Exponential sums, number of solutions of algebraic equations, and Poincaré series

Víctor S. Albis[1]

Departamento de Matemáticas
Universidad Nacional de Colombia

Edilmo Carvajal[2]
Escuela de Matemáticas
Universidad Central de Venezuela, Caracas

Definitions of Gauss and Ramanujan sums over the algebras Λ and L_v are given, and their main properties are proved. Using these results an analogous of an old result of Libri on the number of solutions of algebraic equations with integral coefficients modulo a prime power is obtained, and then used to compute the number of solutions of some equations with coefficients in L_v. Finally, an analogous of a problem of Nageswara Rao on algebraic equations subject to partitions is solved for equations with coefficients in L_v.

Keywords: Gauss sums, Ramanujan sums, number of solutions of algebraic equations over finite algebras, Poincaré series.

Se dan definiciones de suma de Gauss y de Ramanujan sobre las álgebras Λ y L_v, y se muestran sus principales propiedades. Usando estos resultados se demuestra un análogo de un viejo teorema de Libri sobre el númeroo de soluciones de ecuaciones algebraicas con coeficientes enteros, el cual se usa luego para calcular el número de soluciones de algunas ecuaciones algebraicas con coeficientes en L_v. Finalmente, un análogo de un problema de Nageswara Rao sobre ecuaciones algebraicas sujetas a particiones, se resuelve para ecuaciones con coeficientes en L_v.

Palabras claves: Sumas de Gauss, sumas de Ramanujan, número de soluciones de ecuaciones algebricas sobre álgebras finitas, series de Poincaré.

MSC: 11T24, 11T55.

[1] vsalbisg@unal.edu.co
[2] ecarvaja@euler.ciens.ucv.ve

1 Introduction

In [16] Kummer generalizes Gauss quadratic sums to the rings $\mathbb{Z}/p^\ell\mathbb{Z}$, where p is a prime number and $\ell > 0$ is a natural number, obtaining some of their most important properties. Using the Chinese remainder theorem, these sums and their properties can be extended to the rings $\mathbb{Z}/m\mathbb{Z}$. In particular, the representation of arithmetical functions modulo m as discrete (finite) Fourier series is obtained (see, *e.g.*, [4, Chap. 8, p. 172]). In the 20th century Gauss sums are studied in finite fields $\mathbb{F}_q$, $q = p^t$, where p is a prime number and $t > 1$ is an integer, and used, for example, to determine the number of solutions of forms $\mathbb{F}_q[t_1, \cdots, t_n]$, see [26, 14] or to decide if a polynomial $f(t_1, \cdots, t_n) \in \mathbb{F}_q[t_1, \cdots, t_n]$ is or is not a permutation polynomial [23, 24]. Due to the analogy between the rings $\mathbb{Z}$ and $\mathbb{F}_q[X]$, a natural generalization of Gauss sums is done by Carlitz in [5, 6], and later precised by Cohen in [8]. Analogously to the rational case, they find that any arithmetical function defined on $\mathbb{F}_q[X]$, modulo a unitary (primary) polynomial $h(X)$, admits a discrete Fourier series. In the 50's of the last century, Lamprecht [17] (see also [7]) further extends the notion of Gauss sums and their properties to a wide class of commutative finite rings. According to Moreno [20], under quite natural conditions, the results on Gauss sums in these rings are analogous to those of Kummer. Also, he pinpoints their importance, not only in the classical case, but in recent developments in digital signal processing, self–correcting codes and Igusa's stationary phase method [3], among others.

On the other hand, in 1967, Nageswara Rao [21] extends previous results in the rational case on the number of solutions of certain algebraic equations, some of them with partition conditions [9, 10, 11, 22] to the case of the rings $\mathbb{F}_q[X]/(h(X))$, where $h(X)$ is a unitary polynomial in $\mathbb{F}_q[X]$.

Our purpose in this paper is twofold. In the first place, in section 2, we present a somewhat detailed selfcontained exposition of Gauss and Ramanujan sums over the algebras $\Lambda = \mathbb{F}_q[X]/(h(X))$ and $L_v = \mathbb{F}_q[X]/(p(X)^v)$, where $h(X)$ is a unitary polynomial and $p(X)$ is a irreducible unitary polynomial. In the second place, in section 3, we use the results in section 2, to prove in these algebras analogous results to the classical old results of Libri [18, 19] and use them to obtain the number of solutions of some algebraic equations with coefficients in Λ and L_v. In particular, we present a somewhat different proof of a result of Nageswara Rao.

2 Notations and preliminaries

In this paper, the group of units of a unitary commutative ring A will be denoted by $A^\times$.

Let $K = \mathbb{F}_q$ be a finite field with $q = p^t$ (t a positive integer) elements. If F is an extension de K of degree $s = [F : K]$, we define as usual the trace of $\alpha \in F$ sobre K by the relation

$$\mathrm{tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{s-1}} .$$

The following proposition contains the main properties of the function $\mathrm{tr}_{F/K}$ (see [14, Chap. 10, p. 125]).

Proposition 1. *Let $K \subseteq F$ finite fields. If α, $\beta \in F$ and $a \in K$, then*

i) $\mathrm{tr}_{F/K}(\alpha) \in K$.

ii) $\mathrm{tr}_{F/K}(\alpha + \beta) = \mathrm{tr}_{F/K}(\alpha) + \mathrm{tr}_{F/K}(\beta)$.

iii) $\mathrm{tr}_{F/K}(a\alpha) = a\mathrm{tr}_{F/K}(\alpha)$.

iv) $\mathrm{tr}_{F/K} : F \to K$ *is onto.*

If $h(X) = \alpha\, p_1(X)^{a_1} \cdots p_r(X)^{a_r} \in \mathbb{F}_q[X]$, where $\alpha \in \mathbb{F}_q^{\times}$ and $p_i(X)$ is an irreducible polynomial in $\mathbb{F}_q[X]$, we denote by $(h(X))$ the ideal generated by this polynomial. The Chinese remainder theorem in the ring $\mathbb{F}_q[X]$ tell us that:

$$\mathbb{F}_q[X]/(h(X)) = \prod_{i=1}^{r} \mathbb{F}_q[X]/(p_i(X)^{a_i}) , \tag{1}$$

and

$$[\mathbb{F}_q[X]/(h(X))]^{\times} = \prod_{i=1}^{r} [\mathbb{F}_q[X]/(p_i(X)^{a_i})]^{\times} . \tag{2}$$

Therefore, we may restrict our considerations to rings of the form $\mathbb{F}_q[X]/(p(X)^v)$ where $p(X)$ is an irreducible polynomial. It is well known that $\mathbb{F}_q[X]/(p(X)) = L$ is a finite field containing an isomorphic copy of $\mathbb{F}_q$. Also, if the degree of $p(X)$ is d, then the degree of the extension $L/\mathbb{F}_q$ is d. Consequently, L has q^d elements. For these residual rings we have the following results [2, 1, 25].

Proposition 2. *With above notations we get:*

i) $\mathbb{F}_q[X]/(p(X)^v)$ *contains a field L isomorphic to* $\mathbb{F}_q[X]/(p(X))$.

ii) $\mathbb{F}_q[X]/(p(X)^v) = L_v$ *is an L–algebra of dimension v and q^{vd} elements.*

iii) $L_v = \{\lambda(z_v) = \lambda_0 + \lambda_1 z_v + \cdots + \lambda_{v-1} z_v^{v-1} \ : \lambda_i \in L\}$, *where* $z_v^i \neq 0$ *for* $i = 1, 2, \cdots, v-1$ *and* $z_v^k = 0$ *if* $k \geq v$. *Moreover, the set* $\{1, z_v, \cdots, z_v^{v-1}\}$ *is a base for this* L*–algebra.*

iv) $L_v^\times = L^\times \times \{1 + \lambda_1 z_v + \lambda_2 z_v^2 + \cdots + \lambda_{v-1} z_v^{v-1} \ : \lambda_j \in L\}$ *where* $z_v^i \neq 0$ *for* $i = 1, 2, \cdots, v-1$ *and* $z_v^k = 0$ *if* $k \geq v$. *Therefore,* $L_v^\times$ *has* $(q^d - 1)q^{d(v-1)}$ *elements.*

Now, using the following notations

$$\begin{aligned} \Lambda &= \mathbb{F}_q[X]/(h(X)), \\ L_{v_i} &= \mathbb{F}_q[X]/(p_i(X)^{v_i}), \end{aligned}$$

we get the following isomorphisms:

$$\Lambda \approx \bigoplus_{i=1}^{r} L_{v_i}, \tag{3}$$

$$\Lambda^\times \approx \bigoplus_{i=1}^{r} L_{v_i}^\times. \tag{4}$$

Thus an element of the $\mathbb{F}_q$–algebra Λ has the form $(\alpha(z_{v_1)}, \cdots, \alpha(z_{v_r}))$ where $\alpha(z_{v_i})$ is an element of the $\mathbb{F}_q$–algebra L_{v_i} for $i = 1, \cdots, r$. In what follows, if there is no confusion, we will denote $(\alpha(z_{v_1}), \cdots, \alpha(z_{v_r}))$ by $\boldsymbol{\alpha}(z_v)$. It is clear that $\boldsymbol{\alpha}(z_v) \in \Lambda^\times$ if, and only if, $\alpha(z_{v_i}) \in L_{v_i}^\times$.

