Researches on the Elementary Modular Matrix Transformations and the System of Linear Congruence Equations

Wang Daiwei
No.1 Middle School Attached to Central China Normal University, Wuhan, Hubei

Abstract

The linear congruence equations are the ancient and significant research contents. Most discussions of the linear congruence equations focus on the special cases, for example, there is a linear congruent theorem for solving the congruent linear equation in one unknown and the Chinese remainder theorem for solving the simultaneous congruent linear equations in one unknown, which are involved to find a special solution using the properties of the integer number, and some papers discuss the equation in n unknowns. But all the results are not convenient and efficient to solve the equations and not adapt to solving the general system of congruent linear equations in n unknowns. There is no uniform, convenient and efficient technique and theory for the general system of congruent linear equations, like the theory of linear equations over real numbers. The inspiration arose from the elimination of variables when solving the linear equations over real numbers, Generalized the elementary transformations of matrix over real numbers to the integer numbers modulo m, the paper discussed the properties of the modular matrix under the elementary transformations and a similar equivalent transforming theorem for matrix modulo m theorem was obtained that any matrix modulo m can be transformed into a canonical diagonal form by means of a finite number of elementary row and column operations. furthermore, by means of the equivalent transforming theorem, the solution criterion theorem and structure theorem were proposed for the general congruent linear equations based on the modular matrix transformations, which extended the theories of the congruent linear equations, and finally, the detailed steps of the uniform method were given for solving the general system of congruent linear equations based on the elementary transformations of matrix modulo *m*, it can be easily written out the solutions of the system immediately as determining solutions of the system conveniently by elementary matrix transformations. Analysis and discussions indicate that the results are most valuable in science and the proposed technique for solving the system is convenient, efficient and adaptable.

Keywords: Elementary Modular Matrix Transformation, Equivalent Canonical Form, Congruent Linear Equations, Criterion and Solving

1. Introduction

1.1 Backgrounds

During the process of learning the dividing property of integers and congruent equations, we found that we can adopt the elimination method for real coefficient linear equations and solution of matrix transform to solve the system of linear congruence equations. Using the properties of integers and congruence, we do a series of matrix transformations on the coefficient matrix of the system of linear congruence equations, and then get the solutions.

The linear congruence equations are the ancient and significant research contents, which are involved with most theory and application about integers.

There is a linear congruence theorem for solving the linear congruence equation in one unknown and the Chinese remainder theorem for solving the simultaneous congruent linear equations in one unknown. But there are nearly no paper focus on the discussion of the s linear congruence equations in *n* unknowns[1][2][3][16][17]. At present, the presented solutions always discuss the solution by the dividing property of integers. But all the results are not convenient and efficient to solve the equations and not adapt to solving the general system of linear congruence equations in *n* unknowns.

There is no uniform, convenient and efficient technique and theory for the general system of congruent linear equations, like the theory of linear equations over real numbers in Linear Algebra. So it seems be a significative research.

1.2 research situation

The congruent linear equations are the ancient and significant research contents, which are involved with most theory and application about integers.

There is most linear congruent theorem for solving the linear congruence equation in one unknown and the Chinese remainder theorem is the best known solution for solving the simultaneous linear congruence equations in one unknown. But the Chinese remainder theorem is only true of linear congruence equations in one unknown, which has a strict condition, that the moduli of the equations must be pairwise coprime. If the modules are not pairwise coprime, we must take prime factorization on the modular, and then apply the theory to solve the congruent linear equations. In the process of solution, not only the prime factorization is very difficult, but also the complexity and calculated amount in solving process with Chinese remainder theorem are worthless. At present, there are nearly no paper focus on the discussion of the equation in *n* unknowns[1][2][3][16][17]. all the results are not convenient and efficient to solve the equations and not adapt to solving the general system of linear congruence equations in *n* unknowns.

Given the inspiration arose from the elimination of variables when solving the linear equations over real numbers, we can solve the linear congruence equations easily by the matrix transformation method. This method is not only easy and feasible, but also especially applicable to the solution for the system of linear congruence equations in *n* unknowns. But there is no uniform, convenient and efficient technique and theory for the general system of congruent linear equations, like the theory of linear equations over real numbers.

In the field of real number, document [4] and [5] proposed the solutions which can perfectly transform a matrix to the canonical form under the elementary transformations. Besides, document [5] give the canonical form matrix under Principal Ideal Domain, Euclid domain and others. All the integral domain has a shared characteristic that the nonzero element in domain can be invertible or eliminable. But the element of matrix modulo *m* can be invertible, or zero divisor, and the cancellation law does not hold for the zero divisor, so the discussion is more complex. In document [6]-[13], [15], all the solutions of congruent equation avoid the discussion for canonical form under the elementary transformation. Some of them directly use the conclusion of integer matrix; others are only discussing the congruent equation or indeterminate equation, not the system of linear congruence [indeterminate] equations. They only need to do the elementary transformations on the column matrix or row matrix, which is reduced to finding the great common divisor among a set of numbers. So the discussion in literatures [6]-[18] are deficient.

In this paper, based on the properties of modulo *m* which is different from the real number and integer, we discuss the properties of elementary transformations and elementary matrices modulo *m*, and then adopt them to compute the Great Common Divisor and Least Common Multiple of finite integers.

Besides, we analyze the canonical form under the elementary transformations, which is similar to the conclusion on the integer matrix. All these works extend the conclusion in the literature [5] and provide a theory basis for the followed solution of linear congruence equations.

A similar equivalent transforming theorem for matrix modulo m theorem was obtained that any matrix modulo m can be transformed into a canonical diagonal form by means of a finite number of elementary row and column operations. Then on the basis of the canonical form, we propose the solution criterion theorem and structure theorem for the general congruent linear equations, give the solution criterion theorem and necessary and sufficient condition of solution of any congruent linear equations, extend the solution criterion theorem of Chinese remainder theorem and perfect the solution theory of congruent linear equations.

If the modulo of each equation in the system of linear congruence equations are different, we may obtain the criterion theorem and solution of equations after transform the original equations to an equivalent system of linear congruence equations under unified modulo by means of the least common multiple of all the modulus of the equations of the original system.

The general solution structure and expression of the system of linear congruence equations modulo uniform *m* are given in this paper. Besides, the solution criterion theorem and structure theorem were proposed for the general congruent linear equations, and finally, the detailed steps of the uniform method were given for solving the general system of congruent linear that equations based on the elementary transformations of matrix modulo *m*. It is indicated that the proposed method is most valuable in science and convenient, efficient and adaptable for solving the general system.

All kinds of the congruent linear equations are covered in this paper, so the results described in literature [6]-[13, 15] are special type of conclusions of this paper.

On the above discussion, the complete theory and method of solution are given for congruent linear equations with all different types in this paper. The given method not only has few solution steps and small computational complexity, but also is most valuable in science and convenient, efficient and adaptable.

1.3 Objectives and Basic Ideas

Objectives: study on the properties of modular matrix transformations, discuss the solution theory for congruent linear equations and propose a uniform solution method for solving the general congruent linear equations by means of the elementary operations on modular matrices..

Basic idea: considering the congruence properties of integers, on the basis study of equivalent theorem among congruent linear equations, we give the equivalent transformations of congruent linear equations, analyze the properties of equivalent transformations, discuss the canonical form of modular matrix under the elementary modular operations and the uniform solving steps for congruent linear equations.

2. Matrix Representation of Linear Congruence Equations

2.1 Linear Congruence Equations modulo m

A general system of linear congruence equations:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{m_1} \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 \pmod{m_2} \\ \cdots \quad \cdots \quad \cdots \\ a_{s1}x_1 + a_{s2}x_2 + \cdots + a_{sn}x_n \equiv b_s \pmod{m_s} \end{cases}$$

Where a_{ij}, b_i, m_i ($1 \le i \le s, 1 \le j \le n$) are integers and $x_1, x_2, \cdots, x_n$ are *n* variables taking in integers.

In general, the moduli $m_i (1 \le i \le s)$ are not the same. By the properties of linear congruence, multiplying both sides of the equation and the corresponding modulus of the system by a proper integer respectively, we can obtain a system of linear congruence equations modulo a same modulus, which has the same solutions as the original one. For example, one can multiply each equation and the corresponding modulus by proper multiple such that the uniform modulus *m* is the least common multiple of the moduli $m_i (1 \le i \le s)$, $m = lcm(m_1, m_2, \cdots, m_s)$.

To illustrate this, let $\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 5 \pmod{8} \\ x \equiv 13 \pmod{25} \end{cases}$ be a system of linear congruence equations with different moduli, multiplying each equation by proper integer, we obtain the following linear congruence equations with the same modulus: $\begin{cases} 40x \equiv 40 \times 8 (\bmod 15 \times 40) \\ 75x \equiv 75 \times 5 (\bmod 8 \times 75) \\ 24x \equiv 24 \times 13 (\bmod 25 \times 24) \end{cases}$. It is evident that two systems are equivalent and have same solutions. And the later system of linear congruence equations has the uniform modulus 600.

So any system of linear congruence equations can be transformed into a system of linear congruence equations modulo a uniform modulus.

