An Additive Characterization of Fibers of Characters on $\mathbb{F}_p^*$

Chris Monico
Texas Tech University
Lubbock, TX
c.monico@ttu.edu

Michele Elia
Politecnico di Torino
Torino, Italy
elia@polito.it

January 30, 2009

Abstract

Let p be an odd prime, and χ a character on $\mathbb{F}_p^*$ of order n. We show that a partition $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \cdots \cup \mathcal{A}_n$ of $\{1, 2, \ldots, p-1\}$ is the partition by fibers of χ if and only if the $\mathcal{A}_i$ satisfy certain additive properties.

Keywords: nth power residue, cyclotomic coset, character.
Mathematics Subject Classification (2000): 11A15, 11N69, 11R32.

1 Introduction and Notations

In [9], Oskar Perron gave some additive properties of the fibers of the quadratic character on $\mathbb{F}_p^*$. Specifically, he showed that if $A, B \subset \mathbb{F}_p$ are the subsets of quadratic residues and non-residues respectively, then

1. Every element of A [respectively B] can be written as a sum of two elements of A [respectively B] in exactly $\left[\frac{p+1}{4}\right] - 1$ ways.
2. Every element of A [respectively B] can be written as a sum of two elements of B [respectively A] in exactly $\left[\frac{p+1}{4}\right]$ ways.

It's natural to inquire about just how strong this result is, and in [8] we showed that these additive properties completely characterize the even partition of $\mathbb{F}_p^*$ into quadratic residues and nonresidues. That is, the partition of $\mathbb{F}_p^*$ into quadratic residues and nonresidues is the only even partition having the specified additive properties. The present paper generalizes this result (and removes the 'even' restriction) to fibers of arbitrary characters on $\mathbb{F}_p^*$, with suitable cyclotomic numbers in place of the constants above.

The notation we establish here will be used throughout. Let p be a fixed odd prime and $\chi : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$ a fixed group character on the multiplicative group $\mathbb{F}_p^*$ of the finite field $\mathbb{F}_p$

of order p. Then for some n dividing $p-1$ and some generator g of $\mathbb{F}_p^*$, the character χ is induced by $\chi(g) = e^{2\pi i/n}$. For each integer k let $\mathcal{A}_k$ be the fiber $\chi^{-1}(\{e^{2k\pi i/n}\})$. Then the fiber $\mathcal{A}_n$ is the set of n-th power residues modulo p and the fibers $\mathcal{A}_1, \ldots, \mathcal{A}_n$ form a partition of $\{1, 2 \ldots, p-1\}$ with $|\mathcal{A}_k| = \frac{p-1}{n} = s$ for each k. The sets $\mathcal{A}_k$ are sometimes called *cyclotomic classes* or *cyclotomic cosets*. For each $k \in \mathbb{Z}$ we define a polynomial $r_k(x) \in \mathbb{Z}[x]$ by

$$r_k(x) = \sum_{j \in \mathcal{A}_k} x^j.$$

Note that $\eta_k = r_k(\exp(2\pi i/p))$ is an s-nomial period [3].

Since the fibers $\mathcal{A}_1, \ldots, \mathcal{A}_n$ form a partition of $\mathbb{F}_p^*$ we have

$$1 + \sum_{1 \le k \le n} r_k(x) = \sum_{0 \le j < p} x^j = \frac{x^p - 1}{x - 1}, \tag{1.1}$$

as well as the following proposition.

