NATIONAL LIBRARY
OTTAWA

BIBLIOTHÈQUE NATIONALE
OTTAWA

CANADA

NAME OF AUTHOR...Teh-chieh KAO...

TITLE OF THESIS...Computations in Matrix Rings...

...

...

UNIVERSITY...Univ. of Alberta...

DEGREE FOR WHICH THESIS WAS PRESENTED...M. Sc...

YEAR THIS DEGREE GRANTED...1976...

(Signed)...Kao Teh-chieh...

PERMANENT ADDRESS:

13, Lane 9, Lishui st.,

Taipei, 106, Taiwan

...

DATED...June 18,...1976

THE UNIVERSITY OF ALBERTA

COMPUTATIONS IN MATRIX RINGS

by

KAO, TEH-CHIEH

©

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES AND RESEARCH

IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE DEGREE

OF MASTER OF SCIENCE

DEPARTMENT OF COMPUTING SCIENCE

EDMONTON, ALBERTA

FALL, 1976

THE UNIVERSITY OF ALBERTA

FACULTY OF GRADUATE STUDIES AND RESEARCH

The undersign certify that they have read, and recommend to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled "COMPUTATIONS IN MATRIX RINGS" submitted by KAO, TEH-CHIEH in partial fulfilment of requirements for the degree of Master of Science

....
Supervisor

....

....

Date..June 9,....... 1976.

ABSTRACT

A variety of algorithms for computations in a matrix ring over the integers are considered.

An integer-arithmetic algorithm for the division of two matrices is given. Derived also is a non-iterative method, which appears to be asymptotically superior to the Euclidean algorithm, for computing a greatest common divisor of two matrices.

Introduced is the concept of a normal prime matrix. The decomposition of an arbitrary matrix into the product of normal prime matrices leads to a new uniqueness result.

ACKNOWLEDGMENTS

I am very much indebted to my supervisor, Professor Stan Cabay for his quidance and constructive advice at all stages of my works. Without his constant assistance, my thesis could never have been completed.

The financial support provided by the Department of Computing Science is gratefully acknowledged.

TABLE OF CONTENTS

CHAPTER PAGE

I. Introduction 1

II. The Euclidean Algorithm For Matrix Rings Over The Integers 4

2.1 : Euclidean Algorithm For Matrix Rings 4

2.2 : Sanov's Rational-Arithmetic Division Algorithm 7

2.3 : An Integer-Arithmetic Division Algorithm 9

III. One-Side Decomposition for Matrix Rings 15

3.1 : Definition Of A Prime Matrix 15

3.2 : Normal Prime Matrices 17

3.3 : Existence of a Left Normal Decomposition 18

3.4 : Uniqueness Of Decomposition 20

IV. Normal Prime Matrices In M(n,Z) 28

4.1 : Preliminary Lemmas 28

4.2 : Diagonalization Of Normal Prime Matrices 35

4.3 : Examples 37

V. A Non-iterative Algorithm For Computing A Left Greatest Common Divisor 41
5.1 : The Algorithm 41
5.2 : The Algorithm For Multiple Matrices 44
5.3 : Complexity Considerations 45

***

Bibliography 48

CHAPTER I

Introduction

Let R be a commutative Euclidean domain with identity 1 and with map d, which assumes integral non-negative values for all nonzero a in R, such that for any a, b in R, b ≠ 0, there exist q and r in R for which a = q•b + r and either r = 0 or d(r) < d(b). Then M(n,R), the set of nxn matrices over R, forms a left Euclidean domain provided R is proper (i.e., if R is not a field and d(a•b) = d(a)•d(b) for every a, b of R) [Sanov; 1967]. If R is proper, then a suitable map for M(n,R) is d(det(A)), where A belongs to M(n,R) and det(A) is the determinant of A. A more general case is discussed by Brungs [Brungs; 1973], but it is not considered here.

In M(n,R), the following theorem on <u>left division</u> holds true [Sanov; 1967] :

<u>Theorem</u> <u>1.1</u>. Let A, B belong to M(n,R). If det(B) ≠ 0, then there exist Q, R in M(n,R) such that

(1) either A = B • Q,

(2) or A = B • Q + R and 0 < d(det(R)) < d(det(B)).

The Euclidean algorithm can therefore be applied in an obvious way to prove the existence of a left greatest common divisor D (which is defined in the chapter II) of two matrices A, B in M(n,R). In chapter II, we show that the application of the Euclidean algorithm to construct a left greatest common divisor D is nontrivial. A more efficient procedure for this construction involves first the computation of the Smith normal form of both A, B.

<u>Theorem 1.2</u>. (Smith normal form) [Newman; 1972, pp. 26-27] Let A belong to M(n,R). Then there exist two unimodular matrices U, V in M(n,R) such that

$$A = U \bullet S \bullet V,$$

where

$$S = \mathrm{diag}(s_1, s_2, \ldots, s_n)$$

and $s_i \mid s_{i+1}$, $1 \leq i \leq n-1$; and $s_{r+1} = \ldots = s_n = 0$ if rank(A) = r.

The theorem states that A is <u>equivalent</u> to a diagonal matrix S. If in addition U and V can be determined so that $V = U^{-1}$, then A is said to be <u>similar</u> to S.

As we shall see, the construction of a matrix D given the Smith normal form of A, B is a simple procedure. Furthermore, in the chapter V, we show that the Bradley's algorithm for computing the Smith normal form of matrices is inexpensive (relative to the direct application of the Euclidean algorithm to A, B). Therefore, the procedure we recommend for computing a left greatest common divisor of two matrices requires essentially the construction of the Smith normal form.

The Smith normal form of a matrix A in addition yields on inspection a decomposition of the matrix into its prime factors. It is perhaps surprising to note that unlike the case for the integers and polynomials the prime decomposition of matrices can not be applied directly for finding a left greatest common divisor.

The decomposition of a matrix into its prime factors is interesting for its own sake, and in chapters III and IV we deviate somewhat from the main theme to explore this subject further. Perhaps the highlight in these two chapters is the introduction of a normal prime matrix which leads to some strong uniqueness results.

In concluding this chapter, we remark that for the sake of simplicity, in many of the results to follow, R is restricted to be the ring of integers Z. The map d is then be the absolute value function "| |". In most cases, however, it should be clear that the results given can easily be generalized to arbitrary Euclidean domains.

CHAPTER II

The Euclidean Algorithm for Matrix Rings over the Integers

2.1 : Euclidean Algorithm for Matrix Rings

In Sanov's paper an algorithm for division in the ring $M(n,Z)$ is given. His algorithm is briefly summarized in section 2.2. As is true for integer and polynomial rings, once division is defined, the Euclidean algorithm can be used to find a greatest common divisor of two elements in $M(n,Z)$. First, however, we give some definitions :

Definition 2.1. If A, B are in $M(n,Z)$, $B \neq 0$ (the zero matrix) then B left divides A if $A = B \cdot C$ for some matrix C in $M(n,Z)$.

Definition 2.2. Let A, B be in $M(n,Z)$, one of which is nonsingular. A left greatest common divisor of A and B, denoted by lgcd(A,B), is a matrix D in $M(n,Z)$ such that D left divides both A and B, and furthermore if D' is any other matrix in $M(n,Z)$ which left divides both A and B then D' left divides D. (The nonsingularity condition is relaxed in chapter V).

Theorem 2.1. Let a left greatest common divisor D of A and B be nonsingular. If D' is another left greatest common divisor of A and B then

$D' = D \bullet U$

where U is a unimodular matrix in $M(n,Z)$.

Proof :

By definition, there exists matrices X and Y such that

$D = D' \bullet X$ and $D' = D \bullet Y$.

Thus,

$D = D \bullet Y \bullet X$.

Since D is nonsingular, $\det(Y \bullet X)$ must be the identity element in Z, and X, Y are therefore both unimodular matrices in $M(n,Z)$.

Q.E.D.

