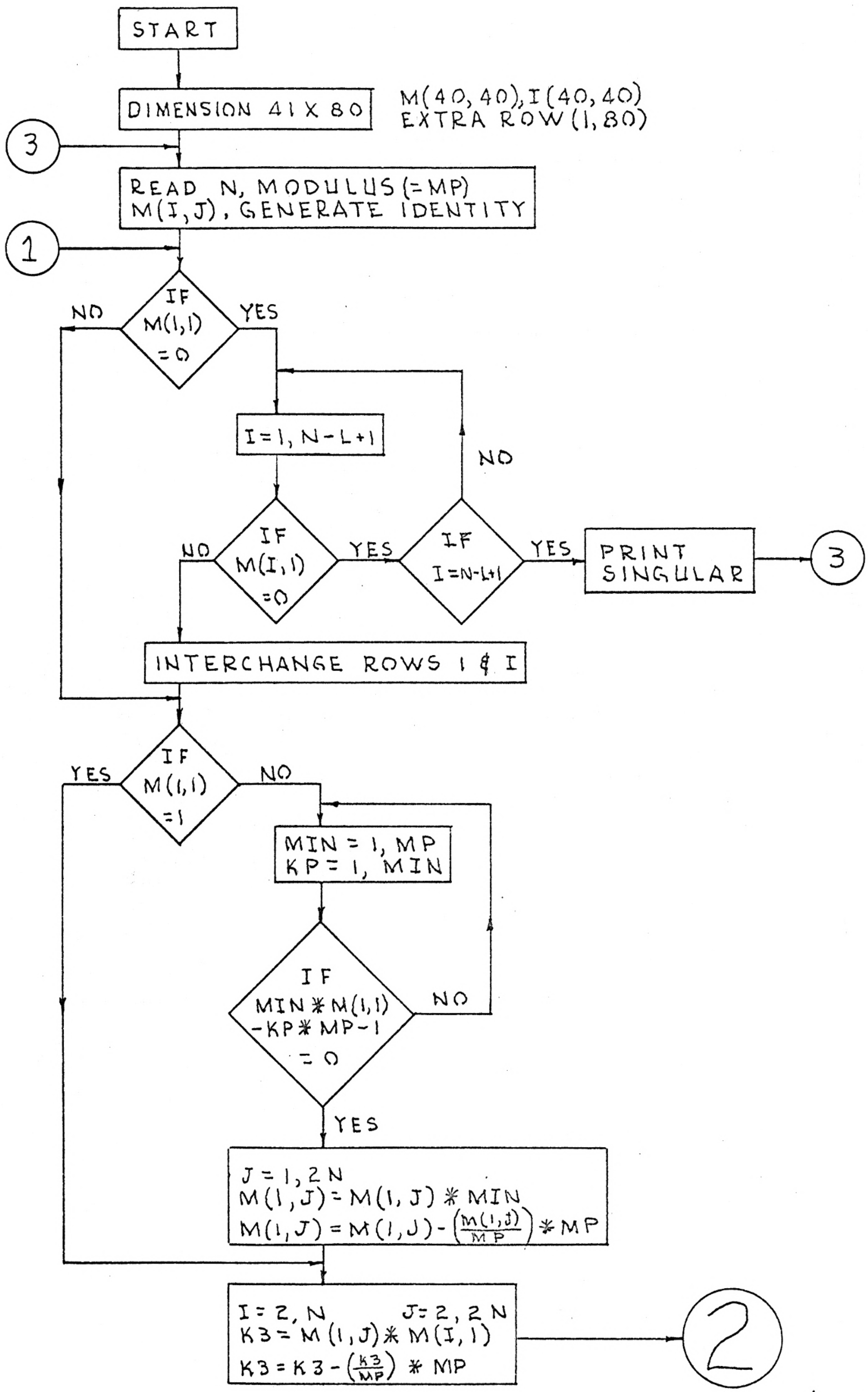
1. Birkhoff, G. and S. Mac Lane, Survey of Modern Algebra, New York: Macmillan Company, 1957

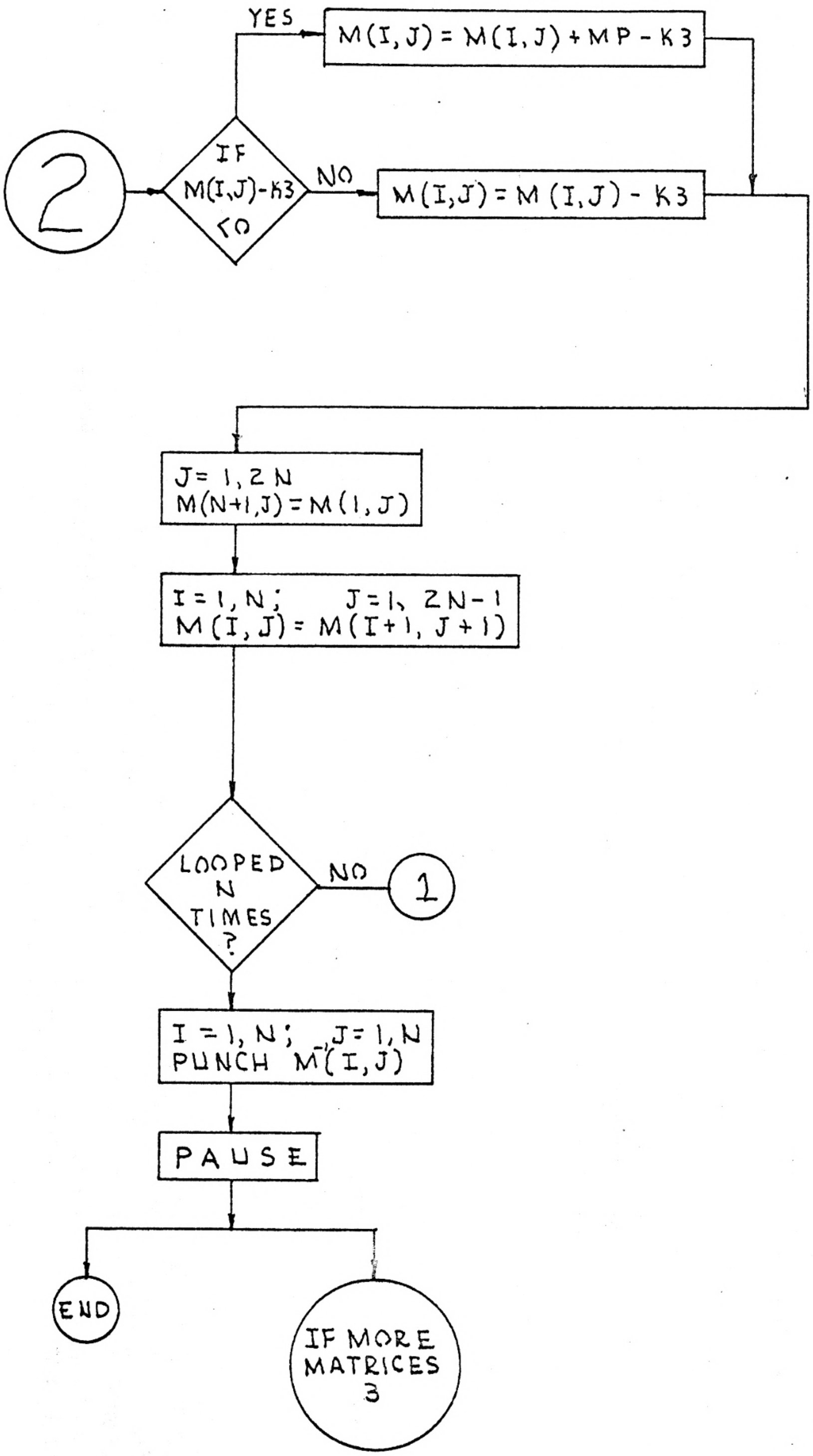
2. Dickson, L. E., Linear Groups with an Exposition of the Galois Field Theory, New York: Dover Publications, Inc., 1958