Proposition 1.1 *The set $\{1\} \cup \{r_k(x) \ : \ 1 \le k \le n\}$ is a basis of a $\mathbb{Q}$-subspace $\mathbf{V}_{n+1}$ of dimension $n+1$ in the p-dimensional vector space $\mathbb{Q}[x]/\langle x^p - 1\rangle$ of polynomials of degree at most $p-1$.*

2 Main Theorem

Our immediate goal is to show that V_{n+1} is actually a $\mathbb{Q}$-subalgebra of $\mathbb{Q}[x]/\langle x^p - 1\rangle$. First a lemma is required. Let $\mathbb{Q}(\zeta_p)$ be the cyclotomic field of p-th roots of unity, with ζ_p denoting a primitive root of unity. The Galois group $G = \mathfrak{G}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is isomorphic to $\mathbb{F}_p^*$ via $a \mapsto \sigma_a$ where

$$\sigma_a(\zeta_p) = \zeta_p^a, \quad a \in \mathbb{F}_p^* \ .$$

Since g is a generator of $\mathbb{F}_p^*$ we have $G = \langle \sigma_g \rangle$. Let G_n and G_s be the subgroups of G having order n and s respectively, so that $G_n = \langle \sigma_g^s \rangle$ and $G_s = \langle \sigma_g^n \rangle$.

We define the *period polynomial* [3] $P_n(y)$ by

$$P_n(y) = \prod_{k=1}^{n} \left(y - r_k(\zeta_p)\right).$$

A priori, $P_n(y) \in \mathbb{Q}(\zeta_p)[y]$, but the following lemma shows that the coefficients are actually integers.

Lemma 2.1 *Let $P_n(y)$ be as above. Then*

1. *$P_n(y) \in \mathbb{Z}[y]$,*
2. *If $E = \mathbb{Q}(r_1(\zeta_p), \ldots, r_n(\zeta_p)) \supset \mathbb{Q}$ is the splitting field of P_n then $[E : \mathbb{Q}] = n$. In particular, $E = \mathbb{Q}[r_1(\zeta_p), \ldots, r_n(\zeta_p)]$.*

Proof: Notice that with $G = \langle \sigma_g \rangle$ as above, we have

$$\sigma_g(r_k(\zeta_p)) = r_k(\zeta_p^g) = \sum_{j \in \mathcal{A}_k} \zeta_p^{gj} = \sum_{j \in g\mathcal{A}_k} \zeta_p^j = r_{k+1}(\zeta_p),$$

with the last equality following from $g\mathcal{A}_k = \mathcal{A}_{k+1}$. Since $r_{n+1}(\zeta_p) = r_1(\zeta_p)$, σ_g permutes of the roots of P_n. In particular, the coefficients of P_n are invariant under the action of the entire Galois group G, and so they are in $\mathbb{Q}$ since $\mathbb{Q}(\zeta_p)$ is Galois over $\mathbb{Q}$. Furthermore, since the $r_k(\zeta_p)$ are algebraic integers, so are the coefficients of P_n, and hence $P_n \in \mathbb{Z}[y]$.

For the second part, notice that for every $1 \leq k \leq n$ we have

$$\sigma_g^n(r_k(\zeta_p)) = r_k(\zeta_p^{g^n}) = r_{k+n}(\zeta_p) = r_k(\zeta_p).$$

Since $G_s = \langle \sigma_g^n \rangle$, it follows that E is fixed by G_s and so $G_s \subseteq \mathfrak{G}(\mathbb{Q}(\zeta_p)|E)$. By the Fundamental Theorem of Galois Theory [4], we then have

$$[\mathbb{Q}(\zeta_p) : E] = |\mathfrak{G}(\mathbb{Q}(\zeta_p)|E)| \geq s,$$

and

$$[E : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_p) : E]} = \frac{ns}{[\mathbb{Q}(\zeta_p) : E]} \leq n.$$

On the other hand, $r_1(\zeta_p), \ldots, r_n(\zeta_p)$ are n linearly independent elements of E so that $[E : \mathbb{Q}] \geq n$. □

The first half of our main theorem is encapsulated by the following lemma, which is closely related to Lemma 10.10.2 of [3].

