ON CERTAIN HIGHER CONGRUENCES*

BY LEONARD CARLITZ

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

$$\prod_{\deg G<m} (t - G) \equiv A \pmod{P}. \tag{1}$$

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

$$(u + x)(u + x^{p^n}) \cdots (u + x^{p^{n(m-2)}}) = \sigma_0 u^{m-1} + \sigma_1 u^{m-2} + \cdots + \sigma_{m-1}.$$

Put

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

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

$$F_{m-1} = (x^{p^{n(m-1)}} - x)(x^{p^{n(m-2)}} - x^{p^n}) \cdots (x^{p^n} - x^{p^{n(m-2)}}).$$

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.

$$\psi_m(t) = \sum_{i=0}^{m} (-1)^{m-i} \begin{bmatrix} m \\ i \end{bmatrix} t^{p^{ni}}, \qquad \begin{bmatrix} m \\ i \end{bmatrix} = \frac{F_m}{F_i L_{m-i}^{p^{ni}}};$$

$$\psi_{m+1}(t) = \psi_m^{p^n}(t) - F_m^{p^n-1}\psi_m(t). \tag{2}$$

We shall require a generalized form of identity (2). From the definition of $\psi_m(t)$, it is clear that

$$\psi_{m+1}(t) = \prod_c (t + c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0), \tag{3}$$

the product extending over all sets $(c_m, \cdots, c_0)$ in the $GF(p^n)$. The right member of (3) may be written in the form

$$\prod_{c_j} \prod_c{}' \{(t + c_j x^j) + (c_m x^m + \cdots + c_{j+1}x^{j+1} + c_{j-1}x^{j-1} + \cdots + c_0)\},$$

the inner product extending over $(c_m, \cdots, c_{j+1}, c_{j-1}, \cdots, c_0)$ only. If we put

$$f_j(t) = \prod_c{}' (t + c_m x^m + \cdots + c_{j+1}x^{j+1} + c_{j-1}x^{j-1} + \cdots + c_0),$$

then (3) becomes

$$\psi_{m+1}(t) = \prod_c f_j(t + cx^j). \tag{4}$$

Now by a formula due to E. H. Moore,* the polynomial $f_j(t)$ may be written as a quotient of two determinants:

$$f_j(t) = \frac{\Delta_j(t)}{D_j}, \tag{5}$$

where†

$$\Delta_j(t) = \left| t^{p^{n(m-i)}}, x^{mp^{n(m-i)}}, \cdots, x^{(j+1)p^{n(m-i)}}, x^{(j-1)p^{n(m-i)}}, \cdots, 1 \right| \tag{6}$$

where $i = 0, 1, \cdots, m$, and

$$D_j = \left| x^{mp^{n(m-1-i)}}, \cdots, x^{(j+1)p^{n(m-1-i)}}, x^{(j-1)p^{n(m-1-i)}}, \cdots, 1 \right|$$

* This Bulletin, vol. 2 (1896), p. 191.

† For brevity we write only the elements in the ith row: $|a_{i0}\, a_{i1} \cdots a_{is}|$, $(i = 0, 1, \cdots, s)$.

where $i=0, 1, \cdots, m-1$. By (5) and (6) it is clear that

$$f_i(t + cx^i) = f_i(t) + cf_i(x^i).$$

We shall evaluate $f_i(x^i)$. Using (6), we have

$$\Delta_i(x^i) = (-1)^{m-i} \left| x^{mp^{n(m-i)}}, \cdots, x^{ip^{n(m-i)}}, \cdots, 1 \right|, \qquad (i = 0, \cdots, m),$$