The set $M(X, \mathbb{F}_q)$ of all unitary polynomials in $\mathbb{F}_q[X]$, is an arithmetical multiplicative monoid [15] on which the analogous notion of arithmetical function in classical number theory can be defined. In particular, we are interested in *periodic multiplicative functions* with period $h(X) \in M(X, \mathbb{F}_q)$, that is, arithmetical functions $F : M(X, \mathbb{F}_q) \to \mathbb{C}$ satisfying $F(a(X)) = F(b(X))$ whenever $a(x) \equiv b(X) (\mathrm{md}\ h(X))$. An example of this type functions are the characters of the finite algebras Λ and L_v. More generally, if A is a unitary finite commutative $L--$algebra, a function $\chi : A \to \mathbb{C}$ satisfying the following conditions:

i) $\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$, for all α and $\beta \in A$.

ii) $\chi(\alpha) = 0$ if α is not invertible.

iii) χ restricted to $A^\times$ is a group with values in $\mathbb{T} = \{z \in \mathbb{C};\ |z| = 1\}$,

is said to be a *Dirichlet multiplicative character* of A.

Also, we will use additive characters, i.e., homomorphisms $\psi : A^+ \to \mathbb{T}$ satisfying $\psi(\alpha + \beta) = \psi(\alpha)\psi(\beta)$.

Let us observe that the restriction of χ to $A^\times$ is a character of the finite commutative group $A^\times$, and, conversely, given a multiplicative character $\chi^\times$ de $A^\times$ it can be extended uniquely to a Dirichlet character χ on A by defining $\chi(\alpha) = \chi^\times(\alpha)$ if $\alpha \in A^\times$ and $\chi(\alpha) = 0$ if $\alpha \notin A^\times$. From now on we will use χ to denote both χ and $\chi^\times$.

Next, we will prove that each character of Λ is the product of characters of the L_{v_i}, $i = 1, \cdots, r$. So we can restrict our study to characters of L_v.

Proposition 3. *Given a multiplicative character θ of Λ, there are multiplicative characters χ_i of L_{v_i}, $i = 1, \cdots, r$, such that $\theta = \prod_{i=1}^r \chi_i$. And, conversely, given characters χ_i of L_{v_i}, for $i = 1, \cdots, r$, then $\prod_{i=1}^r \chi_i$ is a character of Λ.*

Proof. Let us suppose that χ_i, $i = 1, \cdots, r$, are multiplicative characters of L_{v_i} and put $\chi = \prod_{i=1}^r \chi_i$. We now check that χ is a multiplicative character of the algebra Λ. We have

$$\begin{aligned}\chi(\boldsymbol{\alpha}(z_v)\,\beta(z_v)) &= \prod_{i=1}^r \chi_i(\alpha(z_{v_i})\,\beta(z_{v_i})) \\ &= \prod_{i=1}^r \chi_i(\alpha(z_{v_i})) \prod_{i=1}^r \chi_i(\beta(z_{v_i})) = \chi(\boldsymbol{\alpha}(z_v))\,\chi(\boldsymbol{\beta}(z_v))\,.\end{aligned}$$

Indeed, let us recall that $\boldsymbol{\alpha}(z_v) \notin \Lambda^\times$ if, and only if, $\alpha(z_{v_i}) \notin L_{v_i}^\times$ for some $i = 1, \cdots, r$. Since each χ_i is a character of the algebra L_{v_i} then $\chi(\boldsymbol{\alpha}(z_v)) = 0$ if $\boldsymbol{\alpha}(z_v) \notin \Lambda^\times$. On the other hand, $\boldsymbol{\alpha}(z_v) \in \Lambda^\times$ if, and only if, $\alpha(z_{v_i}) \in L_{v_i}^\times$ for each $i = 1, \cdots, r$, and χ_i restricted to $L_{v_i}^\times$ is a group homomorphism with values in $\mathbb{T}$. Therefore, χ, restricted to $\Lambda^\times$, is a group homomorphism. That is, χ is a character of Λ.

Conversely, it is clear that for any $\boldsymbol{\alpha}(z_v) \in \Lambda$ we have:

$$\begin{aligned}\boldsymbol{\alpha}(z_v) &= (\alpha(z_{v_1}),\, 1, \cdots,\, 1) \cdots (1, \cdots,\, \alpha(z_{v_i}), \cdots,\, 1) \cdots \\ &\quad \times (1, \cdots,\, \alpha(z_{v_r}))\,, \end{aligned} \tag{5}$$

and thus

$$\begin{aligned}\theta(\boldsymbol{\alpha}(z_v)) &= \theta((\alpha(z_{v_1}),\, 1, \cdots, 1) \cdots (1, \cdots,\, \alpha(z_{v_i}), \cdots, 1) \cdots \\ &\quad \times (1, \cdots,\, \alpha(z_{v_r}))) \\ &= \theta((\alpha(z_{v_1}),\, 1, \cdots,\, 1)) \cdots \theta((1, \cdots,\, \alpha(z_{v_i}), \cdots,\, 1)) \cdots \\ &\quad \times \theta((1, \cdots,\, \alpha(z_{v_r}))\,. \end{aligned} \tag{6}$$

Using the evident isomorphism

$$1 \times \cdots \times 1 \times L_{v_i} \times 1 \times \cdots \times 1 \approx L_{v_i}\,, \tag{7}$$

we define the following character of L_{v_i}:

$$\chi_i(\alpha(z_{v_i})) = \theta((1, \cdots, \alpha(z_{v_i}), \cdots, 1))\,. \tag{8}$$

From (6) and (8) it follows

$$\theta(\boldsymbol{\alpha}(z_v)) = \chi_1(\alpha(z_{v_1})) \cdots \chi_i(\alpha(z_{v_i})) \cdots \chi_r(\alpha(z_{v_r}))\,, \tag{9}$$

as desired. □

The character defined as follows: $\chi_0(\alpha(z_v)) = 1$ if $\alpha(z_v)$ is invertible and $\chi_0(\alpha(z_v)) = 0$ otherwise, is called the *principal character* of L_v. It is also clear that $L_v^\times$ is a finite commutative group and therefore, from [4, Theo. 6.8] it follows that the group of (Dirichlet) characters of L_v has $(q^d - 1)q^{d(v-1)}$ elements.

The following results are analogous to the ones proved in [4, pp. 133 and ff.], and are easily proved by mimicking their proofs.

Proposition 4. *Let χ be a character of L_v. Then:*

i) $\chi(1) = 1$.

ii) *Putting $\bar{\chi}(\lambda(z_v)) = \overline{\chi(\lambda(z_v))}$ for every $\lambda(z_v) \in L_v$, $\bar{\chi}$ is a character of L_v.*

iii) *For all $\lambda(z_v) \in L_v^\times$ we have $\bar{\chi}(\lambda(z_v)) = \chi(\lambda(z_v))^{-1} = \chi(\lambda(z_v)^{-1})$.*

Proposition 5.

$$\sum_{\lambda(z_v)\in L_v} \chi(\lambda(z_v)) = \begin{cases} (q^d - 1)q^{d(v-1)}, & \text{if } \chi = \chi_0, \\ 0, & \text{if } \chi \neq \chi_0. \end{cases}$$

Proposition 6.

$$\sum_{\chi \text{ character of } L_v} \chi(\lambda(z_v)) = \begin{cases} (q^d - 1)q^{d(v-1)}, & \text{if } \lambda(z_v) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Proposition 7. *Let $\alpha(z_v)$, $\lambda(z_v) \in L_v^\times$, and χ a character of L_v, then*

$$\sum_{\chi \text{ character of } L_v} \bar{\chi}(\lambda(z_v))\chi(\alpha(z_v)) = \begin{cases} (q^d-1)q^{d(v-1)}, & \text{if } \lambda(z_v) = \alpha(z_v), \\ 0, & \text{otherwise.} \end{cases}$$

Following Carlitz, we define the following function τ_v from L_v into $\mathbb{F}_p$:

$$\tau_v(\lambda(z_v)) = \tau_v(\lambda_0 + \lambda_1 z_v + \cdots + \lambda_{v-1} z_v^{v-1}) := \operatorname{tr}_{L/\mathbb{F}_p}(\lambda_{v-1}),$$

and call it the *trace of* $\lambda(z_v)$. This definition makes sense, since $\lambda_{v-1} \in L$ and L is a finite extension of $\mathbb{F}_p$. The following result follows from the definition of τ_v and the properties of $\operatorname{tr}_{L/\mathbb{F}_p}$.

Proposition 8. *The function $\tau_v : L_v \to \mathbb{F}_p$ is a $\mathbb{F}_p$–linear onto mapping.*

To abbreviate we put $\tau' = \operatorname{tr}_{L/\mathbb{F}_p}$, so that

$$\tau_v(\alpha(z_v)) = \operatorname{tr}_{L/\mathbb{F}_p}(\alpha_{v-1}) = \tau'(\alpha_{v-1}).$$

If $\zeta_p = \exp(2\pi i/p)$ is a primitive p–th root of unity in $\mathbb{C}$, we define the function

$$e(\alpha) = \zeta_p^{\tau'(\alpha)},$$

with $\alpha \in L$. With these notations, we prove now

Proposition 9.

$$\sum_{\beta \in L} e(\alpha\beta) = \begin{cases} q^d, & \text{if } \alpha = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Since τ' is onto, there is a $\gamma \in L$ such that $\tau'(\gamma) \neq 0$, and thus $e(\gamma) \neq 1$. Let us compute the following sum:

$$e(\gamma) \sum_{\beta \in L} e(\alpha\beta) = \sum_{\beta \in L} e(\gamma)\, e(\alpha\beta) = \sum_{\beta \in L} e(\gamma + \alpha\beta) = \sum_{\beta \in L} e(\alpha\delta).$$

If $\alpha \neq 0$ we put $\delta = \beta + \dfrac{\gamma}{\alpha}$. But when β runs over L then δ does the same uniquely. Hence,

$$e(\gamma)\sum_{\beta\in L} e(\alpha\beta) = \sum_{\delta\in L} e(\alpha\delta) = \sum_{\beta\in L} e(\alpha\beta)\,.$$

Thus $\{e(\gamma)-1\}\sum_{\beta\in L} e(\alpha\beta) = 0$, and therefore $\sum_{\beta\in L} e(\alpha\beta) = 0$. If $\alpha = 0$, we have $\sum_{\beta\in L} e(\alpha\beta) = \sum_{\beta\in L} 1 = q^d$. □

Denote by $\boldsymbol{\mu}_p$ the group of p–th roots of unity in $\mathbb{C}$, and let us define $\psi_v : L_v \to \boldsymbol{\mu}_p$ by

$$\psi_v(\lambda(z_v)) := \zeta_p^{\tau_v(\lambda(z_v))} = \zeta_p^{\tau'(\lambda_{v-1})}\ .$$

This expression makes sense since $\tau'(\lambda_{v-1}) \in \mathbb{F}_p$.

