ON SOME CONGRUENCES OF IDEMPOTENT MATRICES

by N. A. KHAN, *Muslim University, Aligarh*

(Communicated by S. M. Shah, F.N.I.)

(*Received March 11; read December 6, 1957*)

ABSTRACT

Let A be an idempotent matrix (i.e. $A^2 = A$) with integral elements. It has been proved that if p is a prime or a pseudoprime, then the following congruences

(i) $(I+A)^p - A \equiv I \pmod{p}$, $A \not\equiv 0$

(ii) $[2(I-A)]^p + 2A \equiv 2I \pmod{p}$,

(iii) $[4(I-A)]^p + 4A \equiv 4I \pmod{p}$,

hold and conversely.

Examples have been constructed to show that the above results are nonvacuous.

1. A square matrix $A = (a_{rs})$ is said to be idempotent if $A^2 = A$. Ansari and Shah (1952) have proved certain results for the nilpotent matrices. The author (Khan, 1956) has established certain results on the congruences of involutory matrices. The purpose of this paper is to establish certain congruences involving an idempotent matrix A of order $n > 1$.

If X and Y be two matrices of the same order and if all the elements of $X-Y$ be integral multiples of p, where p is any integer greater than 1, then we shall write $X \equiv Y \pmod{p}$. Following Lehmer, we shall call an integer p a pseudoprime (for results on pseudoprimes see Erdos (1949) and references given therein), if $2^p \equiv 2 \pmod{p}$ and p is not a prime.

2. We now prove the following results on the congruences of idempotent matrices:

THEOREM 1. *Let $A \not\equiv 0$ be an idempotent matrix, whose elements are integers (positive, negative or zero). If p is a prime or a pseudoprime, then the congruence*

$$(I+A)^p - A \equiv I \pmod{p}$$

holds and conversely.

Proof. The theorem is obvious for $A = I$. We therefore prove it for $A \not\equiv I$. If p is a prime or a pseudoprime, $2^p \equiv 2 \pmod{p}$, and by hypothesis the elements of A are all integers. Therefore

$$(I+A)^p - A - I = I + \binom{p}{1}A + \binom{p}{2}A^2 + \binom{p}{3}A^3 + \cdots - A - I$$

$$= I + (2^p - 1)A - A - I$$

$$= (2^p - 2)A \equiv 0 \pmod{p},$$

0 is the null matrix, and

$$(I+A)^p - A \equiv I \pmod{p}.$$

To prove the converse, we have to prove that at least one element of $A \not\equiv 0$ is prime to $p > 1$. Let all the elements of A be integral multiples of p, then $A = pB$, where B is a square matrix of order n with integer elements. Thus

$A^k = A = p^k B^k$ and hence the elements of A are divisible by p^k however large k may be and so $A = 0$, a contradiction. So if $(I+A)^p - A \equiv I \pmod{p}$, the elements of $(2^p-2)A$ are divisible by p. Therefore $2^p - 2 \equiv 0 \pmod{p}$.

Hence either p is a prime or it must be a pseudoprime.

THEOREM 2. *Let A be an idempotent matrix, whose elements are integers (positive, negative or zero). If p is a prime or a pseudoprime, then the congruence*

$$[2(I-A)]^p + 2A \equiv 2I \pmod{p}$$

holds and conversely.

Proof. The theorem is obvious for $A = I$ or 0. We therefore prove it for $A \neq I, 0$. By hypothesis, the elements of A are all integers. Moreover, if p is a prime or a pseudoprime, then

$$2^p \equiv 2 \pmod{p} \quad \text{and}$$

$$\begin{aligned}
[2(I-A)]^p + 2A - 2I &= 2^p \left[I - \binom{p}{1} A + \binom{p}{2} A^2 - \binom{p}{3} A^3 + \dots \right] + 2A - 2I \\
&= 2^p I - 2^p \left[\binom{p}{1} - \binom{p}{2} + \binom{p}{3} - \dots \right] A + 2A - 2I \\
&= (2^p - 2)(I - A) \\
&= 0 \pmod{p}, \text{ where 0 denotes the null matrix.}
\end{aligned}$$

Hence $[2(I-A)]^p + 2A \equiv 2I \pmod{p}$.

To prove the converse, we observe that since the idempotent matrix A is not equal to I, the idempotent matrix $I-A$ is not null. Therefore we can prove, as in the proof of Theorem 1, that at least one element of $I-A$ is prime to $p > 1$. Now, if $[2(I-A)]^p + 2A \equiv 2I \pmod{p}$, the elements of the matrix $(2^p-2)(I-A)$ are integral multiples of p. But all the elements of $I-A$ are not integral multiples of p. Hence $2^p \equiv 2 \pmod{p}$ and so either p is a prime or it must be a pseudoprime.