3. MacDuffee, C. C., Introduction to Abstract Algebra, New York: John Wiley and Sons, Inc., 1961

4. Miller, K. S., Elements of Modern Abstract Algebra, New York: Harper and Brothers, 1958

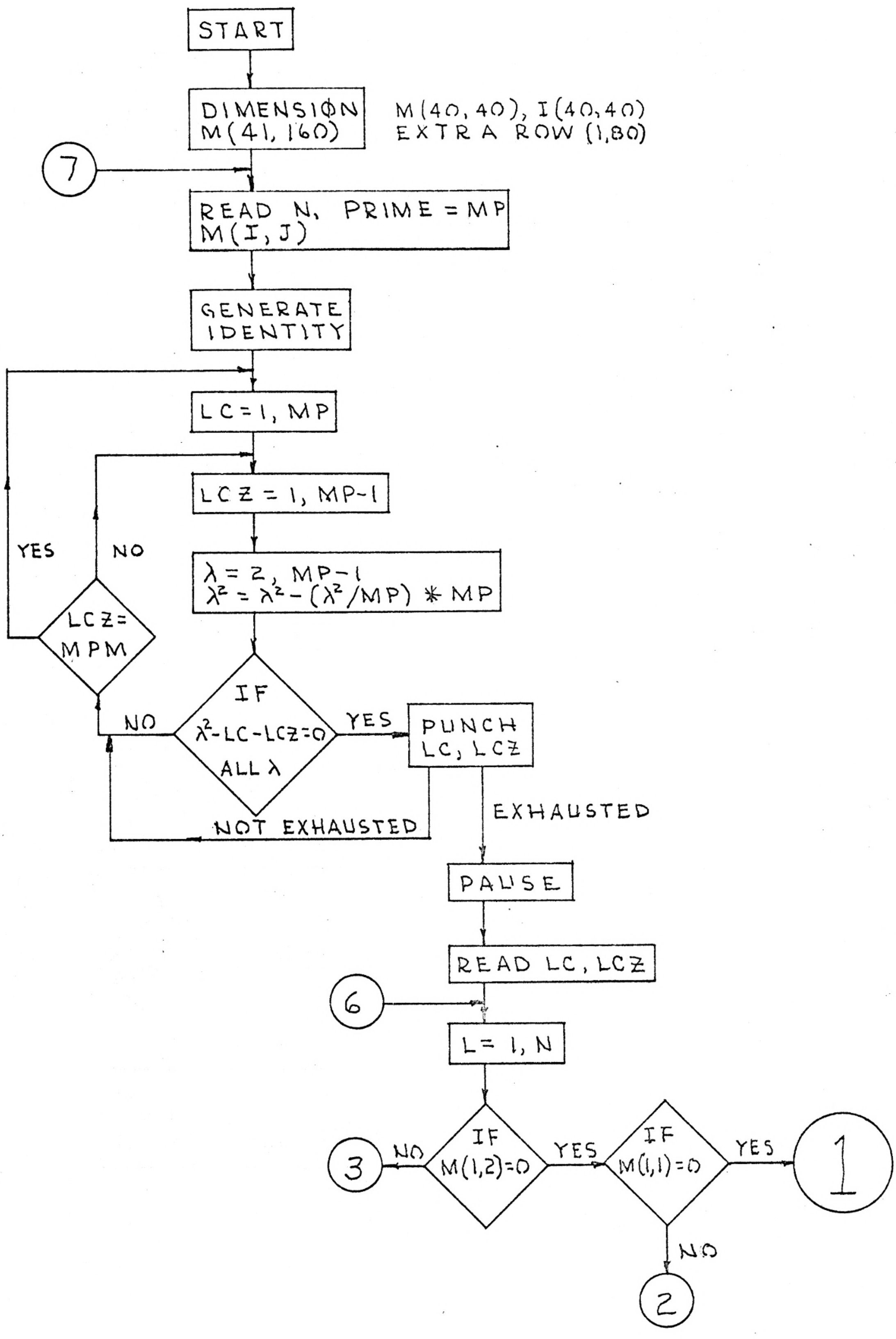
APPENDIX

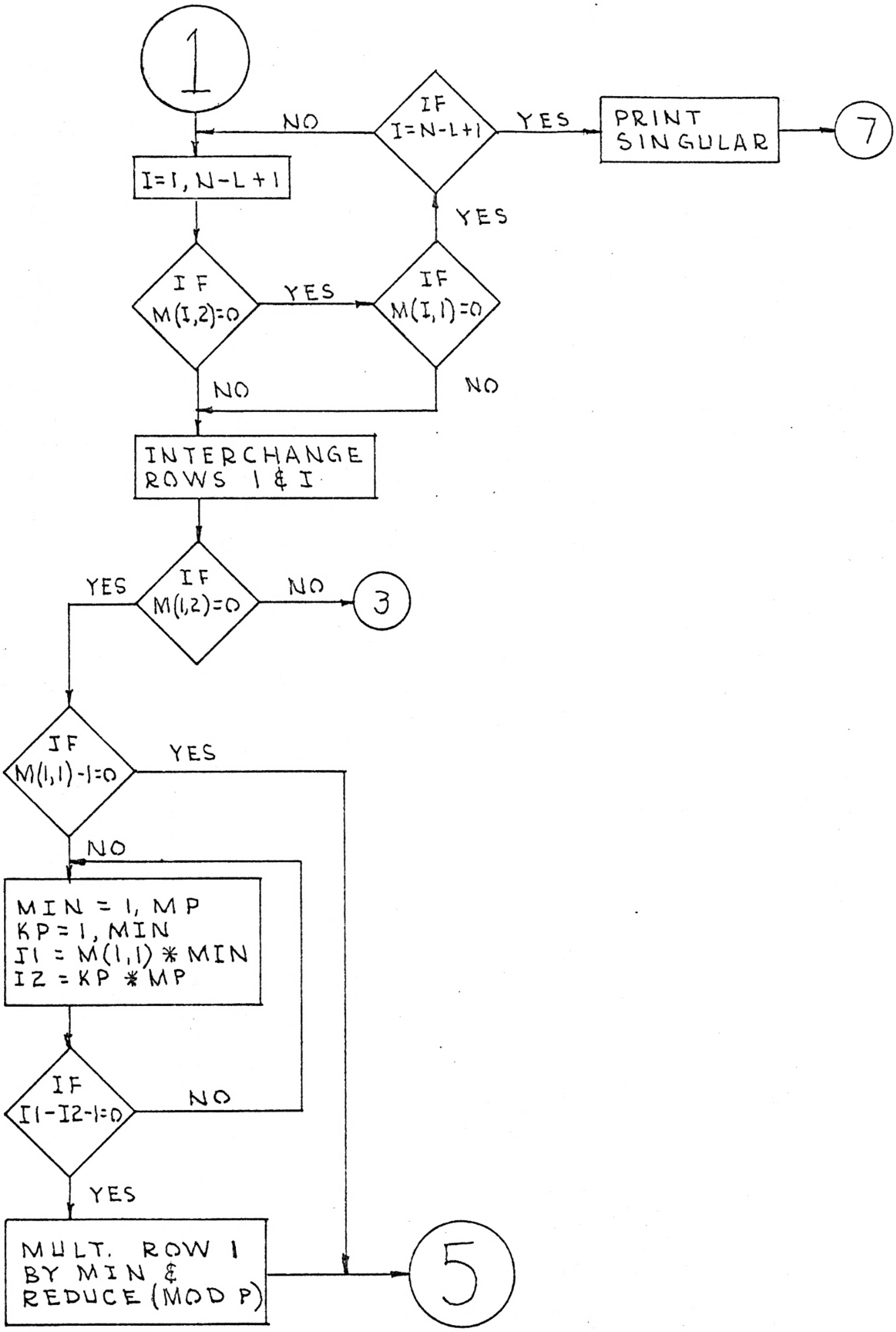

START
DIMENSION 41 X 80
M(40,40), I(40,40)
EXTRA ROW (1,80)
3
READ N, MODULUS (=MP)
M(I,J), GENERATE IDENTITY
1
IF M(1,1) = 0
NO
YES
I = 1, N-L+1
NO
IF M(I,1) = 0
NO
YES
IF I = N-L+1
YES
PRINT SINGULAR
3
INTERCHANGE ROWS 1 & I
IF M(1,1) = 1
YES
NO
MIN = 1, MP
KP = 1, MIN
IF MIN * M(1,1) -KP * MP - 1 = 0
NO
YES
J = 1, 2N
M(1,J) = M(1,J) * MIN
M(1,J) = M(1,J) - (M(1,J)/MP) * MP
I = 2, N J = 2, 2N
K3 = M(1,J) * M(I,1)
K3 = K3 - (K3/MP) * MP
2

