Table des matières du tome XII, fascicule 3

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*.

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

ACTA ARITHMETICA

Warszawa 1 (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 Przedmieście 7.

Prix de ce fascicule 3.00 $.

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

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

PRINTED IN POLAND

W R O C Ł A W S K A   D R U K A R N I A   N A U K O W A

ACTA ARITHMETICA
XII (1967)

Some applications of Carlitz's η-sum

by

K. Nageswara Rao (New Delhi)

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

$$M \equiv X_1 + X_2 + \ldots + X_s \pmod{R}, \tag{1.1}$$

where s_i of the X's$\in\mathscr{D}$, have the property $(X, R) = D_i$ and $\sum_i s_i = s$, and

$$N \equiv Y_0 Z_0 + \ldots + Y_s Z_s \pmod{R}, \tag{1.2}$$

where Y_i, Z_i are polynomials of $\mathscr{D}$.

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 $\mathscr{D}$. This contributed much to the simplicity of the proofs.

2. Notations and preliminaries. Let K be a field of characteristic zero, containing the pth roots of unity. Let F be any polynomial of $\mathscr{D}$, say

$$F = a_0 x^\nu + \ldots + a_\nu, \quad \text{where } a_0 \neq 0, \tag{2.1}$$

then ν is called the *degree of* F and is written as $\deg F = \nu$; F is said to be *primary* if $a_0 = 1$. We use the symbol $|F|$ to denote $p^{n\nu}$.

A single valued function f defined over the elements of $\mathscr{D}$ and assuming values in K, is said to *belong to the class* (R, K) if $f(A) = f(A^1)$ wherever $A \equiv A^1 \pmod{R}$.

The symbol $\sum'_{D|R}$ denotes the summation over all primary divisors D of R.

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

$$L_1 x^{h-1} + \ldots + L_h, \quad L_i \in \mathrm{GF}(p^n). \tag{2.2}$$

Then following Carlitz ([1], § 2) we define $E(A, H)$ to be $e^{2\pi i a_1/p}$, where a_1 is defined to be the integer $(\bmod p)$ which occurs as the initial coefficient in the expression

$$L_1 = a_1 \theta^{n-1} + \ldots + a_n, \tag{2.3}$$

θ being the generator of $\mathrm{GF}(p^n)$ relative to $\mathrm{GF}(p)$.

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

$$\eta(A, R) = \sum_{(Z,R)=1} E_z(A) \tag{2.4}$$

the summation being over all Z of a reduced residue system $(\bmod R)$, where $E_z(A) \equiv E(ZA, R)$.

For arithmetical functions f of the class (R, K) we have the following representation due to Cohen [4] (see also Carlitz [2]):

$$f(A) = \sum_{\deg Z<r} a_z E_z(A), \tag{2.5}$$

where

$$a_z = p^{-nr} \sum_{\deg V<r} f(V) E_z(-V). \tag{2.6}$$

3. Main results and related arithmetical identities.

THEOREM 1. *The number of ordered sets* $(X_1, \ldots, X_s)$, $X_i \pmod R$ *satisfying the congruence* (1.1) *is equal to*

$$\frac{1}{|R|} \sum_{D|R}' \left(\prod_i \eta^{s_i}\left(\frac{R}{D}, \frac{R}{D_i}\right)\right) \eta(M, D). \tag{3.1}$$

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 (2.5) and (2.6), it has the representation given by

$$N(M, R) = \sum_{\deg Z<r} a_z E_z(M), \tag{3.2}$$

where

$$a_z = \frac{1}{|R|} \sum_{\deg V<r} N(V, R) E_z(-V), \tag{3.3}$$

i.e.

$$a_z = \frac{1}{|R|} \sum_{\deg V<r} N(V, R) E_z(-V_1 - V_2 - \ldots - V_s),$$

where

$$V \equiv V_1 + V_2 + \ldots + V_s \pmod R,$$

i.e.

$$a_z = \frac{1}{|R|} \sum_{V_1,\ldots,V_s} E_z(-V_1 - \ldots - V_s).$$

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

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

we have

$$a_z = \frac{1}{|R|} \sum_{V_1,\ldots,V_s} \left(E_z^{s_1}(-V_1) E_z^{s_2}(-V_2) \ldots\right) = \frac{1}{|R|} \eta^{s_1}\left(Z, \frac{R}{D_1}\right) \eta^{s_2}\left(Z, \frac{R}{D_2}\right) \ldots$$

and

$$a_z = \frac{1}{|R|} \prod_i \eta^{s_i}\left(Z, \frac{R}{D_i}\right). \tag{3.4}$$