THEOREM 3. *Let A be an idempotent matrix whose elements are integers (positive, negative or zero). If p is a prime or a pseudoprime, then the congruence*

$$[4(I-A)]^p + 4A \equiv 4I \pmod{p}$$

holds and conversely.

Proof. The theorem is obvious for $A = I, 0$. We therefore prove it for $A \neq I, 0$. If p is a prime or a pseudoprime, $2^p \equiv 2 \pmod{p}$. Also by hypothesis, the elements of A are all integers.

Hence

$$\begin{aligned}
[4(I-A)]^p + 4A - 4I &= 2^{2p}(I-A)^p + 4A - 4I \\
&= 2^{2p}(I-A) + 4A - 4I \\
&= (2^{2p} - 4)(I-A) \\
&= (2^p - 2)(2^p + 2)(I-A) \equiv 0 \pmod{p},
\end{aligned}$$

i.e. $$[4(I-A)]^p + 4A \equiv 4I \pmod{p}.$$

Conversely, if $[4(I-A)]^p + 4A \equiv 4I \pmod{p}$, the elements of the matrix $(2^p-2)(2^p+2)(I-A)$ are all (integer) multiples of p. But, it has been recently proved [Khan (1956), Theorem 1], that $2^{p-1} \not\equiv -1 \pmod{p}$ or $2^p \not\equiv -2 \pmod{p}$

for all integral values of $p > 1$. Also, as proved earlier, at least one element of the idempotent matrix $I-A$ is prime to p. Therefore,

$$2^p-2 \equiv 0 \pmod{p}, \text{ or } 2^p \equiv 2 \pmod{p}.$$

Hence either p is a prime or it must be a pseudoprime.

3. To show that the theorems proved above are nonvacuous, let us consider the following examples:

Example 1. Let $p = 7$, $n = 2$ and $A = \begin{bmatrix} 2 & -1 \\ 2 & -1 \end{bmatrix}$.

$$(I+A)^7-A-I = \begin{bmatrix} 255 & -127 \\ 254 & -126 \end{bmatrix} - \begin{bmatrix} 2 & -1 \\ 2 & -1 \end{bmatrix} - I$$

$$= \begin{bmatrix} 252 & -126 \\ 252 & -126 \end{bmatrix} \equiv 0 \pmod{7}.$$

This matrix A satisfies Theorem 1.

Example 2. Let $p = 5$, $n = 3$ and $A = \begin{bmatrix} 0 & 2 & -1 \\ -2 & 5 & -2 \\ -4 & 8 & -3 \end{bmatrix}$.

$$2^5(I-A)^5+2A-2I = 32 \begin{bmatrix} 1 & -2 & 1 \\ 2 & -4 & 2 \\ 4 & -8 & 4 \end{bmatrix} + \begin{bmatrix} 0 & 4 & -2 \\ -4 & 10 & -4 \\ -8 & 16 & -6 \end{bmatrix} - 2I$$

$$= \begin{bmatrix} 30 & -60 & 30 \\ 60 & -120 & 60 \\ 120 & -240 & 120 \end{bmatrix} \equiv 0 \pmod{5}.$$

Also,

$$[4(I-A)]^5+4A-4I = 1024 \begin{bmatrix} 1 & -2 & 1 \\ 2 & -4 & 2 \\ 4 & -8 & 4 \end{bmatrix} - 4 \begin{bmatrix} 1 & -2 & 1 \\ 2 & -4 & 2 \\ 4 & -8 & 4 \end{bmatrix}$$

$$= 1020 \begin{bmatrix} 1 & -2 & 1 \\ 2 & -4 & 2 \\ 4 & -8 & 4 \end{bmatrix} \equiv 0 \pmod{5}.$$

This matrix A satisfies Theorems 2 and 3.

Acknowledgement

Finally, the author's thanks are due to Professor S. M. Shah for drawing his attention to this problem.

References

Ansari, A. R., and Shah, S. M. (1952). A note on certain nilpotent matrices. *Maths. Student*, **20**, 113.

Erdos, P. (1949). On the converse of Fermat's theorem. *Amer. Math. Monthly*, **56**, 623.

Khan, N. A. (1956). On involutory matrices. *Amer. Math. Monthly*, **63**, 704.

Issued March 3, 1958.