Proposition 10. *The function ψ_v has the following properties:*

i) $\psi_v(0) = 1$.

ii) *ψ_v is an epimorphism from the additive group of L_v into the multiplicative group $\boldsymbol{\mu}_p$ (i.e., ψ_v is an additive character).*

iii) *There exists $\lambda(z_v) \in L_v$ such that $\psi_v(\lambda(z_v)) \neq 1$.*

iv) $\sum_{\lambda(z_v)\in L_v} \psi_v(\lambda(z_v)) = 0$.

v) $$\sum_{\lambda(z_v)\in L_v} \psi_v(\lambda(z_v)\alpha(z_v)) = \begin{cases} q^{vd}, & \text{if } \alpha(z_v) = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Property i) follows from definitions. The linearity of τ_v and i) implies that ψ_v is a group homomorphism. For $a \in \boldsymbol{\mu}_p$, there exists $b \in \mathbb{F}_p$ such that $a = \zeta_p^b$. Since τ_v is onto. there is then a $\lambda(z_v) \in L_v$ such that $\tau_v(\lambda(z_v)) = b$ and, therefore, $\psi_v(\lambda(z_v)) = a$. That is, ψ_v is a epimorphism of groups, which proves ii). From the above, iii) is immediate. To prove iv), let us observe that from iii) there is a $\alpha(z_v) \in L_v$ such that $\psi_v(\alpha(z_v)) \neq 1$. So that

$$\begin{aligned} \psi_v(\alpha(z_v)) \sum_{\lambda(z_v)\in L_v} \psi_v(\lambda(z_v)) &= \sum_{\lambda(z_v)\in L_v} \psi_v(\alpha(z_v)+\lambda(z_v)) \\ &= \sum_{\lambda(z_v)\in L_v} \psi_v(\lambda(z_v)), \end{aligned}$$

where we use ii) and the fact that when $\lambda(z_v)$ runs over L_v so does $\alpha(z_v) + \lambda(z_v)$. From this it follows

$$\{\psi_v(\alpha(z_v)) - 1\} \sum_{\lambda(z_v)\in L_v} \psi_v(\lambda(z_v)) = 0 \ .$$

Consequently, $\sum_{\lambda(z_v)\in L_v} \psi_v(\lambda(z_v)) = 0$.

To prove v), let us take $\alpha(z_v) = \alpha_0 + \alpha_1 z_v + \cdots + \alpha_{v-1} z_v^{v-1}$ and $\lambda(z_v) = \lambda_0 + \lambda_1 z_v + \cdots + \lambda_{v-1} z_v^{v-1}$. Then we have $\alpha(z_v)\lambda(z_v) = \alpha_0\lambda_0 + (\alpha_0\lambda_1 + \alpha_1\lambda_0)z_v + \cdots + (\sum_{k=0}^{v-1} \alpha_k\lambda_{v-1-k})z_v^{v-1}$, since $z_v^k = 0$ if $k \geq v$. Therefore,

$$\begin{aligned}
\sum_{\lambda(z_v)\in L_v} \psi_v(\alpha(z_v)\lambda(z_v)) &= \sum_{\lambda(z_v)\in L_v} \zeta_p^{\tau_v(\alpha(z_v)\lambda(z_v))} \\
&= \sum_{\lambda(z_v)\in L_v} \zeta_p^{\tau'(\sum_{k=0}^{v-1} \alpha_k\lambda_{v-1-k})} \\
&= \sum_{\lambda(z_v)\in L_v} \zeta_p^{\sum_{k=0}^{v-1} \tau'(\alpha_k\lambda_{v-1-k})} \\
&= \sum_{\lambda(z_v)\in L_v} \zeta_p^{\tau'(\lambda_0\alpha_{v-1})} \cdots \zeta_p^{\tau'(\lambda_{v-1}\alpha_0)} \ .
\end{aligned}$$

This last sum equals the sum over all v–uples $(\lambda_0, \lambda_1, \cdots, \lambda_{v-1})$ where $\lambda_i \in L_v$. From this it follows that:

$$\begin{aligned}
&\sum_{\lambda(z_v)\in L_v} \zeta_p^{\tau'(\lambda_0\alpha_{v-1})} \cdots \zeta_p^{\tau'(\lambda_{v-1}\alpha_0)} \\
&\qquad = \sum_{(\lambda_0,\lambda_1,\cdots,\lambda_{v-1})} \zeta_p^{\tau'(\lambda_0\alpha_{v-1})} \cdots \zeta_p^{\tau'(\lambda_{v-1}\alpha_0)} \\
&\qquad = \sum_{\lambda_0\in L} \zeta_p^{\tau'(\lambda_0\alpha_{v-1})} \cdots \sum_{\lambda_{v-1}\in L} \zeta_p^{\tau'(\lambda_{v-1}\alpha_0)} \\
&\qquad = \sum_{\lambda_0\in L} e(\lambda_0\alpha_{v-1}) \cdots \sum_{\lambda_{v-1}\in L} e(\lambda_{v-1}\alpha_0) \\
&\qquad = q^{vd} \, ,
\end{aligned}$$

when $\alpha_0 = \cdots = \alpha_{v-1} = 0$, and 0 otherwise, making use of proposition 9. □

Next we extend functions τ_v and ψ_v to Λ, by defining

$$\tau^*(\boldsymbol{\lambda}(z_v)) := \sum_{i=1}^{r} \tau_{v_i}(\lambda(z_{v_i}))\,, \tag{10}$$

where $\lambda(z_{v_i}) \in L_{v_i}$ and τ_{v_i} is the corresponding τ function on each L_{v_i}, $i = 1, \cdots, r$. In this way we obtain the following analogous to proposition 8.

Proposition 11. *The function τ^* is a $\mathbb{F}_p$–linear mapping from Λ onto $\mathbb{F}_p$.*

To extend ψ_v we define the function $\psi^* : \bigoplus_{i=1}^{r} L_{v_i} \to \boldsymbol{\mu}_p$ by

$$\begin{aligned} \psi^*(\boldsymbol{\lambda}(z_v)) : &= \zeta_p^{\tau^*(\boldsymbol{\lambda}(z_v))} = \zeta_p^{\sum_{i=1}^{r} \tau_{v_i}(\lambda(z_{v_i}))} \\ &= \zeta_p^{\tau_{v_1}(\lambda(z_{v_1}))} \zeta_p^{\tau_{v_r}(\lambda(z_{v_r}))} \\ &= \psi_{v_1}(\lambda(z_{v_1})) \cdots \psi_{v_r}(\lambda(z_{v_r}))\,. \end{aligned}$$

In the following proposition we prove some of their properties.

Proposition 12. *The function ψ^* satisfies the following properties:*

i) $\psi^*(0, \cdots, 0) = 1$.

ii) *ψ^* is an epimorphism of the additive group of Λ onto the multiplicative group $\boldsymbol{\mu}_p$.*

iii) *There exists $\boldsymbol{\lambda}(z_v) \in L_v$ such that $\psi^*(\boldsymbol{\lambda}(z_v)) \neq 1$.*

iv) $\sum_{\boldsymbol{\lambda}(z_v) \in \Lambda} \psi^*(\boldsymbol{\lambda}(z_v)) = 0$.

v) $$\sum_{\boldsymbol{\lambda}(z_v) \in \Lambda} \psi^*(\boldsymbol{\lambda}(z_v)\boldsymbol{\alpha}(z_v)) = \begin{cases} q^m, & \text{if } \boldsymbol{\alpha}(z_v) = 0, \\ 0, & \text{otherwise.} \end{cases}$$

where $m = d_1 v_1 + \cdots + d_r v_r$.

Proof. Part i) follows immediately from the definition of ψ^*. Parts ii) and iii) follow from the fact that the function τ_{v_1} is onto (Proposition 8). To prove iv) we use iii). In v), the sum is q^m if $\boldsymbol{\alpha}(z_v) = 0$. So we only need to consider the case $\alpha(z_{v_i}) \neq 0$ for some i. Thus

$$
\begin{aligned}
&\sum_{\boldsymbol{\lambda}(z_v)\in\Lambda} \psi^*(\boldsymbol{\lambda}(z_v)\,\boldsymbol{\alpha}(z_v)) \\
&\quad= \sum_{\boldsymbol{\lambda}(z_v)\in\Lambda} \psi_{v_1}(\lambda(z_{v_1})\,\alpha(z_{v_1}))\cdots\psi_{v_i}(\lambda(z_{v_i})\,\alpha(z_{v_i}))\cdots \\
&\qquad\qquad \times \psi_{v_r}(\lambda(z_{v_r})\,\alpha(z_{v_r})) \\
&\quad= \sum_{(\lambda(z_{v_1}),\cdots,\lambda(z_{vr}))\in\Lambda} \psi_{v_1}(\lambda(z_{v_1})\,\alpha(z_{v_1}))\cdots\psi_{v_i}(\lambda(z_{v_i})\,\alpha(z_{v_i}))\cdots \\
&\qquad\qquad \times \psi_{v_r}(\lambda(z_{v_r})\,\alpha(z_{v_r})) \\
&\quad= \sum_{\lambda(z_{v_1})\in L_{v_1}} \psi_{v_1}(\lambda(z_{v_1})\,\alpha(z_{v_1}))\cdots \sum_{\lambda(z_{v_i})\in L_{v_i}} \psi_{v_i}(\lambda(z_{v_i})\,\alpha(z_{v_i}))\cdots \\
&\qquad\qquad \times \sum_{\lambda(z_{vr})\in L_{v_r}} \psi_{v_r}(\lambda(z_{v_r})\,\alpha(z_{v_r})) \\
&\quad= 0\,,
\end{aligned}
$$

where we use the fact that $\alpha(z_{v_i}) \neq 0$ and Proposition 10,v). □

Next we show the existence of finite Fourier series for the arithmetical modular functions. To begin with, for $\alpha(z_v) \in L_v$ we define

$$\varepsilon_{\sigma(z_v)}(\alpha(z_v)) := \psi_v(\alpha(z_v)\,\sigma(z_v))\,.$$

The next proposition contains the most relevant properties $\varepsilon_{\sigma(z_v)}$.