The Euclidean Algorithm for Matrix Rings :

Given an arbitrary matrix A and a nonsingular matrix B in $M(n,Z)$, this algorithm finds their greatest common divisor.

Step 1 (Division) :

Set

R <-- A mod B

A <-- B

B <-- R.

Step 2 (Termination) :

If B = 0, then terminate with A as the answer; else go to step 1.

To show the validity of the algorithm we first state without proof that if a matrix A left divides both B and C then A left divides $B \bullet X + C \bullet Y$ for any matrices X, Y in

$M(n,Z)$.

<u>Proof of the Euclidean Algorithm</u> :

First, left divide A by B getting, according to Sanov's division algorithm, a quotient Q_1 and a remainder R_1 such that $A = B \bullet Q_1 + R_1$ with $0 \leq |\det(R_1)| < |\det(B)|$. If $\det(R_1) = 0$ then $R_1 = 0$ (see Theorem 1.1) and B left divides A so that $\mathrm{lgcd}(A,B) = B$. If $\det(R_1) \neq 0$, we divide B by R_1 getting a quotient Q_2 and remainder R_2 such that $B = R_1 \bullet Q_2 + R_2$ with $0 \leq |\det(R_2)| < |\det(R_1)|$. If $\det(R_2) = 0$ the procedure again terminates; whereas, if $\det(R\ ) \neq 0$ we repeat to obtain $R_1 = R_2 \bullet Q_3 + R_3$ with $0 \leq |\det(R_3)| < |\det(R_2)|$.

Eventually the process must terminate with a zero remainder since the decreasing sequence of nonnegative numbers

$$|\det(B)| > |\det(R_1)| > |\det(R_2)| > \ldots\ldots$$

can be repeated at most $|\det(B)|$ times. We therefore obtain the equations :

$$A = B \bullet Q_1 + R_1$$
$$B = R_1 \bullet Q_2 + R_2$$
$$\vdots$$
$$R_{k-3} = R_{k-2} \bullet Q_{k-1} + R_{k-1} \quad (1)$$
$$R_{k-2} = R_{k-1} \bullet Q_k + R_k$$
$$R_{k-1} = R_k \bullet Q_{k+1},$$

where $\det(R_k) > 0$.

We now show that R_k, the last nonzero remainder, is a left greatest common divisor of A and B. Since R_k left divides R_{k-1}, and R_k left divides R_k, the next to the last equation in (1) implies that R_k left divides R_{k-2}. This process may be continued to show that R_k left divides A and B.

On the other hand, if some other matrix R' left divides A and B, then it follows from the second equation in (1) that R' left divides R_2. Continuing this argument step by step, we finally have that R' left divides R_k. Thus R_k is a left greatest common divisor of A and B, so that lgcd(A,B) = R_k.

Q.E.D.

2.2 : Sanov's Rational-Arithmetic Division Algorithm

A short description of the Sanov's division algorithm for two matrices A, B in M(n,Z) with B nonsingular follows :

Step 1 (Triangulation) :

Perform elementary column operations on A and B to get, respectively, lower triangular matrices A' and B'. Let X be the unimodular matrix such that A' = A • X.

Step 2 (Inversion) :

Find the inverse matrices $(B')^{-1}$, X^{-1}.

Step 3 (Multiplication) :

Compute the lower triangular matrix $Q = (q_{ij}) = (B')^{-1} \bullet A'$.

Step 4 (All components of Q are integers) :

If all components of Q are integers then return with R <-- 0 (in this case B left divides A).

Step 5 (Q has non-integral diagonal elements) :

If some elements on the diagonal of Q are non-integral, then construct a lower triangular matrix R' with components (r'_{ij}) as follows :

$$r'_{ii} = \begin{cases} 1, & \text{if } q_{ii} \text{ is an integer,} \\ q_{ii} - \lfloor q_{ii} \rfloor, & \text{if } q_{ii} \text{ is not an integer.} \end{cases}$$

$$r'_{ij} = q_{ij} \quad \text{if } i \neq j.$$

Then set

$$R \leftarrow B' \bullet R' \bullet X^{-1}$$

and return.

Step 6 (Q has integral diagonal elements but non-integral off-diagonal elements) :

Let the first non-integer element be $q_{i+s,i}$. A matrix R' with components $(r'_{j\ell})$ is then constructed as follows :

(1) : Diagonal elements :

$$r'_{jj} = \begin{cases} 0, & \text{if } j = i, i+s, \\ 1, & \text{otherwise.} \end{cases}$$

(2) : Upper off-diagonal elements :

$$r'_{j\ell} = \begin{cases} -1, & \text{if } j = i, l = i+s, \\ 0, & \text{otherwise.} \end{cases}$$

(3) : Lower off-diagonal elements :

i : Along the sth off-diagonal :

$$r'_{j+sj} = \begin{cases} 0, & \text{if } j < i, \\ q_{j+sj}, & \text{if } i < j, \\ q_{i+si} - \lfloor q_{i+si} \rfloor, & \text{otherwise.} \end{cases}$$

ii : Otherwise :

$$r'_{j\ell} = \begin{cases} 0, & \text{if } j - l < s, \\ q_{j\ell}, & \text{if } j - l > s. \end{cases}$$

Then set

$$R \leftarrow B' \bullet R' \bullet X^{-1}$$

and return.

Section 2.3 : <u>An Integer-Arithmetic Division Algorithm</u>

Sanov's division algorithm involves arithmethic operations on rational numbers. Computationally such operations are undesirable, since in order to minimize the growth of intermediate results, common factors must be removed. This requires the computation of the greatest common divisor of numbers which could be large in magnitude. In this section, therefore, a new division algorithm which requires only integral arithmetic operations is given. At this stage of the research, however, no claims on the computational superiority of the new algorithm shall be made.

<u>Integer-Arithmetic Division Algorithm</u> :

Given an arbitrary matrix A and a nonsingular matrix B in M(n,Z), this algorithm finds (A mod B).

Step 1 (Computation of the adjoint matrix) :

Find the adjoint matrix, B^+, of the matrix B.

Step 2 (Multiplication) :

Set $C \leftarrow B^+ \bullet A$.

Step 3 (Smith normal form) :

Find the Smith normal form S, with diagonal components (s_i), of the matrix C such that

$S = U \bullet C \bullet V$.

Step 4 (Split matrix) :

The matrix S is split into the sum of two diagonal matrices Q', R' with components (q'_i), (r'_i), respectively. The components q'_i, r'_i are constructed as follows:

(1) : If det(B) divides s_i, set

$r'_i = \det(B)$,

$q'_i = (s_i / \det(B)) - 1$.

(2) : If det(B) can not divide s_i, set

$r'_i = s_i - \lfloor s_i / \det(B) \rfloor \bullet \det(B)$,

$q'_i = \lfloor s_i / \det(B) \rfloor$.

Step 5 (R' has all elements equal to det(B)) :

If all elements of R' are equal to det(B), then return with $R \leftarrow 0$.

Step 6 (R' has some element less than det(B)) :

If some element of R' is not equal to det(B), then set

$R \leftarrow A - B \bullet (U \bullet Q' \bullet V)$

and return.

<u>Proof of the Integer-Arithmetic Division Algorithm</u> :

By Theorem 1.2, there exist two unimodular matrices U, V in $M(n,Z)$ such that

$$B^{+} \bullet A = U \bullet S \bullet V,$$

where S, with diagnoal components s_i, is the Smith normal form of the matrix $B^{+} \bullet A$. But for all i, there are integers q'_i, r'_i such that

$$s_i = q'_i \bullet \det(B) + r'_i$$

with

$$0 < r'_i \leq \det(B).$$

Let Q' and R' be diagonal matrices with ith diagonal elements q'_i and r'_i, respectively. There are two cases to consider :

(1) : If $r'_i = \det(B)$ for all $i = 1,\ldots,n$, then

$$\begin{aligned} B^{+} \bullet A &= U \bullet S \bullet V \\ &= U \bullet (\det(B) \bullet Q' + R') \bullet V \\ &= \det(B) \bullet U \bullet (Q' + I) \bullet V \end{aligned}$$

By left multiplying the above equation by B, we get

$$A = B \bullet (U \bullet (Q' + I) \bullet V).$$

Thus, B left divides A.