Lemma 2.2 *The $\mathbb{Q}$-vector space V_{n+1} of Proposition 1.1 is a $\mathbb{Q}$-subalgebra of $\mathbb{Q}[x]/\langle x^p - 1 \rangle$. In particular, for every $1 \leq i, j \leq n$ there exist integers c_{ijk} such that*

$$r_i(x) r_j(x) \equiv c_{ij0} + \sum_{k=1}^{n} c_{ijk} r_k(x) \pmod{\langle \mathrm{x^p} - 1 \rangle}.$$

Proof: Let $i, j \in \{1, 2, \ldots, n\}$ and let $\Phi_p(x) = (x^p - 1)/(x - 1)$ be the p-th cyclotomic polynomial. It follows from Lemma 2.1 that there are constants $\widetilde{c}_{ijk}$ and a polynomial $h_{ij}(x) \in \mathbb{Q}[x]$ so that

$$r_i(x) r_j(x) = \sum_{k=1}^{n} \widetilde{c}_{ijk} r_k(x) + h_{ij}(x) \Phi_p(x).$$

Since $\Phi_p(x) = 1 + \sum_{k=1}^{n} r_k(x)$, we have

$$\begin{aligned} r_i(x) r_j(x) &= \sum_{k=1}^{n} \widetilde{c}_{ijk} r_k(x) + h_{ij}(1) \left(1 + \sum_{k=1}^{n} r_k(x) \right) + (h_{ij}(x) - h_{ij}(1)) \Phi_p(x) \\ &\equiv h_{ij}(1) + \sum_{k=1}^{n} (h_{ij}(1) + \widetilde{c}_{ijk}) r_k(x) \pmod{\langle \mathrm{x^p} - 1 \rangle} \\ &\equiv c_{ij0} + \sum_{k=1}^{n} c_{ijk} r_k(x) \pmod{\langle \mathrm{x^p} - 1 \rangle}, \end{aligned}$$

where $c_{ij0} = h_{ij}(1)$ and $c_{ijk} = h_{ij}(1) + \widetilde{c}_{ijk}$ for $1 \leq k \leq n$. It follows that the c_{ijk} are integers since the coefficients of r_i, r_j, and $x^p - 1$ are all integers. $\square$

Remark 2.3 Evaluating the equation stated in Lemma 2.2 at $x = \exp(2\pi i/p)$ and recalling that $\eta_k = r_k(\exp(2\pi i/p))$ we obtain

$$\eta_i \eta_j = c_{ij0} + \sum_{k=1}^{n} c_{ijk} \eta_k.$$

Since the η_i are $\mathbb{Q}$-linearly independent, comparison with Lemma 10.10.2 of [3] shows that $c_{ijk} = (j - i, k - i)_n$, where $(a, b)_n$ denotes a cyclotomic number of order n.

Corollary 2.4 *For $1 \leq i, j, k \leq n$, each element of $\mathcal{A}_k$ can be written as the sum of an element of $\mathcal{A}_i$ and an element of $\mathcal{A}_j$ in precisely c_{ijk} ways, where c_{ijk} are the constants given by Lemma 2.2.*

The goal is to show that the additive property described by Corollary 2.4 completely characterizes the partition $\mathbb{F}_p^* = \mathcal{A}_1 \cup \cdots \cup \mathcal{A}_n$. That is to say, this is the only partition of F_p^* into n sets satisfying the conclusion of the corollary.

Theorem 2.5 *For $1 \leq i, j, k \leq n$, let c_{ijk} be the constants in Lemma 2.2. Suppose $\mathcal{A}'_1, \ldots, \mathcal{A}'_n$ is a partition of $\mathbb{F}_p^*$ with the property that each element of $\mathcal{A}'_k$ can be written as the sum of an element from $\mathcal{A}'_i$ and an element from $\mathcal{A}'_j$ in exactly c_{ijk} ways. Then for some permutation τ of $\{1, 2, \ldots, n\}$, we have $\mathcal{A}'_i = \mathcal{A}_{\tau(i)}$.*