Definition 2.1 The system of linear congruence equations of *n* variables:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{m} \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 \pmod{m} \\ \cdots \quad \cdots \quad \cdots \\ a_{s1}x_1 + a_{s2}x_2 + \cdots + a_{sn}x_n \equiv b_s \pmod{m} \end{cases} \qquad (2.1)$$

is called a **system of linear congruence equations modulo *m***.

The coefficients of the system of linear congruence equations modulo m are the integers modulo m, that is, they are considered the elements of Residue Class Ring $\mathbf{Z}_m$ [5], so the system is the system of linear congruence equations over the residue class ring $\mathbf{Z}_m$.

According to the properties of congruence from [1-3], the following properties are evidently.

Proposition 2.1 Performing the following operations on the equations of the system of linear congruence equations modulo m, the obtained system of linear congruence equations has the same solutions as the original system.

(1) interchanging any two equations in the system;

(2) adding a multiple of one equation to another;

(3) multiplying any equation in the system by an integer which is coprime with the modulus m;

(4) modulo operation on any coefficients of the system: adding a multiple of the modulus m to or subtracting that from any coefficient of the equations.

Note: from the proposition 2.1, the operation (3) is different from that on the system of linear equations over the real numbers [4]. If and only if the integer *a* and *m* are relatively prime, *a* is an invertible element modulo *m*, the inverse element of *a* can be obtained by applying the **Euclidean algorithm**. Because the integers being congruent modulo *m* are the same elements in residue class ring $\mathbf{Z}_m$, one can use the operation (4) to simplify the coefficients of the system.

2.2 Matrix representation of the system of linear congruence equations modulo m

The $s \times n$ matrix $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \ddots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \end{pmatrix}$ is called the **coefficient matrix** of the system (2.1).

If we let $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ and $\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix}$, then the system (2.1) may be rewritten as a single **matrix congruence equation** $A\mathbf{x} \equiv \mathbf{b} (\bmod m)$, here (mod *m*) means that the matrix operations are the operations modulo *m*.

Definition 2.2: the matrix congruence equation $A\mathbf{x} \equiv \mathbf{b} (\bmod m)$ is called the **matrix representation** of the system of linear congruence equations modulo m.

$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \ddots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \end{pmatrix}$ and $(A, \mathbf{b}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ddots & a_{2n} & b_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} & b_s \end{pmatrix}$ are called the **coefficient matrix** and the **augmented matrix** of the system $A\mathbf{x} \equiv \mathbf{b} (\bmod m)$

2.3 Discussions and summaries

By unifying the modular of the linear congruence equations, defined the system of linear congruence equations modulo *m* and its modular matrix representation, gave four elementary operations on the linear congruence equations to transform the system with the same solutions. The proposition tells us that the operations (3) and (4) are different a bit from that for ordinary equations in real numbers in [4], operations (3) is used on the equations seldom besides multiplying or eliminating (-1) or the integer that can be obviously identified being coprime with m.

3. Modular Matrix Transformations

Modular matrix modulo *m* is the matrix over the residue class ring modulo *m*, which has many familiar properties with the real and integer number matrix, but because the entries are the numbers modulo *m*, the modular matrix has its special characteristics. This chapter will discuss the properties on the elementary modular matrix operations and the elementary modular matrix, and the properties that how to compute the great common divisor and least common multiple of integers by using the elementary modular matrix operations, finally, prove and obtain the main result for the Equivalent Transforming Theorem for matrix modulo *m*.

3.1 Matrix modulo m

Definition 3.1 The matrix is called a **matrix modulo m** if its entries are the integers modulo m.

Let A, B are two matrices modulo m of the same type, if their corresponding entries are congruent modulo *m*, then we call that the matrices A and B are the **congruence matrix modulo m**. Set

$A \equiv B (\bmod m)$ when A and B are congruent modulo m, they are the same matrix over $\mathbf{Z}_m$.

Obviously, the laws of the addition and multiplication of the modular matrix are familiar with that of the real number matrix in [4], just only notes that the add and multiple operations between the entries are the operations modulo *m*.

3.2 Elementary Operations on modular m matrix

In this section, we define the elementary operations that are used throughout the paper. We will use these operations to obtain the equivalent transforming theorem for the matrix modulo *m*, to discuss the solvability conditions for the linear congruence equations modulo and to obtain uniform computational methods for determining the solution of a system of linear congruence equations.

From the proposition 2.1 and the matrix representation for the system of linear congruence equations, the elementary matrix operations on the modular matrix arise from the operations for the system of linear congruence equations described in the proposition 2.1.

Definition 3.2: Let A be an $s \times n$ matrix modulo *m*, Any one of the following operations on the rows [column] of A is called an **elementary row [column] operation**:

(1) **location operation**: interchanges any two rows [or columns] of the matrix. Let $r_i \leftrightarrow r_j$ [$c_i \leftrightarrow c_j$] denote the operation interchanging *i*-th row [column] and *j*-th row [column];

(2) **elimination operation**: adding a multiple of each elements of one row [column] to the corresponding elements of another row [column], Let $r_i + r_j \times k$ denote the operation adding the multiple *k* of the elements of *j*-th row [column] to the corresponding elements of *i*-th row [column];

(3) **multiple operation**: multiplying an integer *k* to each elements of one row [column], where *k* and the modular *m* are coprime (that is, *k* must be an invertible element in $\mathbf{Z}_m$), denoted by $r_i \times k$; or eliminating the common divisor *k* of the elements of one row [column] from the row [column], if the common divisor *k* is coprime with the modular *m*, denoted by r_i / k , where $\gcd(k, m) = 1$;

(4) **modulo operation**: applying the modulo operation to any entries of the modular matrix, i.e., adding a multiple of *m* to an element or subtracting a multiple of *m* from any element of the modular matrix, denoted this operation as (mod *m*).

Any one of the above operations is called an elementary operation. Elementary operations are of type 1,type 2, type 3 or type (4) depending on whether they are obtained by (1), (2), (3) or (4).

Note: the operations (4) is not same as in the linear algebra, in fact, modulo operation does not change the element in $\mathbf{Z}_m$, but because this operation is often used in $\mathbf{Z}_m$, we join it as one of the elementary operation on modular matrix.

If a modular matrix A can be transformed into another modular matrix B by means of a finite number row and column elementary operations, we called that the matrix A and B are **equivalent**, noted as A～B.

The following propositions are obvious by proposition 2.1 and the corresponding of the system of linear congruence equations and its matrix representation..

Proposition 3.1: Performing the elementary row operations on the corresponding augmented matrix of a system of linear congruence equations, the obtained system of linear congruence equations has same solutions as the original system of linear congruence equations.

Similar discussion as in the [4], we can get the following proposition.

Proposition 3.2: Performing the elementary row and column operations on the corresponding augmented matrix of a system of linear congruence equations, the obtained system of linear congruence equations is equivalent to the original system of linear congruence equations, i.e., the solutions of one system of linear congruence equations can be obtained from another one by a linear transformation.

3.3 Equivalent transforming for the modular matrix

Using the elementary operations of the modular matrix, we can discuss and obtain some properties for the modular matrix, especially the important property about the canonical diagonal form of a modular matrix under the elementary operations..

Definition 3.3: An $n \times n$ elementary matrix is a matrix obtained by performing an elementary operation on $n \times n$ unit matrix E_n. The elementary matrix is said to be of type 1, 2, 3 or 4 according to whether the elementary operation performed on E_n is a type 1, 2, 3 or 4 operation, respectively.

Denoted the elementary matrix as $E(i, j)$, $E(j(k), i)$, $E(i(k))$ and E_n, which are corresponded to the type 1, 2, 3 and 4 operations, respectively.

Note that not changing the matrix modulo m, the elementary matrix corresponding to the type 4 operation is still the unit matrix itself.

Just paying the attention to the modulo operation on the entries of the modular matrix, we can do the analogical studies in linear algebra [4], and obtain the results similar to the theorem 9, theorem 10 and the corollaries in reference [4] for the elementary operations and elementary modular matrix, which will be declared with no proofs below.

Theorem 3.1: (1) Let *A* be an $s \times n$ modular matrix, and suppose that *B* is obtained from *A* by performing an elementary row [column] operation. Then there exists an $s \times s$ [$n \times n$] elementary matrix *E* such that $B = E \cdot A$ [$B = A \cdot E$]. Where E is in fact obtained from E_s [E_n] by performing the same elementary row [column] operation as that which was performed on *A* to obtained *B*.

Conversely, if *E* is an elementary $s \times s$ [$n \times n$] matrix, then $E \cdot A$ [$A \cdot E$] is the matrix obtained from *A* by performing the same elementary row [column] operation as that which produces *E* from E_s [E_n].

(2) *A* is an $n \times n$ invertible modular matrix if and only if *A* is the product of elementary matrices, say $A = P_1 P_2 \cdots P_l$, where $P_1, P_2, \cdots, P_l$ are the elementary matrices.

(3) Let A and B be two $s \times n$ modular matrices, the sufficient and necessary condition for A～B is that there exists an $s \times s$ invertible matrix *P* and an $n \times n$ invertible matrix *Q* such that $PAQ = B$.

