Some applications of Carlitz’s $\eta$-sum

by

K. NAGASWARA RAO (New Delhi)

1. Introduction. Let $D = GF(p^s, z)$ represent the domain of polynomials over the Galois field $GF(p^s)$ in the indeterminate $x$. Let $R$ be a primary (see § 2) polynomial of $D$ and of degree $r$. Also let $D_1 = \ldots, D_n = R$ be all the primary divisors of $R$. If $M, N$ are any two polynomials of $D$, the main object of the paper is to obtain formulae in terms of Carlitz’s $\eta$-sum (see (2.4)) for the number of solutions of the congruences

\begin{align}
M &= X_1 + X_2 + \ldots + X_s \pmod{R}, \\
N &= Y_1 Z_1 + \ldots + Y_n Z_n \pmod{R},
\end{align}

where $s_i$, of the $X_i^s \in D$, have the property $(X, R) = D_1$ and $\sum s_i = s$, and

\begin{align}
M &= X_1 + X_2 + \ldots + X_s \pmod{R}, \\
N &= Y_1 Z_1 + \ldots + Y_n Z_n \pmod{R},
\end{align}

where $X_i, Y_i$ are polynomials of $D$.

Problems of similar nature in the rational case have been discussed by various writers and reference can be made to Cohen [5] to [10], McCarthy [12], Nicol and Vandiver [15]. We should also refer to Ramanathan [16] who considered the problem (1.1) in the rational case in an equivalent form. The author [13], [14] has also discussed certain generalizations and analogues of (1.1) in the rational case. We also established some arithmetical identities.

In the proofs we utilize the representations due to Cohen [4] (see also Carlitz [2]), of a class of arithmetic functions defined over $D$. This contributed much to the simplicity of the proofs.

2. Notations and preliminaries. Let $K$ be a field of characteristic zero, containing the $p$th roots of unity. Let $F$ be any polynomial of $D$, say

\begin{align}
F &= a_0 + a_1 + \ldots + a_s, \quad \text{where } a_s \neq 0,
\end{align}

then $\nu$ is called the degree of $F$ and is written as $\deg F = \nu$. $F$ is said to be primary if $a_s = 1$. We use the symbol $|F|$ to denote $p^\nu$.

A single valued function $f$ defined over the elements of $D$ and assuming values in $K$, is said to belong to the class $(R, \eta)$ if $f(A) = f(A')$ whenever $A = A' \pmod{R}$.  

---

**Table des matières du tome XII, fascicule 3**

- K. Nageswara Rao, Some applications of Carlitz’s $\eta$-sum ........................................ 213
- Indar S. Luthar, A generalization of a theorem of Landau .............................................. 223
- A. A. Karatsuba, Estimates of $\sum_{x \in D} k^x (\eta(x))^{-1}$ ............................................. 229
- P. Schweiger, Existence of a stationary measure for the Walfisz algorithm .......................... 239
- W. Narkiewicz, On distribution of values of multiplicative functions in residue classes ........... 239
- A. Baker, On Mahler’s classification of transcendental numbers. II: Simultaneous Diophantine approximation .......................................................... 281
- B. M. MacCluer, On a conjecture of Davenport and Lewis concerning exceptional polynomials .......................................................... 289
- Andrew F. Long, Classification of irreducible factorial polynomials over a finite field ................. 289
- K. Mahler and G. Szekeres, On the approximation of real numbers by roots of integers ............... 315

La revue est consacrée à toutes les branches de l’Arithmétique et de la Théorie des Nombres, ainsi qu’aux fonctions ayant de l’importance dans ces domaines.

Prêter d’adresser les textes dactylographiés à l’un des rédacteurs de la revue ou bien à la Rédaction de

ACTA ARITHMETICA

Warszawa I (Pologne), ul. Śniadeckich 8.

La même adresse est valable pour toute correspondance concernant l’échange de Acta Arithmetica.