(2) : If $r'_i \neq \det(B)$ for some i, then

$$0 < |\det(R')| < |\det(B)|^n.$$

On the other hand,

$$\begin{aligned} B^{+} \bullet A &= U \bullet (\det(B) \bullet Q' + R') \bullet V \\ &= \det(B) \bullet U \bullet Q' \bullet V \\ &\quad + U \bullet R' \bullet V \qquad (2) \end{aligned}$$

with

$$0 < |\det(U \bullet R' \bullet V)| < |\det(B)|^n. \qquad (3)$$

If

$$R = A - B \bullet (U \bullet Q' \bullet V),$$

then

$$A = B \bullet (U \bullet Q' \bullet V) + R, \qquad (4)$$

and we now claim that the matrix R satisfies the condition

$$0 < |\det(R)| < |\det(B)|.$$

By left multiplying equation (4) by the matrix B^+ and comparing with the equation (2), it follows that

$$B^+ \bullet R = U \bullet R' \bullet V.$$

Thus, $\det(R) \neq 0$, and moreover by inequality (3)

$$|\det(R)| = |\det(U \bullet R' \bullet V)| \;/\; |\det(B^+)|$$
$$< |\det(B)|^n / |\det(B)|^{n-1}$$
$$= |\det(B)|.$$

Q.E.D.

In concluding this chapter an example is given which illustrates the integer-arithmetic division algorithm.

Example :

Given two matrices

$$A = \begin{bmatrix} 1 & 0 \\ 4 & 4 \end{bmatrix},$$

$$B = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}.$$

We first obtain

$$B^+ = \begin{bmatrix} 2 & 0 \\ -1 & 1 \end{bmatrix}$$

and

$$B^+ \bullet A = \begin{bmatrix} 2 & 0 \\ 3 & 4 \end{bmatrix}.$$

By applying some algorithm for obtaining the Smith normal form, we get

$$B^+ \bullet A = \begin{bmatrix} 2 & -1 \\ 3 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 8 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}.$$

That is, the Smith normal form S is

$$S = \begin{bmatrix} 1 & 0 \\ 0 & 8 \end{bmatrix},$$

and

$$U = \begin{bmatrix} 2 & -1 \\ 3 & -1 \end{bmatrix},$$

$$V = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}.$$

Now split the matrix S according to the step 4 to obtain

$$Q' = \begin{bmatrix} 0 & 0 \\ 0 & 3 \end{bmatrix}.$$

The quotient Q is then given by

$$Q = U \bullet Q' \bullet V = \begin{bmatrix} 0 & -3 \\ 0 & -3 \end{bmatrix},$$

and the remainder R by

$$R = A - B \bullet Q = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}.$$

Note that

$$1 = |\det(R)| < |\det(B)| = 2.$$

CHAPTER III

One-side Decomposition for Matrix Rings

3.1 : Definition of A Prime Matrix

From Theorem 1.1 we know that the matrix ring $M(n,R)$ over a Euclidean domain R is a left Euclidean domain. One of the most interesting properties of principle ideal domains (and therefore of Euclidean domains as well) is that such rings admit a theory of unique factorization [MacLane; 1967, pp. 154-155]. One method for decomposing a matrix into its prime factors is discussed by Sanov [Sanov; 1967]. In this chapter a different decomposition of a matrix in $M(n,Z)$ into its prime factors is introduced. This decomposition permits us to exhibit certain uniqueness result which are not possible using Sanov's decomposition.

With the demonstration of this fact in mind, we first give the following definition :

Definition 3.1. A matrix P in $M(n,Z)$ is called a prime matrix (i.e., P is a prime element in $M(n,Z)$) if $|\det(P)| > 1$ and P has no other left divisors besides unimodular matrices and matrices which are right equivalent to P (matrix B is said to be right equivalent to A if $B = A \cdot V$ for some unimodular matrix V).

This definition is equivalent to saying that for any decomposition, $P = A \bullet B$, of P, either A or B is unimodular.

__Theorem 3.1__. The determinant of any prime matrix in $M(n,Z)$ is a prime element in Z. Conversely, if the determinant of some matrix in $M(n,Z)$ is a prime element in Z, then it must be a prime matrix in $M(n,Z)$.

__Proof__ :

. The second part of the theorem is obvious, and the proof of the first part can be found in [Sanov; 1967].

Q.E.D.

From this theorem, we know that $diag(1,\ldots,p,1,\ldots 1)$, with p a prime in Z, is a prime matrix immediately.

Let

$$A = P_1 \bullet P_2 \bullet \ldots \bullet P_m \tag{1}$$

be a decomposition of a matrix A in $M(n,Z)$ into the prime factors P_k, $1 \le k \le m$. The existence of such a decomposition is proven by Sanov. Given the decomposition (1) and arbitrary unimodular matrices $U_1,\ldots,U_{m-1}$, it is clear that

$$A = (P_1 \bullet U_1^{-1}) \bullet (U_1 \bullet P_2 \bullet U_2^{-1}) \bullet \ldots \bullet (U_{m-2} \bullet P_{m-1} \bullet U_{m-1}^{-1}) \bullet (U_{m-1} \bullet P_m)$$

is another decomposition of A. Since, in addition, $M(n,Z)$ is non-commutative, the question of uniqueness of the decomposition is a nontrivial one. To make this problem more tractable, Sanov restricts the prime matrices to be of lower-triangular type. This leads to uniqueness results which are too confining. In the remainder of this chapter, we discuss the decomposition of a matrix into normal prime factors. Some interesting results on uniqueness then follow.

3.2 : Normal Prime Matrices

Definition 3.2. A prime matrix P in $M(n,Z)$ is a *normal prime matrix* if it is similar to diag(1, ..., 1,p), where p is a prime element in Z.

Examples :

1 : Let

$$P = \begin{bmatrix} -2 & -12 \\ 1 & 5 \end{bmatrix}.$$

Because det(P) = 2 is a prime of Z, the matrix P is a prime matrix. Moreover, by taking

$$U = \begin{bmatrix} 1 & 3 \\ 1 & 4 \end{bmatrix},$$

then

$$U \bullet P \bullet U^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

Thus, P is also a normal prime matrix.

2 : Let

$$Q = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Because det(Q) = 3 is a prime of Z, the matrix Q is a prime. On other hand, there does not exist any unimodular matrix U such that

$$U \bullet Q \bullet U^{-1} = \text{diag}(1,3).$$

Thus, the matrix Q is not normal prime.

<u>Definition 3.3</u>. A decomposition of a nonsingular matrix A, which is not unimodular, in M(n,Z) into the form

$$A = P_1 \bullet P_2 \bullet \dots \bullet P_m \bullet U,$$

where P_k, $1 \le k \le m$, are commuting normal prime matrices, and U is a unimodular matrix is called a <u>left normal decomposition</u> of A.