(4) Each elementary matrix is obtained from the corresponding elementary operation, elementary operation is invertible, so the elementary matrix is also invertible, and the invertible elementary matrix is corresponded to the invertible operation.

By applying the elementary operations of modular matrix, we can calculate the great common divisor and least common multiple of integers conveniently.

Lemma 3.1: (1) suppose that the column modular *m* matrix $\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix}$ is obtained by performing the elementary row operations of type 2 (elimination row operation) on a nonzero column modular *m* matrix $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_s \end{pmatrix}$, then the integer sets $\{a_1, a_2, \cdots, a_s\}$ and $\{b_1, b_2, \cdots, b_s\}$ have the same great common divisors, i.e., $\gcd(a_1, a_2, \cdots, a_s) = \gcd(b_1, b_2, \cdots, b_s)$;

(2) Further, $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_s \end{pmatrix}$ can be transformed into the column matrix $\begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ by a finite number of elementary row operations of type 1 and type 2, and $d = \gcd(a_1, a_2, \cdots, a_s)$;

(3) if $s \geq 2$, then the final $\begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ must be obtained by a finite number of elementary row operations modulo m of type 1-4, and $d = \gcd(a_1, a_2, \cdots, a_s, m)$.

Proof:

(1) Let $d=\gcd(a_1,a_2,\cdots,a_s)$ and $d^{'}=\gcd(b_1,b_2,\cdots,b_s)$, because $\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix}$ is obtained by elementary row operations of type 2 on $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_s \end{pmatrix}$, each one of $b_1,b_2,\cdots,b_s$ is the linear combination of the integers $a_1,a_2,\cdots,a_s$. By the properties of great common divisor, we have $d \mid a_i$, $i=1,2,\cdots,s$, and then $d \mid b_i$, $i=1,2,\cdots,s$, and accordingly $d \mid d^{'}$ is held;

Conversely, for the elementary operations are invertible by theorem 3.1 (4), it can be considered that $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_s \end{pmatrix}$ is obtained by the corresponding invertible elementary row operations of type 2 on $\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix}$, so each one of $a_1,a_2,\cdots,a_s$ is also the linear combination of the integers $b_1,b_2,\cdots,b_s$, and then $d^{'} \mid a_i$, $i=1,2,\cdots,s$ are held by the fact that $d^{'} \mid b_i$, $i=1,2,\cdots,s$, so $d^{'} \mid d$ is held.

So we can claim that $d=d^{'}$, i.e., $\gcd(a_1,a_2,\cdots,a_s)=\gcd(b_1,b_2,\cdots,b_s)$.

(2) Euclidean algorithm [1,2] is the customary approach for calculating the great common divisor of integers. By the property that $\gcd(a_1,a_2)=\gcd(a_1,a_2+ka_1)$ in [1-3], we can claim that performing an elementary row operation of type 2 on a column matrix is meant one step in Euclidean algorithm. Because the GCD (great common divisor) must be appeared by a finite number of division algorithm, $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_s \end{pmatrix}$ can be transformed into a column matrix with one of the entries being GCD *d* by a finite number of elementary row operations of type 2, then d can be interchanged to the first place of the column by the location row operations, and so $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_s \end{pmatrix}$ is transformed into $\begin{pmatrix} d \\ a_2^{'} \\ \vdots \\ a_s^{'} \end{pmatrix}$ by elementary row operations of type 1 and type 2, we know also that each one of $a_2^{'},a_3^{'},\cdots,a_s^{'}$ is the linear combination of

$a_1, a_2, \cdots, a_s$, and $d \mid a_i, i = 1, 2, \cdots, s$, then $d \mid a_i^{'}, i = 2, \cdots, s$, *d* is the divisor of all $a_i^{'}, i = 2, \cdots, s$, so $\begin{pmatrix} d \\ a_2^{'} \\ \vdots \\ a_s^{'} \end{pmatrix}$ can be easily transformed into $\begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ by elementary row operations of type 2, where $d = \gcd(a_1, a_2, \cdots, a_s)$.

(3) Further considering, from (2), if $d \mid m$, then *d* is obviously the GCD of integers $a_1, a_2, \cdots a_s, m$; if $d \nmid m$, as $\begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ is a modular *m* matrix, and for $s \geq 2$, there exists an element besides *d* being zero, then it can be transformed into $\begin{pmatrix} d \\ m \\ \vdots \\ 0 \end{pmatrix}$ by an elementary operation of type 4, i.e., a modulo operation, and finally the column matrix $\begin{pmatrix} d' \\ \\ \vdots \\ 0 \end{pmatrix}$ can be obtained by continuously performing a finite number of elementary row operations of type 2 on the first two rows of the column matrix, and we can see that *d'* is the GCD of *d* , *m*, but *d* is the GCD of $a_1, a_2, \cdots, a_s$ known from (2), so, *d'* is the GCD of $a_1, a_2, \cdots, a_s, m$.

The lemma is proved.

Remark:

There is a ***conjecture*** *from Lemma 3.1(3): The result of Lemma 3.1 (3) is still satisfied when* $s = 1$, *that is, 1-order modular matrix* (a_1) *can be transformed into* (d) *by means of a finite number of elementary operations modulo m（only the operations of tpye3 and tpye4 is applicable），and d is the GCD of* a_1, m *， that is, there exists integer k satisfying gcd(k,m)=1, such that* $k \cdot a_1 \equiv d (\bmod m)$.

（Obviously, there exists an integer k such that $k \cdot a_1 \equiv d (\bmod m)$ *by the Euclidean algorithm, but it is not proved yet here whether the k satisfying gcd(k,m)=1 exists or not. For this, I have a* ***conjecture****: if* $\gcd(k, m) \neq 1$, *then* $k + \frac{m}{d}$ *must be satisfied the condition* $\gcd(k + \frac{m}{d}, m) = 1$.*)*

The least common multiple (LCM) of integers can be calculated by the great common divisor of the integers. By the corollary of the theorem 9 in section 2 of reference [1], we can obtain the following Lemma3.2 for the calculating of the LCM of integers.

Lemma 3.2[1]: Let $a_1, a_2, \cdots, a_s$ be s integers, and let $a = a_1 a_2 \cdots a_s$, $\hat{a}_i = \frac{a}{a_i}, i = 1, 2, \cdots, s$,

then the least common multiple of $a_1, a_2, \cdots, a_s$ is [$\mathrm{lcm}(a_1, a_2, \cdots, a_s)$]=$\frac{a}{\gcd(\hat{a}_1, \hat{a}_2, \cdots, \hat{a}_s)}$. Where

$\mathrm{lcm}(a_1, a_2, \cdots, a_s)$ denotes the least common multiple of $a_1, a_2, \cdots, a_s$.

Based on the Lemma 3.1 and Lemma 3.2, the LCM of integers can also be calculated by means of elementary operations.

The following theorem is the main result of this chapter, which claim that any modular matrix can be transformed into a **canonical diagonal form** or a **reduced diagonal form** by means of a finite number of elementary operations modulo m.

Theorem 3.2(Equivalent transforming theorem): Let A be a nonzero $s \times n$ $(s \neq n)$ matrix modulo *m*, by means of a finite number of elementary row and column operations, A can be transformed into the **canonical diagonal form** D: $D = \begin{pmatrix} D_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$, that is, there are invertible modular matrices P_{ss}, Q_{nn}, such that $PAQ = \begin{pmatrix} D_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$, where $D_r = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_r \end{pmatrix}$, and the elements on the diagonal are satisfied that $d_i \neq 0 (\mathrm{mod}\, m), i = 1, 2, \cdots, r$, and $d_1 \mid d_2 \mid \cdots \mid d_r \mid m$.

D is called a **reduced diagonal form** of modular matrix A if the elements on the diagonal of D are just satisfied that $d_i \neq 0 (\mathrm{mod}\, m), d_i \mid m, i = 1, 2, \cdots, r$.

Proof: if *A* is a row or column matrix modulo *m*, because $s \neq n$, the conclusion of the theorem is correct by the Lemma 3.1.

In general, suppose that $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \ddots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \end{pmatrix}$, consider the great common divisor of all elements of *A* and *m*, denoted as a_1. Based on the Lemma 3.1, by means of a finite number of elementary modular operations, the GCD a_1 will be appeared and then by means of some operations of type 1, *A* can be transformed into a matrix as follow: $A'=\begin{pmatrix} a_1 & a_{12}^{'} & \cdots & a_{1n}^{'} \\ a_{21}^{'} & a_{22}^{'} & \ddots & a_{2n}^{'} \\ \vdots & \ddots & \ddots & \vdots \\ a_{s1}^{'} & a_{s2}^{'} & \cdots & a_{sn}^{'} \end{pmatrix}$.

By the Lemma 3.1, the GCD of all elements of A' and *m* is not changed and still is a_1, then a_1 is the divisor of all elements of A', so, by means of type 2 operations, A can be transformed into the matrix $\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & & \ddots & \\ \vdots & \ddots & A_1 & \vdots \\ 0 & & \cdots & \end{pmatrix}$, and in which a_1 is the divisor of all elements of A$_1$ and *m*.

