THE ORDER OF A MATRIX UNDER MULTIPLICATION (MODULO m)

BY MARGARET WAUGH MAXFIELD

Introduction. This paper concerns, as does the preceding one by Alex S. Davis, the non-singular n by n matrices with integral entries modulo m, with $n > 1$. The purpose here is to find the "orders" of these matrices, the word "order" being used in its group theoretic sense. This is a generalization of a result by Niven [1] presented as Theorem 1. Theorem 2 gives the result for the modulus p^a, a power of a prime. Theorem 3 gives the result for the composite modulus m.

THEOREM 1. *Let p be a prime. Let P be a partition of n,*

$$n = N + n_1 + \cdots + n_h ,$$

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, $1, p, p^2, p^3, \cdots$ that equals or exceeds y. Then the orders of the non-singular n by n matrices (mod p) *are*

$$f = p\{n\}(p - 1),$$

$$g_P = p\{N\}\text{L.C.M.}[p^{n_1} - 1, p^{n_2} - 1, \cdots , p^{n_h} - 1],$$

and their divisors, taken over all possible partitions P.

Proof. Niven's Theorem 2 [1] includes the theorem as a special case.

LEMMA 1. *Let the matrix S have order σ* (mod p^r). *Then its order* (mod p^{r+1}) *is either σ or $p\sigma$.*

Proof. Let σ' be the order of S (mod p^{r+1}). Then σ divides σ'.

Now let $B = S^\sigma$. Since $B \equiv I$ (mod p^r), the entries of B can be written $b_{ij} = a_{ij}p^r + \delta_{ij}$, where the a_{ij} are integers and the δ is Kronecker's delta. For any positive integer t, the entries of B^t will have the form

$$b_{ii}^{(t)} = s_{ii}p^{2r} + (a_{ii}p^r + 1)^t,$$

$$b_{ij}^{(t)} = s_{ij}p^{2r} + ta_{ij}p^r$$

for $i \neq j$, where the s_{ij} are integers. This can be shown by induction on t, taking B^{t+1} as $B^t \cdot B$. From these equations we observe that $B^t = S^{t\sigma}$ is congruent to the identity for $t = p$. We conclude that σ' is a divisor of $p\sigma$, and so is either σ or $p\sigma$, since it is divisible by σ.

Received May 15, 1951.