3.3 : <u>Existence of a Left Normal Decomposition</u>

From Theorem 1.2, we know that for any nonsingular matrix A in M(n,Z), A is equivalent to its Smith normal form diag$(s_1,s_2,\dots,s_n)$, i.e., there are two unimodular matrices U, V in M(n,Z), such that :

$$A = U \bullet \text{diag}(s_1,s_2,\dots,s_n) \bullet V. \tag{2}$$

By standard arguments, we know that all components s_k, $1 \le k \le n$, can be decomposed into products of primes in Z. Let us represent them as follows :

$$s_k = \prod_{i=1}^{n_k} p_{k_i}^{\gamma_{k_i}} \qquad k = 1,\dots,n$$

Now let us take a look at the matrix

$$\text{diag}(1,\dots,1,s_k,1,\dots,1)$$

with s_k on the position (k,k) and 1's in the other diagonal positions. It is obviously that such a matrix can be decomposed into products of prime matrices as follows :

$$\operatorname{diag}(1,\ldots 1,s_k,1,\ldots,1)$$

$= \operatorname{diag}(1,\ldots,1,p_{k_1},1,\ldots,1)$ appears r_{k_1} times

$\bullet \operatorname{diag}(1,\ldots,1,p_{k_2},1,\ldots,1)$ appears r_{k_2} times

$\bullet$

$\bullet$

$\bullet$

$\bullet \operatorname{diag}(1,\ldots,1,p_{n_k},1,\ldots,1)$ appears r_{n_k} times. (3)

However, equality (2) implies that

$$A = U \bullet \operatorname{diag}(s_1,1,\ldots,1) \bullet \operatorname{diag}(1,s_2,1,\ldots,1) \bullet \cdots \bullet \operatorname{diag}(1,\ldots,1,s_n) \bullet V,$$

which together with (3) yields the decomposition

$$A = U \bullet P_1 \bullet P_2 \bullet \ldots \bullet P_m \bullet V, \qquad (4)$$

where

$$P_k = \operatorname{diag}(1,\ldots,1,p_k,1,\ldots,1)$$

and P_k, P_{k+1} are not necessarily different. As mentioned before, we can put in any unimodular matrices W, W^{-1} between P_k and P_{k+1} to obtain another decomposition. Given the decomposition (4), however, we choose instead to consider only

$$A = (U \bullet P_1 \bullet U^{-1}) \bullet (U \bullet P_2 \bullet U^{-1}) \bullet \ldots \bullet (U \bullet P_m \bullet U^{-1}) \bullet (U \bullet V) .$$

__Lemma 3.2__. The matrices $U \bullet P_k \bullet U^{-1}$ are commuting normal prime matrices.

Proof :

For each P_k, there is a unimodular matrix U_k' such that

$$U_k' \bullet P_k \bullet (U_k')^{-1} = \mathrm{diag}(1,\ldots\ldots,1,p_k)$$

Let

$$U_k = U_k' \bullet U$$

Then

$$U_k \bullet (U^{-1} \bullet P_k \bullet U) \bullet (U_k)^{-1}$$
$$= (U_k' \bullet U \bullet U^{-1}) \bullet P_k \bullet (U \bullet U^{-1} \bullet (U_k')^{-1})$$
$$= U_k' \bullet P_k \bullet (U_k')^{-1}$$
$$= \mathrm{diag}(1,\ldots\ldots 1,p_k).$$

Thus, each $U \bullet P_k \bullet U^{-1}$ is a normal prime matrix.

The commutativity is obvious.

Q.E.D.

We have therefore proved

Theorem 3.3. Any nonsingular matrix A, which is not unimodular, in M(n,Z) has a left normal decomposition

$$A = (U \bullet P_1 \bullet U^{-1}) \bullet (U \bullet P_2 \bullet U^{-1}) \bullet\ldots\bullet (U \bullet P_m \bullet U^{-1}) \bullet (U \bullet V),$$

where each P_k is of the form $\mathrm{diag}(1,\ldots,1,p_k,1,\ldots,1)$ and p_k is a prime element in Z.

3.4 : Uniqueness of Decomposition

For any nonsingular matrix A in M(n,Z), by some algorithm, we can transform it into its Smith normal form

$$A = U \bullet \mathrm{diag}(s_1,\ldots\ldots,s_n) \bullet V,$$

and then obtain a left normal decomposition

$$A = (U \bullet P_1 \bullet U^{-1}) \bullet (U \bullet P_2 \bullet U^{-1}) \bullet \dots \bullet (U \bullet P_m \bullet U^{-1}) \bullet (U \bullet V) .$$

Although the Smith normal form of a matrix is unique, there are many different pairs of unimodular matrices U, V such that $U \bullet A \bullet V$ is the Smith normal form of A (e.g., different algorithms may result in different U, V).

Example :

Let

$$A = \begin{bmatrix} 14 & 24 \\ 10 & 18 \end{bmatrix}.$$

By taking

$$U = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix},$$

$$V = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix},$$

we get

$$U \bullet A \bullet V = \begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix}.$$

On the other hand, if

$$U' = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}$$

and

$$V' = \begin{bmatrix} -5 & -12 \\ 3 & 7 \end{bmatrix},$$

then

$$U' \bullet A \bullet V' = \begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix}$$

also results in the Smith normal form.

There is, however, a relationship between different pairs of matrices U, V.

<u>Lemma</u> <u>3.4</u>. Let A be a nonsingular matrix, which is not unimodular, in M(n,Z).

If

$$A = (U \bullet P_1 \bullet U^{-1}) \bullet (U \bullet P_2 \bullet U^{-1}) \bullet \ldots \bullet (U \bullet P_m \bullet U^{-1}) \bullet (U \bullet V)$$

and

$$A = (U' \bullet P_1 \bullet (U')^{-1}) \bullet (U' \bullet P_2 \bullet (U')^{-1}) \bullet \ldots \bullet (U' \bullet P_m \bullet (U')^{-1}) \bullet (U' \bullet V')$$

be two left normal decompositions of A. Then, there exists a unimodular matrix X such that

$$U' = X \bullet U$$

$$U' \bullet V' = (1/\det(A)) \bullet X \bullet (U \bullet V) \bullet A^{+} \bullet X^{-1} \bullet A,$$

where the matrix X satisfies the condition

$$A^{+} \bullet X \bullet A \equiv 0 \quad \text{mod}(|\det(A)|)$$

with congruence being elementwise congruence.

<u>Proof</u> :

We have that

$$(U' \bullet U^{-1}) \bullet A$$

$$= U' \bullet [U^{-1} \bullet (U \bullet P_1 \bullet U^{-1})] \bullet \ldots \bullet (U \bullet p_m \bullet U^{-1}) \bullet (U \bullet V)$$

$$= U' \bullet (p_1 \bullet \ldots \bullet p_m \bullet V') \bullet (V')^{-1} \bullet U^{-1} \bullet (U \bullet V)$$

$$= U' \bullet [p_1 \bullet \ldots \bullet p_m \bullet (U')^{-1} \bullet U' \bullet V'] \bullet [(V')^{-1} \bullet (U')^{-1} \bullet U'] \bullet U^{-1} \bullet (U \bullet V)$$

$$= [U' \bullet P_1 \bullet (U')^{-1}] \bullet \ldots \bullet [U' \bullet P_m \bullet (U')^{-1}] \bullet (U' \bullet V') \bullet (U' \bullet V')^{-1} \bullet U' \bullet U^{-1} \bullet (U \bullet V)$$

$$= A \bullet (U' \bullet V')^{-1} \bullet (U' \bullet U^{-1}) \bullet (U \bullet V).$$

This implies that

$$(U' \bullet U^{-1}) \bullet A = A \bullet (U' \bullet V')^{-1} \bullet (U' \bullet U^{-1}) \bullet (U \bullet V). \quad (5)$$

By taking $X = U' \bullet U^{-1}$ (hence X is unimodular) and by multiplying both sides of equality (5) by the adjoint, A^+, of A, it follows that

$$A^+ \bullet X \bullet A = \det(A) \bullet (U' \bullet V')^{-1} \bullet X \bullet (U \bullet V). \quad (6)$$

Therefore,

$$A^+ \bullet X \bullet A \equiv 0 \qquad \mathrm{mod}(|\det(A)|)$$

and

$$U' = X \bullet U.$$

From equality (6) we have

$$1/\det(A) \bullet A^+ \bullet X \bullet A = (U' \bullet V')^{-1} \bullet X \bullet (U \bullet V). \quad (7)$$

But it can easily be shown that

$$(1/\det(A) \bullet A^+ \bullet X \bullet A)^{-1}$$

$= 1/\det(A) \bullet A^+ \bullet X^{-1} \bullet A$

$= 0 \quad \mod(|\det(A)|).$

Taking the inverse on both sides of equality (7), we finally obtain

$(1/\det(A) \bullet A^+ \bullet X \bullet A)^{-1}$

$= [(U' \bullet V')^{-1} \bullet X \bullet (U \bullet V)]^{-1};$

that is,

$1/\det(A) \bullet A^+ \bullet X^{-1} \bullet A$

$= (U \bullet V)^{-1} \bullet X^{-1} \bullet (U' \bullet V').$

Thus,

$U' \bullet V' = 1/\det(A) \bullet (U \bullet V) \bullet A^+ \bullet X^{-1} \bullet A.$

Q.E.D.

