FINITE FIELDS AND THEIR APPLICATIONS **2,** 422–438 (1996)
ARTICLE NO. 0025

Vanishing Sums of *m*th Roots of Unity in Finite Fields

T. Y. LAM*

University of California, Berkeley, California 94720

K. H. LEUNG†

National University of Singapore, Singapore 119260

Communicated by Peter Jau-Shyong Shiue

Received December 14, 1995; revised February 15, 1996

In an earlier work, the authors determined all possible weights n for which there exists a vanishing sum $\zeta_1 + \cdots + \zeta_n = 0$ of mth roots of unity ζ_i in characteristic 0. In this paper, the same problem is studied in finite fields of characteristic p. For given m and p, results are obtained on integers n_0 such that all integers $n \geq n_0$ are in the "weight set" $W_p(m)$. The main result in this paper guarantees, under suitable conditions, the existence of solutions of $x_1^d + \cdots + x_n^d = 0$ *with all coordinates not equal to zero* over a finite field. © 1996 Academic Press, Inc.

1. INTRODUCTION

By vanishing sum of mth roots of unity, we mean an equation $\alpha_1 + \cdots + \alpha_n = 0$, where $\alpha_i^m = 1$ for each i. The integer n is said to be the *weight* of this vanishing sum. In [LL], considering mth roots of unity in $\mathbb{C}$, we defined $W(m)$ to be the set of integers $n \geq 0$ for which there exists a vanishing sum $\alpha_1 + \cdots + \alpha_n = 0$ as above. The principal result in [LL] gives a complete determination of the weight set $W(m)$ (in characteristic 0), as follows.

* Supported in part by NSF.
† This author's research was carried out while he was on sabbatical leave at U.C. Berkeley from the National University of Singapore. The hospitality of the former institution is gratefully acknowledged.

1071-5797/96 $18.00

THEOREM 1.1. *For any natural number m with prime factorization $p_1^{a_1} \cdots p_r^{a_r}$, the weight set $W(m)$ is exactly given by $\mathbb{N}p_1 + \cdots + \mathbb{N}p_r$. (Here and in the following, $\mathbb{N} := \{0, 1, 2, \cdots\}$.)*

In this paper, we study vanishing sums of mth roots of unity *in characteristic p*. In analogy to the characteristic 0 case, we define $W_p(m)$ to be the set of weights n for which there exists a vanishing sum $\alpha_1 + \cdots + \alpha_n = 0$, where each α_i is an mth root of unity in $\overline{\mathbb{F}}_p$, the algebraic closure of the prime field $\mathbb{F}_p$. Note that, if $m = p^t m'$ where $\gcd(p, m') = 1$, we have $x^m = 1$ in $\overline{\mathbb{F}}_p$ iff $x^{m'} = 1$; in particular, $W_p(m) = W_p(m')$. Therefore, we may assume throughout that $\gcd(p, m) = 1$, i.e., p is not among the prime divisors p_i of m. As in the case of characteristic 0, we have $p_i \in W_p(m)$ for all i. But in characteristic p, we also have $p \in W_p(m)$ (due to the vanishing sum $p \cdot 1 = 0$), so now

$$W_p(m) \supseteq \mathbb{N}p + \mathbb{N}p_1 + \cdots + \mathbb{N}p_r. \tag{1.2}$$

Easy examples (see (2.1)) show that this need not be an equality in general, so we are left with no viable conjecture on the structure of the weight set $W_p(m)$ in characteristic p. However, (1.2) does show that, if $m > 1$, all sufficiently large integers n (in fact all $n \geq (p-1)(p_i - 1)$) belong to $W_p(m)$. A more tractable problem will then be the determination of more accurate bounds n_0 such that all integers $n \geq n_0$ belong to $W_p(m)$.

In this paper, we will show how such an integer n_0 can be determined. Our work is divided into three cases, depending whether $\gcd(p-1, m)$ is 1, 2, or greater. The estimates on n_0 differ from case to case and are given respectively in (5.6), (4.1), and (3.1)–(3.3). Although we have three different estimates on n_0, there does exist a (necessarily weaker) uniform estimate for all cases. In the following, we shall try to explain what this uniform estimate is, and why is it a reasonable one.

