A THEOREM ON HIGHER CONGRUENCES*

BY LEONARD CARLITZ

1. Introduction. Let $\mathbb{D} = \mathbb{D}(x, p^n)$ 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

$$(1) \quad t^n - t \equiv A \pmod{P},$$

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

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

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 $\mathbb{D}$ if and only if $\rho(A) = 0$. A better condition is furnished by the following theorem.

**Theorem.** If we put

$$(2) \quad P = x^k + c_1 x^{k-1} + \cdots + c_k,$$

$$P' = k x^{k-1} + (k - 1) c_1 x^{k-2} + \cdots + c_{k-1},$$

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

$$P' A \equiv b_0 x^{k-1} + \cdots + b_{k-1} \pmod{P}, \quad (b_i \text{ in } GF(p^n)),$$

then $\rho(A) = b_0$.

In this note we give a new and direct proof of this theorem.$\dagger$

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

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

* Presented to the Society, April 19, 1935, under a different title.
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 $GF(p^n)$. 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 $A^{\pi^j}$. Clearly all the coefficients of $f(t)$ lie in $GF(p^n)$. To calculate them we proceed as follows. Let

$$x^tA \equiv \sum_{j=0}^{k-1} a_{ij}x^j \quad (\text{mod } P),$$

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:

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

so that by the remark at the beginning of this section

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

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

$$P' A = \sum_{i=1}^{k} ic_{k-1}x^{i-1}A, \quad (c_0 = 1),$$

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

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

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

Note next that (3) implies

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

$$\equiv \sum_{j=0}^{k-2} a_{ij}x^{i+1} \sum_{j=0}^{k-1} a_{i,j}c_{k-j}x^j,$$

from which it follows that
Put $i = j - 1$, and (6) becomes

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

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

$$b_0 = \sum_{j=1}^{k-1} j(a_{j-1,j-1} - a_{jj}) + kc_0a_{k-1,k-1}$$

$$= a_{00} + a_{11} + \cdots + a_{k-1,k-1}.$$ 

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 $A_{p^i}$ (mod $P$). As we have seen above, the coefficient of $t^{k-1}$ is intimately connected with the congruence (1). Similarly, the last coefficient

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

is connected with the congruence

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

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

---