$$= (-1)^{m-i} F_1 F_2 \cdots F_m. \tag{7}$$

The calculation of D_i is somewhat more involved. Expanding the determinant

$$E_{m+1} = \left| t_{m-i}^{m-j} \right|, \qquad (i, j = 0, \cdots, m),$$

with respect to the elements of the first row, we have on the one hand

$$E_{m+1} = V_0 t_m^m - V_1 t_m^{m-1} + \cdots + (-1)^m V_m, \tag{8}$$

say. On the other hand, it is easy to see that

$$E_{m+1} = (t_m - t_0)(t_m - t_1) \cdots (t_m - t_{m-1}) E_m. \tag{9}$$

If now we put

$$t_m = t, \qquad t_i = x^{p^{ni}}, \qquad (i = 0, \cdots, m-1),$$

(8) and (9) evidently imply

$$D_i = V_i = V_0 \sigma_i^{(m)} = F_1 F_2 \cdots F_{m-1} \sigma_i^{(m)},$$

where $\sigma_i^{(m)}$ is the ith elementary symmetric function of the quantities $x^{p^{ni}}$, $(i=0, \cdots, m-1)$. Then by (5) and (7) we have the formula

$$f_i(x^i) = (-1)^{m-i} \frac{F_m}{\sigma_i^{(m)}}. \tag{10}$$

Returning now to (4), we see that

$$\psi_{m+1}(t) = \prod_c \{ f_i(t) + cf_i(x^i) \},$$

and therefore, making use of (10), we have finally the generalized identity

$$\psi_{m+1}(t) = f_j^{p^n}(t) - \left(\frac{F_m}{\sigma_j^{(m)}}\right)^{p^n-1} f_j(t). \tag{11}$$

For $j=0$, this reduces to the identity (2).

3. *Necessity of the Criterion for Solvability.* Returning to the congruence (1), we see, by repeated applications of (2), that, for $m>k=\deg P$,

$$\psi_m(t) \equiv \psi_{m-1}^{p^n}(t) \equiv \psi_k^{p^{n(m-k)}} \pmod P.$$

In the case $m=k$, it is evident that

$$\psi_k(t) \equiv t^{p^{nk}} - t \pmod P;$$

and clearly the congruence

$$t^{p^{nk}} - t \equiv A \pmod P$$

is solvable only for $A=0$, in which case it has p^{nk} solutions. We may therefore assume without any loss in generality that $m<k$.

Making use of (11), we note that if (1) is solvable, then also the congruences

$$u_j^{p^n} - \left(\frac{F_{m-1}}{\sigma_j^{(m-1)}}\right)^{p^n-1} u_j \equiv A, \qquad (j = 0, \cdots, m-1), \tag{12}$$

are solvable. As for (12), we shall need the following theorem.

If we put

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

then the congruence

$$u^{p^n} - u \equiv A \pmod P$$

is solvable if and only if the product AP' is congruent (mod P) *to a polynomial of degree $<k-1$.**

Applying this criterion to (12) we have the following theorem.

THEOREM 1. *If* (1) *is solvable* ($m<k$), *then necessarily each product*

* Duke Mathematical Journal, vol. 1 (1935), p. 166.

$$\left(\frac{\sigma_j^{(m-1)}}{F_{m-1}}\right)^{p^n} AP', \quad (j = 0, \cdots, m-1), \tag{13}$$

is congruent (mod P) *to a polynomial of degree* $<k-1$.

4. *Sufficiency of the Criterion.* Making a slight change in notation, we rewrite (11) in the form

$$\psi_m(t) = f_j^{p^n}(t) - \alpha_j f_j(t), \qquad \alpha_j = \left(\frac{F_{m-1}}{\sigma_j^{(m-1)}}\right)^{p^n-1}; \tag{14}$$

we put

$$f_j(t) = \sum_{i=0}^{m-1} \beta_{ji} t^{p^n i}, \quad (j = 0, \cdots, m-1). \tag{15}$$

Let us now consider the system of congruences in $t_0, \cdots, t_{m-1}$:

$$\sum_{i=0}^{m-1} \beta_{ji} t_i \equiv u_j \pmod{P}. \tag{16}$$

The determinant $B = |\beta_{ji}|$ is easily calculated. By (14) we have the recursion

$$\beta_{j,i-1}^{p^n} - \alpha_j \beta_{ji} = \begin{bmatrix} m \\ i \end{bmatrix}, \qquad \beta_{j,m-1} = 1.$$