Proposition 13. *If $\alpha(z_v)$, $\beta(z_v)$, $\gamma(z_v)$, $\sigma(z_v)$ and $\sigma_1(z_v) \in L_v$, we have:*

i) $\varepsilon_{\sigma(z_v)}(\alpha(z_v)) = \varepsilon_{\alpha(z_v)}(\sigma(z_v))$.

ii) $\varepsilon_{\sigma(z_v)}(\alpha(z_v) + \beta(z_v)) = \varepsilon_{\sigma(z_v)}(\alpha(z_v))\varepsilon_{\sigma(z_v)}(\beta(z_v))$.

iii) $\varepsilon_{\sigma(z_v)+\sigma_1(z_v)}(\alpha(z_v)) = \varepsilon_{\sigma(z_v)}(\alpha(z_v))\varepsilon_{\sigma_1(z_v)}(\alpha(z_v))$.

iv) $\varepsilon_{\sigma(z_v)}(\alpha(z_v)) = \varepsilon_{\sigma_1(z_v)}(\alpha(z_v))$ *if, and only if,* $\sigma(z_v) = \sigma_1(z_v)$.

v)

$$
\begin{aligned}
&(\varepsilon_{\sigma(z_v)} \cdot \varepsilon_{\sigma_1(z_v)})(\alpha(z_v)) \\
&\qquad := \sum_{\alpha(z_v)=\beta(z_v)+\gamma(z_v)} \varepsilon_{\sigma(z_v)}(\beta(z_v))\,\varepsilon_{\sigma_1(z_v)}(\gamma(z_v)) \\
&\qquad = \begin{cases} q^{vd}\varepsilon_{\sigma(z_v)}(\alpha(z_v)), & \text{if } \sigma(z_v) = \sigma_1(z_v), \\ 0, & \text{otherwise.} \end{cases}
\end{aligned}
$$

Proof. The statements in i), ii) and iii), follow immediately from the properties of ψ_v as in Proposition 10. To prove iv), we use the result $\psi_v(-\alpha(z_v)) = \psi_v(\alpha(z_v))^{-1}$. To prove v), we observe that

$$\begin{aligned}
&\sum_{\alpha(z_v)=\beta(z_v)+\gamma(z_v)} \varepsilon_{\sigma(z_v)}(\beta(z_v))\,\varepsilon_{\sigma_1(z_v)}(\gamma(z_v)) \\
&\qquad = \sum_{\gamma(z_v)\in L_v} \varepsilon_{\sigma(z_v)}(\alpha(z_v)-\gamma(z_v))\,\varepsilon_{\sigma_1(z_v)}(\gamma(z_v)) \\
&\qquad = \sum_{\gamma(z_v)\in L_v} \varepsilon_{\sigma(z_v)}(\alpha(z_v))\,\varepsilon_{\sigma(z_v)}(-\gamma(z_v))\,\varepsilon_{\sigma_1(z_v)}(\gamma(z_v)) \\
&\qquad = \sum_{\gamma(z_v)\in L_v} \varepsilon_{\sigma(z_v)}(\alpha(z_v))\,\varepsilon_{\sigma_1(z_v)-\sigma(z_v)}(\gamma(z_v)) \\
&\qquad = \varepsilon_{\sigma(z_v)}(\alpha(z_v)) \sum_{\gamma(z_v)\in L_v} \varepsilon_{\sigma_1(z_v)-\sigma(z_v)}(\gamma(z_v)) \\
&\qquad = \varepsilon_{\sigma(z_v)}(\alpha(z_v)) \sum_{\gamma(z_v)\in L_v} \psi_v[(\sigma_1(z_v)-\sigma(z_v))\gamma(z_v)] \\
&\qquad = \varepsilon_{\sigma(z_v)}(\alpha(z_v))\,q^{vd}\,,
\end{aligned}$$

when $\sigma_1(z_v) = \sigma(z_v)$ and 0 otherwise, according to Proposition 10,v. □

Since $\varepsilon_{\sigma(z_v)}$ depends on $\sigma(z_v)$, when this quantity runs over L_v, we see that at most there are q^{vd} functions of this type. The next Proposition will tell us that there are exactly q^{vd} of such functions.

Proposition 14. *The q^{vd} functions $\varepsilon_{\sigma(z_v)}$ are linearly independent.*

Proof. Let us consider the linear combination $g = \sum_{\sigma(z_v)\in L_v} a_{\sigma(z_v)}\varepsilon_{\sigma(z_v)}$ $= 0$ where $a_{\sigma(z_v)} \in \mathbb{C}$. Using v) in the last Proposition, we get

$$g\,\varepsilon_{\sigma_1(z_v)} = \sum_{\sigma(z_v)\in L_v} a_{\sigma(z_v)}(\varepsilon_{\sigma(z_v)} \cdot \varepsilon_{\sigma_1(z_v)}) = a_{\sigma_1(z_v)}\,q^{vd}\,\varepsilon_{\sigma_1(z_v)} = 0\,,$$

which requires that $a_{\sigma_1(z_v)} = 0$ since $\varepsilon_{\sigma_1(z_v)} \neq 0$ (by definition). □

Proposition 15. *If F is an arithmetical modular function over L_v, then uniquely we have*

$$F = \sum_{\sigma(z_v)\in L_v} f_{\sigma(z_v)}\,\varepsilon_{\sigma(z_v)}\,,$$

where

$$f_{\sigma(z_v)} = \frac{1}{q^{vd}} \sum_{\gamma(z_v)\in L_v} F(\gamma(z_v))\, \varepsilon_{\sigma(z_v)}(-\gamma(z_v))\,.$$

Proof. For $\alpha(z_v) \in L_v$, we get:

$$\begin{aligned}
&\sum_{\sigma(z_v)\in L_v} f_{\sigma(z_v)}\, \varepsilon_{\sigma(z_v)}(\alpha(z_v)) \\
&\qquad = \sum_{\sigma(z_v)\in L_v} \frac{1}{q^{vd}} \sum_{\gamma(z_v)\in L_v} F(\gamma(z_v))\, \varepsilon_{\sigma(z_v)}(-\gamma(z_v))\, \varepsilon_{\sigma(z_v)}(\alpha(z_v)) \\
&\qquad = \frac{1}{q^{vd}} \sum_{\sigma(z_v)\in L_v} \sum_{\gamma(z_v)\in L_v} F(\gamma(z_v))\, \varepsilon_{\sigma(z_v)}(\alpha(z_v) - \gamma(z_v)) \\
&\qquad = \frac{1}{q^{vd}} \sum_{\gamma(z_v)\in L_v} F(\gamma(z_v)) \sum_{\sigma(z_v)\in L_v} \varepsilon_{\sigma(z_v)}(\alpha(z_v) - \gamma(z_v)) \\
&\qquad = \frac{1}{q^{vd}} \sum_{\gamma(z_v)\in L_v} F(\gamma(z_v)) \sum_{\sigma(z_v)\in L_v} \psi_v(\sigma(z_v)(\alpha(z_v) - \gamma(z_v)) \\
&\qquad = F(\alpha(z_v))\,,
\end{aligned}$$

according to Proposition 10,v). □

This Proposition shows that for each arithmetical function F defined on L_v, there is a finite Fourier expansion with respect to the $\mathbb{C}$-base $\varepsilon_{\sigma(z_v)}$:

$$(F \cdot G)(\alpha(z_v)) := \sum_{\alpha(z_v)=\beta(z_v)+\gamma(z_v)} F(\beta(z_v))\, G(\gamma(z_v))\,.$$

If for $\boldsymbol{\alpha}(z_v) \in \Lambda$ we define

$$\varepsilon_{\boldsymbol{\sigma}(z_v)}(\boldsymbol{\alpha}(z_v)) := \psi^*(\boldsymbol{\alpha}(z_v)\, \boldsymbol{\sigma}(z_v))\,,$$

we obtain for Λ analogous to Propositions 13, 14 and 15, and whose proofs are similar.

Thus, similarly, for each arithmetical function F on Λ, there is a finite Fourier expansion with respect to the $\mathbb{C}$–base $\varepsilon_{\boldsymbol{\sigma}(\boldsymbol{z_v})}$ of the $\mathbb{C}$–algebra of arithmetical functions defined on Λ, where

$$(F \cdot G)(\boldsymbol{\alpha}(z_v)) := \sum_{\boldsymbol{\alpha}(z_v)=\boldsymbol{\beta}(z_v)+\boldsymbol{\gamma}(z_v)} F(\boldsymbol{\beta}(z_v))\, G(\boldsymbol{\gamma}(z_v))\,.$$

3 Gauss and Ramanujan sums in L_v

A Gauss sum is an expression of the form

$$g_v(\beta(z_v);\, \chi) := \sum_{\alpha(z_v)\in L_v^\times} \chi(\alpha(z_v))\, \psi_v(\alpha(z_v)\, \beta(z_v))\,,$$

where χ is a character of L_v. This sum is taken over the invertible elements of L_v. Next we prove some basic properties of these sums.