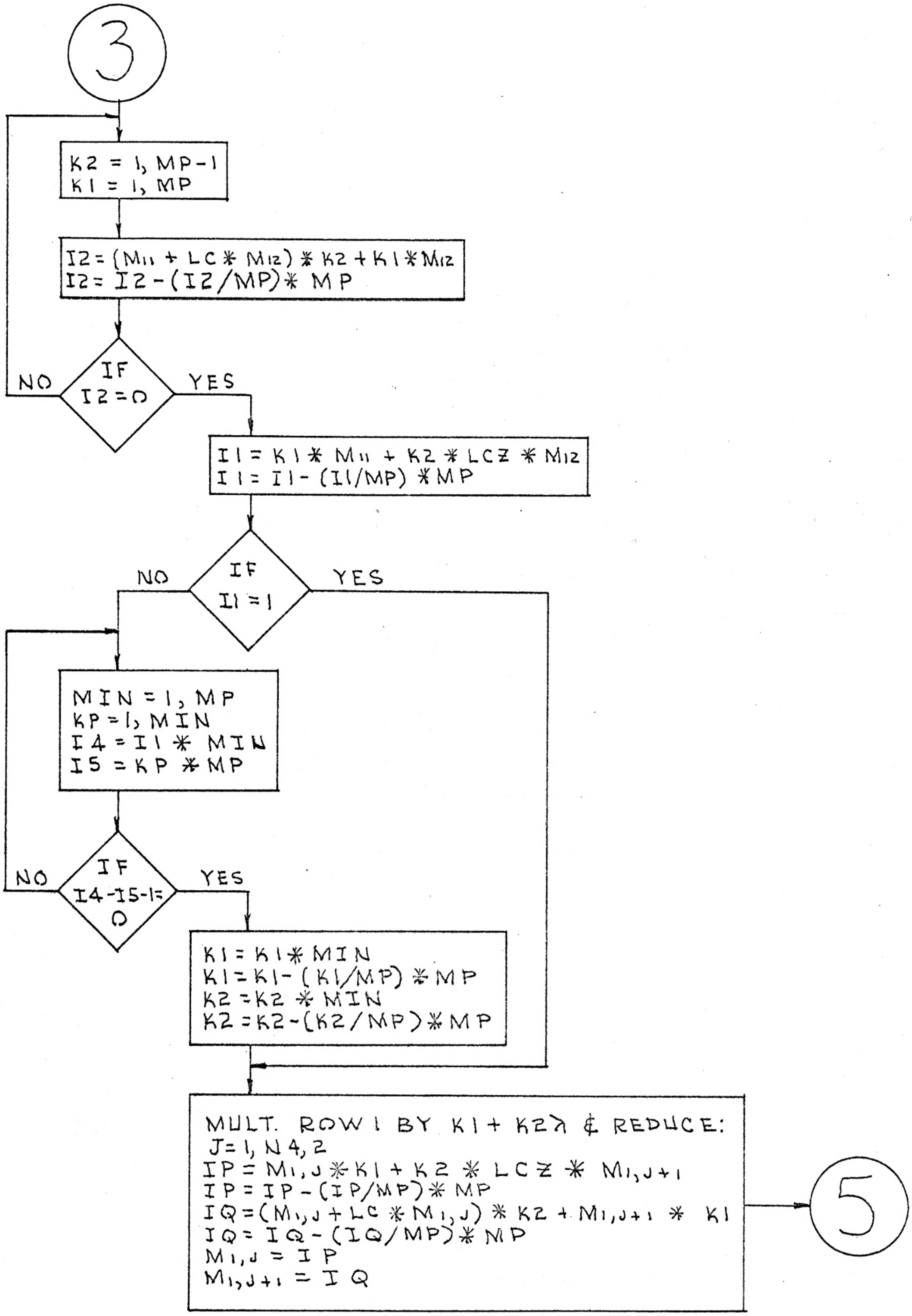

2
IF M(I,J)-K3 <0
YES
M(I,J) = M(I,J) + MP - K3
NO
M(I,J) = M (I,J) - K3
J= 1, 2N
M(N+1,J) = M(1,J)
I = 1, N; J = 1, 2N-1
M(I,J) = M(I+1, J+1)
LOOPED N TIMES ?
NO
1
I = 1, N; J = 1, N
PUNCH M⁻¹(I,J)
PAUSE
END
IF MORE MATRICES 3

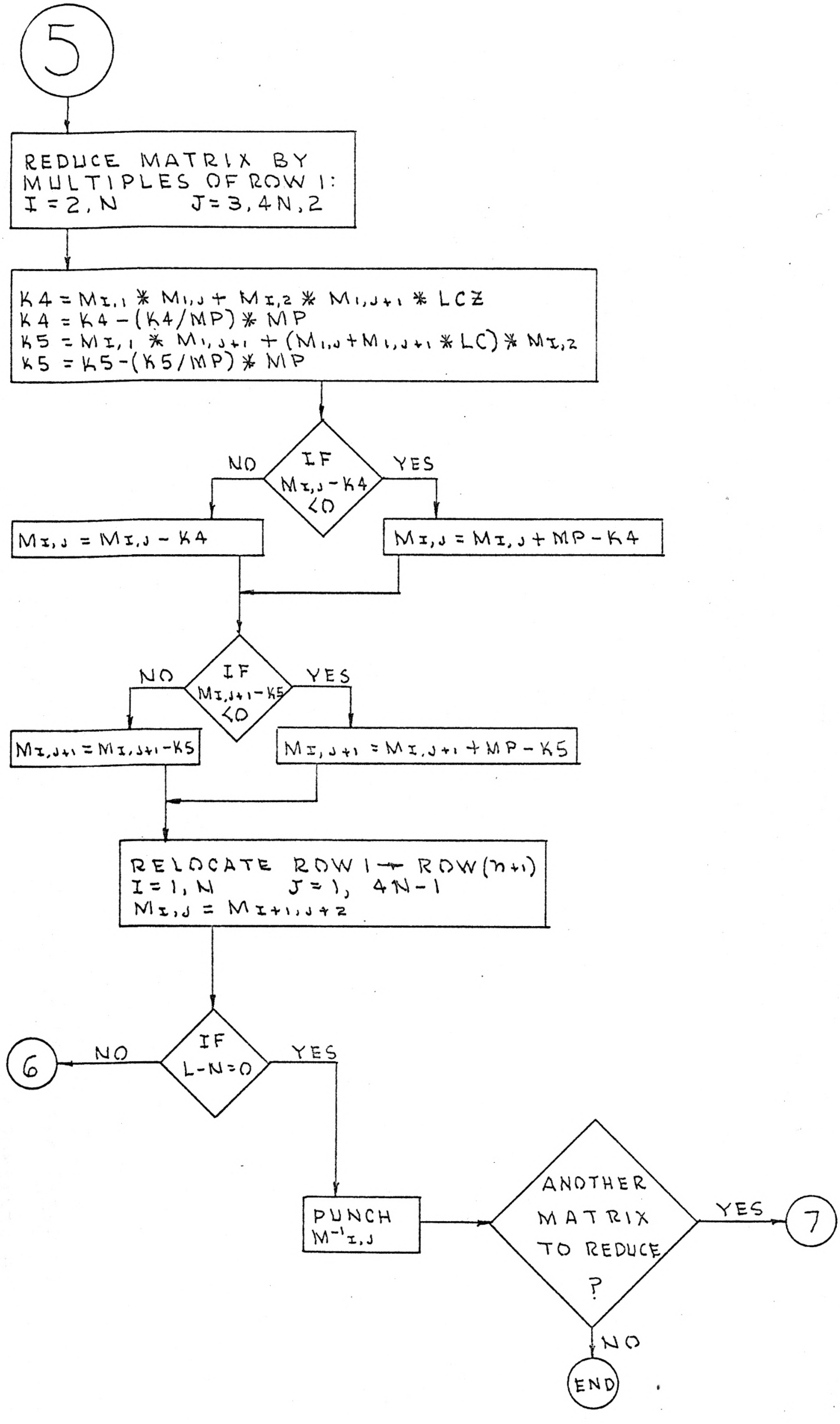
```
C       MATRIX INVERSION OVER GALOIS FIELD GF(P)
        DIMENSION M(61,120)
      1 FORMAT(2I4)
      2 READ1,N,MP
        N1=N+1                                         COMPUTE CONSTANTS
        N2=2*N
        N2M=N2-1

      3 FORMAT(20I4)
        DO4I=1,N                                       READ MATRIX
        READ3,(M(I,J),J=1,N)
      4 CONTINUE

        DO8I=1,N
        DO7J=1,N
        J1=J+N
        IF(I-J)5,6,5
      5 M(I,J1)=0                                      GENERATE IDENTITY MATRIX
        GO TO 7
      6 M(I,J1)=1
      7 CONTINUE
      8 CONTINUE

        DO29L=1,N                                      COMMENCE INVERSION CYCLE

        IF(M(1,1))15,9,15
      9 I4=N-L+1
        DO10I=1,I4
        IF(M(I,1))11,10,11
     10 CONTINUE
    105 FORMAT(9H SINGULAR)
        PRINT 105                                      LOCATE ROW WITH FIRST ELEMENT
        PAUSE                                          NOT ZERO, SINGULAR IF NONE
        GO TO 2
     11 DO12J=1,N2
     12 M(N1,J)=M(I,J)
        DO13J=1,N2
     13 M(I,J)=M(1,J)
        DO14J=1,N2
     14 M(1,J)=M(N1,J)

     15 IF(M(1,1)-1)16,21,16
     16 DO18MIN=1,MP
        MM=MIN
        DO17KP=1,MM
        K4=MIN*M(1,1)                                  DETERMINE M(1,1) INVERSE
        K5=KP*MP
        IF(K4-K5-1)17,19,17
     17 CONTINUE
     18 CONTINUE

     19 DO20J=1,N2
        M(1,J)=M(1,J)*MIN                              MULT ROW 1 BY M(1,1) INVERSE
     20 M(1,J)=M(1,J)-(M(1,J)/MP)*MP                   AND REDUCE MODULO P

     21 DO25I=2,N
        DO24J=2,N2
        K3=M(1,J)*M(I,1)
        K3=K3-(K3/MP)*MP
        IF(M(I,J)-K3)22,23,23                          TRANSFORM OTHER ROWS
     22 M(I,J)=M(I,J)+MP-K3
        GO TO 24
     23 M(I,J)=M(I,J)-K3
     24 CONTINUE
     25 CONTINUE

        DO26J=1,N2
     26 M(N1,J)=M(1,J)                                 ROW 1 INTO ROW N+1

        DO28I=1,N
        DO27J=1,N2M
     27 M(I,J)=M(I+1,J+1)                              SHIFT MATRIX
     28 CONTINUE

     29 CONTINUE                                       N LOOPS STATEMENTS 8+1 - 29

     30 DO31I=1,N
        PUNCH3,(M(I,J),J=1,N)                          PUNCH INVERSE MATRIX
     31 CONTINUE
        PAUSE
        GO TO 2
        END
```