Now suppose that a_2 is the GCD of all elements of A$_1$ and *m*, then we have that $a_1 \mid a_2$. If $A_1 \neq 0,\ then\ a_2 \neq 0$, do the similar works as before, A_1 can be transformed into the following form of matrix $\begin{pmatrix} a_2 & 0 & \cdots & 0 \\ 0 & & \ddots & \\ \vdots & \ddots & A_2 & \vdots \\ 0 & & \cdots & \end{pmatrix}$ by means of a finite number of elementary operations modulo *m*, and a_2 is the GCD of all elements of A$_2$ and *m*.

Then, by means of a finite number of elementary operations modulo *m*, *A* can be transformed into matrix $\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \ddots & 0 \\ \vdots & \ddots & A_2 & \vdots \\ 0 & 0 & \cdots & \end{pmatrix}$, and $a_1 \mid a_2,\ a_2 \neq 0$.

By the mathematic induction, we can obtain the conclusion of the theorem: by means of a finite number of elementary modular operations, *A* can be transformed into the following canonical diagonal form: $D=\begin{pmatrix} D_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$, i.e., there are invertible modular matrices P_{ss}, Q_{nn}, such that

$PAQ=\begin{pmatrix} D_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$, in which $D_r=\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_r \end{pmatrix}$, and $d_1 \mid d_2 \mid \cdots \mid d_r \mid m$,

$d_i \neq 0 (\bmod m), i=1,2,\cdots,r$.

Note that the last nonzero d_r is also satisfied that $d_r \mid m$. Because $s \neq n$, the last row (when s>n) [or last column (when s<*n*)] of $PAQ = \begin{pmatrix} D_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$ must be zero row [or zero column], then performing the modulo operation on the last zero row [or column], and by means of the type 2 operations on the last row [or column] and the last nonzero row [or last nonzero column], we can obtain that the last d_r satisfies that $d_r \mid m$.

The theorem 3.2 is proved.

Corollary 3.1: For $d_1, d_2, \cdots, d_r$ of *D* in the Theorem 3.2, if there is invertible element among $d_1, d_2, \cdots, d_r$, then there must exist some element, say $d_{\bar{r}}, 1 \le \bar{r} \le r$, that $d_{\bar{r}}$ is invertible, and more, $d_i, 1 \le i \le \bar{r}$ are all invertible, but $d_j, \bar{r} < j \le r$ are all zero divisors.

Proof: by the theorem 3.2, $d_1, d_2, \cdots, d_r$ in canonical diagonal form *D* satisfy that $d_1 \mid d_2 \mid \cdots \mid d_r \mid m$, and $d_i \ne 0, i = 1, 2, \cdots, r$, so, if some one $d_k, 1 \le k \le r$ is invertible, then, because $d_1 \mid \cdots \mid d_k$, we can obtained that $d_i, 1 \le i \le k$ are all invertible; and if there is some one $d_k, 1 \le k \le r$ which is not invertible, then it must be a zero divisor, also for that $d_k \mid \cdots \mid d_r$, we have the fact that $d_i, k \le i \le r$ are all zero divisors.

So, if there is any invertible element among $d_1, d_2, \cdots, d_r$, there must exists a maximal $\bar{r}$,such that $d_i, 1 \le i \le \bar{r}$ are all invertible and $d_i, \bar{r} < i \le r$ are not invertible.

Corollary is proved.

3.4 Summary

Based on the properties of integers and modular integers, elementary modular operations and elementary modular matrix are defined, some applications for calculating the GCD and LCM by means of the elementary operations, and finally obtained the main result on the equivalent transforming theorem of modular matrix, which will be useful in subsequent chapters for solving a system of linear congruence equations.

4. Theories on system of linear congruence equations

Based on the previous chapter’s discussion about the elementary transformations of matrix modulo *m*, this chapter will discuss the theories and approaches for solving the system of linear congruence equations, which are the promotion on the results in references [4] [5] , and expand the discussions in the references [6]- [13] and [15] about the congruence equations.

4.1 Criterion for the solutions’ determining

In this section, we will discuss the criterion conditions for the solutions of the system of linear congruence equations according to result on the equivalent transforming theorem about the modular matrix in chapter 3.

Let’s consider the system of linear congruence equations in n unknowns:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n \equiv b_1 (\bmod m) \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n \equiv b_2 (\bmod m) \\ \qquad \cdots \ \cdots \ \cdots \\ a_{s1}x_1 + a_{s2}x_2 + ... + a_{sn}x_n \equiv b_s (\bmod m) \end{cases} \qquad (4.1)$$

Note that if the moduli of the equations in the system are different, we can multiply the both side of the equations by the appropriate multiples, and expand the modulus to the least common multiple of moduli, which make the modulus of each equation is equal.

The coefficient matrix of the system (4.1) is $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \ddots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \end{pmatrix}$, the constant column is $\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix}$, and the unknown vector $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$, then matrix representation of the system (4.1) is that as follows:

$$A\mathbf{x} \equiv \mathbf{b} (\bmod m) \qquad (4.2)$$

Form the theorem 3.2 , properties 3.2, we can easily figure out the theorems about the solution of linear congruence equations modulo m as follows.

Theorem 4.1: Let A be an $s \times n$ matrix modulo m, and P, Q are $s \times s$ invertible matrix and $n \times n$ invertible matrix respectively, then the system (4.2) and the system

$$PAQ\mathbf{y} \equiv P\mathbf{b} (\bmod m) \qquad (4.3)$$

are **equivalent.**

In which $\mathbf{y} \equiv \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$. When the solutions to the systems exist, the relationship of the two systems (4.2) and (4.3) is:

$$\mathbf{x} \equiv Q\mathbf{y} (\bmod m) . \qquad (4.\ 4)$$

Proof: As P and Q are invertible matrices, the conclusion of theorem 4.1 is established apparently. The details of the proof are omitted.

Further more, by the theorem 3.2, A can be transformed into the reduce diagonal form, namely there are invertible matrices *P* and *Q*, such that $PAQ = \begin{pmatrix} D_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$, $D_r = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_r \end{pmatrix}$, and $d_i \mid m$,

$$d_i \neq 0 (\bmod m), i = 1, 2, \cdots, r . \qquad (4.5)$$

Assume that $P\mathbf{b} = \begin{pmatrix} b_1^* \\ b_2^* \\ \vdots \\ b_s^* \end{pmatrix}$, the following **criterion theorem** for determining solutions of the system of linear congruence equations can be obtained apparently according to the Theorem 4.1 and the linear congruence theorem in [1-3] for linear congruence equation in one unknown.

Theorem 4.2 (Criterion Theorem for the solutions' determining):

Suppose that the **reduce diagonal form** of the coefficient matrix A of the system (4.2) is that in (4.5), then the necessary and sufficient conditions for having solutions to the system (4.2) is that:

$$d_i \mid b_i^*, i = 1, 2, \cdots, r \text{ , and } b_j^* \equiv 0(\bmod m), j = r+1, \cdots, s\,. \qquad (4.6)$$

Proof: the conclusion is obvious according to the Theorem 4.1 and the linear congruence theorem in [1-3]..

Notes:

Theorem 4.2 extends the Chinese Remainder Theorem for the criterion of solutions determining to the general system of linear congruence equations. The conclusion is established for the system of linear congruence equations modulo *m*, but it is applicable for the general system with different moduli of the equations, because we can easily transfer the system to a system of linear congruence equations under uniform modulo, taking the uniform modulo as the least common multiple of the moduli..

4.2 The Structure of Solutions

The follow Lemma 4.1 is described in [1, 16] as the linear congruence theorem.

Lemma4.1[1]**:** For the linear congruence equation $ay \equiv b(\bmod m)$, let $d = (a, m),$ when $d \mid b$, there are distinct *d* solutions modulo *m* to the linear congruence equation. If one special solution to the linear congruence equation is known, say y^*, then we can write out the general solutions to the equation as follow: $y = y^* + k \cdot \frac{m}{d}(\bmod m), k = 0, \cdots d-1.$

According to the Lemma 4.1, the key work to figure out the solutions to the equation $ay \equiv b(\bmod m)$ is to find out one of the special solutions y^* to the linear congruence equation.

According to Lemma 4.1, the following theorem for the special case is obviously true.

Theorem4.3: For the linear congruence equation $dy \equiv b(\bmod m)$ that $d \mid m, d \mid b$, then the equation must have *d* distinct solutions modulo *m*, and the general solution is:

$$y = \frac{b}{d} + k \cdot \frac{m}{d}(\bmod m), k = 0, \cdots d-1.$$

The theorem 4.3 is established obviously, because under the condition of the theorem 4.3, obviously, $y^* \equiv \frac{d}{b}(\bmod m)$ is one of the solutions to the equation.

According to the Theorems 4.1, 4.2 and 4.3, the following solution's structure theorem can be immediately established.