Proposition 16. *Let χ be a character of L_v and $\beta(z_v) \in L_v^\times$. Then*

$$g_v(\beta(z_v);\, \chi) = \overline{\chi}(\beta(z_v))\, g_v(1;\, \chi)\,.$$

Proof. For a character χ of L_v, $\chi(\beta(z_v))\overline{\chi}(\beta(z_v)) = 1$, if $\beta(z_v) \in L_v^\times$. Therefore,

$$\chi(\alpha(z_v)) = \chi(\alpha(z_v))\, \chi(\beta(z_v))\, \overline{\chi}(\beta(z_v)) = \chi(\alpha(z_v)\, \beta(z_v))\, \overline{\chi}(\beta(z_v))\,.$$

From this the result follows easily. □

A Gauss sum is said to be separable if

$$g_v(\beta(z_v);\, \chi) = \overline{\chi}(\beta(z_v))\, g_v(1; \chi)\,.$$

The above Proposition shows that $g_v(\beta(z_v); \chi)$ is separable if $\beta(z_v) \in L_v^\times$. When $\beta(z_v) \notin L_v^\times$, we get the following result

Proposition 17. *If χ is a character of L_v and $\beta(z_v) \notin L_v^\times$, the sum $g_v(\beta(z_v); \chi)$ is separable if, and only if, $g_v(\beta(z_v); \chi) = 0$*

Proof. By definition, $\overline{\chi}(\beta(z_v)) = 0$ if $\beta(z_v) \notin L_v^\times$. Consequently, $g_v(\beta(z_v); \chi) = 0$ if, and only if, $g_v(\beta(z_v); \chi) = \overline{\chi}(\beta(z_v))g_v(1; \chi)$, that is, if, and only if, $g_v(\beta(z_v); \chi)$ is separable. □

Proposition 18. *Given a Gauss sum g_v and χ a character of L_v, we have*

$$g_v(\beta(z_v);\chi) = \begin{cases} q^{d(v-1)}(q^d-1), & si\ \chi=\chi_0\ and\ \beta(z_v)=0, \\ 0, & si\ \chi=\chi_0\ and\ \beta(z_v)\neq 0, \\ 0, & si\ \chi\neq\chi_0\ and\ \beta(z_v)=0, \\ \overline{\chi}(\beta(z_v))g_v(1,\chi), & \chi\neq\chi_0\ and\ \beta(z_v)\in L_v^\times\ . \end{cases}$$

Proof. The proof follows from the definition of the principal character, Proposition 10, Proposition 5 and Proposition 16, respectively. □

Proposition 19. *If $g_v(\alpha(z_v);\chi)$ is separable and $\chi\neq\chi_0$, then*

$$|g_v(1;\,\chi)|^2 = \text{Card}\ L_v = q^{vd}\,.$$

Proof. We have

$$\begin{aligned} |g_v(1;\,\chi)|^2 &= g_v(1;\,\chi)\,\overline{g_v(1;\,\chi)} \\ &= g_v(1;\,\chi)\sum_{\alpha(z_v)\in L_v}\overline{\chi}(\alpha(z_v))\,\overline{\psi_v(\alpha(z_v))} \\ &= g_v(1;\,\chi)\sum_{\alpha(z_v)\in L_v}\overline{\chi}(\alpha(z_v))\,\psi_v(-\alpha(z_v)) \\ &= \sum_{\alpha(z_v)\in L_v} g_v(1;\,\chi)\,\overline{\chi}(\alpha(z_v))\,\psi_v(-\alpha(z_v)) \\ &= \sum_{\alpha(z_v)\in L_v} g_v(\alpha(z_v);\,\chi)\,\psi_v(-\alpha(z_v)) \\ &= \sum_{\alpha(z_v)\in L_v}\sum_{\beta(z_v)\in L_v}\chi(\beta(z_v))\,\psi_v(\alpha(z_v)\,\beta(z_v))\,\psi_v(-\alpha(z_v)) \\ &= \sum_{\alpha(z_v)\in L_v}\sum_{\beta(z_v)\in L_v}\chi(\beta(z_v))\,\psi_v(\alpha(z_v)\,(\beta(z_v)-1)) \\ &= \sum_{\beta(z_v)\in L_v}\chi(\beta(z_v))\sum_{\alpha(z_v)\in L_v}\psi_v(\alpha(z_v))(\beta(z_v)-1)) \\ &= \chi(1)q^{vd} = \text{Card}\,L_v\,, \end{aligned}$$

if $\beta(z_v)=1$, according to Proposition 10,v. □

Example: For $\chi\neq\chi_0$, let us take $\gamma(z_v)\in L_v^\times$. From the Gauss sum definition is easy to see that in each summand we can replace $\alpha(z_v)$ by $\gamma(z_v)\alpha(z_v)$ without altering the value of the sum. Thus

$$\begin{aligned}\overline{g_v(1;\,\chi)} &= \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\alpha(z_v)\,\gamma(z_v))\,\overline{\psi_v}(\gamma(z_v)\alpha(z_v)) \\ &= \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\alpha(z_v))\,\overline{\chi}(\gamma(z_v))\,\overline{\psi_v}(\gamma(z_v)\alpha(z_v)) \\ &= \overline{\chi}(\alpha(z_v)) \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\gamma(z_v))\,\overline{\psi_v}(\gamma(z_v)\,\alpha(z_v))\,.\end{aligned}$$

Using Proposition 19, we obtain

$$\begin{aligned}\chi(\alpha(z_v))\,q^{vd} &= \chi(\alpha(z_v))\,g_v(1;\,\chi)\,\overline{g_v(1;\,\chi)} \\ &= \chi(\alpha(z_v))\,g_v(1;\,\chi)\,\overline{\chi}(\alpha(z_v)) \\ &\qquad \times \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\gamma(z_v))\,\overline{\psi_v}(\gamma(z_v)\,\alpha(z_v)) \\ &= g_v(1;\,\chi) \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\gamma(z_v))\,\overline{\psi_v}(\gamma(z_v)\,\alpha(z_v))\,.\end{aligned}$$

From this it follows that

$$\chi(\alpha(z_v)) = \frac{g_v(1;\,\chi)}{q^{vd}} \sum_{\gamma(z_v)\in L_v} \overline{\chi}(\gamma(z_v))\,\overline{\psi_v}(\gamma(z_v)\,\alpha(z_v))\,.$$

If $\alpha(z_v) = 0$, and since $\chi(\alpha(z_v)) = 0$, and $\sum_{\gamma(z_v)\in L_v} \overline{\chi}(\gamma(z_v)) = 0$ the equality is preserved. The above expression is the expansion in a finite Fourier series of $\chi(\alpha(z_v))$.

The following expression is called a Ramanujan sum:

$$c_v(\beta(z_v)) = \sum_{\alpha(z_v)\in L_v^{\times}} \psi_v[\alpha(z_v)\,\beta(z_v)].$$

Let us remark that if we take $\chi = \chi_0$ in the definition of a Gauss sum we see that a Ramanujan sum is a special case of a Gauss sum, and the following Proposition can be easily proved.

Proposition 20.

i) $c_v(0) = \text{Card}\, L_v^{\times}$.

ii) $c_v(\alpha(z_v)\beta(z_v)) = c_v(\beta(z_v))$ *if* $\alpha(z_v) \in L_v^{\times}$.

Now we define Gauss and Ramanujan sums in Λ. For a Gauss sum we set

$$g_h(\boldsymbol{\beta}(z_v));\, \chi) = \sum_{\boldsymbol{\alpha}(z_v)\in\Lambda^\times} \chi(\boldsymbol{\alpha}(z_v))\, \psi^*(\boldsymbol{\alpha}(z_v)\, \boldsymbol{\beta}(z_v))\,,$$

where χ is a character of Λ.

From the characterization done in Proposition 3, we obtain

$$\begin{aligned} &g_h(\boldsymbol{\beta}(z_v));\, \chi) \\ &\qquad = \sum_{\boldsymbol{\alpha}(z_v)\in\Lambda^\times} \chi(\boldsymbol{\alpha}(z_v))\, \psi^*(\boldsymbol{\alpha}(z_v)\, \boldsymbol{\beta}(z_v)) \\ &\qquad = g_{v_1}(\beta(z_{v_1}));\, \chi_1) \cdots g_{v_i}(\beta(z_{v_i}));\, \chi_i) \cdots g_{v_r}(\beta(z_{v_r}));\, \chi_r)\,, \end{aligned}$$

where $\chi = \prod_{i=1}^r \chi_i$.

Taking $\chi = \chi_0$ in the above definition we obtain the definition of a Ramanujan sum over Λ

$$c_h(\boldsymbol{\beta}(z_v)) = \sum_{\boldsymbol{\alpha}(z_v)\in\Lambda^\times} \psi^*(\boldsymbol{\alpha}(z_v)\, \boldsymbol{\beta}(z_v))\,.$$

4 Applications

In this section we use the above results to extend some classical results of Libri [18, 19, 13]) on the number of integral solutions of algebraic equations with coefficients in the ring of integers. This extension will allow us, in the first place, to compute the number of solutions of some algebraic algebraic equations with coefficients in L_v and Λ. In the second place, we extend a result on partitions due to Nageswara Rao in the case of the ring of polynomials $\mathbb{F}_q[X]$ to the algebra L_v [21].

Before going further, let us recall that if N_v represents the number of solutions in L_v^n of the algebraic equation

$$f(t_1, \cdots, t_n) = 0\,,$$

where $f(t_1, \cdots, t_n) \in L[[Z]][t_1, \cdots, t_n]$, the expression

$$1 + \sum_{v=1}^{\infty} N_v\, T^v\,,$$

is called the *Poincaré series of the polynomial* $f(t_1, \cdots, t_n)$. It has been conjectured, as in the rational case (proved by Igusa [1, 3], that this series is always the quotient $\dfrac{R(T)}{Q(R)}$ of two polynomials $R(T)$, $Q(T) \in \mathbb{Z}[T]$. As a consequence of the following results we can verify that this is so in the cases considered here.