Proof: Let $r_i(x)$ be as above and set $r'_i(x) = \sum_{j \in \mathcal{A}'_j} x^j$. The hypotheses imply that $r'_i(x) r'_j(x) \equiv c_{ij0} + \sum_{k=1}^{n} c_{ijk} r'_k(x) \pmod{\langle \mathrm{x^p} - 1 \rangle}$ and in particular,

$$r'_i(\zeta_p) r'_j(\zeta_p) = c_{ij0} + \sum_{k=1}^{n} c_{ijk} r'_k(\zeta_p). \tag{2.2}$$

Consider the map

$$\begin{array}{rcl} \psi : \mathbb{Q}[r'_1(\zeta_p), \ldots, r'_n(\zeta_p)] & \longrightarrow & \mathbb{Q}[r_1(\zeta_p), \ldots, r_n(\zeta_p)] = E \\ r'_j(\zeta_p) & \longmapsto & r_j(\zeta_p). \end{array}$$

Since $r'_1(\zeta_p), \ldots, r'_n(\zeta_p)$ are $\mathbb{Q}$-linearly independent, ψ is a vector space isomorphism. Then (2.2) implies that ψ is actually a $\mathbb{Q}$-algebra isomorphism. Therefore, $\mathbb{Q}[r'_1(\zeta_p), \ldots, r'_n(\zeta_p)]$ is a field of degree n over $\mathbb{Q}$. But since the Galois group $\mathfrak{G}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ is cyclic, there is only one such subfield of $\mathbb{Q}(\zeta_p)$, namely E. So there are constants $m_{ij} \in \mathbb{Q}$ for which

$$r'_i(\zeta_p) = \sum_{j=1}^{n} m_{ij} r_j(\zeta_p).$$

By writing the $r_i'(\zeta_p), r_j(\zeta_p)$ in terms of the basis $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ of $\mathbb{Q}(\zeta_p)$, we see that $m_{ij} \in \{0,1\}$ since the coefficients of $r_i'(x), r_j(x)$ are in $\{0,1\}$ and the terms of each $r_i'(x)$ [and $r_i(x)$] are distinct. Now with $K = \mathbb{Q}(\zeta_p)$ we have

$$\begin{aligned} -ns = \mathrm{Tr}_{K|\mathbb{Q}}\left(\sum_{i=1}^{n} r_i'(\zeta_p)\right) &= \sum_{i=1}^{n} \mathrm{Tr}_{K|\mathbb{Q}}(r_i'(\zeta_p)) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}\mathrm{Tr}_{K|Q}(r_j(\zeta_p)) \\ &= -s\sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}. \end{aligned}$$

Therefore, $\sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij} = n$. But since $M = (m_{ij})$ is invertible $n \times n$ and the entries are in $\{0,1\}$, it follows that M must have exactly one 1 in each row and one 1 in each column.

So there is a permutation τ of $\{1, 2, \ldots, n\}$ with $r_i'(\zeta_p) = r_{\tau(i)}(\zeta_p)$ for all $1 \le i \le n$. Fix $i \in \{1, 2, \ldots, n\}$ and let $h_i(x) \in \mathbb{Z}[x]$ so that $r_i'(x) = r_{\tau(i)}(x) + h_i(x)\Phi_p(x)$. Evaluation at $x = 1$ shows that $r_i'(1) = s + h_i(1) \cdot p$, and hence $r_i'(1) \equiv s \pmod{\mathrm{p}}$. By construction, $0 < r_i'(1) \le p$, so we must have $r_i'(1) = s$. Then $r_i'(x) - r_{\tau(i)}(x) \in \langle \Phi_p(x)\rangle \cap \langle x-1\rangle = \langle x^p - 1\rangle$. But since $r_i'(x), r_{\tau(i)}(x)$ each have degree at most $p-1$, it follows that $r_i'(x) = r_{\tau(i)}(x)$ and hence $\mathcal{A}_i = \mathcal{A}_{\tau(i)}$. □

Notice that given p and the polynomial P_n, the fibers of χ may be recovered by expressing the roots of P_n in terms of the basis $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ of $\mathbb{Q}(\zeta_p)$. So the polynomial P_n encodes the fibers of χ in some sense. From [8], it follows that if χ is the quadratic character on $\mathbb{F}_p$, then

$$P_2(y) = \begin{cases} y^2 + y - \left[\frac{p+1}{4}\right], & \text{if } p \equiv 1 \pmod 4, \\ y^2 + y + \left[\frac{p+1}{4}\right], & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where $[-]$ is the greatest integer function. For arbitrary characters we do not have such an explicit result, but the following proposition gives some information.