Definition 3.4. For any nonsingular matrix A in M(n,Z), a unimodular matrix X in M(n,Z) such that

$A^+ \bullet X \bullet A \equiv 0 \quad \mod(|\det(A)|)$

is called a uniconqruential matrix of A.

Proposition 3.5. For any nonsingular matrix A, which is not unimodular, in M(n,Z), the set of all unicongruential matrices in M(n,Z) of A forms a subgroup, the unicongruential subgroup of matrix A , of the group of units in M(n,Z) (i.e., the set of all unimodular matrices in M(n,Z)).

Let u be any nonzero element in Z, then the principal congruence subgroup of the group of units of level u is the set of all unimodular matrices W such that

$W \equiv I \quad \mod(u).$

Further studies on this kind of subgroup can be found in

[Newman; 1972, chapter VII].

<u>Proposition 3.6</u>. Let A be a nonsingular matrix, which is not unimodular, in M(n,Z). Then the principal congruence subgroup of level det(A) is a subgroup of the uncongruential subgroup of the matrix A.

From the propositions above we immediately get that the unicongruential subgroup of any nonsingular and non-unimodular matrix in M(n,Z) is a nontrivial group (a trivial group consists of the identity matrix only).

<u>Theorem 3.7</u>. (Uniqueness of Left Normal Decomposition). Let A be a nonsingular matrix, which is not unimodular, in M(n,Z). Then, there exists a left normal decomposition

$$A = P_1 \bullet P_2 \bullet \ldots \bullet P_s \bullet U.$$

Moreover, if

$$A = Q_1 \bullet Q_2 \bullet \ldots \bullet Q_r \bullet V$$

is another left normal decomposition. Then r = s, and there exists a matrix X in the unicongruential subgroup of A such that

$$Q_i = X \bullet P_i \bullet X^{-1}$$

and

$$V = X \bullet U \bullet (A^{-1} \bullet X^{-1} \bullet A).$$

<u>Proof</u> :

Let A be a nonsingular matrix, which is not unimodular, in M(n,Z). The existence of a left normal decomposition was proved in the section 3.3. Now assume that matrix A has another left normal decomposition given by

$$A = Q_1 \bullet Q_2 \bullet \ldots \bullet Q_r \bullet V.$$

Then by the fact that the determinants of matrices P_i and Q_j are prime numbers, it is easy to see that the number, s, of matrices P_i should be equal to the number, r, of matrices Q_j .

Secondly, by the fact that the matrices P_i are commuting normal prime matrices, there exists a unimodular matrix W so that $W^{-1} \bullet P_i \bullet W = P'_i$, for all i, where P' is a diagonal matrix (see Thm 4.3 for the proof of this fact). Similarly, there exists a unimodular matrix Y so that $Y^{-1} \bullet Q_j \bullet Y = Q'_j$, for all j, where Q' is a diagonal matrix. Thus, the decompositions become

$$A = (W \bullet P'_1 \bullet W^{-1}) \bullet \ldots\ldots \bullet (W \bullet P'_s \bullet W^{-1}) \bullet (W \bullet U') \tag{8}$$

and

$$A = (Y \bullet Q'_1 \bullet Y^{-1}) \bullet \ldots\ldots \bullet (Y \bullet Q'_s \bullet Y^{-1}) \bullet (Y \bullet V'), \tag{9}$$

where

$$W \bullet U' = U$$

and

$$Y \bullet V' = V.$$

Furthermore, by a suitable rearrangement of the factors in the equations (8) and (9) and by Lemma 3.4, we have

$$\begin{aligned} Q_i &= Y \bullet Q'_i \bullet Y^{-1} \\ &= X \bullet W \bullet P'_i \bullet W^{-1} \bullet X^{-1} \\ &= X \bullet P_i \bullet X^{-1}, \qquad 1 \le i \le s, \end{aligned}$$

where X is a unicongruential matrix of A. In addition,

$$V = Y \bullet V'$$
$$= (1/\det(A)) \bullet X \bullet (W \bullet U') \bullet (A^{+} \bullet X^{-1} \bullet A)$$
$$= X \bullet U \bullet (A^{-1} \bullet X^{-1} \bullet A).$$

Q.E.D.

In concluding this chapter, we point out that the one-sided decomposition of matrices given above does not bear exactly the same meaning as the theorem of unique factorization in principle ideal domains, because we have restricted our 'prime factors' to be a subclass of all prime elements in M(n,Z).

CHAPTER IV

Normal Prime Matrices in M(n,Z)

The normal prime matrices introduced in the previous chapter possess some special properties, and we devote this chapter to exploring these. In section 4.2 we show that two commutative normal prime matrices can be diagonalized simultaneously. The first section gives two lemmas which permit us to prove this result.

4.1 : Preliminary Lemmas

Lemma 4.1. Let $P = \mathrm{diag}(1,\ldots,1,p)$,

$$Q = U^{-1} \bullet \mathrm{diag}(1,\ldots 1,q) \bullet U$$

be two normal prime matrices with

$$U = \begin{bmatrix} U^{n-1} & U^{1} \\ U^{2} & u \end{bmatrix}.$$

If $P \bullet Q = Q \bullet P$ and $u \neq 0$

then we have

$$Q = \begin{bmatrix} I^{n-1} & O \\ O & q \end{bmatrix}.$$

Proof :

Let

$$Q = \begin{bmatrix} Q^{n-1} & Q^{1} \\ Q^{2} & x \end{bmatrix}$$

with Q^{n-1} : $(n-1) \times (n-1)$ matrix

Q^{1} : $(n-1)$-column vector

Q^{2} : $(n-1)$-row vector.

Then, by assumption

$$P \bullet Q = Q \bullet P,$$

so that

$$\begin{bmatrix} Q^{n-1} & Q^{1} \\ pQ^{2} & px \end{bmatrix} = \begin{bmatrix} Q^{n-1} & Q^{1}p \\ Q^{2} & xp \end{bmatrix}.$$

But $p > 1$, so we get

$$Q^{1} = \begin{bmatrix} 0 \\ \bullet \\ \bullet \\ \bullet \\ 0 \end{bmatrix}$$

and

$$Q^{2} = (0, \ldots\ldots, 0).$$

Furthermore, from

$$Q = U^{-1} \bullet \mathrm{diag}(1, \ldots, 1, q) \bullet U$$

we have

$$U \bullet Q = \mathrm{diag}(1; \ldots, 1, q) \bullet U,$$

i.e.,

$$\begin{bmatrix} U^{n-1} & U^{1} \\ U^{2} & u \end{bmatrix} \begin{bmatrix} Q^{n-1} & 0 \\ 0 & x \end{bmatrix}$$

$$= \begin{bmatrix} I^{n-1} & 0 \\ 0 & q \end{bmatrix} \begin{bmatrix} U^{n-1} & U^1 \\ U^2 & u \end{bmatrix};$$

i.e.,

$$\begin{bmatrix} U^{n-1} \bullet Q^{n-1} & U^1 x \\ U^2 \bullet Q^{n-1} & ux \end{bmatrix} = \begin{bmatrix} U^{n-1} & U^1 \\ qU^2 & qu \end{bmatrix}.$$

Then we get the following equations :

$$U^{n-1} \bullet Q^{n-1} = U^{n-1}, \quad (1)$$

$$U^1 \bullet x = U^1, \quad (2)$$

$$ux = qu. \quad (3)$$

But by assumption $u \neq 0$. Thus from equation (3) it follows that

$$x = q \neq 0.$$

Combining this with equation (2) we have

$$U^1 \bullet x = U^1 \bullet q = U^1,$$

so that

$$U^1 = \begin{bmatrix} 0 \\ \bullet \\ \bullet \\ \bullet \\ 0 \end{bmatrix}.$$

Moreover, because U is unimodular then $u = \pm 1$. Therefore, from

$$u \bullet (\det(U^{n-1}))$$
$$= \pm(\det(U^{n-1}))$$
$$= \det(U)$$
$$= \pm 1.$$

We have proved that U^{n-1} is a unimodular matrix. Now by equation (1), we conclude that

$$Q^{n-1} = I$$

which completes the proof.

