A THEOREM ON HIGHER CONGRUENCES*

BY LEONARD CARLITZ

1. *Introduction.* Let $\mathfrak{D}=\mathfrak{D}(x, p^n)$ denote the totality of polynomials in an indeterminate x with coefficients in a Galois field $GF(p^n)$ of order p^n. Consider the congruence

$$t^{p^n} - t \equiv A \qquad (\mathrm{mod}\ P), \tag{1}$$

where A and P are in $\mathfrak{D}$, and P is irreducible of degree k, say. The sum

$$A + A^{p^n} + \cdots + A^{p^{n(k-1)}}$$

is congruent (mod P) to a quantity in $GF(p^n)$; we denote this residue by $\rho(A)$. It is easily seen that the congruence (1) is solvable in $\mathfrak{D}$ if and only if $\rho(A)=0$. A better condition is furnished by the following theorem.

THEOREM. *If we put*

$$\begin{aligned} P &= x^k + c_1x^{k-1} + \cdots + c_k, \\ P' &= kx^{k-1} + (k-1)c_1x^{k-2} + \cdots + c_{k-1}, \end{aligned} \tag{2}$$

where c_i is in $GF(p^n)$, then the congruence (1) *is solvable in $\mathfrak{D}$ if and only if $P'A$ is congruent* (mod P) *to a polynomial of degree $<k-1$. More generally, if*

$$P'A \equiv b_0x^{k-1} + \cdots + b_{k-1} \qquad (\mathrm{mod}\ P), \qquad (b_j \text{ in } GF(p^n)),$$

then $\rho(A)=b_0$.

In this note we give a new and direct proof of this theorem.†

2. *Proof of the Theorem.* For arbitrary A (mod P) we construct the polynomial

$$f(t) \equiv (t-A)(t-A^{p^n})\cdots(t-A^{p^{n(k-1)}}) \qquad (\mathrm{mod}\ P),$$

---

* Presented to the Society, April 19, 1935, under a different title.

† See L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Mathematical Journal, vol. 1 (1935), p. 164.