MATRIX INVERSION OVER GALOIS FIELD: GF(P)

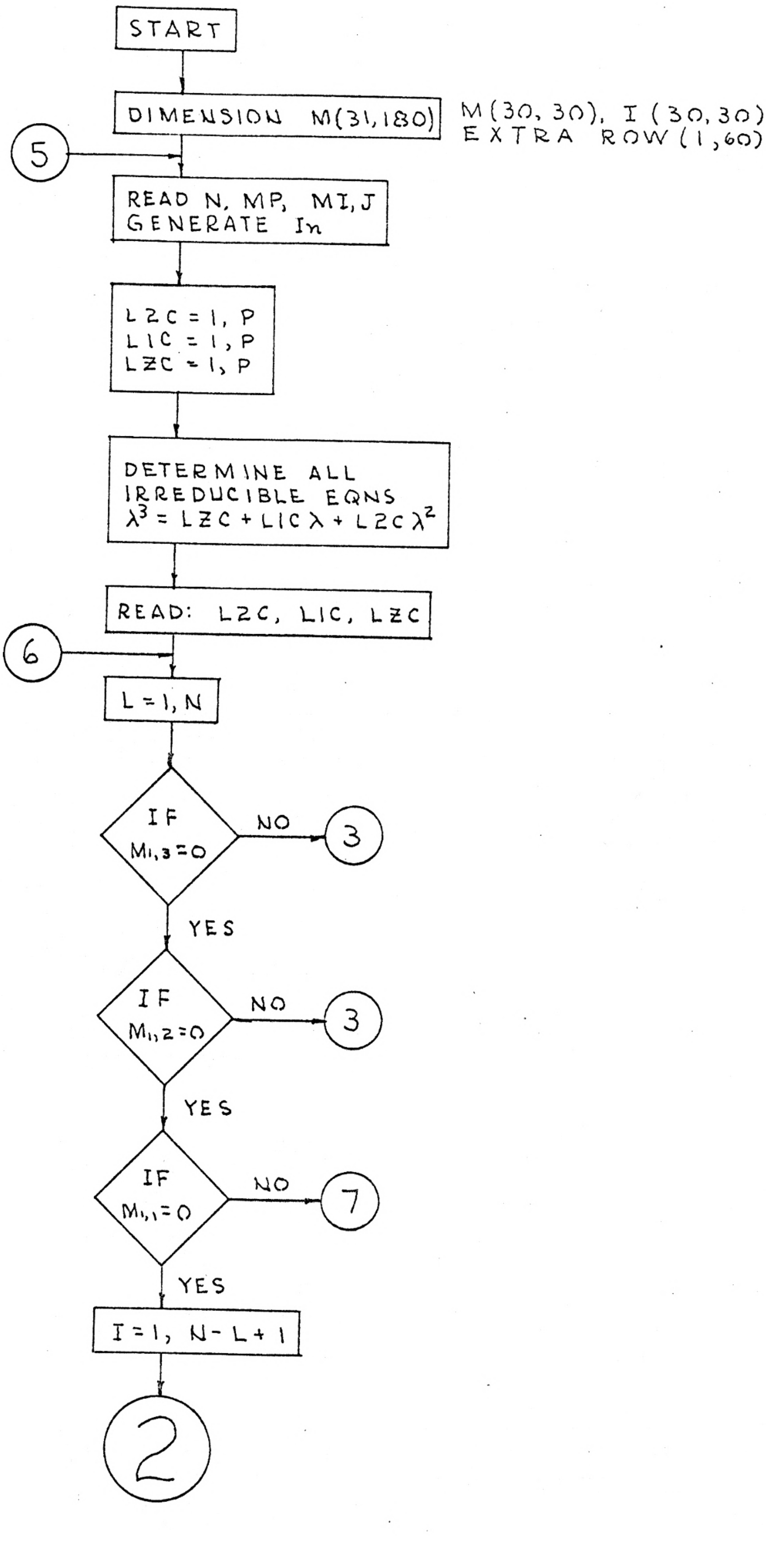



1
I=1, N-L+1
IF M(I,2)=0
YES
IF M(I,1)=0
YES
IF I=N-L+1
YES
PRINT SINGULAR
7
NO
NO
NO
INTERCHANGE ROWS 1 & I
IF M(1,2)=0
NO
3
YES
IF M(1,1)-1=0
YES
NO
MIN = 1, MP
KP = 1, MIN
I1 = M(1,1) * MIN
I2 = KP * MP
IF I1-I2-1=0
NO
YES
MULT. ROW 1 BY MIN & REDUCE (MOD P)
5

