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

$$t^{p^n} - t \equiv A \pmod{P}, \tag{1}$$

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*

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

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

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

* 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.

in which the coefficient of t^{k-1} is evidently $-\rho(A)$. For our purposes it will be convenient to make use of an alternative definition of $f(t)$. Let x denote a root of $P=0$; then x defines the $GF(p^{nk})$. Then $A=A(x)$ is an element of the enlarged Galois field; $f(t)$ is evidently the unique polynomial, with leading coefficient $=1$, having the roots $A^{p^{nj}}$. Clearly all the coefficients of $f(t)$ lie in $GF(p^n)$. To calculate them we proceed as follows. Let

$$x^iA \equiv \sum_{j=0}^{k-1} a_{ij}x^j \qquad (\text{mod } P), \tag{3}$$

where a_{ij}, $(i, j=0, \cdots, k-1)$, are in $GF(p^n)$. But the equations (3) evidently imply the following representation of $f(t)$ as a determinant:

$$f(t) = (-1)^k \left| a_{ij} - \delta_{ij}t \right|,$$

so that by the remark at the beginning of this section

$$\rho(A) = \sum_{i=0}^{k-1} a_{ii}. \tag{4}$$

On the other hand, making use of (2) and (3),

$$P'A = \sum_{i=1}^{k} ic_{k-i}x^{i-1}A, \qquad (c_0 = 1),$$
$$\equiv \sum_{i=1}^{k} ic_{k-i}\sum_{j=0}^{k-1} a_{i-1,j}x^j \qquad (\text{mod } P),$$

so that the coefficient of x^{k-1} is

$$b_0 = \sum_{i=1}^{k} ic_{k-1}a_{i-1,k-1}. \tag{5}$$

Note next that (3) implies

$$x^{i+1}A \equiv \sum_{j=0}^{k-1} a_{ij}x^{j+1} \qquad (\text{mod } P)$$
$$\equiv \sum_{j=0}^{k-2} a_{ij}x^{j+1} - \sum_{j=0}^{k-1} a_{i,k-1}c_{k-j}x^j,$$

from which it follows that

(6) $$a_{i+1,j} = a_{i,j-1} - a_{i,k-1}c_{k-j}.$$

Put $i=j-1$, and (6) becomes

$$a_{j-1,j-1} - a_{jj} = a_{j-1,k-1}c_{k-j}, \qquad (j = 1, \cdots, k-1).$$

Substituting into the right member of (5), we see that

$$\begin{aligned} b_0 &= \sum_{j=1}^{k-1} j(a_{j-1,j-1} - a_{jj}) + kc_0a_{k-1,k-1} \\ &= a_{00} + a_{11} + \cdots + a_{k-1,k-1}. \end{aligned}$$

If we compare with equation (4), we have at once $\rho(A)=b_0$. This completes the proof of the generalized form of the theorem. In particular, if $P'A$ is congruent (mod P) to a polynomial of degree $<k-1$, then $b_0=0$, and the congruence (1) is solvable.

3. *Concluding Remark.* The coefficients of $f(t)$ are, but for sign, the elementary symmetric functions of the quantities $A^{p^{nj}}$ (mod P). As we have seen above, the coefficient of t^{k-1} is intimately connected with the congruence (1). Similarly, the last coefficient

$$A^{1+p^n+\cdots+p^{n(k-1)}} \equiv \left\{\frac{A}{P}\right\} \qquad (\text{mod } P)$$

is connected with the congruence

$$t^{p^n-1} \equiv A \qquad (\text{mod } P).$$

Indeed, the method of §2 leads very naturally to F. K. Schmidt's proof of the theorem of reciprocity:

$$\left\{\frac{P}{Q}\right\} = (-1)^{kl}\left\{\frac{Q}{P}\right\},$$

where P and Q are primary irreducible of degree k and l, respectively.*

The question arises whether the remaining coefficients in $f(t)$ are connected in any direct manner with criteria for the solvability of higher congruences.

Duke University

* F. K. Schmidt, Sitzungsberichte der Physikalischmedizinischen Societät zu Erlangen, vol. 58–59 (1928), pp. 159–172.