A guiding prinicple for our work throughout is the fact that a finite field is a C_1-field (see [Gr]). If $K = \mathbb{F}_{p^k}$ is a finite field containing all mth roots of unity, then, for $d := (p^k - 1)/m$, the mth roots of unity in $\overline{\mathbb{F}}_p$ comprise the group $\dot{K}^d$. Therefore, a vanishing sum of mth roots of unity of weight n corresponds precisely to a "good" solution of $x_1^d + \cdots + x_n^d = 0$ in K, where by a "good" solution we mean one with *each* $x_i \neq 0$. If $n > d$, the fact that K is C_1 implies that we have a solution $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$. It certainly seems tempting to speculate that there exists in fact a "good" solution (in K). If this is indeed the case, then by what we said earlier in this paragraph, *any* integer $n > d$ will be in the weight set $W_p(m)$.

The desired conclusion that, for $n > d$, $x_1^d + \cdots + x_n^d = 0$ has a "good" solution in K is, however, not rue in general! For instance, if $d = p^k - 1$, then $x^d = 1$ for each $x \in \dot{K}$, so we have a "good" solution for $x_1^d + \cdots +$

$x_n^d = 0$ in K only when n is a multiple of p. In a similar vein, if $k = 1$, p is odd, and $d = (p-1)/2$, then any nonzero dth power in K is ± 1. For any odd integer $n \in (d, p)$, the equation $x_1^d + \cdots + x_n^d = 0$ again has no "good" solution in $\mathbb{F}_p$. The trouble with these cases is that $m \leq 2$, for which we do not have "enough" mth roots to play with. As it turns out, as soon as we ignore the above cases, we have the following uniform result for getting "good" solutions.

THEOREM 1.3. *Let $K = \mathbb{F}_{p^k}$ and $d = (p^k - 1)/m$ as above, and assume that $m \neq 1$, $(m, k) \neq (2, 1)$. Then, whenever $n > d$, the equation $x_1^d + \cdots + x_n^d = 0$ has a "good" solution in K. In other words, the weight set $W_p(m)$ contains all integers $\geq d + 1$.*

The results in Sections 3–5 will cover this theorem in the case $m \geq 3$. In the case $m = 2$, (1.3) is quickly checked as follows. Since we assume in this case that $k \geq 2$, we have $d \geq (p^2 - 1)/2 \geq p - 1$. Given $n \geq d + 1 \geq p$, it is easy to solve the equation $\alpha_1 + \cdots + \alpha_n = 0$ with $\alpha_i = \pm 1$, by considering the parity of n. Having disposed of the trivial cases $m = 1$, 2, *we may assume in Sections* 3–6 *of this paper that* $m \geq 3$.

In the case when p is odd and $d = 2$, (1.3) says precisely that, for any $n > 2$, the quadratic form $x_1^2 + \cdots + x_n^2$ has a "good" zero over any finite field of more than five elements. This is a special case of a well-known observation of Witt for isotropic diagonal quadratic forms (see [Wi, p. 39; BS, p. 394; La, p. 25, Ex. 7]). Thus, (1.3) may be thought of as a generalization of Witt's result to the higher degree diagonal forms $x_1^d + \cdots + x_n^d$ over finite fields. Note that $d | (p^k - 1)$ is not a really essential assumption in (1.3). In dealing with the equation $x_1^e + \cdots + x_n^e = 0$, we can replace the degree e by $d := \gcd(p^k - 1, e)$ and define m to be $(p^k - 1)/d$. Then $\dot{K}^e = \dot{K}^d$, so under the assumptions of (1.3), $x_1^e + \cdots + x_n^e = 0$ will have a "good" solution as long as $n > d$.