Then

$$\begin{aligned} B^{p^n} &= |\beta_{ji}|^{p^n} = |\beta_{ji}^{p^n}|, \qquad (i, j = 0, \cdots, m-1), \\ &= \left| \begin{bmatrix} m \\ 1 \end{bmatrix} + \alpha_j \beta_{j1}, \cdots, \begin{bmatrix} m \\ m-1 \end{bmatrix} + \alpha_j \beta_{j,m-1}, 1 \right| \\ &= |\alpha_j \beta_{j1}, \cdots, \alpha_j \beta_{j,m-1}, 1| \\ &= \frac{L_m}{F_m} |\alpha_j \beta_{j1}, \cdots, \alpha_j \beta_{j,m-1}, (-1)^{m-1} \alpha_j \beta_{j0}| \\ &= \frac{\alpha_0 \alpha_1 \cdots \alpha_{m-1}}{(F_1 F_2 \cdots F_{m-1})^{p^n-1}} B, \end{aligned}$$

and therefore

$$B = \frac{c}{\sigma_1 \sigma_2 \cdots \sigma_{m-1}} \frac{F_{m-1}^m}{F_1 F_2 \cdots F_{m-1}}, \qquad (c \text{ in } GF(p^n)). \tag{17}$$

In particular $B \not\equiv 0 \pmod{P}$, and hence for fixed u_j the system (16) has a unique set of solutions t_i. It remains to show that, if the u_j satisfy the congruence (12), then

$$t_{i+1} \equiv t_i^{p^n}, \qquad (i = 0, \cdots, m-2). \tag{18}$$

The proof follows closely the proof of (17). For simplicity we take only the case $i=0$ of (18); the general case may be treated in exactly the same way, but the notation is somewhat more complicated. We have

$$\begin{aligned} Bt_0 &\equiv \begin{vmatrix} u_j & \beta_{j1} & \cdots & \beta_{j,m-1} \end{vmatrix}, \\ Bt_1 &\equiv \begin{vmatrix} \beta_{j0} & u_j & \cdots & \beta_{j,m-1} \end{vmatrix}, \end{aligned} \qquad (j = 0, \cdots, m-1). \tag{19}$$

Then

$$\begin{aligned} B^{p^n} t_0^{p^n} &\equiv \begin{vmatrix} u_j^{p^n} & \beta_{j1}^{p^n} & \cdots & 1 \end{vmatrix} \\ &\equiv \left| A + \alpha_j u_j, \begin{bmatrix} m \\ 2 \end{bmatrix} + \alpha_j \beta_{j2}, \cdots, \begin{bmatrix} m \\ m-1 \end{bmatrix} + \alpha_j \beta_{j,m-1}, 1 \right| \\ &\equiv \begin{vmatrix} \alpha_j u_j, \alpha_j \beta_{j2}, \cdots, \alpha_j \beta_{j,m-1}, 1 \end{vmatrix} \\ &\equiv \frac{L_m}{F_m} \begin{vmatrix} \alpha_j \beta_{j0}, \alpha_j u_j, \alpha_j \beta_{j2}, \cdots, \alpha_j \beta_{j,m-1} \end{vmatrix} \\ &\equiv \frac{L_m}{F_m} \alpha_0 \alpha_1 \cdots \alpha_{m-1} B t_1. \end{aligned}$$

Comparing with (17) and (19), we see at once that $t_1 \equiv t_0^{p^n}$. We have therefore proved the following result.

THEOREM 2. *The criterion* (13) *furnishes a set of sufficient conditions that the congruence* (1) *be solvable. To carry out the solution we first solve the congruences* (12) *for* u_j, *substitute these values in the right member of* (16), *and solve for* $t_j \equiv t^{p^{nj}}$.

Note finally that the general solution of (1) is $t+G$, where t is a particular solution and G is any polynomial of degree $<m$; this follows from

$$\psi_m(t+G) = \psi_m(t) + \psi_m(G) = \psi_m(t).$$

5. *Another Criterion.* It is easily seen that the congruence

$$u^{p^n} - u \equiv A \pmod{P}$$

is solvable only when

$$A + A^{p^n} + \cdots + A^{p^{n(k-1)}} \equiv 0. \tag{20}$$

In any event the sum (20) is congruent to a quantity in $GF(p^n)$; we denote this residue by $\rho(A)$. Thus the congruence (12) is solvable only when

$$\rho\left\{\left(\frac{\sigma_j^{(m-1)}}{F_{m-1}}\right)^{p^n} A\right\} = 0, \qquad (j = 0, \cdots, m-1). \tag{21}$$