Q.E.D.

<u>Lemma 4.2</u>. Let $P = \mathrm{diag}(1,\ldots,1,p)$,

$$Q = U^{-1} \bullet \mathrm{diag}(1,\ldots,1,q) \bullet U$$

be two normal prime matrices with

$$U = \begin{bmatrix} U^{n-1} & U^1 \\ U^2 & 0 \end{bmatrix}.$$

If $P \bullet Q = Q \bullet P$ then we have

$$Q = \begin{bmatrix} Q^{n-1} & 0 \\ 0 & 1 \end{bmatrix},$$

with Q^{n-1} being a normal prime matrix.

<u>Proof</u> :

As in the proof of Lemma 4.1, the matrix Q must be of the form

$$Q = \begin{bmatrix} Q^{n-1} & 0 \\ 0 & x \end{bmatrix}.$$

Furthermore, $U^1 \neq 0$, otherwise U is not unimodular. Now from

$$U \bullet Q = \mathrm{diag}(1,\ldots,1,q) \bullet U,$$

i.e.,

$$\begin{bmatrix} U^{n-1} & U^1 \\ U^2 & 0 \end{bmatrix} \begin{bmatrix} Q^{n-1} & 0 \\ 0 & x \end{bmatrix}$$

$$= \begin{bmatrix} I^{n-1} & 0 \\ 0 & q \end{bmatrix} \begin{bmatrix} U^{n-1} & U^1 \\ U^2 & 0 \end{bmatrix};$$

i.e.,

$$\begin{bmatrix} U^{n-1} \bullet Q^{n-1} & U^1 x \\ U^2 \bullet Q^{n-1} & 0 \end{bmatrix} = \begin{bmatrix} U^{n-1} & U^1 \\ qU^2 & 0 \end{bmatrix},$$

and we get the following equations :

$$U^{n-1} \bullet Q^{n-1} = U^{n-1}, \tag{4}$$

$$U^1 \bullet x = U^1. \tag{5}$$

From equation (5) and the fact that $U^1 \neq 0$ we get

$$x = 1,$$

and therefore

$$|\det(Q^{n-1})| = |\det(Q)| = q.$$

Now, in order to prove Q^{n-1} is normal prime we need to find a unimodular matrix T^{n-1} such that

$$T^{n-1} \bullet Q^{n-1} \bullet (T^{n-1})^{-1}$$

$$= \mathrm{diag}(1, \ldots, 1, q)$$

But, if we let

$$T = \begin{bmatrix} T^{n-1} & 0 \\ 0 & 1 \end{bmatrix}, \tag{6}$$

then

$$T \bullet Q \bullet T^{-1}$$

$$= \begin{bmatrix} T^{n-1} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} Q^{n-1} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} (T^{n-1})^{-1} & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \mathrm{diag}(1,\ldots,1,q,1)$$

$$= Y^{-1} \bullet \mathrm{diag}(1,\ldots,1,q) \bullet Y,$$

with

$$Y = \begin{bmatrix} I^{n-2} & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix};$$

i.e.,

$$(Y \bullet T) \bullet Q \bullet (Y \bullet T)^{-1}$$

$$= \mathrm{diag}(1,\ldots,1,q).$$

Thus, if there exists a matrix T^{-1} which transforms Q^{n-1} to its Smith normal form, then the matrix $V = Y \bullet T$ transforms Q into its Smith normal form. The matrix $V = Y \bullet T$ assumes the special form

$$V = \begin{bmatrix} V^{n-2} & V^1 & 0 \\ 0 & 0 & 1 \\ V^2 & v & 0 \end{bmatrix}. \qquad (7)$$

Therefore if such a matrix V can be constructed, then T^{n-1} can be obtained from $T = Y^{-1} \bullet V$ and will assume the form (6).

From equation (4) and from the fact that $|\det(Q^{-1})| = q$, we get that U^{n-1} must be a singular matrix. Moreover, by Theorem 1.2, there exist two unimodular matrices H^{n-1} and K^{n-1} such that

$$H^{n-1} \bullet U^{n-1} \bullet K^{n-1}$$

$$= \mathrm{diag}(u^1,\ldots,u^{n-2},0)$$

with $u \geq 0$ for $i = 1,\ldots,n-2$

Now let

$$H = \begin{bmatrix} H^{n-1} & 0 \\ 0 & 1 \end{bmatrix},$$

$$K = \begin{bmatrix} K^{n-1} & 0 \\ 0 & 1 \end{bmatrix}.$$

Then,

$$H \bullet U \bullet K = \begin{bmatrix} U'^{n-2} & 0 & W \\ 0 & 0 & 1 \\ Z & 1 & 0 \end{bmatrix}.$$

Taking

$$S = \begin{bmatrix} I^{n-2} & -W & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

so that

$$S^{-1} = \begin{bmatrix} I^{n-2} & W & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

we obtain

$$\begin{aligned} & S \bullet (H \bullet U \bullet K) \bullet K^{-1} \bullet Q \bullet K \\ & \qquad \bullet (H \bullet U \bullet K)^{-1} \bullet S^{-1} \\ & = S \bullet H \bullet U \bullet Q \bullet U^{-1} \bullet H^{-1} \bullet S^{-1} \\ & = S \bullet H \bullet \mathrm{diag}(1,\ldots 1,q) \bullet U \bullet U^{-1} \bullet H^{-1} \bullet S^{-1} \\ & = S \bullet \mathrm{diag}(1,\ldots,1,q) \bullet H \bullet H^{-1} \bullet S^{-1} \\ & = S \bullet \mathrm{diag}(1,\ldots,1,q) \bullet S^{-1} \end{aligned}$$

$= \mathrm{diag}(1,\ldots,1,q)$.

On the other hand,

$$S \bullet (H \bullet U)$$

$$= S \bullet (H \bullet U \bullet K) \bullet K^{-1}$$

$$= \begin{bmatrix} I^{n-2} & -W & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} U'^{n-2} & 0 & W \\ 0 & 0 & 1 \\ Z & 1 & 0 \end{bmatrix} \begin{bmatrix} J^{n-2} & J^1 & 0 \\ J^2 & j & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} U'^{n-2} & 0 & 0 \\ 0 & 0 & 1 \\ Z & 1 & 0 \end{bmatrix} \begin{bmatrix} J^{n-2} & J^1 & 0 \\ J^2 & j & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} U'^{n-2} \bullet J^{n-2} & U'^{n-2} \bullet J^1 & 0 \\ 0 & 0 & 1 \\ Z \bullet J^{n-2} + J^2 & Z \bullet J^1 + j & 0 \end{bmatrix}$$

Therefore, let $V = S \bullet (H \bullet U)$, and this is the desired unimodular matrix of the form (7).

Q.E.D.

4.2 : Diagonalization of Normal Prime Matrices

Any two matrices A, B in $M(n,Z)$, even if they are commutative, can not in general be diagonalized by the same sequence of elementary operations. The situation, however, is quite different if A and B are both normal prime matrices.