4.1 An analogous of an old result of Libri [18, 19, 13]

The analogous that theoretically allows us to compute N_v for each v, is the following

Proposition 21. *Let* $F(t_1, \cdots, t_n) \in L_v[t_1, \cdots, t_n]$ *and let* N_v *be the number of solutions of the equation* $F(t_1, \cdots, t_n) = 0$. *Then*

$$\begin{aligned} N_v &= \frac{1}{q^{vd}} \sum_{\alpha(z_v)\in L_v} \sum_{t_1\in L_v} \cdots \sum_{t_n\in L_v} \psi_v[\alpha(z_v)\, F(t_1, \cdots, t_n)] \\ &= \frac{1}{q^{vd}} \sum_{\alpha(z_v)\in L_v} \sum_{(t_1,t_2,\cdots,t_n)\in L_v^n} \psi_v[\alpha(z_v)\, F(t_1, \cdots, t_n)]\,. \end{aligned}$$

Proof. The right hand side of this equation can be written as

$$\begin{aligned} &\frac{1}{q^{vd}} \sum_{\alpha(z_v)\in L_v} \left\{ \sum_{\substack{(t_1,\cdots,t_n)\in L_v^n \\ F(t_1,\cdots,t_n)=0}} \psi_v[\alpha(z_v)\, F(t_1, \cdots, t_n)] \right. \\ &\qquad\qquad \left. + \sum_{\substack{(t_1,\cdots,t_n)\in L_v^n \\ F(t_1,\cdots,t_n)\neq 0}} \psi_v[\alpha(z_v)\, F(t_1, \cdots, t_n)] \right\} \\ = \;& \frac{1}{q^{vd}} \sum_{\alpha(z_v)\in L_v} N_v + \left\{ \sum_{\substack{(t_1,\cdots,t_n)\in L_v^n \\ F(t_1,\cdots,t_n)\neq 0}} \sum_{\alpha(z_v)\in L_v} \psi_v[\alpha(z_v)\, F(t_1, \cdots, t_n)] \right\} \\ = \;& N_v\,, \end{aligned}$$

where we have used Proposition 10, v). □

For each $\alpha(z_v) \in L_v$ we define $w(\alpha(z_v))$ to be the smallest exponent of the powers of z_v which appear in $\alpha(z_v) \neq 0$ and $w(0) = 0$. Thus $0 \leqslant w(\alpha(z_v)) \leqslant v - 1$. From this definition, if $\alpha(z_v) \in L_v^{\times}$, $w(\alpha(z_v)) = 0$

since $\alpha_0 \neq 0$; on the other hand, if $w(\alpha(z_v)) \neq 0$, we have $\alpha(z_v) \notin L_v^\times$ and $\alpha(z_v) \neq 0$.

Proposition 22. *Let $\alpha(z_v) \in L_v$, $w(\alpha(z_v)) = j$, and $\gamma(z_v) = \gamma_0 + \gamma_1 z_v + \cdots + \gamma_{v-j} z_v^{v-j} + \cdots + \gamma_{v-1} z_v^{v-1}$ be such that $\alpha(z_v)\gamma(z_v) = 0$. Then $\gamma_0 = \gamma_1 = \cdots = \gamma_{v-j-1} = 0$. That is to say, $\gamma(z_v) = \gamma_{v-j} z_v^{v-j} + \cdots + \gamma_{v-1} z_v^{v-1}$.*

Proof. Since $w(\alpha(z_v)) = j$ we have $\alpha(z_v) = \alpha_j z_v^j + \cdots + \alpha_{v-1} z_v^{v-1}$, where the $\alpha_i \in L$, $i = j, \cdots, v-1$ and $\alpha_j \neq 0$. Doing the product and making it equal to zero we obtain:

$$\begin{aligned} \gamma_0\,\alpha_j &= 0\,, \\ \gamma_0\,\alpha_{j+1} + \gamma_1\,\alpha_j &= 0\,, \\ &\vdots \\ \gamma_0\,\alpha_{v-1} + \gamma_1\,\alpha_{v-2} + \cdots + \gamma_{v-j-1}\,\alpha_j &= 0\,, \end{aligned}$$

recalling that $z_v^t = 0$ if $t \geqslant v$. Since $\alpha_j \neq 0$, from the first equation it follows tha $\gamma_0 = 0$. From the second one we obtain $\gamma_1 = 0$ since $\gamma_0 = 0$ and $\alpha_j \neq 0$. Recurrently we get $\gamma_0 = \gamma_1 = \cdots = \gamma_{v-j-1} = 0$. Let us remark that the values taken by γ_k for $k \geqslant v - j$ do not matter, and that when these values are null they show that L_v has zero divisors. □

Next we apply Proposition 21 to the simplest case of linear equations.

Proposition 23. *Let $F(t) = \alpha(z_v)t + \beta(z_v) \in L_v[t]$, $\alpha(z_v) \neq 0$, $w(\alpha(z_v)) = j$ and let N_v be the number of solutions of the equation $F(t) = 0$ Then*

$$N_v = \begin{cases} q^{dj}, & \text{if } j > 0 \text{ and } \beta(z_v) = 0, \\ q^{dj}, & \text{if } j \geqslant 0 \text{ and } w(\beta(z_v)) \geqslant j, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. From the above Proposition we get

$$\begin{aligned} q^{vd}\, N_v &= \sum_{\gamma(z_v)\in L_v} \sum_{t\in L_v} \psi_v[\gamma(z_v)\, F(t)] \\ &= \sum_{\gamma(z_v)\in L_v} \sum_{t\in L_v} \psi_v[\gamma(z_v)\, (\alpha(z_v)\, t + \beta(z_v))] \\ &= \sum_{\gamma(z_v)\in L_v} \sum_{t\in L_v} \psi_v[\gamma(z_v)\, \alpha(z_v)\, t]\, \psi_v[\gamma(z_v)\, \beta(z_v)] \\ &= \sum_{\gamma(z_v)\in L_v} \psi_v[\gamma(z_v)\, \beta(z_v)] \sum_{t\in L_v} \psi_v[\gamma(z_v)\, \alpha(z_v)\, t] \\ &= \sum_{\substack{\gamma(z_v)\in L_v \\ \gamma(z_v)\alpha(z_v)=0}} \psi_v[\gamma(z_v)\, \beta(z_v)]\, q^{vd}\,. \end{aligned} \tag{11}$$

Since $w(\alpha(z_v)) = j$ we have $\alpha(z_v) = \alpha_j z_v^j + \cdots + \alpha_{v-1} z_v^{v-1}$ where the $\alpha_i \in L$, $i = j, \cdots, v-1$, and $\alpha_j \neq 0$. From Proposition 22 we get $\gamma(z_v) = \gamma_{v-j} z_v^{v-j} + \cdots + \gamma_{v-1} z_v^{v-1}$ and a simple count shows that there are q^{dj} of these $\gamma(z_v)$, i.e, the sum (11) has q^{dj} summands.

If $F(t) = 0$ has a solution, then there exists $\sigma(z_v) \in L_v$ such that $\alpha(z_v)\sigma(z_v) + \beta(z_v) = 0$, hence $\beta(z_v) = -\alpha(z_v)\sigma(z_v)$. Therefore, $w(\beta(z_v)) = w(\alpha(z_v)\sigma(z_v))$. If we take $w(\sigma(z_v)) = k$, and since $w(\alpha(z_v)) = j$ we have $\beta(z_v) = 0$ or $w(\beta(z_v)) \geqslant j$. Indeed, $\alpha(z_v)\sigma(z_v) = 0$ if $k + j \geqslant v$ since $z_v^t = 0$ for all $t \geqslant v$; otherwise, $z_v^{k+j} \neq 0$ and $w(\beta(z_v)) = k + j \geqslant j$. Replacing the value $\beta(z_v)$ in the sum (11) we obtain:

$$\begin{aligned} &\sum_{\substack{\gamma(z_v)\in L_v \\ \gamma(z_v)\alpha(z_v)=0}} \psi_v[\gamma(z_v)\, \beta(z_v)]\, q^{vd} \\ &\qquad = \sum_{\substack{\gamma(z_v)\in L_v \\ \gamma(z_v)\alpha(z_v)=0}} \psi_v[\gamma(z_v)\, (-\alpha(z_v)\, \sigma(z_v))]\, q^{vd} \\ &\qquad = \sum_{\substack{\gamma(z_v)\in L_v \\ \gamma(z_v)\alpha(z_v)=0}} \psi_v[-(\gamma(z_v)\, \alpha(z_v))\, \sigma(z_v)]\, q^{vd} \\ &\qquad = q^{vd}\, q^{dj}\,, \end{aligned}$$

and therefore $N_v = q^{dj}$. □

Proposition 24. *Let*

$$F(t_1, \cdots, t_n) = \beta(z_v) + \alpha_1(z_v)\, t_1 + \cdots + \alpha_n(z_v)\, t_n \in L_v[t_1, \cdots, t_n]\,,$$

$w(\alpha_i(z_v)) = j_i$, $j = \operatorname{mn}\{j_i\}$, $i = 1, \cdots, n$ *and let* N_v *be the number of solutions of equation* $F(t_1, \cdots, t_n) = 0$. *Then*

$$N_v = \begin{cases} q^{dj}(q^{vd})^{n-1}, & \text{if } j > 0 \text{ and } \beta(z_v) = 0, \\ q^{dj}(q^{vd})^{n-1}, & \text{if } j \geqslant 0 \text{ and } w(\beta(z_v)) \geqslant j\ , \\ 0, & \text{otherwise.} \end{cases}$$