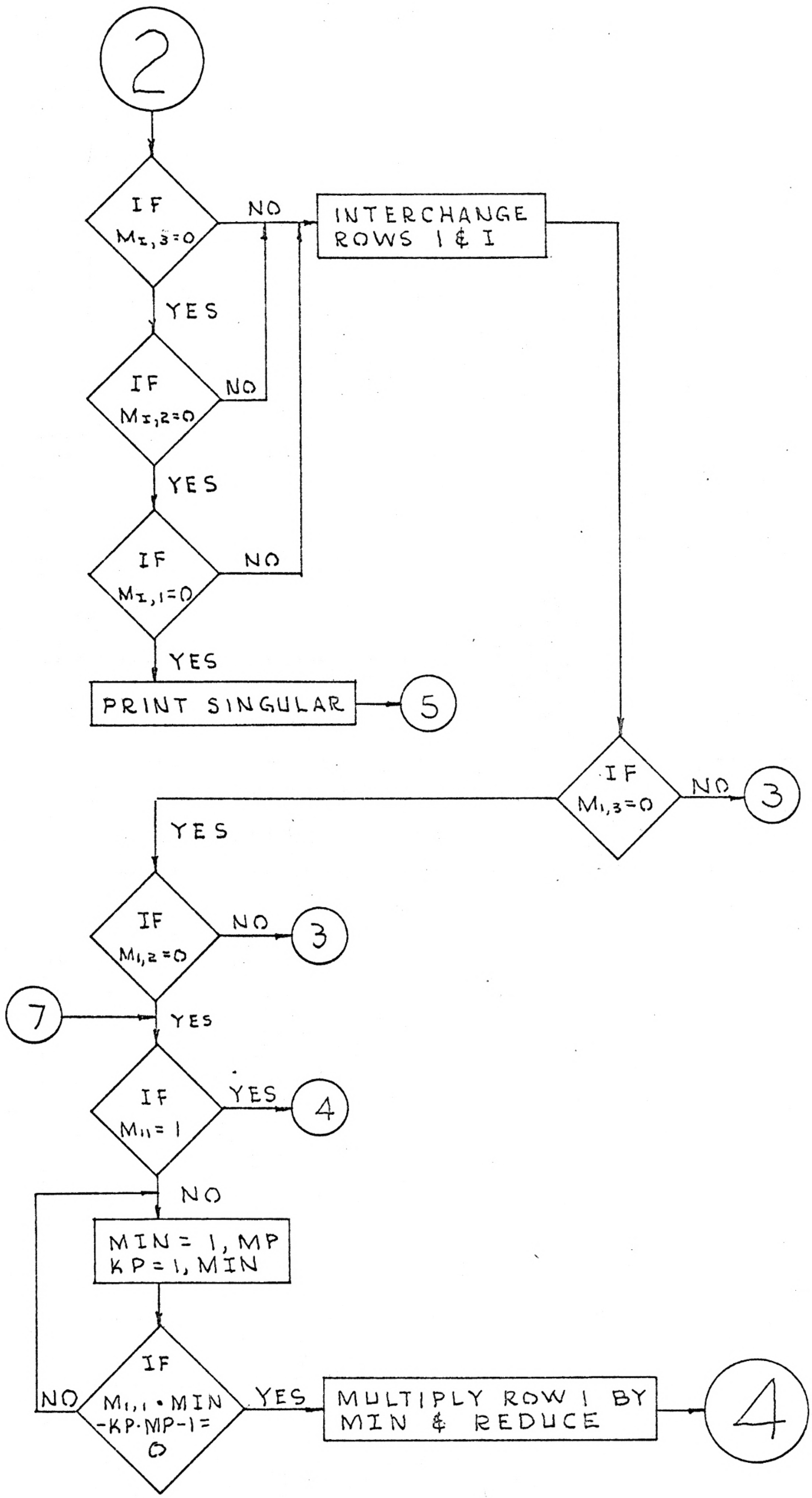

3
K2 = 1, MP-1
K1 = 1, MP
I2 = (M11 + LC * M12) * K2 + K1 * M12
I2 = I2 - (I2/MP) * MP
IF I2 = 0
NO
YES
I1 = K1 * M11 + K2 * LCZ * M12
I1 = I1 - (I1/MP) * MP
IF I1 = 1
NO
YES
MIN = 1, MP
KP = 1, MIN
I4 = I1 * MIN
I5 = KP * MP
IF I4-I5-1 = 0
NO
YES
K1 = K1 * MIN
K1 = K1 - (K1/MP) * MP
K2 = K2 * MIN
K2 = K2 - (K2/MP) * MP
MULT. ROW 1 BY K1 + K2λ & REDUCE:
J = 1, N4, 2
IP = M1,J * K1 + K2 * LCZ * M1,J+1
IP = IP - (IP/MP) * MP
IQ = (M1,J + LC * M1,J) * K2 + M1,J+1 * K1
IQ = IQ - (IQ/MP) * MP
M1,J = IP
M1,J+1 = IQ
5

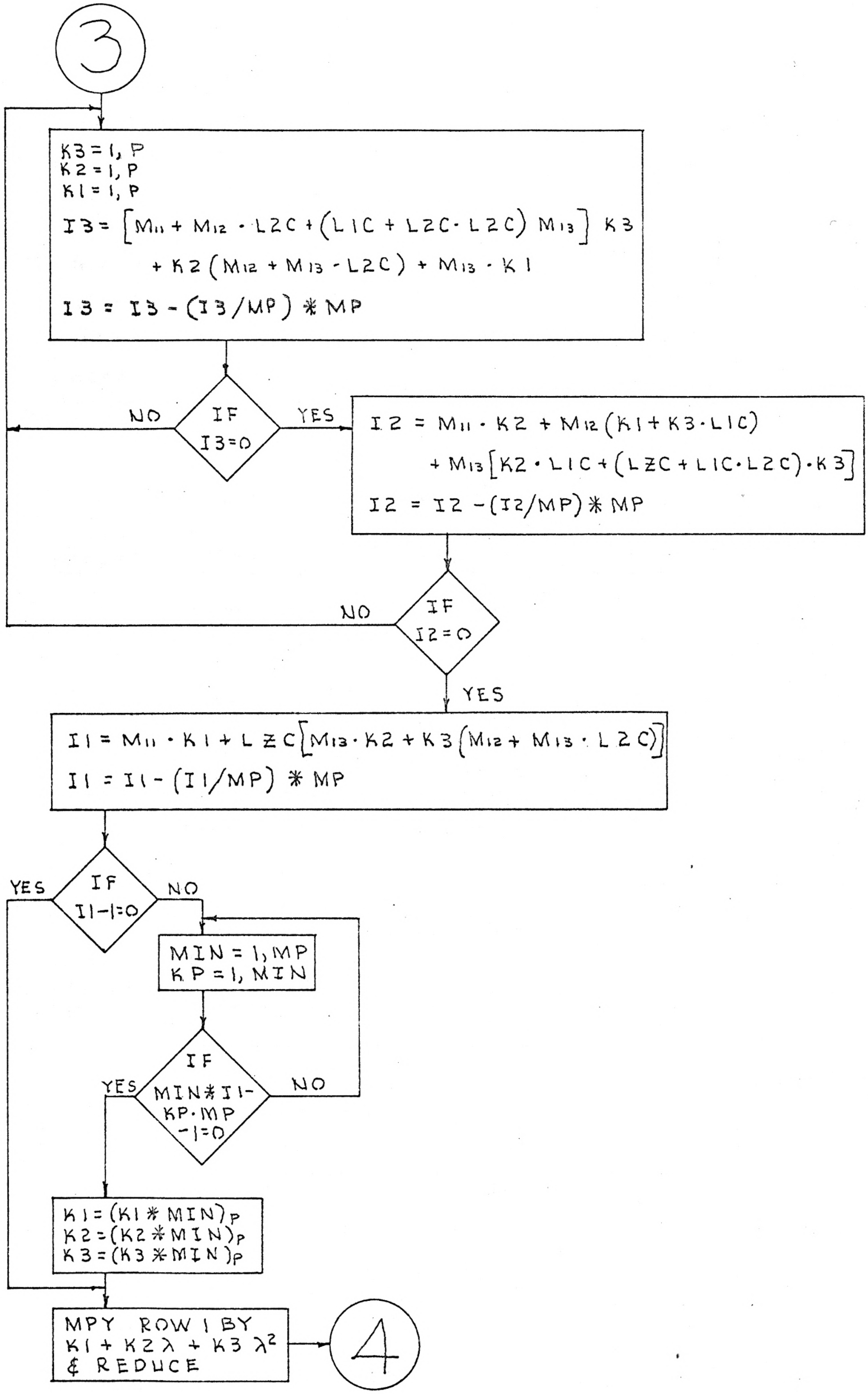

5
REDUCE MATRIX BY MULTIPLES OF ROW 1:
I = 2, N J = 3, 4N, 2
$K4 = M_{I,1} * M_{1,J} + M_{I,2} * M_{1,J+1} * LCZ$
$K4 = K4 - (K4/MP) * MP$
$K5 = M_{I,1} * M_{1,J+1} + (M_{1,J} + M_{1,J+1} * LC) * M_{I,2}$
$K5 = K5 - (K5/MP) * MP$
IF $M_{I,J} - K4 < 0$
NO
YES
$M_{I,J} = M_{I,J} - K4$
$M_{I,J} = M_{I,J} + MP - K4$
IF $M_{I,J+1} - K5 < 0$
NO
YES
$M_{I,J+1} = M_{I,J+1} - K5$
$M_{I,J+1} = M_{I,J+1} + MP - K5$
RELOCATE ROW 1 → ROW (n+1)
I = 1, N J = 1, 4N-1
$M_{I,J} = M_{I+1,J+2}$
IF L-N=0
NO
6
YES
PUNCH $M^{-1}_{I,J}$
ANOTHER MATRIX TO REDUCE ?
YES
7
NO
END