Consider now the sum

$$\begin{aligned}
\rho_m(M) &\equiv \sum_{j=0}^{m-1} (-1)^{m-1-j} x^{m-1-j} \rho(\sigma_j^{p^n} M) \\
&\equiv \sum_{j=0}^{m-1} (-1)^{m-1-j} x^{m-1-j} \sum_{i=0}^{k-1} \sigma_j^{p^{n(i+1)}} M^{p^{ni}} \\
&\equiv \sum_{i=0}^{k-1} M^{p^{ni}} \sum_{j=0}^{m-1} (-1)^{m-1-j} \sigma_j^{p^{n(i+1)}} x^{m-1-i} \\
&\equiv \sum_{i=0}^{k-1} M^{p^{ni}} (x^{p^{n(i+1)}} - x) \cdots (x^{p^{n(m+i-1)}} - x) \\
&\equiv \sum_{i=0}^{k-m} M^{p^{ni}} \frac{L_{m+i-1}}{L_i},
\end{aligned} \tag{22}$$

where for brevity we put

$$\sigma_j = \sigma_j^{(m-1)}, \qquad M = \frac{A}{F_{m-1}^{p^n}}.$$

Clearly (21) implies $\rho_m(M) = 0$. Conversely, it is easy to see that if $\rho_m = 0$, then (21) must hold. Indeed, since the sum (22) is congruent to a polynomial of degree $m-1$ (which is surely $< k$), its vanishing entails the vanishing of its m coefficients; these are precisely the left members of (21). Thus we have the following theorem.

THEOREM 3. *The congruence*

$$\psi_m(t) \equiv MF_{m-1}^{p^n} \pmod{P}$$

is solvable if and only if

$$\rho_m(M) \equiv \sum_{i=0}^{k-m} M^{p^{ni}} \frac{L_{m+i-1}}{L_i} \equiv 0.$$

It will be remarked that in general the first criterion is more useful. However, the latter is of some interest in itself. Furthermore, it suggests possible criteria for more general classes of congruences; I hope to develop the matter elsewhere.

DUKE UNIVERSITY

A DIFFERENTIAL EQUATION FOR APPELL POLYNOMIALS†

BY I. M. SHEFFER

By a *set* of polynomials $\{P_n(x)\}$, $(n=0, 1, 2, \cdots)$, we shall mean an infinite sequence in which $P_n(x)$ is of degree *exactly*‡ n. Corresponding to a given set $\{P_n\}$ there are infinitely many sequences of polynomials $\{L_n(x)\}$ (with $L_n(x)$ of degree not exceeding n) and sequences of numbers $\{\lambda_n\}$ such that $\{P_n\}$ satisfies the linear differential equation (usually of infinite order) with parameter:§

$$L[y(x)] \equiv \sum_{n=0}^{\infty} L_n(x) y^{(n)}(x) = \lambda y(x), \tag{1}$$

which for $\lambda=\lambda_n$ gives $P_n(x)$. In fact, suppose $\{P_n\}$ is given. Let $\{\lambda_n\}$ be any sequence of numbers subject only to the condition that λ_n is not identically zero in n. Then a unique sequence $\{L_n(x)\}$ exists such that $L[P_n(x)]=\lambda_n P_n(x)$, $(n=0, 1, \cdots)$, where not all the L_n's are identically zero, and where no $L_n(x)$ is of degree exceeding n. The polynomial $L_n(x)$ is readily obtained by recurrence from $L_0, \cdots, L_{n-1}$. If we write

$$L_n(x) = l_{n0} + l_{n1}x + \cdots + l_{nn}x^n, \tag{2}$$

---

† Presented to the Society, April 25, 1935.

‡ For many purposes it suffices to have $P_n(x)$ of degree not exceeding n. Here, however, it is convenient to use the stricter condition.

§ See Sheffer, American Journal of Mathematics, vol. 53 (1931), pp. 29–30, for a relation suggestive of (1).