In the literature, there are many results dealing with diagonal equations over finite fields; see, for instance, [LN, Sch, Sm] and more recently [QY]. Conventionally, one could apply algebro-geometric methods or alternatively the method of Gauss and Jacobi sums. As the referee of this paper pointed out, these methods can be utilized to show the existence of "good" solutions to a diagonal equation $x_1^d + \cdots + x_n^d = 0$ $(n > 2)$ in $\mathbb{F}_q$ if q is suitably large compared to d (without the condition $n > d$). However, these conventional methods do not seem to give enough information if q is "small" in comparison to d. In our setting, working mostly with $n > d$ and taking full advantage of the additive nature of the special equation $x_1^d + \cdots + x_n^d = 0$, we apply instead the methods of additive number theory. These methods do give fairly precise results, without reference to the size of $\mathbb{F}_q$. In fact, the analysis in Sections 3–5 will not only prove (1.3), but also show that, in various cases, the equations $x_1^d + \cdots + x_n^d = 0$ has a "good" solution in K often for much smaller values of n (than $n > d + 1$). Thus, the more precise results in this paper are to be found in (3.1)–(3.3), (4.1), and (5.6). Theorem 1.3 is only a common denominator of these results giving a convenient and uniform summary of the main work in this paper.

2. Some Basic Examples

We shall begin with some examples and computations of the weight sets $W_p(m)$. The first couple of examples show that various properties of weight sets in characteristic 0 are no longer valid in characteristic p. For convenience of expressing weight sets, let us use the notation $[n, \infty)_{\mathbb{Z}}$ for the set of integers $\geq n$.

Example 2.1. Referring to (1.2), *the smallest positive element in the set* $W_p(m)$ *may not be* $\min\{p, p_1, \ldots, p_r\}$. For instance, when $p = 11$ and $m = 5$, the 5th roots of unity in $\overline{\mathbb{F}}_{11}$ are $\{1, 3, 9, 5, 4\}$. Observing that $1 + 1 + 9 = 0$ in $\mathbb{F}_{11}$, we see that $W_{11}(5)$ contains 3, which is smaller than 5 and 11. By (2.3) below, we have $W_{11}(5) = \{0\} \cup [3, \infty)_{\mathbb{Z}}$. Thus, not only does (1.2) fail to be an equality, but also $W_{11}(5)$ is not even of the form $\sum_i \mathbb{N}q_i$ for a set of primes q_i's.

Example 2.2. Contrary to the characteristic 0 case, *the set* $W_p(m)$ *may be larger than* $W_p(m_0)$, *where* m_0 *is the square-free part of* m. For instance, let $p = 5$ and $m = 4$, so $m_0 = 2$. It is easy to see that $W_5(2) = \{0, 2\} \cup [4, \infty)_{\mathbb{Z}}$, but $W_5(4) = \{0\} \cup [2, \infty)_{\mathbb{Z}}$.

Example 2.3. Let $q = p^a > 5$, where p is an odd prime, and let $m = (q - 1)/2$. Then $d := (q - 1)/m = 2$. For any $n \geq 3$, the quadratic form $X_1^2 + \cdots + X_n^2$ is isotropic over $\mathbb{F}_q$, so by the theorem of Witt referenced before, it has a "good" zero in $\mathbb{F}_q$. Therefore, $n \in W_p(m)$. It follows that $W_p(m) = \{0\} \cup [2, \infty)_{\mathbb{Z}}$ if $q \equiv 1 \pmod 4$, and $W_p(m) = \{0\} \cup [3, \infty)_{\mathbb{Z}}$ if $q \equiv 3 \pmod 4$.

Example 2.4. ($\mathbb{F}_p$ contains all mth roots of unity.) Let $p = 31$, and $m = 3$. The third roots of unity are $\{1, 5, 25\}$, so the equation $25 + 6 \cdot 1 = 0 \in \mathbb{F}_{31}$ shows that $7 \in W_{31}(3)$. A routine computation shows that $W_{31}(3) = \{0, 3, 6, 7\} \cup [9, \infty)_{\mathbb{Z}}$.

Example 2.5. ($\mathbb{F}_p$ contains no mth roots of unity other than 1.) Let $p = 2$, and $m = 73$. We work in $K = \mathbb{F}_{2^9}$, which contains all 73rd roots of unity. By standard tables of irreducible polynomials over finite fields, the trinomial $f(X) = X^9 + X + 1$ is irreducible over $\mathbb{F}_2$, so we can take K to be $\mathbb{F}_2[X]/(f(X))$. Let $\alpha := \overline{X} \in K$. We have $0 = (\alpha^9 + \alpha + 1)^8 = \alpha^{72} +$

$\alpha^8 + 1$, so $\alpha^{73} = \alpha(\alpha^8 + 1) = \alpha^9 + \alpha = 1$. Thus, the relation $\alpha^9 + \alpha + 1 = 0$ shows that $3 \in W_2(73)$, and it follows easily that $W_2(73) = \{0\} \cup [2, \infty)_{\mathbb{Z}}$.