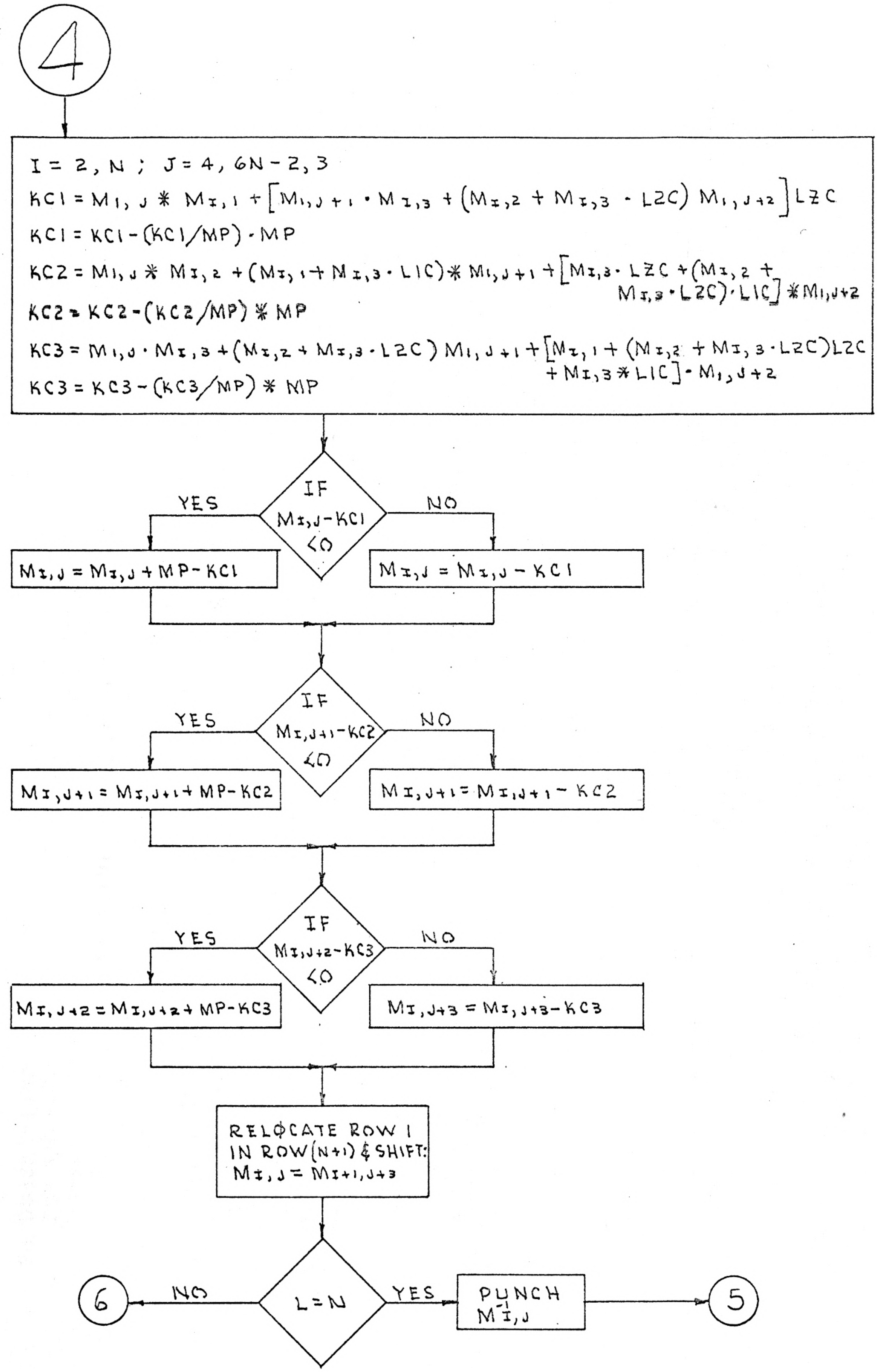
```
C      MATRIX INVERSION OVER GALOIS FIELD GF(P SQRD)
       DIMENSION M(41,160)
     1 FORMAT(2I4)
     2 READ1,N,MP
       N2=2*N                                           COMPUTE CONSTANTS
       N1=N+1
       N4=4*N
       N4M=N4-2
       MPM=MP-1

     3 FORMAT(20I4)
       DO4I=1,N
       READ3,(M(I,J),J=1,N2)                            READ MATRIX
     4 CONTINUE

       DO8I=1,N
       I1=I*2-1
       DO7J=1,N2
       J1=N2+J
       IF(I1-J)5,6,5                                    GENERATE IDENTITY MATRIX
     5 M(I,J1)=0
       GO TO 7
     6 M(I,J1)=1
     7 CONTINUE
     8 CONTINUE

       DO11LC=1,MP
       DO10LCZ=1,MPM
       DO9LAM=1,MPM
       LAM2=LAM*LAM
       LAM2=LAM2-(LAM2/MP)*MP
       L3=LAM*LC+LCZ                                    DETERMINING IRREDUCIBLE
       L3=L3-(L3/MP)*MP                                 POLYNOMIALS
       IF(LAM2-L3)9,10,9
     9 CONTINUE
       PUNCH1,LC,LCZ
    10 CONTINUE
    11 CONTINUE
       PAUSE

       READ1,LC,LCZ                                     READ MODULUS

       DO47L=1,N                                        COMMENCE INVERSION CYCLE

       IF(M(1,2))26,12,26
    12 IF(M(1,1))20,13,20
    13 I4=N-L+1
       DO15I=1,I4
       IF(M(I,2))16,14,16
    14 IF(M(I,1))16,15,16
    15 CONTINUE
   155 FORMAT(9H SINGULAR)                              LOCATE ROW WITH FIRST ELEMENT
       PRINT 155                                        NOT ZERO, SINGULAR IF NONE
       PAUSE
       GO TO 2
    16 DO17J=1,N4
    17 M(N1,J)=M(I,J)
       DO18J=1,N4
    18 M(I,J)=M(1,J)
       DO19J=1,N4
    19 M(1,J)=M(N1,J)

       IF(M(1,2))26,20,26
    20 IF(M(1,1)-1)21,36,21
    21 DO23MIN=1,MP
       MM=MIN
       DO22KP=1,MM                                      DETERMINE INVERSE IF
       I2=M(1,1)*MIN                                    COEFFICIENT OF L IS ZERO
       I3=KP*MP
       IF(I2-I3-1)22,24,22
    22 CONTINUE
    23 CONTINUE

    24 DO25J=1,N4
       M(1,J)=M(1,J)*MIN                                MULT ROW 1 BY THIS INVERSE
    25 M(1,J)=M(1,J)-(M(1,J)/MP)*MP                     AND REDUCE MODULO P
       GO TO 36

    26 DO28K2=1,MPM
       DO27K1=1,MP
       I2=(K1+K2*LC)*M(1,2)+K2*M(1,1)                   INVERSE IF COEFF OF L IS NOT
       I2=I2-(I2/MP)*MP                                 ZERO
       IF(I2)27,29,27
    27 CONTINUE
    28 CONTINUE

    29 I1=K1*M(1,1)+K2*LCZ*M(1,2)
       I1=I1-(I1/MP)*MP
       IF(I1-1)30,34,30
    30 DO32MIN=1,MP
       MM=MIN
       DO31KP=1,MM
       I1=I1*MIN                                        IF CONSTANT COEFF NOT 1(MOD P)
       I3=KP*MP                                         FIND ITS INVERSE
       IF(I1-I3-1)31,33,31
    31 CONTINUE
    32 CONTINUE
    33 K1=K1*MIN
       K1=K1-(K1/MP)*MP
       K2=K2*MIN
       K2=K2-(K2/MP)*MP

    34 DO35J=1,N4,2
       I5=M(1,J)*K1+M(1,J+1)*K2*LCZ
       I5=I5-(I5/MP)*MP
       I6=(K1+K2*LC)*M(1,J+1)+M(1,J)*K2                 MULT ROW 1 BY THIS INVERSE AND
       I6=I6-(I6/MP)*MP                                 REDUCE MODULO P
       M(1,J)=I5
       M(1,J+1)=I6
    35 CONTINUE

    36 DO43I=2,N
       DO42J=3,N4,2
       K4=M(I,1)*M(1,J)+M(I,2)*M(1,J+1)*LCZ
       K4=K4-(K4/MP)*MP
       K5=M(I,1)*M(1,J+1)+(M(1,J)+LC*M(1,J+1))*M(I,2)
       K5=K5-(K5/MP)*MP
       IF(M(I,J)-K4)37,38,38
    37 M(I,J)=M(I,J)+MP-K4                              TRANSFORMING OTHER ROWS
       GO TO 39
    38 M(I,J)=M(I,J)-K4
    39 IF(M(I,J+1)-K5)40,41,41
    40 M(I,J+1)=M(I,J+1)+MP-K5
       GO TO 42
    41 M(I,J+1)=M(I,J+1)-K5
    42 CONTINUE
    43 CONTINUE

       DO44J=1,N4
    44 M(N1,J)=M(1,J)                                   ROW 1 INTO ROW N+1

       DO46I=1,N
       DO45J=1,N4M
    45 M(I,J)=M(I+1,J+2)                                SHIFT MATRIX
    46 CONTINUE

    47 CONTINUE                                         N LOOPS, STATEMENTS 11+3 - 47

       DO48I=1,N
       PUNCH3,(M(I,J),J=1,N2)                           PUNCH INVERSE MATRIX
    48 CONTINUE

       PAUSE
       GO TO 2
       END
```



