THE EULER-FERMAT THEOREM FOR MATRICES

By Alex S. Davis

J. B. Marshall [2] has proved the following theorem which is analogous to Fermat's theorem in number theory.

Theorem 1. *Let p be an arbitrary prime, $n > 1$ an arbitrary integer, p^r the least power of p that is equal to or greater than n, and finally let q be the* L.C.M. *of $p^r, p^n - 1, p^{n-1} - 1, \cdots, p - 1$. If A is a matrix of order n whose determinant is prime to p and I is the unit matrix, then*

$$A^q \equiv I \pmod{p}.$$

For certain small values of p and n, Marshall has shown that q is the least power for which this is true. This has been proved in general by Ivan Niven [3].

In this paper we generalize this theorem as Euler did Fermat's theorem and show that the exponent obtained is the least possible. This more general theorem can be stated as follows.

Theorem 2. *Let $m = p_1^{a_1} \cdots p_s^{a_s}$ be an arbitrary number with the s distinct prime divisors $p_1, \cdots, p_s$, $n > 1$ an arbitrary integer, $p_i^{r_i}$ the least power of p_i greater than or equal to n, q_i the* L.C.M. *of $p_i^{r_i}, p_i^n - 1, \cdots, p_i - 1$, and finally let w be the* L.C.M. *of $q_1p_1^{a_1-1}, q_2p_2^{a_2-1}, \cdots, q_sp_s^{a_s-1}$. If A is a matrix of order n whose determinant is prime to m and I is the unit matrix, then*

$$A^w \equiv I \pmod{m}$$

and w is the least exponent for which this is true.

To prove this theorem we first establish the following lemma.

Lemma 1. *If p is an arbitrary prime, a an arbitrary positive integer, I the unit matrix of order n, and B any matrix of order n such that $B \equiv I \pmod{p}$, then $B^{p^{a-1}} \equiv I \pmod{p^a}$.*

Proof. Since $B \equiv I \pmod{p}$ the theorem holds for $a = 1$. Assuming the lemma holds for $a = k$ we show that it then must hold for $a = k + 1$.

Let $p = 2$ and consider the identity

$$(B^{2^{k-1}} - I)^2 = B^{2^k} - 2B^{2^{k-1}} + I.$$

Obviously we can write this in the following form

$$(B^{2^{k-1}} - I)^2 = (B^{2^k} - I) - 2(B^{2^{k-1}} - I).$$

Received March 6, 1951. For calling his attention to this problem and for assistance in preparing this paper, the author wishes to thank Professor A. T. Brauer.