CERTAIN MATRIX EQUATIONS OVER RINGS OF INTEGERS

By Ronald W. Davis

1. Introduction. In his paper [4] concerning scalar polynomial equations over finite fields, John H. Hodges gave canonical forms, relative to similarity, for n by n matrix solutions Y over $GF(q)$ of the equation

$$g(Y) = 0 \tag{1}$$

where g is a given monic polynomial over $GF(q)$. Using a result of Dickson [3; 236] on the number of matrices commuting with a given matrix, he also obtained the number of solutions of (1).

The present paper is concerned with the equation (1) when g (not necessarily monic) and Y are over Zp^k, the ring of integers modulo p^k, where p is a prime. For certain g, canonical forms and the number of solutions will be obtained. Two special cases, namely $g = x^e - 1$, for $(e, p) = 1$, and $g = x^2 - x$ will be discussed in §5. The last section concerns the general modulus.

2. Preliminary lemmas and remarks. Finding solutions of (1) over Zp^k is equivalent to finding incongruent solutions of

$$f(X) \equiv 0 \pmod{p^k} \tag{2}$$

where f and X are over the ring R of p-adic integers, and $f \in R[x]$ reduces to $g \in Zp^k[x]$. Recall that each element of R can be written uniquely as a power series in p with coefficients between 0 and $p - 1$, so that congruence (mod p^k) and reduction (mod p^k) are well-defined.

For an arbitrary ring S, let $(S)_n$ denote the ring of n by n matrices over S; $T \in (S)_n$ is invertible iff det T is a unit in S. Two matrices X and Y in $(R)_n$ are *similar modulo* p^k if there exists an invertible T in $(R)_n$ such that

$$XT \equiv TY \pmod{p^k}.$$

We shall be concerned with generating solutions of (2) from solutions of

$$f(X_0) \equiv 0 \pmod{p^{k-1}}; \tag{3}$$

i.e., we shall investigate solutions X of (2) such that $X \equiv X_0 \pmod{p^{k-1}}$ where X_0 satisfies (3). Such an X is of the form $X_0 + p^{k-1}H$, for some $H \in (R)_n$.

Now, for any $f \in R[x]$, whenever X_0 and H in $(R)_n$ satisfy

$$X_0H \equiv HX_0 \pmod{p},$$

Received December 23, 1966. This paper is essentially the author's doctoral thesis, directed by John H. Hodges, to whom the author wishes to express his gratitude for much advice and encouragement.