START
DIMENSION M(31,180)
M(30, 30), I (30,30)
EXTRA ROW (1,60)
5
READ N, MP, MI, J
GENERATE In
L2C = 1, P
L1C = 1, P
LZC = 1, P
DETERMINE ALL
IRREDUCIBLE EQNS
λ³ = LZC + L1C λ + L2C λ²
READ: L2C, L1C, LZC
6
L = 1, N
IF
M1,3 = 0
NO
3
YES
IF
M1,2 = 0
NO
3
YES
IF
M1,1 = 0
NO
7
YES
I = 1, N - L + 1
2


2
IF $M_{I,3}=0$
NO
INTERCHANGE ROWS 1 & I
YES
IF $M_{I,2}=0$
NO
YES
IF $M_{I,1}=0$
NO
YES
PRINT SINGULAR
5
IF $M_{1,3}=0$
NO
3
YES
IF $M_{1,2}=0$
NO
3
7
YES
IF $M_{11}=1$
YES
4
NO
MIN = 1, MP
KP = 1, MIN
IF $M_{1,1} \cdot MIN - KP \cdot MP - 1 = 0$
NO
YES
MULTIPLY ROW 1 BY MIN & REDUCE
4


3
K3 = 1, P
K2 = 1, P
K1 = 1, P
I3 = [M11 + M12 · L2C + (L1C + L2C · L2C) M13] K3
+ K2 (M12 + M13 · L2C) + M13 · K1
I3 = I3 − (I3/MP) * MP
NO
IF I3=0
YES
I2 = M11 · K2 + M12 (K1 + K3 · L1C)
+ M13 [K2 · L1C + (L2C + L1C · L2C) · K3]
I2 = I2 − (I2/MP) * MP
NO
IF I2=0
YES
I1 = M11 · K1 + L2C [M13 · K2 + K3 (M12 + M13 · L2C)]
I1 = I1 − (I1/MP) * MP
YES
IF I1−1=0
NO
MIN = 1, MP
KP = 1, MIN
IF MIN*I1−KP·MP−1=0
YES
NO
K1 = (K1 * MIN)P
K2 = (K2 * MIN)P
K3 = (K3 * MIN)P
MPY ROW 1 BY
K1 + K2λ + K3λ²
& REDUCE
4


