Matrix number theory, I: factorization of 2×2 unimodular matrices[1])

By BERNARD JACOBSON (Lancaster, Penn.)
and ROBERT J. WISNER (University Park, N. M.)

1. Introduction

The subject of matrices enjoys a duly-earned place in mathematics, and the fact that matrices can be presented as representations of linear transformations does not obviate their importance as rectangular arrays of numbers in other fields of mathematics or in applications. This paper, however, arises neither from algebraic considerations nor from a desire to examine new applications. The spirit here is number-theoretic, exploring classes of matrices as one might explore the positive integers and their properties. Indeed, we shall in this first of a projected series of papers on matrix number theory consider only 2×2 matrices with integral entries; moreover, strictest attention centers upon the case in which the entries are positive or nonnegative integers and in which the matrices are unimodular. This being the case, matrix addition is not a closed operation while matrix mulriplication is; and our attention is confined to basic multiplicative number-theoretic properties of factorization.

We first establish some notation and recall some elementary facts. The set of integers is denoted, as usual, by Z; and we let Z^1 designate the set of positive integers, while Z^0 will be used to represent the set of nonnegative integers. Elements of Z will be labelled $a, b, c, \ldots,$ and 2×2 matrices will be labelled, $A, B, C, \ldots$. A is called *unimodular* if $|A|=1$, and the set of unimodular matrices over Z^1, Z^0, or Z is a multiplicative semigroup.

In this paper, the factorization properties of 2×2 unimodular matrices are explored, first with the entires coming from Z^1, then from Z^0, finally from Z.

B is said to be a *left divisor* (or *factor*) of A if for some matrix C, $A=BC$; a *right divisor* if $A=DB$ for some matrix D. *A unit* in a semigroup of matrices is a matrix which is a divisor of every matrix of the semigroup, and in the cases to be considered, all units are both left and right; a *prime* in a matrix semigroup is a matrix which is not a unit and has at most units and itself as divisors; all other nonunit matrices are *composite*.

---

[1]) Presented to the 600- th meeting of the American Mathematical Society April 26, 1963

It appears that few of the results about 2×2 matrices can be generalized to the $n\times n$ case. However, the 2×2 case is of interest in itself, and it lends itself uniquely to number-theoretic studies which will be presented later.

In § 2, the result (nonunique factorization of 2×2 matrices over Z^1) is of small interest in itself, but it is used here to prove the result in § 3 (unique factorization of 2×2 matrices over Z^0). This latter fact seems to be a new piece of knowledge about an unstudied segment of the classical modular group. Hopefully, this sort of information may lead to advances in some difficult problems which arise in investigating the structure of the modular group, about which precious little is known.

2. Entries in Z^1

We let here the symbol U_2^1 designate the multiplicative semigroup of all unimodular 2×2 matrices over Z^1, exploring some questions about the divisibility of such matrices.

The first thing to notice is that since each entry of a matrix in U_2^1 is a positive integer, the definition of matrix multiplication assures that each entry of a product of two matrices in U_2^1 is a sum of two positive integers; consequently, no matrix with 1 as an entry has a divisor, so there are no units in U_2^1. This makes the concept of a prime in U_2^1 very simple: *A is a prime in U_2^1 if it cannot be written as a product of elements in U_2^1*. Thus, it is clear that if the element $A\in U_2^1$ contains 1 as an entry, then A is prime. The "only if" counterpart of this statement is also true, as will be seen in the proof of Theorem 1.

Theorem 1. *Let $A\in U_2^1$, and let m be the minimum value of the entries of A. U_2^1 has no units; A is prime if $m=1$; and A factors uniquely as a product of primes if and only if $m=2$.*

PROOF. Suppose

$$A=\begin{pmatrix} m & a \\ b & c \end{pmatrix}\in U_2^1$$

with minimal entry m (we shall later implore the reader to check that the position of m is unimportant). If $m=1$, then A is prime, as seen above. If $m>1$, then we compute some new positive integers: let k be the least positive residue of a, mod m, and let l be the least positive residue of b, mod m. That is, write

$$a=rm+k \tag{1}$$

$$b=sm+l$$

where, since $|A|=1$ and $m>1$ and minimal, it is easy to check that $r\geqq 1$, $s\geqq 1$, $1\leqq k<m$, $1\leqq l<m$. Notice that since $mc-ab=1$, m divides $ab+1$. Moreover, computing $ab+1$ as expressed in (1) yields the fact that m divides $kl+1$; simple arithmetic assures that each of the entries in the following factorizations of A is