---

Les volumes IV et suivants de ACTA ARITHMETICA sont à obtenir chez

Ars Polona, Warszawa 5 (Pologne), Krakowskie Przedmioty 7.

Prix de ce fascicule 3.00 $.

Les volumes I-III (rééditions) sont à obtenir chez

Johnson Reprint Corp., 111 Fifth Ave, New York, N. Y.

---

PRINTED IN POLAND

WROCŁAWSKA DRUKARZNA NAUKOWA
The symbol $\sum_{d|D}$ denotes the summation over all primary divisors $D$ of $R$.

Let $H$ be a primary polynomial of $\mathfrak{B}$, with $\deg H = h$ and let $A$ be a polynomial such that $A \mod H$ is equal to

$$L_1 \theta^{h-1} + \ldots + L_h, \quad \theta \in \text{GF}(p^2).$$

Then following Carlitz ([1], § 2) we define $R(A, H)$ to be $\theta^m \alpha(m)$, where $\alpha$ is defined to be the integer $\mod p$ which occurs as the initial coefficient in the expression

$$L = a_1 \theta^{n-1} + \ldots + a_h,$$

$\theta$ being the generator of $\text{GF}(p^2)$ relative to $\text{GF}(p)$.

Carlitz ([1], § 4) introduced the sum $\eta(A, R)$ defined as follows

$$\eta(A, R) = \sum_{E_k \equiv \alpha \mod R} E_k(A),$$

the summation being over all $E$ of a reduced residue system $\mod R$, where $E_k(A) = E(RA_1)$. For arithmetical functions $f$ of the class $(R, K)$ we have the following representation due to Cohen [4] (see also Carlitz [2]):

$$f(A) = \sum_{a \equiv \alpha \mod R} a \sum_{E_k \equiv \alpha \mod R} f(E_k) E_k(A),$$

where

$$a_\alpha = p^{\alpha-1} \sum_{V \equiv \alpha \mod R} f(\alpha) E_k(A).$$

5. Main results and related arithmetical identities.

Theorem 1. The number of ordered sets $(X_1, \ldots, X_h)$, $X_i \equiv \alpha \mod R$ satisfying the congruence (1.1) is equal to

$$\frac{1}{|R|} \sum_{D \equiv \alpha \mod R} \left( \prod_{i} \eta \left( \frac{R}{D_i}, \frac{R}{D_j} \right) \right) \eta(M, D).$$

Proof. Let $N(M, R)$ represent the number of solutions of (1.1). It is evident that $N(M, R)$ belongs to the class $(R, K)$ and hence by (2.8) and (3.2), it has the representation given by

$$N(M, R) = \sum_{a \equiv \alpha \mod R} a \sum_{E_k \equiv \alpha \mod R} E_k(A).$$

where

$$a_a = \frac{1}{|R|} \sum_{a \equiv \alpha \mod R} N(V, R) E_k(-V),$$

i.e.

$$a_a = \frac{1}{|R|} \sum_{a \equiv \alpha \mod R} N(V, R) E_k(-V_1 - V_2 - \ldots - V_s),$$

where

$$V = V_1 + V_2 + \ldots + V_s \mod R,$$

i.e.

$$a_a = \frac{1}{|R|} \sum_{a \equiv \alpha \mod R} E_k(-V_1 - \ldots - V_s).$$

From the definition of $N(V, R)$, where $s_i$ of the $V_i$'s are such that

$$(V_i, R) = D_i (i = 1, 2, \ldots) \quad \text{and} \quad \sum_{i=1}^{s_i} s_i = s$$

we have

$$a_a = \frac{1}{|R|} \sum_{i=1}^{s_i} E_k(-V_1) E_k(-V_2) \ldots = \frac{1}{|R|} \eta \left( \frac{R}{D_1} \right) \eta \left( \frac{R}{D_2} \right) \ldots$$