Theorem 4.3. Let P, Q be two normal prime matrices in $M(n,Z)$. If

$P \bullet Q = Q \bullet P$

then there exists a unimodular matrix U in $M(n,Z)$ such that $U^{-1} \bullet P \bullet U$ and $U^{-1} \bullet Q \bullet U$ are both of diagonal form.

<u>Proof</u> :

Step 1 :

By the definition of a normal prime matrix, there is a unimodular matrix U' such that

$$U'^{-1} \bullet P \bullet U' = \mathrm{diag}(1,\ldots,1,p).$$

Step 2 :

Apply U' to the matrix Q to obtain

$$U'^{-1} \bullet Q \bullet U = Q'.$$

Since Q' is still commutative with $\mathrm{diag}(1,\ldots,1,p)$, by lemma 4.1 and lemma 4.2, Q' can assume one of two forms.

Step 3 :

If

$$Q' = \begin{bmatrix} I^{n-1} & 0 \\ 0 & q \end{bmatrix},$$

then U' is as desired and we have finished.

Step 4 :

Otherwise,

$$Q' = \begin{bmatrix} Q'^{n-1} & 0 \\ 0 & 1 \end{bmatrix}$$

and Q'^{n-1} is still a normal prime matrix.

Thus, there exists a matrix U''^{n-1} such that

$$(U''^{n-1})^{-1} \bullet Q'^{n-1} \bullet U''^{n-1}$$

$$= \mathrm{diag}(1,\ldots,1,q).$$

Step 5 :

Obviously,

$$\begin{bmatrix} (U''^{n-1})^{-1} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} Q'^{n-1} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} U''^{n-1} & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \mathrm{diag}(1,\ldots,1,q,1).$$

Step 6 :

By taking

$$\tilde{U} = U' \bullet \begin{bmatrix} (U''^{n-1}) & 0 \\ 0 & 1 \end{bmatrix},$$

the theorem follows.

Q.E.D.

By induction we can easily generalize the theorem above for m commutative normal prime matrices.

Theorem 4.4. Let $P^1, P^2, \ldots, P^m$ be normal prime matrices. If they are commutative, then there exists a [illegible]modular matrix $\tilde{U}$ such that $U^{-1} \bullet P^i \bullet U$ is a diagonal matrix for all i, $1 \le i \le m$.

4.3 : Examples

In concluding this chapter we give two examples to illustrate Theorem 4.3.

Examples :

1 :

Let

$$P = \begin{bmatrix} -2 & -12 \\ 1 & 5 \end{bmatrix},$$

$$Q = \begin{bmatrix} -11 & -48 \\ 4 & 17 \end{bmatrix},$$

then

$$P \bullet Q = \begin{bmatrix} -26 & -108 \\ 9 & 37 \end{bmatrix}$$

$$= Q \bullet P.$$

Hence, P and Q are commutative. If

$$U = \begin{bmatrix} 4 & -3 \\ -1 & 1 \end{bmatrix},$$

then

$$U^{-1} \bullet P \bullet U = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix},$$

$$U^{-1} \bullet Q \bullet U = \begin{bmatrix} 5 & 0 \\ 0 & 1 \end{bmatrix}.$$

2 :

Given two matrices

$$P = \begin{bmatrix} 1 & 0 & 0 \\ -8 & 1 & 4 \\ -4 & 0 & 3 \end{bmatrix},$$

$$Q = \begin{bmatrix} 52 & 15 & -30 \\ 34 & 11 & -20 \\ 102 & 30 & -59 \end{bmatrix}.$$

Then

$$P \bullet Q = \begin{bmatrix} 52 & 15 & -30 \\ 26 & 11 & -16 \\ 98 & 30 & -57 \end{bmatrix}$$

$$= Q \bullet P.$$

Hence, P and Q are commutative.

We first obtain

$$U' = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 1 & 2 \\ 4 & 2 & 1 \end{bmatrix}$$

and

$$(U')^{-1} \bullet P \bullet U' = \mathrm{diag}(1,1,3).$$

Apply U' to the matrix Q to obtain

$$Q' = (U')^{-1} \bullet Q \bullet U'$$

$$= \begin{bmatrix} 0 & 2 & 0 \\ -1 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then according to the step 4 a matrix U" can be obtained such that

$$(U'')^{-1} \bullet (Q')^2 \bullet (U'')$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix},$$

where

$$U'' = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

and

$$Q'^2 = \begin{bmatrix} 0 & 2 \\ -1 & 3 \end{bmatrix}.$$

The matrix U is then given by

$$U = U' \bullet \begin{bmatrix} U'' & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 3 & 0 \\ 3 & 2 & 2 \\ 10 & 6 & 1 \end{bmatrix}$$

and

$$U^{-1} = \begin{bmatrix} -10 & -3 & 6 \\ 17 & 5 & -10 \\ -2 & 0 & 1 \end{bmatrix}.$$

Then we have

$$U^{-1} \bullet P \bullet U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix},$$

$$U^{-1} \bullet Q \bullet U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

CHAPTER V

A Non-iterative Algorithm for Computing A Left Greatest Common Divisor

5.1 : The Algorithm

Unlike the case of integers and polynomials, because of the non-commutativity of matrix rings, the prime decomposition of two matrices does not yield their left greatest common divisor. Having defined an algorithm for the division of two matrices, however, the Euclidean algorithm can be used to obtain a greatest common divisor. In this chapter, a new algorithm for the computation of a left greatest common divisor is given. This algorithm requires only the computation of the Smith normal form of a matrix, and thereby avoids the iterative nature of the Euclidean algorithm.

We begin with a definition of a left greatest common divisor, more general than that given in Definition 3.2.

Definition 5.1 : Let A, B be arbitrary elements in M(n,z), A left greatest common divisor of A and B is an element D, denoted by lgcd(A,B) = D, in M(n,z) such that D left divides both A and B; and if D' is any element in M(n,z) which left divides both A and B also, then D' left divides D.

The Non-iterative LGCD Algorithm :

Given two matrices A and B in M(n,z), this new algorithm computes D = lgcd(A,B) and two multipliers X and Y such that

$$A \bullet X + B \bullet Y = D.$$

Step 1 (Smith normal form) :

Augment the matrices A, B to form an nx2n matrix C = [A , B]. Then find two unimodular matrices U, V such that U • C • V = [S , O] is the Smith normal form of C.

Step 2 (Inversion) :

Compute U^{-1}.

Step 3 (Termination) :

D <--- U^{-1} • (the first n columns of U • C • V).

X <--- the first n rows and first n columns of V.

Y <--- the last n rows and first n columns of V.

Proof of the validity of the Algorithm :

By Theorem 1.2, there are two unimodular matrices U(nxn), V(2nx2n) such that

$$U \bullet C \bullet V = [\ S\ ,\ O\ ]$$

is the Smith normal form of C. Partition the matrix V into four nxn submatrices as follows :

$$V = \begin{bmatrix} V^1 & V^2 \\ V^3 & V^4 \end{bmatrix}.$$

Hence,

$$[\ A \bullet V^1 + B \bullet V^3\ ,\ A \bullet V^2 + B \bullet V^4\ ]$$

$$= [\, A , B \,] \begin{bmatrix} V^1 & V^2 \\ V^3 & V^4 \end{bmatrix}$$

$$= C \bullet V$$

$$= U^{-1} \bullet [\, S , O \,]$$

$$= [\, U^{-1} \bullet S , O \,]$$

$$= [\, D , O \,];$$

i.e.,

$$A \bullet V^1 + B \bullet V^3 = D.$$

To prove D is a left greatest common divisor we show that D left divides both A, B and any other left common divisor of A, B left divides D. The second part is quite obvious, and we need only to prove the first part.

Since the matrix V is unimodular, its inverse

$$V^{-1} = \begin{bmatrix} W^1 & W^2 \\ W^3 & W^4 \end{bmatrix},$$

where W^i are nxn matrices, exists.

