FERMAT'S THEOREM FOR MATRICES

By Ivan Niven

1. **Introduction.** For a prime p and an integer $n > 1$, let G_1 designate the group of matrices A of order n with integral elements such that $| A |$ is prime to p. It has been proved by J. B. Marshall [3] that $A^q \equiv I \pmod{p}$ for every A in G_1 where $q = p^r q_n$, p^r being the lowest power of p which is greater than or equal to n, and q_n being determined by the recurrence relation $q_1 = p - 1$, $q_n = \text{L.C.M.}\ [q_{n-1}, p^n - 1]$. For certain small values of n and p, Marshall showed that q is a minimum, that is, that q is the L.C.M. of the orders of the elements of the group G_1. We prove this in general, and generalize the result to any finite field, as follows.

Theorem 1. *Let G_m be the group of non-singular matrices of order n with elements in $GF(p^m)$. The* L.C.M. *of the orders of the elements of G_m is $q = p^r q_n$ with r defined by $p^r \geq n > p^{r-1}$, and*

$$q_n = \text{L.C.M.}\ [p^m - 1, p^{2m} - 1, \cdots, p^{nm} - 1]. \tag{1}$$

This theorem is proved in §2.

Marshall gives the values of his q_j for $j = 1, 2, \cdots, 6$. For example, $q_5 = (p^5 - 1)(p^4 - 1)(p^3 - 1)/(p - 1)^2$. It seems to be assumed that the L.C.M. in the number theoretic sense is the same as that in the polynomial sense. In fact it is; in §3 we prove that for any positive integers a and r

$$\begin{aligned} &\text{L.C.M.}\ [x - 1, x^2 - 1, \cdots, x^r - 1]_{x=a} \\ &\qquad = \text{L.C.M.}\ [a - 1, a^2 - 1, \cdots, a^r - 1], \end{aligned} \tag{2}$$

where the notation on the left means L.C.M. in the polynomial sense evaluated at $x = a$.

The group G_m is not cyclic, so that the integer q in Theorem 1 is not the order of any element of the group. In §4 we prove that the orders of the individual elements are given by the following algorithm. (The problem of determining these orders was suggested to the writer by Prof. L. Carlitz.)

Theorem 2. *Let n be written in all possible ways in the form $n = N + n_1 + n_2 + \cdots + n_h$, with $N \geq 0$, $h \geq 1$, $2 \leq n_1 < n_2 < \cdots < n_h$. Let $p\{y\}$ designate the first in the series $1, p, p^2, p^3, \cdots$ which equals or exceeds y. Then the orders of the elements of the group G_m are the values*

$$p\{n\}(p - 1), \tag{3}$$

$$p\{N\}\ \text{L.C.M.}\ [p^{mn_1} - 1, p^{mn_2} - 1, \cdots, p^{mn_h} - 1], \tag{4}$$

and their divisors.

Received January 7, 1948; in revised form, April 22, 1948.