ON CERTAIN HIGHER CONGRUENCES*

BY LEONARD CARLITZ

1. *Introduction*. This note is concerned with the higher congruence

$$(1)\qquad \prod_{\deg G<m} (t-G) \equiv A \qquad (\mathrm{mod}\ P).$$

Here A, P, G denote polynomials in an indeterminate x with coefficients in a Galois field $GF(p^n)$ of order p^n. The product in the left member extends over all G of degree less than some fixed m; the modulus P is assumed irreducible of degree k. As will appear below, we may without loss assume $k>m$.

The congruence (1) has either no solution at all, or else has p^{nm} distinct solutions; if t is any solution, then the general solution is furnished by $t+G$, where deg $G<m$. Define σ_j by means of

$$(u+x)(u+x^{p^n})\cdots(u+x^{p^{n(m-2)}})$$
$$=\sigma_0u^{m-1}+\sigma_1u^{m-2}+\cdots+\sigma_{m-1}.$$

Put

$$P = x^k+c_1x^{k-1}+\cdots+c_k,$$
$$P' = kx^{k-1}+(k-1)c_1x^{k-2}+\cdots+c_{k-1},$$
$$F_{m-1} = (x^{p^{n(m-1)}}-x)(x^{p^{n(m-2)}}-x^{p^n})\cdots(x^{p^n}-x^{p^{n(m-2)}}).$$

Then we prove the criterion: *The congruence* (1) *is solvable if and only if each product* $(\sigma_j/(F_{m-1})^{p^n})AP'$, $(j=0,\cdots,m-1)$, *is congruent* (mod P) *to a polynomial of degree* $<k-1$.

2. *Some Properties of* $\psi_m(t)$. We denote by $\psi_m(t)$ the product appearing in the left member of (1). Also, we let

$$F_m=\prod_{i=0}^{m-1}(x^{p^{nm}}-x^{p^{ni}}),\quad L_m=\prod_{i=0}^{m-1}(x^{p^{n(m-i)}}-x),\quad F_0=L_0=1.$$

Then†

---

* Presented to the Society, September 10, 1935.

† L. Carlitz, Duke Mathematical Journal, vol. 1 (1935), p. 141.