4
I = 2, N ; J = 4, 6N - 2, 3
KC1 = M1,J * MI,1 + [M1,J+1 · MI,3 + (MI,2 + MI,3 · L2C) M1,J+2] L2C
KC1 = KC1 - (KC1/MP) · MP
KC2 = M1,J * MI,2 + (MI,1 + MI,3 · L1C) * M1,J+1 + [MI,3 · L2C + (MI,2 + MI,3 · L2C) · L1C] * M1,J+2
KC2 = KC2 - (KC2/MP) * MP
KC3 = M1,J · MI,3 + (MI,2 + MI,3 · L2C) M1,J+1 + [MI,1 + (MI,2 + MI,3 · L2C) L2C + MI,3 * L1C] · M1,J+2
KC3 = KC3 - (KC3/MP) * MP
IF MI,J - KC1 < 0
YES
NO
MI,J = MI,J + MP - KC1
MI,J = MI,J - KC1
IF MI,J+1 - KC2 < 0
YES
NO
MI,J+1 = MI,J+1 + MP - KC2
MI,J+1 = MI,J+1 - KC2
IF MI,J+2 - KC3 < 0
YES
NO
MI,J+2 = MI,J+2 + MP - KC3
MI,J+3 = MI,J+3 - KC3
RELØCATE ROW 1 IN ROW (N+1) & SHIFT: MI,J = MI+1,J+3
L = N
NO
6
YES
PUNCH $M^{-1}_{I,J}$
5

```
C     MATRIX INVERSION OVER GALOIS FIELD GF(P CUBE)
      DIMENSION M(31,180)
    1 FORMAT(2I4)
    2 READ1,N,MP
      N3=N*3
      N6=N*6                                           COMPUTE CONSTANTS
      N6M=N6-3
      N1=N+1
      MPM=MP-1

      DO4I=1,N
    3 FORMAT(20I4)
      READ3,(M(I,J),J=1,N3)                            READ MATRIX
    4 CONTINUE

      DO8I=1,N
      I1=I*3-2
      DO7J=1,N3
      J1=N3+J
      IF(I1-J)5,6,5                                    GENERATE IDENTITY MATRIX
    5 M(I,J1)=0
      GO TO 7
    6 M(I,J1)=1
    7 CONTINUE
    8 CONTINUE

      DO14L2=1,MP
      DO13L1=1,MP
      DO12LZ=1,MPM
      DO10LAM=1,MPM
    9 LAM3=LAM*LAM*LAM
      LAM3=LAM3-(LAM3/MP)*MP
      K1=LZ+L1*LAM+L2*LAM*LAM
      K1=K1-(K1/MP)*MP                                 GENERATE IRREDUCIBLE
      IF(LAM3-K1)10,12,10                              POLYNOMIALS
   10 CONTINUE
   11 FORMAT(3I4)
      PUNCH11,LZ,L1,L2
   12 CONTINUE
   13 CONTINUE
   14 CONTINUE
   15 PAUSE

      READ11,LZ,L1,L2                                  READ MODULUS

      DO60L=1,N                                        COMMENCE INVERSION CYCLE

      IF(M(1,3))34,16,34
   16 IF(M(1,2))34,17,34
   17 IF(M(1,1))29,18,29
   18 I4=N-L+1
      DO21I=2,I4
      IF(M(I,3))24,19,24
   19 IF(M(I,2))24,20,24
   20 IF(M(I,1))24,21,24
   21 CONTINUE
   22 FORMAT(9H SINGULAR)                              LOCATE ROW WITH FIRST ELEMENT
   23 PRINT 22                                         NOT ZERO, SINGULAR IF NONE
      PAUSE
      GO TO 2
   24 DO25J=1,N6
   25 M(N1,J)=M(I,J)
      DO26J=1,N6
   26 M(I,J)=M(1,J)
      DO27J=1,N6
   27 M(1,J)=M(N1,J)

      IF(M(1,3))34,28,34
   28 IF(M(1,2))34,29,34
   29 IF(M(1,1)-1)30,46,30
   30 DO32MIN=1,MP
      MM=MIN                                           DETERMINE INVERSE IF COEFF
      DO31KP=1,MM                                      OF L AND L SQUARE ARE ZERO
      I5=M(1,1)*MIN
      I6=KP*MP
      IF(I5-I6-1)31,325,31
   31 CONTINUE
   32 CONTINUE

  325 DO33J=1,N6
      M(1,J)=M(1,J)*MIN                                MULT ROW 1 BY THIS INVERSE
   33 M(1,J)=M(1,J)-(M(1,J)/MP)*MP                     AND REDUCE MODULO P
      GO TO 46


   34 DO38K3=1,MP
      DO37K2=1,MP
      DO36K1=1,MP
      I3=M(1,1)*K3+(K2+K3*L2)*M(1,2)+(K1+K3*L1+(K2+K3*L2)*L2)*M(1,3)    INVERSE
      I3=I3-(I3/MP)*MP                                                  IF COEFF
      IF(I3)36,35,36                                                    OF L OR
   35 I2=M(1,1)*K2+(K1+K3*L1)*M(1,2)+(K2*L1+(LZ+L2*L1)*K3)*M(1,3)       L SQ ARE
      I2=I2-(I2/MP)*MP                                                  NOT ZERO
      IF(I2)36,39,36
   36 CONTINUE
   37 CONTINUE
   38 CONTINUE

   39 I1=M(1,1)*K1+(M(1,2)*K3+(K2+K3*L2)*M(1,3))*LZ
      I1=I1-(I1/MP)*MP
      IF(I1-1)40,44,40
   40 DO42MIN=1,MP
      MM=MIN
      DO41KP=1,MM
      I5=I1*MIN
      I6=KP*MP
      IF(I5-I6-1)41,43,41                              FIND INVERSE IF CONSTANT
   41 CONTINUE                                         COEFF IS NOT 1(MOD P)
   42 CONTINUE
   43 K1=K1*MIN
      K1=K1-(K1/MP)*MP
      K2=K2*MIN
      K2=K2-(K2/MP)*MP
      K3=K3*MIN
      K3=K3-(K3/MP)*MP

   44 DO45J=1,N6,3
      I7=M(1,J)*K1+(M(1,J+1)*K3+(K2+K3*L2)*M(1,J+2))*LZ
      I7=I7-(I7/MP)*MP                                                MULT ROW
      I8=M(1,J)*K2+(K1+K3*L1)*M(1,J+1)+(K2*L1+(LZ+L2*L1)*K3)*M(1,J+2)   1 BY
      I8=I8-(I8/MP)*MP                                                THIS INV.
      I9=M(1,J)*K3+(K2+K3*L2)*M(1,J+1)+(K1+K3*L1+(K2+K3*L2)*L2)*M(1,J+2)   AND
      I9=I9-(I9/MP)*MP                                                REDUCE
      M(1,J)=I7                                                       MOD P
      M(1,J+1)=I8
      M(1,J+2)=I9
   45 CONTINUE

   46 DO56I=2,N
      DO55J=4,N6,3
      K7=M(1,J)*M(I,1)+(M(1,J+1)*M(I,3)+(M(I,2)+M(I,3)*L2)*M(1,J+2))*LZ
      K7=K7-(K7/MP)*MP
      K8=M(1,J)*M(I,2)+(M(I,1)+M(I,3)*L1)*M(1,J+1)+(M(I,3)*LZ+(M(I,2)+M(
     1I,3)*L2)*L1)*M(1,J+2)
      K8=K8-(K8/MP)*MP
      K9=M(1,J)*M(I,3)+(M(I,2)+M(I,3)*L2)*M(1,J+1)+(M(I,1)+(M(I,2)+M(I,3
     1)*L2)*L2+M(I,3)*L1)*M(1,J+2)
      K9=K9-(K9/MP)*MP
      IF(M(I,J)-K7)47,48,48
   47 M(I,J)=M(I,J)+MP-K7                              TRANSFORM OTHER ROWS
      GO TO 49
   48 M(I,J)=M(I,J)-K7
   49 IF(M(I,J+1)-K8)50,51,51
   50 M(I,J+1)=M(I,J+1)+MP-K8
      GO TO 52
   51 M(I,J+1)=M(I,J+1)-K8
   52 IF(M(I,J+2)-K9)53,54,54
   53 M(I,J+2)=M(I,J+2)+MP-K9
      GO TO 55
   54 M(I,J+2)=M(I,J+2)-K9
   55 CONTINUE
   56 CONTINUE

      DO57J=1,N6
   57 M(N1,J)=M(1,J)                                   ROW 1 INTO ROW N+1

      DO59I=1,N
      DO58J=1,N6M
   58 M(I,J)=M(I+1,J+3)                                SHIFT MATRIX
   59 CONTINUE

   60 CONTINUE                                         N LOOPS, STATEMENTS 15+2 - 60

      DO61I=1,N
      PUNCH3,(M(I,J),J=1,N3)                           PUNCH INVERSE MATRIX
   61 CONTINUE
      GO TO 2
      END
```

A TECHNIQUE FOR DETERMINING THE INVERSE OF A MATRIX WITH ELEMENTS IN CERTAIN GALOIS FIELDS

by

EDWARD PHIL FABRICIUS

B. S., Kansas State University, 1960

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1963

ABSTRACT

This report is concerned with the inversion, using an electronic computer, of a matrix with elements in certain finite fields. The fields considered in detail are the Galois Fields $GF(p)$, $GF(p^2)$, and $GF(p^3)$. The flow charts and a listing of the actual programs are contained in the report. The general Galois Field $GF(p^t)$ is also examined, but there is no program written for this case.

In the general Galois Field $GF(p^t)$, each element is of the form

$$a_0 + a_1L + \cdots + a_{t-1}L^{t-1}.$$

The product of two elements

$$(b_0+b_1L+\cdots+b_{t-1}L^{t-1})(c_0+c_1L+\cdots+c_{t-1}L^{t-1})$$

is a polynomial in L having the form

$$d_0 + d_1L + \cdots + d_{2t-2}L^{2t-2}.$$

Each term involving L to a degree greater than L^{t-1} is reduced by replacing each factor L^t with the modulus of the field. The modulus is given by an irreducible equation of the form

$$L^t = a_0 + a_1L + \cdots + a_{t-1}L^{t-1}.$$

When all terms have been transformed, like terms are collected and their coefficients are reduced modulo p. It is this transformation of the product that leads to serious difficulties in

devising a program for inversion over the general Galois Field.

The method of inversion is a modification of the Gaussian Elimination method. In this technique, one first augments the matrix with the identity matrix and then applies the following five operations;

(1) locating a nonzero m_{11};

(2) multiplying the elements of row 1 by m_{11}^{-1};

(3) transforming the other rows by replacing each m_{ij} with the difference $m_{ij}-m_{i1}m_{1j}$;

(4) relocating each element of row 1 into row n+1;

(5) replacing each m_{ij} with $m_{i+1,\,j+1}$.

To invert a matrix in this field, one must determine the multiplicative inverse of m_{11}. If m_{11} is zero, the first row is interchanged with another row that has a nonzero element as the first element. In step (2), each product has to be transformed using the modulus of the field. Each product must also be reduced modulo p. In step (3), the product $m_{i1}m_{1j}$ must also be transformed by the modulus and reduced modulo p. Also, the difference must be nonnegative as there are no negative integers in this field. Steps (4) and (5) are included as an aid in the programming. The process is repeated n times, with n being the number of rows in the given matrix. When completed, the inverse matrix will be in the locations originally occupied by the given matrix and the identity matrix will not appear. The inverse matrix will be exact, and each element will be an element of the field.