and

$$a_a = \frac{1}{|R|} \prod_{i=1}^{s_i} \eta \left( \frac{R}{D_i} \right).$$

Let $(Z, R) = E(D)$, then

$$a_a = \frac{1}{|R|} \prod_{i=1}^{s_i} \eta \left( \frac{R}{D_i} \right).$$

Therefore (3.2) can be written as

$$N(M, R) = \sum_{a \equiv \alpha \mod R} \frac{1}{|R|} \prod_{i=1}^{s_i} \eta \left( \frac{R}{D_i} \right) \left( \sum_{E_k \equiv \alpha \mod R} E_k(M) \right).$$

Now the result follows as stated in the theorem.

Remark 1. The above result can now be interpreted as follows. Consider a complete residue system $\mod R$. This can be divided into classes $C(D_1), \ldots, C(D_n)$ so that $C(D_i)$ consists of all those elements $E$ of the complete residue system $\mod R$ which are such that $(N, E) = D_i$.

In analogy with a well known result of Vaidyanathaswamy [17] (see also Menon [11]), Theorem 3, where $s_i = 1 = s_j$ and $s_k = 0, t \neq i, t \neq j$, shows that the classes $C(D_i)$ combine by addition. That is to say, if
$C(D_k) \otimes C(D_l)$ stands for the totality of all sums of the form $A + B$ (repetitions retained), where $A \in C(D_k), B \in C(D_l)$, then every number of $C(D_k)$ occurs the same number of times in $C(D_k) \otimes C(D_l)$. The same can be put as follows. For any given $M \in C(D_k)$ the number of solutions $A, B$ of the congruence

$$M \equiv A + B \pmod{R}$$

with the restrictions that $A \in C(D_k), B \in C(D_k)$, is independent of $M$ in $C(D_k)$.

**Corollary 1.** The number of solutions $\phi^0(M, E)$ of the congruence

$$M = X_1 + \ldots + X_s \pmod{R},$$

where $(X_i, R) = 1 \ (i = 1, \ldots, s)$ is given by

$$\phi^0(M, R) = \frac{1}{|R|} \sum_{D \mid R} \nu\left(\frac{R}{D}, D\right) \eta(M, D).$$

By putting $s_1 = s$ and $s_i = 0$ for $i > 1$ in Theorem 3 we obtain the above corollary.

**Theorem 2.** We have

$$\sum_{\delta \in M \subset R} \phi^0(M, R) = [\Phi(E)(E)]^s,$$

where $\Phi(E) = \Phi(0, E)$, the Euler totient for $G \Phi(p^s, x)$.

**Proof.** We have

$$\phi^0(M, R) = \frac{1}{|R|} \sum_{D \mid R} \nu\left(\frac{R}{D}, D\right) \eta(M, D),$$

$$\phi^0(M, E) = \frac{1}{|R|} \sum_{\delta \in M \subset R} \nu\left(\frac{R}{D}, D\right) \eta(M, D),$$

$$\sum_{\delta \in M \subset R} \phi^0(M, E) = \frac{1}{|R|} \sum_{\delta \in M \subset R} \nu\left(\frac{R}{D}, D\right) \left(\sum_{\delta \in M \subset R} E_\delta(M)\right).$$

But the inner sum vanishes unless $Z \equiv 0 \pmod{R}$ and in the latter case it is $|R|$ (see Cohen [4], (7)). Hence follows the result.