Then, from

$$[\, A , B \,] \bullet V = [\, D , O \,],$$

we obtain

$$[\, A , B \,] = [\, D , O \,] \bullet V^{-1}$$

$$= [\, D , O \,] \begin{bmatrix} W^1 & W^2 \\ W^3 & W^4 \end{bmatrix}$$

$$= [\, D \bullet W^1 , D \bullet W^2 \,];$$

i.e.,

$A = D \bullet W^1,$

$B = D \bullet W^2.$

Thus, D left divides both A and B. Furthermore, by setting $X = V^1$, $Y = V^3$, it follows that

$A \bullet X + B \bullet Y = D.$

Q.E.D.

5.2 : The Algorithm for Multiple Matrices

The previous algorithms can be applied m - 1 times to compute a left greatest commom divisor of m (m > 2) matrices in M(n,Z). It turns out that by making a small modification to the non-iterative LGCD algorithm we get a new efficient algorithm for computing their left greatest commom divisor.

The Non-iterative Algorithm for m Matrices :

Given m (m > 2) matrices $A^1, A^2, \ldots, A^m$ in M(n,Z), this algorithm computes $D = \text{lgcd}(A^1, A^2, \ldots, A^m)$ and m multipliers $X^1, X^2, \ldots, X^m$ such that

$A^1 \bullet X^1 + \ldots + A^m \bullet X^m = D.$

Step 1 (Smith normal form) :

Augment the matrices A^1, A^2, ..., A^m to form an nx(mxn) matrix $C = [A^1, A^2, \ldots, A^m]$. Then find two unimodular matrices U, V such that $U \bullet C \bullet V = [S, 0, \ldots, 0]$ is the Smith normal form of C.

Step 2 (Inversion) :

Compute U^{-1}.

Step 3 (Termination) :

D <--- U^{-1} • (the first n columns of U • C • V).

X^1 <--- the first n rows and first n columns of V.

X^2 <--- the second n rows and first n columns of V.

.

.

.

X^m <--- the last n rows and first n columns of V.

5.3 : Complexity Considerations

There are now three methods of computing a greatest common divisor lgcd(A,B) of two matrices A and B, namely,

Method (1) :

Euclidean algorithm using Sanov's division algorithm (see section 2.2).

Method (2) :

Euclidean algorithm using the integer-arithmetic algorithm (see section 2.3).

and

Method (3) :

The non-iterative lgcd algorithm given in the previous section.

We first count the number of operations required to perform the divisions in methods 1 and 2. Sanov's algorithm, in steps 1, 2 and 3 includes the triangularization of a matrix, a matrix inversion and a matrix multiplication. This requires $O(n^3)$ operations. Steps 5 and 6 require an additional $O(n^3)$ operations. Thus, Sanov's division algorithm requires at least $O(n^3)$ operations.

On the other hand, the integer-arithmetic division algorithm involves a matrix multiplication, the computation of the adjoint of a matrix, and finding the Smith normal form of a matrix. The Smith normal form of a matrix can be obtained by means of Bradley's algorithm, which requires $O(n^3) + O(n^2 \bullet \text{determinant of the matrix})$ operations [Bradley; 1971]. Indeed, this is the dominating cost of the integer-arithmetic division algorithm. Thus, with respect to total operations required, this crude analysis does not permit us to determine which of the methods 1 or 2 is superior.

Methods 1 and 2 are iterative, requiring at most $\min\{ |\det(A)|, |\det(B)| \}$ steps (i.e., matrix divisions) before termination occurs. Method 3, on other hand, requires simply one matrix inversion, and the Smith normal form of one nx2n matrix. Clearly then, method 3 is asymptotically superior to both methods 1 and 2 with respect to the total number of operations required.

The above analysis has ignored the cost of each of the operations involved. Method 1, for example, uses rational arithmetic; and even if matrices A, B have single-precision components, all methods may require multiple-precision arithmetic. Thus, the cost of the methods depends not only on the total number of operations required, but also on the size of intermediate results on which multiple-precision arithmetic is being performed. Indeed, we suspect that all three methods suffer because of "intermediate expression growth", a phenomenon common to most algorithms in algebraic and symbolic manipulation. That is, the length of intermediate results may be large even for problems where the length of the initial and final results is small. An analysis of the three methods which takes these matters into consideration, however, is a major undertaking, and we leave it as a subject for further research.

BIBLIOGRAPHY

Aho, A.V., Hopcroft, J.E. & Ullman, J.D. 1974

The design and analysis of computer algorithms, Addison-Wesley, Reading, Mass..

Bareiss, E.H. 1972

"Computational solutions of Matrix problems over integral domain", J. Inst. Math. Applics., V.10, pp.68-104.

Blankinship, W.A. 1963

"A new version of the Euclidean algorithm", Amer. Math. Mon., V.70, pp.742-745.

Blankinship, W.A. 1966

"Algorithm 287, Matrix triangulation with integer arithmetic [F1]", Comm. ACM, V.9, pp.513.

Blankinship, W.A. 1966

"Algorithm 288, solution of simultaneous linear diophantine equations [F4]", Comm. ACM, V.9, pp.514.

Bradley, G.H. 1970

"Algorithm and bound for the greatest common divisor of n integers", Comm. ACM, V.13, pp.433-436.

Bradley, G.H. 1971

"Algorithms for Hermite and Smith normal matrices and linear Diophantine equations", Math. of Comput., v.25, No.116, pp.897-907.

Brown, W.S. 1971

"On Euclid's algorithm and the computation of polynomial greatest commom divisors", _J. ACM_, v.18, pp.478-504.

Brung, H.H. 1973

"Left Euclidean rings", _Pacific J. of Math._, v.45, No.1, pp.27-33.

Collins, G.E. 1968

"Computing Multiplicative Inverses in GF(p)", _U. of Wisconsin Comput. Sc. TR#22_.

Collins, G.E. 1969

"Computing time analysis for some arithmetic and algebraic algorithms", _Proc. 1968 Summer Institute on Symbolic Math. Comp._, IBM Corp., Cambridge,Mass., pp.197-231.

Collins, G.E. 1974

"The computing time of the Euclidean algorithm", _SIAM J. Comput._, V.3, No.1, pp.1-10.

Hu, T.C. 1969

Integer programming and network flows, Addison-Wesley, Reading, Mass., pp.317-354, 377-381

Jacobson, N. 1953

Lectures in abstract algebra, V.II, linear algebra, Von Nostrand, Princeton, N.J..

Kallman, R.E., Falb, P.L. & Arbib, M.A. 1969

Topics in Mathematical system theory, McGraw-Hill, New York.

Kelisky, R.P. 1965

"Concerning the Euclidean algorithm", _Fibonacci Quarterly_, V.3, No.3, pp.219-223.

Knuth, D.E. 1968

The art of computer programming, V.I, Fundamental algorithms, Addison-Wesley, Reading, Mass..

Knuth, D.E. 1969

The art of computer programming, V.II, Seminumerical algorithms, Addison-Wesley, Reading, Mass..

Macduffee, C.C. 1940

An introduction to abstract algebra, Wiley, New York.

Maclane, S. & Birkhoff, G. 1967

Algebra, MacMillan, New York.

Newman, M. 1972

Integral Matrices, Academic Press, New York.

Rosser, J.B. 1952

"A method of computing exact inverses of matrices with integer coefficients", J. Res. Nat. Bur. Standards, V.49, pp.349-358.

Sanov, I.N. 1967

"Euclid's algorithm and one-sided decomposition into prime factors for matrix rings", Siberian Math. J., V.8, No.4, pp.640-645.

Smith, D.A. 1966

"A basis algorithm for finitely generated Abelian groups", Math. Algorithms, V.1, pp.13-26.

Uspensky, J.V. & Heaslet, M.A. 1939

Elementary number theory, Mcgraw-Hill, New York, pp.222-225.

Van Der Waerden, B.L. 1950

Moderne algebra, V.II, English transl., Ungar, NEW

York.

Zadeh, L.A. & Polak, E. 1969
Systems theory, Mcgraw-Hill, New York.