Theorem4.4 (the structure theorem of the solution):

Suppose that the reduce diagonal form of the coefficient matrix *A* of the system (4.2) is *D*:

$D = \begin{pmatrix} D_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$, when there exist solutions to the systems, the original system (4.2) is equivalent to the following simple system of linear congruence equations modulo *m*:

$$\begin{cases} d_1 y_1 \equiv b_1^* (\bmod m) \\ \qquad \vdots \\ d_r y_r \equiv b_r^* (\bmod m) \\ 0 y_{r+1} \equiv 0 (\bmod m) \\ \qquad \vdots \\ 0 y_s \equiv 0 (\bmod m) \end{cases} \qquad (4.7)$$

And according to the theorem 4.3, the general solution to the system 4.7) can be written out::

$$\begin{cases} y_1 = \dfrac{b_1^*}{d_1} + k_1 \cdot \dfrac{m}{d_1} (\bmod m) \\ y_2 = \dfrac{b_2^*}{d_2} + k_2 \cdot \dfrac{m}{d_2} (\bmod m) \\ \vdots \\ y_r = \dfrac{b_r^*}{d_r} + k_r \cdot \dfrac{m}{d_r} (\bmod m) \\ y_{r+1} = k_{r+1} (\bmod m) \\ \vdots \\ y_n = k_n (\bmod m) \end{cases} , \begin{matrix} k_1 = 0, \cdots d_1 - 1 \\ k_2 = 0, \cdots d_2 - 1 \\ \vdots \\ k_r = 0, \cdots d_r - 1 \\ k_{r+1} = 0, \cdots m - 1 \\ \vdots \\ k_n = 0, \cdots m - 1 \end{matrix} \qquad （4.8）$$

Or it can be expressed by column vectors (column matrix):

$$\mathbf{y}^* \equiv \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} \dfrac{b_1^*}{d_1} + k_1 \cdot \dfrac{m}{d_1} \\ \dfrac{b_2^*}{d_2} + k_2 \cdot \dfrac{m}{d_2} \\ \vdots \\ \dfrac{b_r^*}{d_r} + k_r \cdot \dfrac{m}{d_r} \\ k_{r+1} \\ \vdots \\ k_n \end{pmatrix} (\bmod m), \begin{matrix} k_1 = 0, \cdots d_1 - 1 \\ k_2 = 0, \cdots d_2 - 1 \\ \vdots \\ k_r = 0, \cdots d_r - 1 \\ k_{r+1} = 0, \cdots m - 1 \\ \vdots \\ k_n = 0, \cdots m - 1 \end{matrix} \qquad (4.9)$$

The solution to the original system (4.2) can be obtained from the solution to the system (4.7):

$$\mathbf{x} \equiv \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \equiv Q \cdot \mathbf{y}^* \equiv Q \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} (\bmod m) \qquad (4.10)$$

From theorem4.1 and 4.3, the conclusions in the theorem 4.4 are obviously true. And we can get the process of figuring out the solution to the system of linear congruence equations.

在定理 4.4 中，设$Q = \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1n} \\ q_{21} & q_{22} & \cdots & q_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ q_{n1} & q_{n2} & \cdots & q_{nn} \end{pmatrix}$，$Q$的列向量为$\mathbf{q}_j = \begin{pmatrix} q_{1j} \\ q_{2j} \\ \vdots \\ q_{nj} \end{pmatrix}, j = 1, \cdots, n$，则方程组（4.2）的解可展开表示为向量线性组合的形式：

In the theorem 4.4, suppose that $Q = \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1n} \\ q_{21} & q_{22} & \cdots & q_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ q_{n1} & q_{n2} & \cdots & q_{nn} \end{pmatrix}$, its the column vectors are

$\mathbf{q}_j = \begin{pmatrix} q_{1j} \\ q_{2j} \\ \vdots \\ q_{nj} \end{pmatrix}, j = 1, \cdots, n$, then the solution of the system (4.2) can be expressed as a form of the linear combination of vectors

$$\mathbf{x} \equiv \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \equiv Q\mathbf{y}^* \equiv (\mathbf{q}_1, \mathbf{q}_2, \cdots, \mathbf{q}_n) \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \equiv y_1\mathbf{q}_1 + y_2\mathbf{q}_2 + \cdots + y_n\mathbf{q}_n (\operatorname{mod} m). \qquad \text{（4.11）}$$

or it can be representation as a full-scale form:

$$\begin{cases} x_1 = (\frac{b_1^*}{d_1} + k_1 \cdot \frac{m}{d_1})q_{11} + (\frac{b_2^*}{d_2} + k_2 \cdot \frac{m}{d_2})q_{12} + \cdots + (\frac{b_r^*}{d_r} + k_r \cdot \frac{m}{d_r})q_{1r} + k_{r+1}q_{1r+1} + \cdots + k_n q_{1n} (\operatorname{mod} m) \\ x_2 = (\frac{b_1^*}{d_1} + k_1 \cdot \frac{m}{d_1})q_{21} + (\frac{b_2^*}{d_2} + k_2 \cdot \frac{m}{d_2})q_{22} + \cdots + (\frac{b_r^*}{d_r} + k_r \cdot \frac{m}{d_r})q_{2r} + k_{r+1}q_{2r+1} + \cdots + k_n q_{2n} (\operatorname{mod} m) \\ \vdots \\ x_r = (\frac{b_1^*}{d_1} + k_1 \cdot \frac{m}{d_1})q_{r1} + (\frac{b_2^*}{d_2} + k_2 \cdot \frac{m}{d_2})q_{r2} + \cdots + (\frac{b_r^*}{d_r} + k_r \cdot \frac{m}{d_r})q_{rr} + k_{r+1}q_{rr+1} + \cdots + k_n q_{rn} (\operatorname{mod} m) \\ x_{r+1} = (\frac{b_1^*}{d_1} + k_1 \cdot \frac{m}{d_1})q_{r+11} + (\frac{b_2^*}{d_2} + k_2 \cdot \frac{m}{d_2})q_{r+1,2} + \cdots + (\frac{b_r^*}{d_r} + k_r \cdot \frac{m}{d_r})q_{r+1,r} + k_{r+1}q_{r+1,r+1} + \cdots + k_n q_{r+1n} (\operatorname{mod} m) \\ \vdots \\ x_n = (\frac{b_1^*}{d_1} + k_1 \cdot \frac{m}{d_1})q_{n1} + (\frac{b_2^*}{d_2} + k_2 \cdot \frac{m}{d_2})q_{n2} + \cdots + (\frac{b_r^*}{d_r} + k_r \cdot \frac{m}{d_r})q_{nr} + k_{r+1}q_{nr+1} + \cdots + k_n q_{nn} (\operatorname{mod} m) \end{cases},$$

$$\text{其中，} \begin{array}{l} k_1 = 0, \cdots d_1 - 1 \\ k_2 = 0, \cdots d_2 - 1 \\ \quad \vdots \\ k_r = 0, \cdots d_r - 1 \\ k_{r+1} = 0, \cdots m - 1 \\ \quad \vdots \\ k_n = 0, \cdots m - 1 \end{array} \text{。} \qquad \text{（4.12）}$$

4.3 Discussion and Summary

Theorem 4.1 and 4.2 proposed the necessary and sufficient conditions for determining the solutions to the general linear congruence equations, promoted the Chinese Remainder Theorem.

Chinese remainder theorem is only for the linear congruence equations in one unknown. we need to determine whether the moduli are pairwise relatively prime When using the Chinese remainder theorem to judge and figure out the solution to the linear congruence equations, it is very trouble. If the moduli are not pairwise relatively prime, we should factorize the modular and decompose each of the equations into several equations with small modulo, then combined them to find the solutions by means of Chinese remainder theorem, but the problem is that, when the modulo is considerable large, the modulo factorization itself is a difficult work, and it is not suitable for solving.

Theorem 4.2 can be applied to any multivariate linear congruence equations, and it only needs to do a series of elementary transformations, and we can determine the solutions soon.

In addition, when discussing the linear congruence equations for the moduli are different, we only need to convert equations into linear congruence equations, which is under the each modulo's least common multiple. So we can use the theorem 4.2 to determine, discuss and judge when the solution exists.

And it is feasible when we figure the GCD and LCM, this is not like computing large modulus factorization, which is difficult.

Theorem 4.4 gives the solution structure of the general linear congruence equations modulo m, and the representation of the solution in detail.

From discussion about the theorem 4.1 to 4.4, this chapter not only gives the determination of the solution and the structure of the solution, but also gives the solving method.

5. Solving the System of Linear Congruence Equations based on elementary modular operations

For the linear congruence equation in one unknown and the system of linear congruence equations in one unknowns, we need to determine whether the moduli are pairwise relatively prime When using the Chinese remainder theorem to judge and figure out the solution to the linear congruence equations. If the moduli are not pairwise relatively prime, we should factorize each modulo and decompose each of the equations into several congruence equations of small modulo, and then combined some ones such that the moduli are pairwise relatively prime to use of Chinese remainder theorem[1], but the problem is that, when the modulo is considerable large, the modulo's factorization itself is a difficult work, and it is not suitable for solving. At the same time, according to the module decomposition, which makes an equation into the multiple equations, and then combine, make the numbers of equations increases, and how to combine relation is not a unified and it is trivial and isn't have a routing solution followed.