**Theorem 3.** We have

$$\sum_{D \mid R} \nu\left(\frac{R}{D}, D\right) \eta(M, D) = \begin{cases} |R| & \text{if} \ (M, E) = D_1, \\ 0 & \text{otherwise}. \end{cases}$$

To prove this theorem we need the following

**Lemma 1.**

$$\sum_{\delta \in M \subset R} \nu\left(\frac{R}{D}, D\right) E_\delta(M) = \begin{cases} |R| & \text{if} \ (M, E) = D_1, \\ 0 & \text{otherwise}. \end{cases}$$

**Proof of Lemma 1.** For any primary divisor $D_i$ of $R$, set

$$P^0(M, R) = \begin{cases} 1 & \text{if} \ (M, E) = D_1, \\ 0 & \text{otherwise}. \end{cases}$$

Evidently $P^0(M, R)$ is a function of the class $(R, E)$ and hence by (2.5) and (2.6) we have the representation

$$P^0(M, E) = \sum_{\delta \in M \subset R} a_\delta E_\delta(M),$$

where

$$a_\delta = \frac{1}{|R|} \sum_{\delta \in F \subset R} E_\delta(-V),$$

i.e.,

$$a_\delta = \frac{1}{|R|} \sum_{\delta \in M \subset R} E_\delta(-V).$$

Since $(V, E) = D_1$ if and only if $\left(\frac{V}{D_i}, \frac{R}{D_i}\right) = 1$, we have

$$a_\delta = \frac{1}{|R|} \left(\frac{R}{D_i}\right).$$

Now by substituting for $a_\delta$ in (3.13), the truth of lemma is established.

**Proof of Theorem 3.** From Lemma 1, we have that

$$P^0(M, R) = \frac{1}{|R|} \sum_{\delta \in M \subset R} \nu\left(\frac{R}{D}, D\right) E_\delta(M).$$

Let $(Z, R) = \frac{R}{D}$, then

$$P^0(M, R) = \frac{1}{|R|} \sum_{\delta \in M \subset R} \nu\left(\frac{R}{D}, D\right) \left(\sum_{\delta \in M \subset R} E_\delta(M)\right)$$

and

$$P^0(M, R) = \frac{1}{|R|} \sum_{\delta \in M \subset R} \nu\left(\frac{R}{D}, D\right) \eta(M, D).$$
Now Theorem 3 results from (3.12) after multiplying both sides of (3.17) by $|E|$. As immediate consequences of Lemma 1, we obtain the following corollaries.

**Corollary 2.**
\[
\sum_{\alpha \in E \cap U} \eta(E, D) = 0 \quad \text{if} \quad D \neq R.
\]

A result obtained by setting $M = 0$ in Lemma 1.

**Corollary 3.**
\[
\sum_{\alpha \in E \cap U} \eta(E, D) E_1(1) = |E|
\]

results for $M = 1$ and $D_1 = 1$ in Lemma 1.

**Theorem 4.** The number of solutions of the congruence (1.2) is equal to
\[
|E|^{2s} \sum_{\alpha \in E \cap U} \eta(N, D) |D|^{s+1}.
\]

We need some preliminary results for the proof of Theorem 4.

**Lemma 2.** The number of solutions $S(A, E)$ in $Y \equiv Z \pmod{R}$ of the congruence
\[
A = Y \equiv Z \pmod{R}
\]

is given by
\[
S(A, E) = \sum_{\alpha \in E \cap U} \eta(A, D).
\]

**Proof.** It is clear that $S(A, E)$ belongs to the class $(R, K)$ and hence by (2.5) and (2.6) we have the representation
\[
S(A, E) = \sum_{\alpha \in E \cap U} a_\alpha E_\alpha(A),
\]

where
\[
a_\alpha = \frac{1}{|E|} \sum_{\alpha \in E \cap U} S(Y, E_\alpha(-Y)) = \frac{1}{|E|} \sum_{\alpha \in E \cap U} \sum_{\psi \equiv \alpha \pmod{R}} \psi E_\alpha(-\psi \alpha)
\]

from the definition of $S(Y, E)$

\[
= \frac{1}{|E|} \sum_{\alpha \in E \cap U} \sum_{\psi \equiv \alpha \pmod{R}} \psi E_\alpha(-\psi \alpha) = \frac{1}{|E|} \sum_{\alpha \in E \cap U} \left( \sum_{\psi \equiv \alpha \pmod{R}} \psi E_\alpha(-\psi \alpha) \right)
\]

\[
= \frac{1}{|E|} \sum_{\psi \equiv \alpha \pmod{R}} |E| = |E| - 1,
\]

and
\[
a_\alpha = \frac{|E|}{R} \quad \text{if} \quad (Z, R) = \frac{R}{D}.
\]