a positive integer and that each matrix involved as a factor is unimodular:

$$(2)\qquad A=\begin{pmatrix} m & a \\ b & c \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ \dfrac{b-l}{m} & \dfrac{m+b-l}{m} \end{pmatrix}\begin{pmatrix} m-l & \dfrac{(m-l)a-1}{m} \\ l & \dfrac{la+1}{m} \end{pmatrix}=$$

$$=\begin{pmatrix} m-k & k \\ \dfrac{(m-k)b-1}{m} & \dfrac{kb+1}{m} \end{pmatrix}\begin{pmatrix} 1 & \dfrac{a-k}{m} \\ 1 & \dfrac{m+a-k}{m} \end{pmatrix}$$

These factorizations of A form the crux of the proof, showing also that if $m>1$, then A is not a prime, thus completing the aforementioned characterization of primes in U_2^1. We leave it to the reader to check that other positionings of the minimal element $m>1$ may cause (2) to undergo changes, but that there will still exist two factorizations, one with the first factor containing a row of 1's, the other with the second factor containing a column of 1's, and each factor being an element of U_2^1.

Two things are clear. First, if the two factorizations given in (2) are the same, then $m=2$, and it is easy to see that A can be factored in no other way. Second, if $m>2$, then the two factorizations as given are not the same, but neither are the factors necessarily prime.

However, in case $m>2$ (and now we stress that m need not be placed in the first row and first column as in (2)), we proceed as follows: factor the given matrix to obtain-as in the first factorization of (2)-a prime initial factor with a row of 1's, and in case the second factor is not a prime, repeat the process until a factorization is obtained in which we may write

$$(3)\qquad A=A_1A_2\ \ldots\ A_h$$

where $A_1, A_2, \ldots, A_{h-1}$ each contains a row of 1's and A_h is prime. Next, begin again the factorization of the given matrix, this time concentrating on obtaining by repetition final prime factors as in the second part of (2), so that eventually,

$$(4)\qquad A=B_1B_2\ \ldots,\ B_j$$

where $B_2, B_3, \ldots, B_j$ each contains a column of 1's, and B_1 is prime.

Now if (3) and (4) are not identical, then it follows that A does not factor uniquely as a product of primes. If (3) and (4) are the same and $h=j=2$, then it is easy to conclude that the minimal element m of A is 2, contradicting our assumption that $m>2$. Thus, (3) and (4) being the same means that $h=j>2$, and the non-unique factorization of A will clearly be assured if we but show that each product of three matrices PQR where P has a row of 1's, Q has a row of 1's and a column of 1's, and R has a column of 1's (each of course being in U_2^1) can be factored into primes in another way. There are clearly only eight cases to consider, and the full

demonstration, completing the proof, is:

$$\begin{pmatrix}1 & 1\\ u & u+1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}1 & v\\ 1 & v+1\end{pmatrix}=\begin{pmatrix}2 & 1\\ 2u+1 & u+1\end{pmatrix}\begin{pmatrix}2 & 2v+1\\ 1 & v+1\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\ u & u+1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}v+1 & 1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}2 & 1\\ 2u+1 & u+1\end{pmatrix}\begin{pmatrix}2v+1 & 2\\ v & 1\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\ u & u+1\end{pmatrix}\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & v\\ 1 & v+1\end{pmatrix}=\begin{pmatrix}1 & 2\\ u & 2u+1\end{pmatrix}\begin{pmatrix}1 & v\\ 2 & 2v+1\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\ u & u+1\end{pmatrix}\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}v+1 & 1\\ v & 1\end{pmatrix}=\begin{pmatrix}1 & 2\\ u & 2u+1\end{pmatrix}\begin{pmatrix}v+1 & 1\\ 2v+1 & 2\end{pmatrix}$$

$$\begin{pmatrix}u+1 & u\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}1 & v\\ 1 & v+1\end{pmatrix}=\begin{pmatrix}2u+1 & u\\ 2 & 1\end{pmatrix}\begin{pmatrix}2 & 2v+1\\ 1 & v+1\end{pmatrix}$$