Proposition 2.6 *Let p, n and P_n be as above. Then*

$$P_n(y) \equiv (y + 1/n)^n \pmod{\mathrm{p}}.$$

Proof: Consider the ring homomorphism $\psi : \mathbb{Z}[\zeta_p] \longrightarrow \mathbb{F}_p$ determined by $\psi(\zeta_p) = 1$. This naturally extends to a homomorphism $\psi : \mathbb{Z}[\zeta_p][y] \longrightarrow \mathbb{F}_p[y]$ with $\psi(y) = y$ and

$$\psi(f(y)) = \psi\left(\prod_{k=1}^{n}(y - r_k(\zeta_p))\right) \equiv \prod_{k=1}^{n}(y - r_k(1)) \equiv \prod_{k=1}^{n}\left(y - \frac{p-1}{n}\right) \equiv (y + 1/n)^n \pmod{\mathrm{p}}.$$

On the other hand, the coefficients of P_n are actually in $\mathbb{Z}$ so that $P_n(y) \equiv (y+1/n)^n \pmod{\mathrm{p}}$. □

3 Examples

It's not difficult to see that the polynomial $P_n(y)$ depends only on p and n and not on the particular character χ (of course, n depends on χ since n is the cardinality of the image of χ). The polynomials corresponding to $n = 4$ for the first several primes $p \equiv 1 \pmod 4$ are given in the following table.

p	$f(y)$
5	$y^4 + y^3 + y^2 + y + 1$
13	$y^4 + y^3 + 2y^2 - 4y + 3$
17	$y^4 + y^3 - 6y^2 - y + 1$
29	$y^4 + y^3 + 4y^2 + 20y + 23$
37	$y^4 + y^3 + 5y^2 + 7y + 49$
41	$y^4 + y^3 - 15y^2 + 18y - 4$
53	$y^4 + y^3 + 7y^2 - 43y + 47$
61	$y^4 + y^3 + 8y^2 + 42y + 117$

In [8] the complete additive characterization of the quadratic residues based on two polynomials $r_1(x)$ and $r_2(x)$ was given. The three polynomials $1, r_1(x), r_2(x)$ define a polynomial algebra of dimension 3 in the polynomial ring $\mathbb{Q}[x]$ modulo $\langle x^p - 1\rangle$. These three polynomials are solutions to

$$Z^2 + Z - (-1|p)\left[\frac{p+1}{4}\right] + \left[\frac{p+1}{4}\right]\Phi_p(x) \equiv 0 \pmod{\langle \mathrm{x^p} - 1\rangle}.$$

Furthermore, the multiplication constants for this algebra were explicitly determined in that paper. Multiplication by 1 is trivial, and with $d_p = [(p+1)/4]$, the products of the other basis polynomials are

$$\left\{\begin{array}{rcll} r_1(x)^2 & \equiv & (1+(-1|p))\left(\frac{p-1}{4}\right) r_0(x) + (d_p - 1)r_1(x) + d_p r_2(x) & \pmod{\langle \mathrm{x^p} - 1\rangle} \\ r_2(x)^2 & \equiv & (1+(-1|p))\left(\frac{p-1}{4}\right) r_0(x) + d_p r_1(x) + (d_p - 1)r_2(x) & \pmod{\langle \mathrm{x^p} - 1\rangle} \\ r_1(x)r_2(x) & \equiv & (1-(-1|p))\left(\frac{p-1}{4}\right) r_0(x) + [p/4]r_1(x) + [p/4]r_2(x) & \pmod{\langle \mathrm{x^p} - 1\rangle} \end{array}\right.$$

Here, the uniqueness of polynomials $r_1(x)$ and $r_2(x)$ satisfying the above equations follows from properties of the Galois group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ with ζ_p a p-th root of unity. The general result will now be illustrated with two further numerical examples for 3-power and 4-power residues obtained considering $p = 13$.