But for solving general multivariate linear congruence equations is rarely illustrated in literatures.

Here, according to the discussions in chapter 3, chapter 4, we can obtain the general steps to solve the linear congruence equations, by using the elementary operations of the matrix modulo *m*.

The general steps to solve the linear congruence equations as follows:

According to the results of theorems 3.2, 4.2 and 4.4, a general and uniform technique for solving the system of linear congruence equations is proposed.

The steps of the solving techniques are as follow:

(1) Unifying the modulus of the system of equations;

Using the properties of the linear congruence, let the least common multiple *m* of the moduli of the linear congruent equations as the uniform modulus, to obtain the system $A\mathbf{x} \equiv \mathbf{b} (\bmod m)$ of congruent linear equations modulo *m*.

(2) Construct the block matrix $C = \begin{pmatrix} A & \mathbf{b} \\ E & \mathbf{0} \end{pmatrix}$, suppose *A* is s row *n* column matrix, *E* is $n \times n$ unit matrix, and s is not equal to *n*;

(3) By a finite number elementary row and column modular transformations modulo *m* on *A*, *A* can be transformed into the canonical diagonal matrix *D*, and *C* can be transformed into the following form: $C = \begin{pmatrix} A & \mathbf{b} \\ E & \mathbf{0} \end{pmatrix} \xrightarrow[\text{elementary column operations}]{\text{elementary row operations}} \begin{pmatrix} D & \mathbf{b}^* \\ Q & \mathbf{0} \end{pmatrix}$, in which *Q* is the product of the elementary matrices of the corresponding column elementary transformations.

(4) By means of the matrix $(D\ \mathbf{b}^*)$ to determine solutions of the system by the criterion theorem;

(5) By the structure theorem, if the system is consistent, it's easy to obtain the solution $\mathbf{y} \equiv (y_1, \cdots, y_n)^{\mathrm{T}} (\operatorname{mod} m)$ of the system of congruent linear equations $D\mathbf{y} \equiv \mathbf{b}^* (\operatorname{mod} m)$, and the solution of the original system can written out immediately as $\mathbf{x} \equiv Q \cdot (y_1, \cdots, y_n)^{\mathrm{T}} \equiv y_1\mathbf{q}_1 + \cdots + y_n\mathbf{q}_n (\operatorname{mod} m)$ by the structure theorem .

Notes:

1) The congruent linear equation in one unknown $ax \equiv b(\operatorname{mod} m)$ can be solved by means of the system of congruent linear equations associated with the trivial equation $mx \equiv 0(\operatorname{mod} m)$;

2) For the system of congruent linear equations in one unknown, the solutions can be obtained only by elementary row transformations;

3) If the coefficient matrix of the system is square, it can be associated with a trivial equation to obtain a new system such that the coefficient matrix of the new system is not a square matrix, and then to ensure the above method can be applied to solve the system.

According to the specific characteristics of the linear congruence equation(s) in one unknown, the linear congruence equation(s) in n unknowns, we give the examples, solving methods and steps respectively,

5.1 The linear congruence equation in one unknown

Suppose a linear congruence equation in one unknown:

$$ax \equiv b(\operatorname{mod} m) \qquad (5.1)$$

Because the equation $mx = 0(\operatorname{mod} m)$ is a trivial equation, the equation $ax \equiv b(\operatorname{mod} m)$ has the same solutions as the equations $\begin{cases} ax \equiv b(\operatorname{mod} m) \\ mx \equiv 0(\operatorname{mod} m) \end{cases}$, Thus the congruence equation $ax \equiv b(\operatorname{mod} m)$ can be solved by means of solving the system of equations $\begin{cases} ax \equiv b(\operatorname{mod} m) \\ mx \equiv 0(\operatorname{mod} m) \end{cases}$, according to the conclusions in chapter 4.

The specific solving steps:

(1) According to the congruence equation (5.1), set the modular m matrix $\begin{pmatrix} a & b \\ m & 0 \end{pmatrix}$;

(2) Performing the elementary **row** operations on the matrix $\begin{pmatrix} a & b \\ m & 0 \end{pmatrix}$, such that $\begin{pmatrix} a \\ m \end{pmatrix}$ is transformed into the reduce diagonal form $\begin{pmatrix} d \\ 0 \end{pmatrix}$, and $\begin{pmatrix} a & b \\ m & 0 \end{pmatrix}$ is become the form $\begin{pmatrix} d & b^* \\ 0 & \tilde{b} \end{pmatrix}$, the process of the transformation can be marked as $\begin{pmatrix} a & b \\ m & 0 \end{pmatrix} \xrightarrow{\text{elementary row operations}} \begin{pmatrix} d & b^* \\ 0 & \tilde{b} \end{pmatrix} (\operatorname{mod}\ m)$. As the coefficient matrix is the reduce form, it is sure that $d \mid m$ (If it doesn't meet, continue to do the row operations, until it satisfies)

(3) By means of the reduce form $\begin{pmatrix} d & b^* \\ 0 & \tilde{b} \end{pmatrix}$ to determine the congruence equation having solutions or not by the criterion theorem: if and only if $m \mid \tilde{b}$ (i.e., $\tilde{b} \equiv 0(\operatorname{mod} m)$) and $d \mid b^*$, the equation has solutions;

(4) When determined that the equation has solutions, it's easy to write out the solutions of the equation by the structure theorem: the equation has a unique solution modulo $\frac{m}{d}$: $x \equiv \frac{b^*}{d} (\operatorname{mod} \frac{m}{d})$,

or has *d* solutions modulo *m*: $x \equiv \frac{b^*}{d} + i \cdot \frac{m}{d} (\bmod\ m), i = 0,1,....,(d-1)$.

【**Example 1**】 $15x \equiv 20(\bmod 35)$

【**Answer**】:（1）Set matrix based on the equation: $\begin{pmatrix} 15 & 20 \\ 35 & 0 \end{pmatrix}$;

（2）Performing the row operations on $\begin{pmatrix} 15 & 20 \\ 35 & 0 \end{pmatrix}$;

$$\begin{pmatrix} 15 & 20 \\ 35 & 0 \end{pmatrix} \xrightarrow{r_2 + r_1 \times(-2)} \begin{pmatrix} 15 & 20 \\ 5 & -40 \end{pmatrix} \xrightarrow{\bmod 35} \begin{pmatrix} 15 & 20 \\ 5 & -5 \end{pmatrix} \xrightarrow{r_1 + r_2 \times(-3)} \begin{pmatrix} 0 & 35 \\ 5 & 30 \end{pmatrix} \xrightarrow{r_2 \leftrightarrow r_1}$$

$$\xrightarrow{r_2 \leftrightarrow r_1} \begin{pmatrix} 5 & 30 \\ 0 & 35 \end{pmatrix} \xrightarrow{\bmod 35} \begin{pmatrix} 5 & 30 \\ 0 & 0 \end{pmatrix};$$

（3）$\because d = 5, b^* = 30, \tilde{b} \equiv 0(\bmod 35), d \mid b^*$, $\therefore$ equation has solution, and $x \equiv \frac{30}{5} = 6(\bmod 7)$ is its unique solution modulo 7, or has 5 solutions modulo 35: $x \equiv 6 + 7i(\bmod 35), (i = 0,1,2,3,4)$ 。

5.2 The system of linear congruence equations in one unknown

Assume a system of linear equations in one unknown:

$$\begin{cases} a_1 x \equiv b_1 (\bmod m_1) \\ a_2 x \equiv b_2 (\bmod m_2) \\ \quad \cdots \quad \cdots \\ a_n x \equiv b_n (\bmod m_n) \end{cases}, \qquad (5.2)$$

Usually, the moduli of the congruence equations may not be same. So, unify the modular of the equations at first, and then to solve the system of equations.

The Solving steps:

(1) Calculate the LCM of $m_i (i = 1, \cdots, n)$: $m = lcm(m_1, \cdots, m_n)$:

1) calculate $M = m_1 m_2 \cdots m_n$, $\hat{m}_i = \frac{M}{m_i}, (i = 1,2,\cdots,n)$

2）by means of the method in Lemma 3.1, calculate the GCD of $\hat{m}_1, \hat{m}_2, \cdots, \hat{m}_n$: $\gcd(\hat{m}_1, \hat{m}_2, \cdots, \hat{m}_n)$;

3） calculate the LCM of $m_i (i = 1, \cdots, n)$:

$$m = lcm(m_1, m_2, \cdots, m_n) = \frac{M}{\gcd(\hat{m}_1, \hat{m}_2, \cdots, \hat{m}_n)};$$

(2) multiplying the coefficients of the equation $a_i x \equiv b_i (\bmod m_i)$ in (5.2) and the modular *m* by $\frac{m}{m_i}$, obtain the equation $\frac{m}{m_i} a_i x \equiv \frac{m}{m_i} b_i (\bmod m)$, which has the same solutions to the equation $a_i x \equiv b_i (m_i)$, so the original system of equations (5.2) and the following system have the same solutions:

$$\begin{cases} \dfrac{m}{m_1}a_1x \equiv \dfrac{m}{m_1}b_1(\bmod m) \\ \dfrac{m}{m_2}a_2x \equiv \dfrac{m}{m_2}b_2(\bmod m) \\ \qquad \cdots \;\; \cdots \\ \dfrac{m}{m_n}a_nx \equiv \dfrac{m}{m_n}b_n(\bmod m) \end{cases} \tag{5.3}$$

(3) Solving the system (5.3): Let its coefficient matrix $A=\begin{pmatrix} \dfrac{m}{m_1}a_1 \\ \vdots \\ \dfrac{m}{m_n}a_n \end{pmatrix}$, the constant column $\mathbf{b}=\begin{pmatrix} \dfrac{m}{m_1}b_1 \\ \vdots \\ \dfrac{m}{m_n}b_n \end{pmatrix}$, by means of the elementary **row** modular operations , transform (A，**b**) into the form $\begin{pmatrix} d & b^* \\ 0 & b_2^* \\ \vdots & \vdots \\ 0 & b_n^* \end{pmatrix}$, and further, into the form $\begin{pmatrix} d & b^* \\ 0 & \tilde{b} \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix}$, where $d \mid m$ (if $d \nmid m$, then perform a modular operation on some zero in the first column, continue row operations, such that the only nonzero element divides *m*.)