In the balance of this section, let us consider $W_p(m)$ in the case when m is a prime power (not divisible by p). Under a special hypothesis on the cyclotomic polynomial $\Phi_m(X)$, the weight set $W_p(m)$ can be determined explicitly.

THEOREM 2.6. *Let $m = l^a$, where l is a prime different from p, and assume that the cyclotomic polynomial $\Phi_m(X) \in \mathbb{Z}[X]$ remains irreducible modulo p. Then $W_p(m) = \mathbb{N}p + \mathbb{N}l$.*

Proof. Of course, it suffices to prove the inclusion "$\subseteq$". Let ζ be a primitive mth root of unity in $\overline{\mathbb{F}}_p$. Let $m' := m/l$, and $\alpha := \zeta^{m'}$ (a primitive lth root of unity). Let $K = \mathbb{F}_p(\zeta)$, and $L = \mathbb{F}_p(\alpha)$. Since $\Phi_m(X)$ is irreducible mod p, $[K : \mathbb{F}_p] = \varphi(m) = m'(l - 1)$. From this, it is easy to see that $[K : L] = m'$ and $[L : \mathbb{F}_p] = l - 1$.

Any vanishing sum of mth roots of unity can be written in the form $\sum_{i=0}^{m'-1} g_i \zeta^i = 0$, where each g_i is a sum of lth roots of unity. Since the degree of ζ over L is m', the elements $1, \zeta, \ldots, \zeta^{m'-1}$ are linearly independent over L. Therefore, each $g_i \in L$ is itself a vanishing sum, and it suffices to show that its weight is in $\mathbb{N}p + \mathbb{N}l$. Starting over again, we are now down to considering a vanishing sum $\sum_{i=0}^{l-1} a_i \alpha^i = 0$, where each $a_i \in \mathbb{N}$. Let a_j be the smallest among the a_i's. Since the minimal equation of α over $\mathbb{F}_p$ is $1 + \alpha + \cdots + \alpha^{l-1} = 0$, it follows easily that $a_0 = a_1 = \cdots = a_{l-1} \in \mathbb{F}_p$. The weight of the vanishing sum in question is $\sum_i a_i \equiv la_j \pmod p$. Since $\sum_i a_i \geq la_j$, it follows that $\sum_i a_i = la_j + bp$ for some $b \in \mathbb{N}$, as desired.

Q.E.D.

Remark 2.7. A vanishing sum of mth roots of unity is said to be *minimal* if no proper subsum of it is also vanishing. In general, the problem of determining the minimal vanishing sums is difficult (both in characteristic 0 and in characteristic p). Under the hypothesis of (2.6), however, this problem can be solved. In fact, the argument presented in the proof above can be used to show that, in the setting of (2.6), the minimal vanishing sums of mth roots of unity are, up to multiplicaton by a power of ζ: (1) $p \cdot 1 = 0$, and (2) $1 + \alpha + \cdots + \alpha^{l-1} = 0$. (Of course, this implies that $W_p(m) = \mathbb{N}p + \mathbb{N}l$.) For this conclusion, however, the assumption on the irreducibility of $\Phi_m(X)$ modulo p is essential, as the examples (2.1), (2.4) and (2.5) show. (In (2.1) and (2.4), $\Phi_m(X)$ splits completely modulo p, and in (2.5), $\Phi_m(X)$ splits into the product of eight irreducible factors of degree 9 in $\mathbb{F}_p[X]$.)

3. The Case $\gcd(p-1, m) \geq 3$

In dealing with $W_p(m)$, our main goal is to find good estimates for integers n_0 such that $[n_0, \infty)_{\mathbb{Z}} \subseteq W_p(m)$. We begin our analysis with the case when $\gcd(p-1, m) \geq 3$. This case turns out to be fairly easy if we use the right tools from additive number theory modulo p. It will be convenient to use the following notations. For a subset A in a field, we shall write $|A|$ for the cardinality of A, and for any integer $n \geq 1$, we write $n * A$ for the set $A + \cdots + A$ with n summands of A.