A primitive root in $\mathbb{F}_{13}^*$ is $g = 2$, and for the 3-power residues we consider the character determined by $\chi(2) = e^{2\pi i/3}$. The fibers of this character are $\mathcal{A}_1 = \{2, 3, 10, 11\}$, $\mathcal{A}_2 = \{4, 6, 7, 9\}$, and $\mathcal{A}_3 = \{1, 5, 8, 12\}$. The associated polynomials are

$$\left\{\begin{array}{rcl} r_1(x) & = & x^2 + x^3 + x^{10} + x^{11}, \\ r_2(x) & = & x^4 + x^6 + x^7 + x^9, \\ r_3(x) & = & x + x^5 + x^8 + x^{12}. \end{array}\right.$$

Together with the polynomial 1, these are precisely the solutions of the equation

$$Z^3 + Z^2 - 4Z + 1 - 5\Phi_{13}(x) = 0 \pmod{\langle \mathrm{x^{13}} - 1\rangle} \quad .$$

The vector space $V_4 \subset \mathbb{Q}[x]/\langle x^{13}-1\rangle$ has basis $\{1, r_1, r_2, r_3\}$. Associating an element $\alpha_0 + \alpha_1 r_1 + \alpha_2 r_2 + \alpha_3 r_3$ with the vector $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$, the multiplication on V_4 is given by the following.

	$(1,0,0,0)$	$(0,1,0,0)$	$(0,0,1,0)$	$(0,0,0,1)$
$(1,0,0,0)$	$(1,0,0,0)$	$(0,1,0,0)$	$(0,0,1,0)$	$(0,0,0,1)$
$(0,1,0,0)$	$(0,1,0,0)$	$(4,0,1,2)$	$(0,1,2,1)$	$(0,2,1,1)$
$(0,0,1,0)$	$(0,0,1,0)$	$(0,1,2,1)$	$(4,2,0,1)$	$(0,1,1,2)$
$(0,0,0,1)$	$(0,0,0,1)$	$(0,2,1,1)$	$(0,1,1,2)$	$(4,1,2,0)$

From this, one may immediately read off the c_{ijk} constants from Lemma 2.2; for example, $c_{230} = 0, c_{231} = 1, c_{232} = 1, c_{233} = 2$. From $c_{231} = 1$ we conclude that each element of $\mathcal{A}_1$ can be written as the sum of an element of $\mathcal{A}_2$ and an element of $\mathcal{A}_3$ in exactly one way. Note also that in each column we may read the matrices, of a matrix representation of the polynomial algebra V_4. The cubic polynomial $f(Z) = Z^3 + Z^2 - 4Z + 1$ is obtained as a factor of the characteristic polynomial of any of these matrices.

For the 4-power residues in $\mathbb{F}_{13}^*$ we consider the character determined by $\chi(2) = e^{2\pi i/4}$. The fibers of this character are $\mathcal{A}_1 = \{2,5,6\}$, $\mathcal{A}_2 = \{4,10,12\}$, $\mathcal{A}_3 = \{7,8,11\}$, and $\mathcal{A}_4 = \{1,3,9\}$ and the associated polynomials are

$$\begin{cases} r_1(x) &= x^2 + x^5 + x^6, \\ r_2(x) &= x^4 + x^{10} + x^{12}, \\ r_3(x) &= x^7 + x^8 + x^{11}, \\ r_4(x) &= x + x^3 + x^9. \end{cases}$$

Together with the polynomial 1 these are precisely solutions of the equation

$$Z^4 + Z^3 + 2Z^2 - 4Z + 3 - 9\Phi_{13}(x) = 0 \pmod{\langle \mathrm{x}^{13} - 1\rangle} \quad .$$

As above, the multiplication constants c_{ijk} of the polynomial algebra are given in the following table.