Proof. By Proposition 21 we have

$$\begin{aligned}
&q^{vd}\, N_v \\
&\quad = \sum_{\gamma(z_v)\in L_v} \sum_{t_1\in L_v} \cdots \sum_{t_n\in L_v} \psi_v[\gamma(z_v)\, F(t_1, \cdots, t_n)] \\
&\quad = \sum_{\gamma(z_v)\in L_v} \sum_{t_1\in L_v} \cdots \sum_{t_n\in L_v} \psi_v[\gamma(z_v) \\
&\qquad \times (\beta(z_v) + \alpha_1(z_v)\, t_1 + \cdots + \alpha_n(z_v)\, t_n)] \\
&\quad = \sum_{\gamma(z_v)\in L_v} \sum_{t_1\in L_v} \cdots \sum_{t_n\in L_v} \psi_v[\gamma(z_v)\, \beta(z_v)]\, \psi_v[\gamma(z_v)\, \alpha_1(z_v)\, t_1] \cdots \\
&\qquad \times \psi_v[\gamma(z_v)\, \alpha_n(z_v)\, t_n] \\
&\quad = \sum_{\gamma(z_v)\in L_v} \psi_v[\gamma(z_v)\, \beta(z_v)] \sum_{t_1\in L_v} \psi_v[\gamma(z_v)\, \alpha_1(z_v)\, t_1] \cdots \\
&\qquad \times \sum_{t_n\in L_v} \psi_v[\gamma(z_v)\, \alpha_n(z_v)\, t_n] \\
&\quad = \sum_{\gamma(z_v)\in L_v} \psi_v[\gamma(z_v)\, \beta(z_v)] \cdots \\
&\qquad \times \sum_{\substack{t_{n-1}\in L_v \\ \alpha_n(z_v)\gamma(z_v)=0}} \psi_v[\gamma(z_v)\, \alpha_{n-1}(z_v)\, t_{n-1}]\, q^{vd} \\
&\quad = \sum_{\substack{\gamma(z_v)\in L_v \\ \alpha_1(z_v)\gamma(z_v)=0, \cdots, \alpha_n(z_v)\gamma(z_v)=0}} \psi_v[\gamma(z_v)\, \beta(z_v)]\, (q^{vd})^n\,, \qquad (12)
\end{aligned}$$

making reiterative use of Proposition 10,v. By Proposition 22, $w(\gamma(z_v)) = v - j$ and since $j = \operatorname{mn}\{j_i\}$, it is clear that $\alpha_i(z_v)\gamma(z_v) = 0$, $i = 1, \cdots, n$, and the sum (12) has thus q^{dj} summands.

If $F(t_1, \cdots, t_n) = 0$ has a solution then there exist $\sigma_1(z_v), \cdots, \sigma_n(z_v) \in L_v$ such that

$$\beta(z_v) = -(\alpha_1(z_v)\,\sigma_1(z_v) + \cdots + \alpha_n(z_v)\,\sigma_n(z_v))\,. \tag{13}$$

Therefore, $w(\beta(z_v)) = w(\alpha_1(z_v)\sigma_1(z_v) + \cdots + \alpha_n(z_v)\sigma_n(z_v))$. Let us put $w(\sigma_i(z_v)) = k_i$ and $k = \min\{k_i\}$, $i = 1, \cdots, n$. Since $w(\alpha_i(z_v)) \geq j$, we get $\beta(z_v) = 0$ or $w(\beta(z_v)) \geq j$. Indeed, $\alpha_i(z_v)\sigma_i(z_v) = 0$, $i = 1, \cdots, n$, if $k + j \geq v$ since $z_v^t = 0$ for all $t \geq v$ and therefore $\beta(z_v) = 0$; also it may happen that while doing all the sums in (13) we obtain 0 and thus $\beta(z_v) = 0$. Otherwise, there is a $z_v^r \neq 0$ with $k + j \leq r < v$, so that $w(\beta(z_v)) = r \geq j$. Replacing the value $\beta(z_v)$ in (12) we obtain $N_v = (q^{vd})^{n-1} q^{dj}$. □

Proposition 25. *Let* $F(t_1, \cdots, t_n) = \beta(z_v) + t_1 + \alpha_2(z_v)t_2^{k_2} + \cdots + \alpha_n(z_v)t_n^{k_n} \in L_v[t_1, \cdots, t_n]$, *where* k_i, $i = 2, \cdots, n$, *are positive integers and let* N_v *be the number of solutions of the equation* $F(t_1, \cdots, t_n) = 0$. *Then*

$$N_v = (q^{vd})^{n-1}\,.$$

Proof. Again by Proposition 21 we get

$$\begin{aligned} q^{vd}\,N_v &= \sum_{\gamma(z_v)\in L_v} \sum_{t_1\in L_v} \cdots \sum_{t_n\in L_v} \psi_v[\gamma(z_v) \\ &\qquad \times (\beta(z_v) + t_1 + \alpha_2(z_v)\,t_2^{k_2} + \cdots + \alpha_n(z_v)\,t_n^{k_n})] \\ &= \sum_{\gamma(z_v)\in L_v} \psi_v[\gamma(z_v)\,\beta(z_v)] \sum_{t_n\in L_v} \psi_v[\gamma(z_v)\,\alpha_n(z_v)\,t_n^{k_n}] \cdots \\ &\qquad \times \sum_{t_1\in L_v} \psi_v[\gamma(z_v)\,t_1] \\ &= (q^{vd})^n\,, \end{aligned}$$

if $\gamma(z_v) = 0$ according to Proposition 10,v. □

4.2 A result of Nageswara Rao

Let n be an integer greater than zero and let $n_1, \cdots, n_v$ be integers greater or equal to zero satisfying the condition $n = n_1 + \cdots + n_v$. Let us take $m_k = n_1 + \cdots + n_k$, $k = 1, \cdots, v$. For $\alpha(z_v) \in L_v$ let $N_v(\alpha(z_v))$ be the number of solutions $(\gamma_1(z_v), \cdots, \gamma_n(z_v))$ of the equation

$$\gamma_1(z_v) + \cdots + \gamma_n(z_v) = \alpha(z_v)\,,$$

satisfying:

$$\begin{aligned} w(\gamma_{j_1}(z_v)) &= 0\,, \\ w(\gamma_{j_2}(z_v)) &= 1\,, \\ &\vdots \\ w(\gamma_{j_v}(z_v)) &= v-1\,, \end{aligned}$$

with $j_1 = 1, \cdots, m_1,$, $\gamma_{j_1}(z_v) \neq 0$, $j_2 = m_1 + 1, \cdots, m_2$ and $j_v = m_{v-1} + 1, \cdots, m_v = n$.

Proposition 26. *With the above notations we have*

$$N_v(\alpha(z_v)) = \frac{1}{q^{vd}} \sum_{j=0}^{v-1} \left\{ \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau_j^*(z_{v-i+1})) \right\} c_{v-j}(\alpha^*(z_{v-j}))\,.$$

Proof. It is clear that $N_v(\cdot)$ is an arithmetical function. Thus by virtue of Proposition 15 we get:

$$N_v(\alpha(z_v)) = \sum_{\tau(z_v) \in L_v} f_{\tau(z_v)}\, \varepsilon_{\tau(z_v)}(\alpha(z_v))\,, \tag{14}$$

where $f_{\tau(z_v)} = \frac{1}{q^{vd}} \sum_{\beta(z_v) \in L_v} N(\beta(z_v)) \varepsilon_{\tau(z_v)}(-\beta(z_v))$, that is,

$$\begin{aligned} f_{\tau(z_v)} &= \frac{1}{q^{vd}} \sum_{\beta(z_v) \in L_v} N_v(\beta(z_v))\, \psi_v[-\tau(z_v)\, \beta(z_v)] \\ &= \frac{1}{q^{vd}} \sum_{\beta(z_v) \in L_v} \sum_{\substack{(\beta_1(z_v), \cdots, \beta_n(z_v)) \\ w(\beta_{j_i}(z_v)) = i-1}} \psi_v[-\tau(z_v) \\ &\qquad \times \beta_1(z_v) + \beta_2(z_v) + \cdots + \beta_n(z_v))]\,, \end{aligned}$$

where the sum is taken over the $(\beta_1(z_v), \cdots, \beta_n(z_v))$ satisfying

$$\beta(z_v) = \beta_1(z_v) + \beta_2(z_v) + \cdots + \beta_n(z_v)\,,$$

and

$$\begin{aligned} w(\beta_{j_1}(z_v)) &= 0\,, \\ w(\beta_{j_2}(z_v)) &= 1\,, \\ &\vdots \\ w(\beta_{j_v}(z_v)) &= v-1\,, \end{aligned}$$

with $j_1 = 1, \cdots, m_1$, $\beta_{j_1}(z_v) \neq 0$, $j_2 = m_1 + 1, \cdots, m_2$ and $j_v = m_{v-1} + 1, \cdots, m_v = n$, whose number is precisely $N_v(\beta(z_v))$. Using Proposition 10 we get:

$$f_{\tau(z_v)} = \frac{1}{q^{vd}} \sum_{\beta(z_v)\in L_v} \sum_{\substack{(\beta_1(z_v),\cdots,\beta_n(z_v)) \\ w(\beta_{j_i}(z_v))=i-1}} \prod_{k=1}^{n} \psi_v[-\tau(z_v)\,\beta_k(z_v)]\,.$$

Making $\beta_{j_i}(z_v) = \beta_{ji}(z_v)$ we can write

$$f_{\tau(z_v)} = \frac{1}{q^{vd}} \sum_{\substack{\beta_{ji}(z_v) \\ w(\beta_{ji}(z_v))=i-1}} \prod_{i=1}^{v} \prod_{j=1}^{n_i} \psi_v[-\tau(z_v)\,\beta_{ji}(z_v)]\,,$$

replacing $\beta_{ji}(z_v)$ by $\sigma(z_v) \in L_v$ such that $w(\sigma(z_v)) = i-1$ we obtain

$$\begin{aligned} f_{\tau(z_v)} &= \frac{1}{q^{vd}} \sum_{\substack{\sigma(z_v) \\ w(\sigma(z_v))=i-1}} \prod_{i=1}^{v} \prod_{j=1}^{n_i} \psi_v[-\tau(z_v)\sigma(z_v)] \\ &= \frac{1}{q^{vd}} \prod_{i=1}^{v} \prod_{j=1}^{n_i} \sum_{\substack{\sigma(z_v) \\ w(\sigma(z_v))=i-1}} \psi_v[-\tau(z_v)\,\sigma(z_v)]\,. \end{aligned} \tag{15}$$