Some applications of Corrul's $\eta$-sum

Substituting the value of $a_\alpha$ in (3.20), we get that
\[
S(A, E) = \sum_{\alpha \in E \cap U} \frac{R}{D} \quad \text{if} \quad (Z, R) = \frac{R}{D},
\]

which is equal to (3.19).

**Lemma 3.**
\[
S(x, E) E_1(-x) = |E| \quad \text{if} \quad (Z, R) = \frac{R}{D},
\]

where $(x, R) = \frac{R}{D}$.

**Proof.** The left side of the lemma is equal to
\[
\sum_{\alpha \in E \cap U} a_\alpha E_\alpha(x) E_\alpha(-x) = \sum_{\alpha \in E \cap U} a_\alpha E_\alpha(y - z) \quad \text{(see (3.20))}
\]

\[
= \sum_{\alpha \in E \cap U} a_\alpha \sum_{\alpha \in E \cap U} E_\alpha(y - z).
\]

But the inner sum is $|E|$ if $Y - Z = 0 \pmod{R}$ and 0, otherwise (see Cohen [4], (7)).

The left side of the Lemma 3 is equal to
\[
|E| a_\alpha.
\]

But in Lemma 2, it is shown that $a_\alpha = \frac{R}{D}$. If $(Z, R) = \frac{R}{D}$, then

This completes the proof of Lemma 3.

We now go to the proof of Theorem 4. Let $S_\alpha(N, E)$ represent the number of solutions of (1.3). It is clear that $S_\alpha(N, E) = S(N, E)$. We note that $S_\alpha(N, E)$ is a function of the class $(R, K)$ and hence by (2.5) and (2.6) we have the following representation for $S_\alpha(N, E)$

\[
S_\alpha(N, E) = \sum_{\alpha \in E \cap U} A_\alpha E_\alpha(N),
\]

where
\[
A_\alpha = \frac{1}{|E|} \sum_{\alpha \in E \cap U} S_\alpha(Y, E_\alpha(-Y)).
\]

It is clear that
\[
S_\alpha(V, E) = \sum_{\alpha \in E \cap U} \int_0^1 S_\alpha(z, E),
\]
where $x_i = y_i z_1, y_i z_2 (\mod R)$ $(i = 0, \ldots, s)$

$$A_s = \frac{1}{|R|} \sum_{\varepsilon_1, \ldots, \varepsilon_s (\mod R)} \left( \prod_{i=1}^{s} S(x_i, R) E_s(-x_i) \right)$$

$$= \frac{1}{|R|} \sum_{\varepsilon_1, \ldots, \varepsilon_s (\mod R)} \left( \prod_{i=1}^{s} S(x_i, R) E_s(-x_i) \right)$$

$$= \frac{1}{|R|} \prod_{i=1}^{s} S(x_i, R) E_s(-x_i),$$

(3.29) \[ A_s = \frac{1}{|R|} \left| \frac{E}{D} \right|^{s+1}, \]

by Lemma 3 if $(Z, R) = R/D$.

Substituting in (3.25) the value for $A_s$ we obtain

$$S_s(N, R) = \left| \frac{E}{D} \right|^{s+1} \sum_{\varepsilon_1, \ldots, \varepsilon_s (\mod R), (\varepsilon_1, \ldots, \varepsilon_s = 0)} \frac{1}{|D|^{s+1}} E_s(N) = \left| \frac{E}{D} \right|^{s+1} \sum_{|D|} \frac{\gamma(N, D)}{|D|^{s+1}}.$$

Thus the proof of Theorem 4 is completed.

References