$$\begin{pmatrix}u+1 & u\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}v+1 & 1\\ v & 1\end{pmatrix}=\begin{pmatrix}2u+1 & u\\ 2 & 1\end{pmatrix}\begin{pmatrix}2v+1 & 2\\ v & 1\end{pmatrix}$$

$$\begin{pmatrix}u+1 & u\\ 1 & 1\end{pmatrix}\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & v\\ 1 & v+1\end{pmatrix}=\begin{pmatrix}u+1 & 2u+1\\ 1 & 2\end{pmatrix}\begin{pmatrix}1 & v\\ 2 & 2v+1\end{pmatrix}$$

$$\begin{pmatrix}u+1 & u\\ 1 & 1\end{pmatrix}\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}v+1 & 1\\ v & 1\end{pmatrix}=\begin{pmatrix}u+1 & 2u+1\\ 1 & 2\end{pmatrix}\begin{pmatrix}v+1 & 1\\ 2v+1 & 2\end{pmatrix}$$

3. Entries in Z^0

Now let U_2^0 designate the set of unimodular 2×2 matrices over Z^0, and it will be seen that a striking change takes place by admitting 0 as an entry. Whereas § 2 displayed an infinite number of primes in U_2^1 with nonunique factorization, the present circumstance reduces the number of primes to two, and there is unique factorization in U_2^0.

It should be noted that the identity matrix I_2 is the only unit in U_2^0; a prime in U_2^0 is, then, an element which cannot be written as the product of two nonunits.

Theorem 2. *In U_2^0, the only primes are the elements*

$$P_{12}=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad \textit{and} \quad P_{21}=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$$

and each element of U_2^0 is either the unit I_2, a prime, or is expressible uniquely as the product of primes.

PROOF. That I_2 is the only unit in U_2^0 is trivial.

To show that P_{12} and P_{21} are the only primes is easy. For if $A \in U_0^2$ has 0 as an entry, then the conditions which define the class U_2^0 force A to be of the form

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$$

and it is clear that

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^a = P_{12}^a$$

and that

$$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^b = P_{21}^b$$

where the exponent, as usual, denotes the indicated number of repeated matrix factors, with the 0 exponent defined to yield I_2. On the other hand, if $A \in U_2^0$ has all its entries positive, then by the results of § 2, A either has a minimal entry of 1 or can be factored (not necessarily in a unique manner) as a product of matrices in U_2^1, and hence in U_2^0, each of which has 1 as a minimal entry. But it is easy to check that the following equations hold:

$$\begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = P_{21}^b P_{12}^a$$

$$\begin{pmatrix} a & 1 \\ ab-1 & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b-1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} = P_{21}^{b-1} P_{12} P_{21}^{a-1}$$

$$\begin{pmatrix} ab+1 & a \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = P_{12}^a P_{21}^b$$

$$\begin{pmatrix} a & ab-1 \\ 1 & b \end{pmatrix} = \begin{pmatrix} 1 & a-1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & b-1 \\ 0 & 1 \end{pmatrix} = P_{12}^{a-1} P_{21} P_{12}^{b-1}$$

which then guarantee that every matrix in U_2^0, except for I_2, is divisible by P_{12} or P_{21}. Straightforward calculation yields that neither P_{12} nor P_{21} is a proper divisor of the other, so they are the only primes. It follows that A is expressible as the product of primes. (An alternate proof of this fact will be given in a later paper, where its approach gives rise to other natural questions.)

Finally, factorization of

$$A = P_{12}^{\alpha_1} P_{21}^{\alpha_2} P_{12}^{\alpha_3} P_{21}^{\alpha_4} \ldots,$$

where almost all of the exponents are 0, is unique. For if not, then it would be necessary that

$$P_{12}B = P_{21}C$$

or

$$DP_{12} = EP_{21}$$

for suitable matrices B, C or D, E in U_2^0. But

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

implies

$$\begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} e & f \\ e+g & f+h \end{pmatrix}$$

from which it follows that

$$a+c=e$$

$$c=e+g$$

so that

$$a+e+g=e$$

from which we conclude that $a=g=0$. But $a=0$ is impossible. A similar argument holds to show the impossibility of the equation $DP_{12}=EP_{21}$, and the proof is complete.

4. Entries in Z

Letting U_2 designate the multiplicative semigroup of all unimodular 2×2 matrices with entries in Z, we recall merely that U_2 is the classical modular group; and in a group, the usual concept of a prime is impossible.

(Received December 12, 1964.)