Theorem 3.1. *Assume that* $m_0 := \gcd(p-1, m) \geq 3$ *and let* $d_0 = (p-1)/m_0$. *Then* $[d_0+1, \infty)_{\mathbb{Z}} \subseteq W_p(m_0) \subseteq W_p(m)$.

Proof. Since $m_0 \mid (p-1)$, the group H of m_0th roots of unity in $\mathbb{F}_p$ is exactly $\dot{\mathbb{F}}_p^{d_0}$ and has exactly m_0 elements. We clain that $|n * H| \geq nm_0$ for $n \leq d_0$, and $|n * H| = p$ for $n \geq d_0 + 1$. It suffices to prove this for $n = 1, 2, \ldots, d_0 + 1$ (for, once we show that $|(d_0+1) * H| = p$, then $(d_0 + 1) * H = \mathbb{F}_p$, and this implies that $(d_0 + i) * H = \mathbb{F}_p$ for any $i \geq 1$). We proceed by induction on n, the case $n = 1$ being clear. Assume that $|n * H| \geq nm_0$ where $n < d_0$. By the Cauchy–Davenport Theorem (see [Ma, Cor. 1.2.3]), $|(n+1) * H|$ is either p (and hence $\geq (n+1)m_0$), or else

$$|(n+1) * H| \geq |n * H| + |H| - 1 \geq (n+1)m_0 - 1.$$

In the latter case, $|(n+1)*H \setminus \{0\}| \geq (n+1)m_0 - 2$. Since H acts on $(n+1)*H \setminus \{0\}$ by multiplication, $|(n+1)*H \setminus \{0\}|$ is a multiple of m_0. Since $m_0 \geq 3$, we must therefore have $|(n+1)*H \setminus \{0\}| \geq (n+1)m_0$, which gives what we want. This proves our claim for $n \leq d_0$. In particular, $|d_0 * H| \geq d_0 m_0 = p - 1$. By the Cauchy–Davenport Theorem again, $(d_0 + 1) * H$ must be $\mathbb{F}_p$, for otherwise we would have

$$|(d_0+1) * H| \geq |d_0 * H| + |H| - 1 \geq d_0 m_0 + m_0 - 1 = p + (m_0 - 1) > p,$$

a contradiction. This completes our inductive proof. Thus, for any $n \geq d_0 + 1$, we have $0 \in n * H$. This means that $n \in W_p(m_0)$, and so $[d_0+1, \infty)_{\mathbb{Z}} \subseteq W_p(m_0) \subseteq W_p(m)$. Q.E.D.

Example 3.2. In many cases Theorem 3.1 gives the best result. For instance, if $p \equiv 3 \pmod 4$ and $m = (p-1)/2 \geq 3$, then $d_0 = 2$ and we have $d_0 \notin W_p(m)$ since m is odd. Even in the case $p \equiv 1 \pmod 4$, Theorem 3.1 may still give the best result. For instance, if $p = 13$ and $m = 4$, then $d_0 = 3$ and $G = \{\pm 1, \pm 8\}$. By a simple calculation, $3 * G = \dot{\mathbb{F}}_{13}$, so again $d_0 = 3 \notin W_p(m)$. On the other hand, if m is divisible by two distinct primes p_1, p_2, then the fact that $p_1, p_2 \in W_p(m)$ implies that $[n_0, \infty)_{\mathbb{Z}} \subseteq W_p(m)$

for $n_0 := (p_1 - 1)(p_2 - 1)$ (see [LeV, p. 22, Ex. 4]). In case the number d_0 in (3.1) is "large," $[n_0, \infty)_{\mathbb{Z}} \subseteq W_p(m)$ will of course give a better result.

We can now derive the first case of Theorem 1.3.