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

$$a_z = \frac{1}{|R|} \prod_i \eta^{s_i}\left(\frac{R}{D}, \frac{R}{D_i}\right). \tag{3.5}$$

Therefore (3.2) can be written as

$$N(M, R) = \sum_{D|R} \frac{1}{|R|} \prod_i \eta^{s_i}\left(\frac{R}{D}, \frac{R}{D_i}\right) \Big(\sum_{\substack{\deg Z<r \\ (Z,R)=R/D}} E_z(M) \Big). \tag{3.6}$$

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 $(\bmod R)$. This can be divided into classes $C(D_1), \ldots, C(D_m)$ so that $C(D_i)$ consists of all those elements N of the complete residue system $(\bmod R)$ which are such that $(N, R) = D_i$. In analogy with a well known result of Vaidyanathaswamy [17] (see also Menon [11]), Theorem 3, where $s_i = 1 = s_j$ and $s_t = 0$, $t \neq i$, $t \neq j$, shows that the classes $C(D_i)$ combine by addition. That is to say, if

$C(D_i)\oplus C(D_j)$ stands for the totality of all sums of the form $A+B$ (repetitions retained), where $A\epsilon C(D_i)$, $B\epsilon C(D_j)$, then every number of $C(D_k)$ occurs the same number of times in $C(D_i)\oplus C(D_j)$. The same can be put as follows. For any given $M\epsilon C(D_k)$ the number of solutions A, B of the congruence

$$M \equiv A+B \pmod{R} \tag{3.7}$$

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

Corollary 1. *The number of solutions $\Phi^{(s)}(M, R)$ of the congruence*

$$M \equiv X_1+\ldots+X_s \pmod{R}, \tag{3.8}$$

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

$$\Phi^{(s)}(M, R) = \frac{1}{|R|}\sum_{D|R}{}' \eta^s\left(\frac{R}{D}, R\right)\eta(M, D). \tag{3.9}$$

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

Theorem 2. *We have*

$$\sum_{\deg M<r}\Phi^{(s)}(M, R) = [\Phi(R)]^s,$$

where $\Phi(R) = \eta(0, R)$, the Euler totient for GF$[p^n, x]$.

Proof. We have

$$\Phi^{(s)}(M, R) = \frac{1}{|R|}\sum_{D|R}{}' \eta^s\left(\frac{R}{D}, R\right)\eta(M, D),$$

$$\Phi^{(s)}(M, R) = \frac{1}{|R|}\sum_{\deg Z<r}\eta^s(Z, R)E_z(M), \tag{3.10}$$

$$\sum_{\deg M<r}\Phi^{(s)}(M, R) = \frac{1}{|R|}\sum_{\deg Z<r}\eta^s(Z, R)\Big(\sum_{\deg M<r}E_z(M)\Big). \tag{3.11}$$

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*

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

To prove this theorem we need the following

Lemma 1.

$$\sum_{\deg Z<r}\eta\left(Z, \frac{R}{D_i}\right)E_z(M) = \begin{cases}|R| & \text{if } (M, R) = D_i,\\ 0 & \text{otherwise.}\end{cases}$$

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

$$P^{(i)}(M, R) = \begin{cases}1 & \text{if } (M, R) = D_i,\\ 0 & \text{otherwise.}\end{cases} \tag{3.12}$$

Evidently $P^{(i)}(M, R)$ is a function of the class (R, K) and hence by (2.5) and (2.6) we have the representation

$$P^{(i)}(M, R) = \sum_{\deg Z<r}a_z E_z(M), \tag{3.13}$$

where

$$a_z = \frac{1}{|R|}\sum_{\deg V<r}P^{(i)}(V, R)E_z(-V), \tag{3.14}$$

i.e.

$$a_z = \frac{1}{|R|}\sum_{\substack{\deg V<r\\ (V,R)=D_i}}E_z(-V). \tag{3.15}$$

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

$$a_z = \frac{1}{|R|}\eta\left(z, \frac{R}{D_i}\right). \tag{3.16}$$

Now by substituting for a_z in (3.13), the truth of lemma is established.