	$(1,0,0,0,0)$	$(0,1,0,0,0)$	$(0,0,1,0,0)$	$(0,0,0,1,0)$	$(0,0,0,0,1)$
$(1,0,0,0,0)$	$(1,0,0,0,0)$	$(0,1,0,0,0)$	$(0,0,1,0,0)$	$(0,0,0,1,0)$	$(0,0,0,0,1)$
$(0,1,0,0,0)$	$(0,1,0,0,0)$	$(0,0,1,2,0)$	$(0,1,1,0,1)$	$(3,0,1,0,1)$	$(0,1,0,1,1)$
$(0,0,1,0,0)$	$(0,0,1,0,0)$	$(0,1,1,0,1)$	$(0,0,0,1,2)$	$(0,1,1,1,0)$	$(3,1,0,1,0)$
$(0,0,0,1,0)$	$(0,0,0,1,0)$	$(3,0,1,0,1)$	$(0,1,1,1,0)$	$(0,2,0,0,1)$	$(0,0,1,1,1)$
$(0,0,0,0,1)$	$(0,0,0,0,1)$	$(0,1,0,1,1)$	$(3,1,0,1,0)$	$(0,0,1,1,1)$	$(0,1,2,0,0)$

4 Conclusion and Remarks

In conclusion, we have proved that the partition $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \cdots \cup \mathcal{A}_s$, of the residue set $\mathbb{Z}_p^* = 1, 2, \ldots, p-1\}$ modulo p into fibers of a character has also an additive characterization. It seems likely that this result should extend to characters on $\mathbb{F}_{p^n}^*$, but the technique used in this paper does not immediately generalize to that case; one could certainly replace our

$r_k(x)$ by multivariate polynomials, but the techniques in this paper relied heavily on the fact that r_k is univariate.

In [11], Winterhof gave a different generalization of Perron's [9] result. With the notations as in this paper, he proved that if $a \in \mathbb{F}_p^*$, ω is a primitive n-th root of unity, and s_k is the number of $x \in \mathbb{F}_p$ with

$$\chi(x) = \omega^k \chi(x + a),$$

then $s_0 + 1 = s_1 = \cdots = s_{n-1} = (p-1)/n$ (in fact, his result was proven for arbitrary finite fields). It would be interesting to know if this property also characterizes the fibers of χ.

We would like to thank an anonymous referee for pointing out the connection to the cyclotomic numbers, as well as several other suggestions that improved the presentation.

References

[1] A.A. Albert, *Structure of Algebras*, AMS, Providence, R.I. 2003.

[2] G.E. Andrews, *Number Theory*, Dover, New York, NY 1994.

[3] B.C. Berndt, R.J. Evans, K.S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Wiley, New York, NY 1998.

[4] D.A. Cox, *Galois Theory*, Wiley, New York, NY 2004.

[5] H. Davenport, *Multiplicative Number Theory*, Springer, New York, NY 1980.

[6] L.E. Dickson, *Algebras and their Arithmetics*, Dover, New York, NY 1960.

[7] F. Lemmermeyer, *Reciprocity Laws, From Euler to Eisenstein*, Springer, New York, NY 2000.

[8] C. Monico, M. Elia, Note on an Additive Characterization of Quadratic Residues Modulo p, *Journal of Combinatorics, Information & System Sciences*, 31 (2006), 209–215.

[9] O. Perron, Bemerkungen über die Verteilung der quadratischen Reste, *Mathematische Zeitschrift*, 56(1952), 122–130.

[10] L.C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, NY 1997.

[11] A. Winterhof, On the Distribution of Powers in Finite Fields, *Finite Fields and their Applications*, 4(1998), 43–54.