Since $w(\sigma(z_v)) = i-1$, we see that $\sigma(z_v) = \sigma_{i-1} z_v^{i-1} + \cdots + \sigma_{v-1} z_v^{v-1}$ where $\sigma_{i-1} \neq 0$ and $\sigma_i, \cdots, \sigma_{v-1} \in L$ are arbitrary. If we take $\tau(z_v) = \tau_0 + \tau_1 z_v + \cdots + \tau_{v-1} z_v^{v-1}$ we have

$$\sigma(z_v)\,\tau(z_v) = \tau_0\,\sigma_{i-1}\,z_v^{i-1} + \cdots + \left(\sum_{k=0}^{v-i} \sigma_{v-k-1}\,\tau_k\right) z_v^{v-1}\,, \tag{16}$$

and applying ψ_v we arrive at

$$\psi_v[-\sigma(z_v)\,\tau(z_v)] = \zeta_p^{\mathrm{tr}_{L/\mathbb{F}_p}(-\sum_{k=0}^{v-i}\sigma_{v-k-1}\tau_k)}.$$

From here it is clear that in order to find the value of $\psi_v[-\sigma(z_v)\tau(z_v)]$ only the $v-i+1$ values $\tau_0,\tau_1,\cdots,\tau_{v-i}$ are relevant in the expression of $\tau(z_v)$, and the $v-i+1$ values $\sigma_{i-1},\cdots,\sigma_{v-1}$ in the expression of $\sigma(z_v)$. Moreover, all these values are arbitrary, with the exception de σ_{i-1}. Due to this fact, we will consider the following elements over L_{v-i+1},

$$\begin{aligned}\sigma^*(z_{v-i+1}) &= \sigma_{i-1}+\sigma_i z_{v-i+1}\cdots+\sigma_{v-1}z_{v-i+1}^{v-i}\,,\\ \tau^*(z_{v-i+1}) &= \tau_0+\tau_1 z_{v-i+1}+\cdots+\tau_{v-i}z_{v-i+1}^{v-i}\,,\end{aligned}$$

so that

$$\begin{aligned}\psi_{v-i+1}[-\sigma^*(z_{v-i+1})\,\tau^*(z_{v-i+1})] &= \zeta_p^{tr_{L/\mathbb{F}_p}(-\sum_{k=0}^{v-i}\sigma_{v-k-1}\tau_k)}\\ &= \psi_v[-\sigma(z_v)\,\tau(z_v)]\,.\end{aligned}$$

That is, we can replace the sum

$$\sum_{w(\sigma(z_v))=i-1}\psi_v[-\tau(z_v)\,\sigma(z_v)]\,,$$

of (15) by the sum

$$\sum_{w(\sigma^*(z_{v-i+1}))=0}\psi_{v-i+1}[-\tau^*(z_{v-i+1})\,\sigma^*(z_{v-i+1})]\,,$$

corresponding to the Ramanujan sum $c_{v-i+1}(\tau^*(z_{v-i+1}))$. From this we get

$$\begin{aligned}f_{\tau(z_v)} &= \frac{1}{q^{vd}}\prod_{i=1}^{v}\prod_{j=1}^{n_i}\sum_{w(\sigma^*(z_{v-i+1}))=0}\psi_{v-i+1}[-\tau^*(z_{v-i+1})\,\sigma^*(z_{v-i+1})]\\ &= \frac{1}{q^{vd}}\prod_{i=1}^{v}\prod_{j=1}^{n_i}c_{v-i+1}(\tau^*(z_{v-i+1}))\\ &= \frac{1}{q^{vd}}\prod_{i=1}^{v}c_{v-i+1}^{n_i}(\tau^*(z_{v-i+1}))\,. \qquad (17)\end{aligned}$$

Replacing (17) in (14) we obtain,

$$\begin{aligned} & N_v(\alpha(z_v)) \\ & = \frac{1}{q^{vd}} \sum_{\tau(z_v)\in L_v} \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau^*(z_{v-i+1}))\, \varepsilon_{\tau(z_v)}(-\alpha(z_v)) \\ & = \frac{1}{q^{vd}} \sum_{\tau(z_v)\in L_v} \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau^*(z_{v-i+1}))\, \psi_v[-\tau(z_v)\,\alpha(z_v)] \\ & = \frac{1}{q^{vd}} \sum_{j=0}^{v-1} \left\{ \sum_{w(\tau(z_v))=j} \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau^*(z_{v-i+1}))\, \psi_v[-\tau(z_v)\,\alpha(z_v)] \right\}. \end{aligned} \tag{18}$$

We had $\tau^*(z_{v-i+1}) = \tau_0 + \tau_1 z_{v-i+1} + \cdots + \tau_{v-i} z_{v-i+1}^{v-i}$. If $w(\tau(z_v)) = j$ define

$$\tau_j^*(z_{v-i+1}) := \begin{cases} \tau_j z_{v-i+1}^{j} + \cdots + \tau_{v-i} z_{v-i+1}^{v-i}, & \text{si } j < v-i+1, \\ 0, & \text{si } j \geq v-i+1, \end{cases} \tag{19}$$

and applying (19) to (18) we get,

$$\begin{aligned} & N_v(\alpha(z_v)) \\ & = \frac{1}{q^{vd}} \sum_{j=0}^{v-1} \left\{ \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau_j^*(z_{v-i+1})) \sum_{w(\tau(z_v))=j} \psi_v[-\tau(z_v)\,\alpha(z_v)] \right\}. \end{aligned}$$

Since $w(\tau(z_v)) = j$ and doing the same reasoning as in (16) we have:

$$N_v(\alpha(z_v)) = \frac{1}{q^{vd}} \sum_{j=0}^{v-1} \left\{ \prod_{i=1}^{v} c_{v-i+1}^{n_i}(\tau_j^*(z_{v-i+1})) \right\} c_{v-j}(\alpha^*(z_{v-j}))\,,$$

as required. □

References

[1] V. S. Albis and R. Chaparro, *On a conjecture of Borevich and Shafarevich*, Rev. Acad. Colomb. Cienc. **21**, 313 (1997).

[2] V. S. Albis, *Lecciones sobre la aritmética de polinomios*, Notas de clase (Departamento de Matemáticas, Universidad Nacional de Colombia, Bogotá, 1999).

[3] V. S. Albis and W. Zuñiga, *Una introducción elemental a la teoría de las funciones zeta locales de Igusa*, Lecturas Matemáticas **20**, 5 (1999).

[4] T. Apostol, *Introduction to Analytic Number Theory* (Springer Verlag, New York, 1976).

[5] L. Carlitz, *The arithmetic of polynomials in a Galois field*, Am. J. Math. **54**, 39 (1932).

[6] L. Carlitz, *The singular series form sums of squares of polynomials*, Duke Math. J. **14**, 1105 (1947).

[7] C. Chevalley, *Review of [17]*, MR0054578 (1953).

[8] E. Cohen, *Arithmetic functions of polynomials*, Proc. Am. Math. Soc. **3**, 352 (1953).

[9] E. Cohen, *An extension of Ramanujan sums. II. Additive properties*, Duke Math. J. **22**, 534 (1955).

[10] E. Cohen, *An extension of Ramanujan sums. III. Connections with totient functions*, Duke Math. J. **22**, 623 (1956).

[11] E. Cohen, *Representations of even functions* (mod r). *I. Arithmetical identies*, Duke Math. J. **25**, 401 (1958).

[12] R. Dedekind, *Abriss einer Theorie der höheren Congruenze in Bezug auf reellen Primzal–Modulus*, J. f. reine u. ange. Mathematik **54**, 1 (1857).

[13] L. E. Dickson, *History of Number Theory* (Chelsea, New York, 1919).

[14] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Springer Verlag, New York, 1982).

[15] J. Knopfmacher, *Abstract Analytical Number Theory* (Dover, New York, 1990).

[16] E. Kummer, *Note sur une expression analogue à la resolvante de Lagrange pour l'équation* $z^p = 1$, Atti dell'Academia Pontifica de Nouvi Lincei **6**, 327 (1852–1853).

[17] E. Lamprecht, *Algemeine Theorie der Gaussschien Summen in endliche kommutativen Ringen*, Math. Nachr. **9**, 149 (1953).

[18] G. Libri, *Mémoirs de divers savants*, Acad. Sci. de l'Institut de France (Math.) **5**, 32 (1838).

[19] G. Libri, *Mémoire sur la théorie des nombres*, J. für angew. reine Math. **9**, 54 (1832).

[20] C. J. Moreno, private communication (2000).

[21] K. Nageswara Rao, *Some applications of Carlitz's* η*–sum*, Acta Arithmetica **12**, 213 (1967).

[22] K. Nageswara Rao, *On a congruence equation and related arithmetical identities*, Monatsh. Math **71**, 24 (1967).

[23] H. Niederreiter, *Permutation polynomials in several variables over finite fields*, Proc. Japan Acad. **46**, 1001 (1970).

[24] H. Niederreiter, *Orthogonal systems of polynomials in finite fields*, Proc. Amer. Math. Soc. **28**, 415 (1971).

[25] T. H. Smits, *On the group of units of* $GF(q)[X]/(a(X))$, Indag. Math. **44**, 355 (1982).

[26] A. Weil, *Number of solutions of equations in finite fields*, Bull. Am. Math. Soc. **55**, 497 (1949).