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

$$P^{(i)}(M, R) = \frac{1}{|R|}\sum_{\deg Z<r}\eta\left(z, \frac{R}{D_i}\right)E_z(M).$$

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

$$P^{(i)}(M, R) = \frac{1}{|R|}\sum_{D|R}{}' \eta\left(\frac{R}{D}, \frac{R}{D_i}\right)\Big(\sum_{\substack{(Z,R)=R/D\\ \deg Z<r}}E_z(M)\Big)$$

and

$$P^{(i)}(M, R) = \frac{1}{|R|}\sum_{D|R}{}' \eta\left(\frac{R}{D}, \frac{R}{D_i}\right)\eta(M, D). \tag{3.17}$$

Now Theorem 3 results from (3.12) after multiplying both sides of (3.17) by $|R|$.

As immediate consequences of Lemma 1, we obtain the following corollaries.

COROLLARY 2.

$$\sum_{\deg Z<r} \eta\left(z, \frac{R}{D_i}\right) = 0 \quad \text{if} \quad D_i \neq R.$$

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

COROLLARY 3.

$$\sum_{\deg Z<r} \eta(Z, R) E_z(1) = |R|$$

results for $M = 1$ *and* $D_i = 1$ *in Lemma* 1.

THEOREM 4. *The number of solutions of the congruence* (1.2) *is equal to*

$$|R|^{2s+1} \sum_{D|R}' \eta(N, D)/|D|^{s+1}.$$

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

LEMMA 2. *The number of solutions* $S(A, R)$ *in* $Y_0, Z_0 \pmod R$ *of the congruence*

$$A \equiv Y_0 Z_0 \pmod R \tag{3.18}$$

is given by

$$S(A, R) = \sum_{D|R}' \left|\frac{R}{D}\right| \eta(A, D). \tag{3.19}$$

Proof. It is clear that $S(A, R)$ belongs to the class (R, K) and hence by (2.5) and (2.6) we have the representation

$$S(A, R) = \sum_{\deg Z<r} a_z E_z(A), \tag{3.20}$$

where

$$a_z = \frac{1}{|R|} \sum_{\deg V<r} S(V, R) E_z(-V) = \frac{1}{|R|} \sum_{\deg V<r} \sum_{V \equiv y_0 z_0 \pmod R} E_z(-y_0 z_0) \tag{3.21}$$

from the definition of $S(V, R)$

$$= \frac{1}{|R|} \sum_{\deg y_0, \deg z_0<r} E_z(-y_0 z_0) = \frac{1}{|R|} \sum_{\deg y_0<r} \left(\sum_{\deg z_0<r} E_z(-y_0 z_0)\right)$$

$$= \frac{1}{|R|} \sum_{y_0 z \equiv 0 \pmod R} |R| = \sum_{y_0 z \equiv 0 \pmod R}' 1,$$

$$a_z = \left|\frac{R}{D}\right| \quad \text{if} \quad (Z, R) = \frac{R}{D}. \tag{3.22}$$

Substituting the value of a_z in (3.20), we get that

$$S(A, R) = \sum_{\substack{\deg Z<r \\ (z,R)=R/D}} \left|\frac{R}{D}\right| E_z(A), \tag{3.23}$$

which is equal to (3.19).

LEMMA 3.

$$\sum_{\deg x<r} S(x, R) E_z(-x) = |R| \left|\frac{R}{D}\right|,$$

where $(z, R) = \dfrac{R}{D}$.

Proof. The left side of the lemma is equal to

$$\sum_{\deg x<r} \left(\sum_{\deg y<r} a_y E_y(x)\right) E_z(-x) = \sum_{\deg x<r} \left(\sum_{\deg y<r} a_y E_x(y-z)\right) \qquad \text{(see (3.20))}$$

$$= \sum_{\deg y<r} a_y \left(\sum_{\deg x<r} E_x(y-z)\right).$$

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

The left side of the Lemma 3 is equal to

$$|R| a_z. \tag{3.24}$$

But in Lemma 2, it is shown that $a_z = \left|\dfrac{R}{D}\right|$ if $(Z, R) = \left|\dfrac{R}{D}\right|$. This completes the proof of Lemma 3.