(4) From the above canonical form, we can easy determine: $d \mid b^*, m \mid \tilde{b} \Leftrightarrow$ the system has solutions, and through the simple equation $dx \equiv b^*(\bmod m)$, the d solutions of original system can be written out easily: $x \equiv \dfrac{b^*}{d} + i \cdot \dfrac{m}{d}(\bmod m)$,（*i*=0，1，⋯*d*-1）。

【**Example 2**】 $\begin{cases} 2x \equiv 1(\bmod 4) \\ 3x \equiv 2(\bmod 7) \\ 4x \equiv 3(\bmod 6) \end{cases}$

【**Answer**】 Unifying the modular: *m*=[4,7,6]=84

The original system of equations has the same solutions to the system of equations modulo 84:

$\begin{cases} 42x \equiv 21(\bmod 84) \\ 36x \equiv 24(\bmod 84) \\ 56x \equiv 42(\bmod 84) \end{cases}$, performing a finite number of elementary row operations on its augmented matrix:

$$\begin{pmatrix} 42 & 21 \\ 36 & 24 \\ 56 & 42 \end{pmatrix} \to \begin{pmatrix} 6 & -3 \\ 36 & 24 \\ 20 & 18 \end{pmatrix} \to \begin{pmatrix} 6 & -3 \\ 10 & 9 \\ 20 & 18 \end{pmatrix} \to \begin{pmatrix} 6 & -3 \\ 4 & 12 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 6 & -3 \\ -2 & 15 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 0 & 42 \\ 2 & -15 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & -15 \\ 0 & 42 \\ 0 & 0 \end{pmatrix}$$

$\because \tilde{b} = 42 \not\equiv 0(84)$, $\therefore$ the system has no solution.

【Example 3】: $\begin{cases} 2x \equiv 1(\bmod 5) \\ 3x \equiv 2(\bmod 7) \\ 4x \equiv 1(\bmod 11) \end{cases}$

【Answer】: The LCM of the moduli m_1=5, m_2=7 and m_3=11 is m=385.

The original system has the same solutions to the following system: $\begin{cases} 154x \equiv 77(\bmod 385) \\ 165x \equiv 110(\bmod 385) \\ 140x \equiv 35(\bmod 385) \end{cases}$,

Performing elementary row operations on the augmented matrix:

$$\begin{pmatrix} 154 & 77 \\ 165 & 110 \\ 140 & 35 \end{pmatrix} \xrightarrow[r_2-r_3]{r_1-r_3} \begin{pmatrix} 14 & 42 \\ 25 & 75 \\ 140 & 35 \end{pmatrix} \xrightarrow[r_3-r_1\times 10]{r_2-r_1} \begin{pmatrix} 14 & 42 \\ 11 & 33 \\ 0 & -385 \end{pmatrix} \xrightarrow[\bmod 385]{r_1-r_2} \begin{pmatrix} 3 & 9 \\ 11 & 33 \\ 0 & 0 \end{pmatrix} \xrightarrow[\because (3,385)=1]{r_1/3}$$

$$\to \begin{pmatrix} 1 & 3 \\ 11 & 33 \\ 0 & 0 \end{pmatrix} \xrightarrow{c_2-c_1\times 11} \begin{pmatrix} 1 & 3 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$\therefore d$=1, b^*=3, $d \mid b^*$, so the original system has unique solution modulo 385: $x \equiv 3(\bmod 385)$。

5.3 The system of linear congruence equations in n unknowns

Suppose a system of linear congruence equations modulo m as follow:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \equiv b_1(\bmod m) \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \equiv b_2(\bmod m) \\ \cdots \quad \cdots \quad \cdots \\ a_{s1}x_1 + a_{s2}x_2 + \ldots + a_{sn}x_n \equiv b_s(\bmod m) \end{cases} \tag{5.4}$$

Note: if the moduli are different, similar work as in section 5.2 to obtain the system (5.4) and they have the same solutions.

The coefficient matrix, constant column and the variable column are as following , respectively,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \ddots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sn} \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix}, \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}。$$

The Steps for solving the system (5.4) are as follow:

(1) Set the block matrix $C = \begin{pmatrix} A & \mathbf{b} \\ E & \mathbf{0} \end{pmatrix}$, A is $s \times n$ matrix, E is $n \times n$ unit matrix;

(2) Performing the elementary row and column operations on the rows and columns of C which belong to A, A can be transformed into the reduce diagonal form:

$C = \begin{pmatrix} A & \mathbf{b} \\ E & \mathbf{0} \end{pmatrix} \xrightarrow{\text{row and column operations}} \begin{pmatrix} D & \mathbf{b}^* \\ Q & \mathbf{0} \end{pmatrix}$, where D 为 is the reduce diagonal form

$\begin{pmatrix} d_1 & 0 & ... & 0 & 0 & ... & 0 \\ 0 & d_2 & ... & 0 & 0 & ... & 0 \\ .... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & d_r & 0 & ... & 0 \\ 0 & 0 & ... & 0 & 0 & ... & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & 0 & 0 & ... & 0 \end{pmatrix}$, and all nonzero d_i divide *m*, *Q* is the result obtained by performing the corresponding column operations on E. $\mathbf{b}^* = \begin{pmatrix} b_1^* \\ \vdots \\ b_r^* \\ b_{r+1}^* \\ \vdots \\ b_s^* \end{pmatrix}$ is the result obtained by performing the corresponding row operations on $\mathbf{b}$.

(3) The original system is equivalent to the sysyem (5.5):

$$\begin{cases} d_1 y_1 \equiv b_1^* (\bmod m) \\ \qquad\vdots \\ d_r y_r \equiv b_r^* (\bmod m) \\ 0 y_{r+1} \equiv b_{r+1}^* (\bmod m) \\ \qquad\vdots \\ 0 y_s \equiv b_s^* (\bmod m) \end{cases} \qquad (5.5)$$

(4) From the system (5.5), the following works are easy::

If and only if $d_i \mid b_i^*$, $(i = 1,...,r)$, and $m \mid b_j^*$, $j = r+1,...,s$, the system has solutions; (*D* is the reduce diagonal form, so $d_i \mid m$, $(i = 1,...,r)$ satisfy);

(5) Obtain the solutions of the system (5.5): $\mathbf{y}^* \equiv \begin{pmatrix} y_1^* \\ y_2^* \\ \vdots \\ y_n^* \end{pmatrix} (\bmod m)$, then the solutions of the original system can be obtained by means of $\mathbf{x} \equiv \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \equiv Q \cdot \mathbf{y}^* \equiv Q \begin{pmatrix} y_1^* \\ y_2^* \\ \vdots \\ y_n^* \end{pmatrix} (\bmod m)$.

【Example 4】: $\begin{cases} 2x_1 + 2x_2 + x_3 \equiv 1 (\bmod 5) \\ 3x_1 - x_2 + 2x_3 \equiv 2 (\bmod 7) \end{cases}$

【Answer】: Calculate the LCM *m*=35 of m_1=5, m_2=7. the original system has the same solutions to the system of equations: $\begin{cases} 14x_1 + 14x_2 + 7x_3 \equiv 7 (\bmod 35) \\ 15x_1 - 5x_2 + 10x_3 \equiv 10 (\bmod 35) \end{cases}$, its coefficient matrix, constant column are $A=\begin{pmatrix}14 & 14 & 7\\ 15 & -5 & 10\end{pmatrix}$, $\mathbf{b}=\begin{pmatrix}7\\ 10\end{pmatrix}$, respectively.

