A CONGRUENCE EQUATION IN $GF[p^n, x]$ AND SOME RELATED ARITHMETICAL IDENTITIES

By K. Nageswara Rao

1. Introduction. Let $\Omega = GF[p^n, x]$ represent the domain of polynomials over the Galois field $GF(p^n)$ in the indeterminate x. Let R be a primary polynomial in Ω of degree r (see §2 for definitions). If r_1, r_2, s_1, s_2 are any four non-negative integers and $A_0, \cdots, A_{s_1}, B_0, \cdots, B_{s_2}$ are elements of Ω so that $(A_i, R) = (B_j, R) = 1$ ($i = 0, \cdots, s_1$; $j = 0, \cdots, s_2$), the object of this paper is to obtain the number of solutions $N_{r_1, r_2}^{(s_1; s_2)}(A, R)$, in $X_i^{(j)} \pmod R$ ($i = 1, \cdots, r_1 + 1$; $j = 0, \cdots, s_1$) and $Y_k^{(l)} \pmod R$ ($k = 1, \cdots, r_2 + 1$; $l = 0, \cdots, s_2$) of the congruence

$$(1.1) \qquad A \equiv A_0 X_1^{(0)} \cdots X_{r_1+1}^{(0)} + \cdots + A_{s_1} X_1^{(s_1)} \cdots X_{r_1+1}^{(s_1)} + B_0 Y_1^{(0)} \cdots Y_{r_2+1}^{(0)} + \cdots + B_{s_2} Y_1^{(s_2)} \cdots Y_{r_2+1}^{(s_2)} \pmod R$$

with the restrictions

$$(1.2) \qquad (Y_k^{(l)}, R) = 1 \qquad (k = 1, \cdots, r_2 + 1; l = 0, \cdots, s_2)$$

In fact we obtain a recurring relation for $N_{r_1, r_2}^{(s_1; s_2)}(A, R)$ in terms of Carlitz's η-sum (see §2) and establish related arithmetical identities involving some known functions.

For discussion of problems of similar nature in algebraic number fields we refer to Cohen [5; (1.4)] and in the rational case to Gyires [7]. The author has also discussed certain congruence equations of similar kind in the rational case and also in $GF[p^n, x]$ (see [8], [9]).

2. Preliminaries and notations. Let K be a field of characteristic zero containing the p-th roots of unity. Let M be any polynomial in Ω, say,

$$(2.1) \qquad M = \alpha_0 x^m + \cdots + \alpha_m, \qquad \alpha_i \in GF(p^n), \qquad \alpha_0 \neq 0$$

then we write $\deg M = m$, $\operatorname{Sgn} M = \alpha_0$, if $\alpha_0 = 1$, then M is primary; also we put $|M| = p^{nm}$. By $\sum'_{D \mid M}$ we mean the summation over all the primary divisors D of M.

We say that a single-valued function f defined for all elements of Ω and assuming values in K, is (R, K) arithmetic or simply arithmetic, if $f(A) = f(A^1)$ for $A \equiv A^1 \pmod R$ (R being a primary polynomial of degree r).

We define Cauchy product of two arithmetic functions f and g to be the function $h = f \cdot g$ defined by

$$(2.2) \qquad h(F) = f \cdot g(F) = \sum_{F = A + B} f(A) g(B)$$

Received December 16, 1965.