We now go to the proof of Theorem 4. Let $S_s(N, R)$ represent the number of solutions of (1.2). It is clear that $S_0(N, R) \equiv S(N, R)$. We note that $S_s(N, R)$ is a function of the class (R, K) and hence by (2.5) and (2.6) we have the following representation for $S_s(N, R)$

$$S_s(N, R) = \sum_{\deg Z<r} A_z E_z(N), \tag{3.25}$$

where

$$A_z = \frac{1}{|R|} \sum_{\deg V<r} S_s(V, R) E_z(-V). \tag{3.26}$$

It is clear that

$$S_s(V, R) = \sum_{V \equiv x_0 + \ldots + x_s \pmod R} \prod_{i=0}^{s} S(x_i, R), \tag{3.27}$$

where $x_i = y_i z_i, y_i, z_i \pmod{R}$ $(i = 0, \ldots, s)$

$$A_z = \frac{1}{|R|} \sum_{\deg V<r} \Big(\sum_{V=x_0+\ldots+x_s \pmod{R}} \prod_{i=0}^{s} S(x_i, R) \Big) E_z(-x_0-x_1-\ldots-x_s)$$

$$= \frac{1}{|R|} \sum_{x_0\ldots x_s \pmod{R}} \Big(\prod_{i=0}^{s} S(x_i, R) E_z(-x_i) \Big)$$

$$= \frac{1}{|R|} \prod_{i=0}^{s} \Big(\sum_{\deg x_i<r} S(x_i, R) E_z(-x_i) \Big),$$

$$(3.28) \qquad A_z = \frac{1}{|R|} |R|^{s+1} \left| \frac{R}{D} \right|^{s+1},$$

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

Substituting in (3.25) the value for A_z we obtain

$$S_s(N, R) = |R|^{2s+1} \sum_{\substack{\deg Z<r \\ (z,R)=R/D}} \frac{1}{|D|^{s+1}} E_z(N) = |R|^{2s+1} \sum_{D|R}{}' \frac{\eta(N, D)}{|D|^{s+1}}.$$

Thus the proof of Theorem 4 is completed.

References

[1] L. Carlitz, *The singular series for sums of squares of polynomials*, Duke Math. Journ. 14 (1947), pp. 1015-1120.

[2] — *Representations of arithmetic functions in* GF$[p^n, x]$, Duke Math. Journ. 14 (1947), pp. 1121-1137.

[3] E. Cohen, *Rings of arithmetic functions*, Duke Math. Journ. 19 (1952), pp. 115-129.

[4] — *Arithmetic functions of polynomials*, Proc. Amer. Math. Soc. 3 (1953), pp. 352-358.

[5] — *An extension of Ramanujan sum. II. Additive properties*, Duke Math. Journ. 22 (1955), pp. 543-550.

[6] — *Some totient functions*, Duke Math. Journ. 23 (1956), pp. 515-522.

[7] — *An extension of Ramanujan sum. III. Connections with totient functions*, Duke Math. Journ. 23 (1956), pp. 623-650.

[8] — *Representations of even functions* (mod r). *I. Arithmetical identities*, Duke Math. Journ. 25 (1958), pp. 401-421.

[9] — *Trigonometric sums in elementary number theory*, Amer. Math. Monthly 66 (1959), pp. 105-116.

[10] — *A class of residue systems* (mod$r$). *A generation of Möbius inversion*, Pacific Journ. Math. 9 (1959), pp. 13-23.

[11] P. K. Menon, *On Vaidyanathaswamy's class division of the residue classes modulo N*, Journ. Indian Math. Soc. 26 (1962), pp. 167-186.

[12] P. J. Mc Carthy, *The generation of arithmetical identities*, Journ. Reine Angew. Math. 203 (1960), pp. 55-63.

[13] K. Nageswara Rao, *On a congruence equation and related arithmetical identities*, to appear in Monatsh. Math.

[14] — *Unitary class division of integers* mod$n$ *and related arithmetical identities*, to appear.

[15] C. A. Nicol and H. S. Vandiver, *A Vonsterneck arithmetical function and restricted partition with respect to modulus*, Proc. Nat. Acad. Sci. USA, 40 (1954), pp. 825-835.

[16] K. G. Ramanathan, *Some applications of Ramanujan's trigonometrical sum* $C_M(N)$, Proc. Indian Acad. Sci., Sect. A, 20 (1944), pp. 62-69.

[17] R. Vaidyanathaswamy, *A remarkable property of integers* mod$N$ *and its bearing on group theory*, Proc. Indian Acad. Sci., Sect. A, 5 (1937), pp. 63-75.

SRI VENKATESWARA COLLEGE
UNIVERSITY OF DELHI, INDIA
THE CENTRE FOR ADVANCED STUDY IN MATHEMATICS, CHANDIGARH

Reçu par la Rédaction le 25. 11. 1965