Performing the elementary row and column operations modulo 35 on A:

$$C=\begin{pmatrix}A & \mathbf{b}\\ E & \mathbf{0}\end{pmatrix}=\begin{pmatrix}14 & 14 & 7 & 7\\ 15 & -5 & 10 & 10\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{pmatrix}$$

$$\begin{pmatrix}14 & 14 & 7 & 7\\ 15 & -5 & 10 & 10\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{pmatrix}\xrightarrow{r_2-r_1}\begin{pmatrix}14 & 14 & 7 & 7\\ 1 & -19 & 3 & 3\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{pmatrix}\xrightarrow[\text{mod}35]{r_1-r_2\times 14}\begin{pmatrix}0 & 0 & 0 & 0\\ 1 & -19 & 3 & 3\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{pmatrix}\longrightarrow$$

$$\xrightarrow{r_1\leftrightarrow r_2}\begin{pmatrix}1 & -19 & 3 & 3\\ 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{pmatrix}\xrightarrow[c_3-c_1\times 3]{c_2+c_1\times 19}\begin{pmatrix}1 & 0 & 0 & 3\\ 0 & 0 & 0 & 0\\ 1 & 19 & -3 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{pmatrix}, \text{ so, } D=\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 0\end{pmatrix},$$

$$\mathbf{b}^*=\begin{pmatrix}3\\ 0\end{pmatrix},\ Q=\begin{pmatrix}1 & 19 & -3\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

From the canonical diagonal form, we can see that $d_1=1, d_2=0, b_1^*=3, b_2^*=0, d_1\mid b_1^*, d_1\mid m$, and known that the original system has solutions.

Consider the simple system of linear equations corresponding the matrix as its augmented matrix $(D,\mathbf{b}^*)=\begin{pmatrix}1 & 0 & 0 & 3\\ 0 & 0 & 0 & 0\end{pmatrix}$, easy to know that the system of equations is $y_1+0y_2+0y_3\equiv 3(\text{mod}\,35)$. In which y_2, y_3 are free variables, and the general solutions of the system can be expressed as $\begin{pmatrix}y_1\\ y_2\\ y_3\end{pmatrix}\equiv\begin{pmatrix}3\\ k_1\\ k_2\end{pmatrix}(\text{mod}\,35)$, where $k_1=0,1,\dots,34; k_2=0,1,\dots,34$.

So, the original system has the solution as follow:

$$\begin{pmatrix}x_1\\ x_2\\ x_3\end{pmatrix}\equiv Q\begin{pmatrix}y_1\\ y_2\\ y_3\end{pmatrix}\equiv\begin{pmatrix}1 & 19 & -3\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}3\\ k_1\\ k_2\end{pmatrix}\equiv\begin{pmatrix}3+19k_1-3k_2\\ k_1\\ k_2\end{pmatrix}(\text{mod}\,35),$$

i.e. $\begin{cases}x_1\equiv 3+19k_1-3k_2(\text{mod}\,35)\\ x_2\equiv k_1(\text{mod}\,35)\\ x_3\equiv k_2(\text{mod}\,35)\end{cases}$, $k_1=0,1,\dots,34; k_2=0,1,\dots,34$ 。

5.4 Discussion and Summary

The equations discussed in this chapter cover all types of linear congruence equation and linear congruence equations, thus, it can be seen that the discussions in documents [6]-[13] are just the special types discussed in this paper.

Through the discussion, all types of linear congruence equation and linear congruence of equations have a complete and unified theory and the solving method, the method is unified, simple, practical, when we judge the existence of the solution, the solution of equation is figured out at the same time, which reduce the computational complexity and solving steps.

6. Summary

6.1 Summary of the Researches

Congruence theory and congruence equation are ancient and meaningful. The existing literature usually discusses that how to solve the congruence equation or equations in one unknown and the multivariate congruence equation, and the methods for solving the congruence equations are neither simple nor practical. In the real number field, there are many comprehensive theories and methods to solve linear equations, but no such theories and methods for any congruent linear equations. Therefore, study of this project is very meaningful and challenging for us.

Inspired by solving linear equations with real coefficients, this article is based on the properties which are expressed by the different number modulo *m*, real numbers and integers, etc. extends the matrix transformations to the modular *m* matrix transformations, discusses the properties of elementary modular operations and elementary modular matrices, and then obtain and prove the equivalent transforming theorem for modular matrix, which is similar to but different from that for the real numbers or integer matrix, therefore, the discussions promote the relevant theoretical results in mathematics and enriched the matrix transformation theory, and made a solid theoretical foundation for researching congruent linear equations;

For congruent linear equations, the traditional method just only discusses the special equations in special condition, the judging method and solving method are different, which is cumbersome and impractical, not suitable for discussing and solving general congruent linear equations. Based on the results and theorems discussed, the congruent linear equations are equivalent to a system of simple congruent equations. Then we obtained a simple and effective judging theory of any congruent linear equations, and gave the complete methods linear for determining and solving the any linear congruence equations, which promoted the Chinese Remainder Theorem, enriched and improved linear congruence equations theory.

As for the technique of solving the system of congruent linear equations, the paper proposed a uniform method to solve any system of congruent linear equations based on the elementary matrix transformations. Further more, by means of the obtained criterion theorem and structure theorem, it can be easily written out the solutions of the system immediately as determining solutions to the system conveniently by elementary matrix transformations. So the proposed technique is a convenient, efficient, uniform and most adaptable method for solving the any type of the congruent linear equations.

The methods discussed can judge whether the equations have solutions, and find the solutions if the equations have in the judging process. The methods are simple and practical, adaptable for solving any congruent linear equations.

6.2 Conclusions

1) Generalized the elementary transformations of matrix over real numbers to the integer numbers modulo *m*, and a familiar theorem was obtained that any matrix modulo *m* can be transformed into a canonical diagonal form by means of a finite number of elementary row and column operations.

2) For the congruent linear equations, most discussions are devoted on the special congruent linear equations in special cases by special methods based on the integer number properties in the published papers and books, for example, the Chinese remainder theorem, such special methods are not applicable to solving the general system of congruent linear equations in *n* unknowns. Generalizing the elementary transformations to the modular matrices and discussing the properties of the modular matrix transformations, the paper obtained the solution criterion theorem and solution structure theorem for any system of congruent linear equations based on the modular matrix transformations, which extended the theories of the congruent linear equations.

3) As for the technique of solving the system of congruent linear equations, the paper proposed a uniform method to solve any system of congruent linear equations based on the elementary matrix transformations. Further more, by means of the obtained criterion theorem and structure theorem, it can be easily written out the solutions of the system immediately as determining solutions of the system conveniently by elementary matrix transformations. So the proposed technique is a convenient, efficient, uniform and most adaptable method for solving the congruent linear equations.

Acknowledgements

I would like to thank Mr. Wang Weijia, my teacher for this research. During my study on the subject, Mr. Wang gave me much help and paid hardly work;

And also, I want to give my honorable thanks to Professor Chen Chuanli, Dr. Wang Maocai, they gave much advice and help for my researches.

And I must also thank my parents for their unconditional support in my scientific and academic activities.

It is necessary to thank the Yau High School Mathematics Awards Committee, which provided a wonderful opportunity for us to communicate and learn from each other.

Finally thanks all the teachers and schoolmates that have ever helped me.

References

1．熊全淹，初等整数论（第二版），湖北教育出版社，1989 年

2．洪伯阳，整数的性质及其应用，湖北教育出版社，1983 年

3．U.杜德利著，周仲良译，基础数论，上海科学技术出版社，1980 年

4．同济大学数学教研室，线性代数，高等教育出版社，1982 年

5．T.W.Hungerford，冯克勤译，聂灵沼校，代数学，湖南教育出版社，1985 年版

6．徐彦明，一次同余方程的求解技巧，高等教学研究，2003,6(2):29-31,63

7．唐宗明，矩阵初等变换在解同余方程中的应用，西藏科技，2002 年 9 期（总 113 期）:34-36

8．戴娟，一次同余方程组的一种矩阵解法，常州信息职业技术学院学报，2006 年 5 卷 3 期:6-8

9．段炼，n元一次同余方程的解与自由模 Zm(n)，河南师范大学学报（自然科学版），2005,33(3):131-133

10．李鹤年,凌鄂生，解同余方程$a_1x_1+a_2x_2+\cdots+a_nx_n\equiv b(\bmod m)$. 华东交通大学学报,1994 年

11卷4期: 72-78

11. 张清利,王培根，*n*元一次不定方程的矩阵解法，北京广播电视大学学报,2002年第4期:43-47

12. 徐全德，浅论矩阵初等变换法在数论中的应用，数学通报，2002年第8期:43,47

13. 王丽萍，魏炜，*n*元不定方程组的整数解，数学通报，2003年第5期:41-42

14. 李秀丽，郭爽，关于一次同余方程解法的探讨，大庆师范学院学报，2006,26(2):20-21

15. Florentin Smarandache, ALGORITHMS FOR SOLVING LINEAR CONGRUENCES AND SYSTEMS OF LINEAR CONGRUENCES

16. Solving Linear Congruences,
http://marauder.millersville.edu/~bikenaga/numbertheory/linear-congruences/linear-congruences.html

17. Linear Congruence equations,
http://www.trans4mind.com/personal_development/mathematics/numberTheory/CongruenceEquationsLinear.htm

18. Linear Congruence equations:
http://www.math.mtu.edu/mathlab/COURSES/holt/dnt/lincong3.html