COROLLARY 3.3. *Let $K = \mathbb{F}_{p^k}$ be a finite field containing all mth roots of unity, and let $d = (p^k - 1)/m$. If $m_0 := \gcd(p - 1, m) \geq 3$, then $[d + 1, \infty)_{\mathbb{Z}} \subseteq W_p(m_0) \subseteq W_p(m)$.*

Proof. Say $p - 1 = m_0 d_0$ and $m = m_0 m_1$. Then

$$d = \frac{(p-1)(p^{k-1} + \cdot \cdot \cdot + p + 1)}{m} = d_o \cdot \frac{p^{k-1} + \cdot \cdot \cdot + p + 1}{m_1}.$$

Since $\gcd(d_0, m_1) = 1$, the fraction on the right-hand side above is an integer. Therefore, we have $d_0 | d$, and the desired conclusion follows from Theorem 3.1. Q.E.D.

4. THE CASE $\gcd(p - 1, m) = 2$

We shall assume throughout this section that $\gcd(p - 1, m) = 2$ (and as before $m \geq 3$). In particular, p is odd and m is even. In this case, $W_p(m)$ contains $2\mathbb{N}$ and is stable under addition by 2. Thus, once we have an odd integer $n \in W_p(m)$, we will have automatically $[n - 1, \infty)_{\mathbb{Z}} \subseteq W_p(m)$. This observation will be used without further mention in the following.

Let $K = \mathbb{F}_{p^k}$ be any finite field containing the group G of all mth roots of unity. The followiing result gives a somewhat sharper form of Theorem 1.3 in the case $\gcd(p - 1, m) = 2$ (in that the index $[\dot{K} : G]$ itself is shown to be a weight, with a minor exception).

THEOREM 4.1. *Assume that $\gcd(p - 1, m) = 2$, and let $d = [\dot{K} : G] = (p^k - 1)/m$. Then $[d, \infty)_{\mathbb{Z}} \subseteq W_p(m)$ unless $p = 3$ and $m = 3^k - 1$, in which case $[d + 1, \infty)_{\mathbb{Z}} \subseteq W_3(m)$.*

Proof. Let us first check Theorem 4.1 when $m = 4$. In this case, the assumption $\gcd(p - 1, m) = 2$ implies that G is not contained in $\mathbb{F}_p$, so $k \geq 2$. If $p > 3$, then $d \geq (p^2 - 1)/4 \geq p$, and we have $[d, \infty)_{\mathbb{Z}} \subseteq [p, \infty)_{\mathbb{Z}} \subseteq W_p(m)$. If $p = 3$, then $d \geq (9 - 1)/4 = 2$, and we have again $[d, \infty)_{\mathbb{Z}} \subseteq [2, \infty)_{\mathbb{Z}} \subseteq W_3(m)$ (since $W_3(m)$ contains both 2 and 3). *In the following, we may therefore assume that $m \geq 6$.*

Write $m = 2m'$, so that

$$d = \frac{(p-1)(p^{k-1} + \cdot \cdot \cdot + p + 1)}{2m'} = \frac{p-1}{2} \cdot \frac{p^{k-1} + \cdot \cdot \cdot + p + 1}{m'}. \quad (4.2)$$

Since $\gcd(m', (p-1)/2) = 1$, we have $m' | (p^{k-1} + \cdots + p + 1)$. If $m' < p^{k-1} + \cdots + p + 1$, the second factor on the right-hand side in (4.2) is ≥ 2, so $d \geq p - 1$. Since $p \in W_p(m)$, we have $[d, \infty)_{\mathbb{Z}} \subseteq [p-1, \infty)_{\mathbb{Z}} \subseteq W_p(m)$, as desired. Therefore, *in the following we may assume that*

$$m' = p^{k-1} + \cdots + p + 1, \qquad \text{and} \qquad d = (p-1)/2. \tag{4.3}$$

In this case $\dot{K} = \dot{\mathbb{F}}_{p-1} \cdot G$, so any coset of G in $\dot{K}$ has a "scalar" representative. We fix a generator ζ for the group G, and try to put a lower bound on the cardinality of the set $A := \mathbb{F}_p \cap 2 * G$.

Recalling that $m \geq 6$, write

$$(\zeta - 1)G = a_1 G, \quad (\zeta^2 - 1)G = a_2 G, \quad \text{and} \quad (\zeta^4 - 1)G = a_3 G,$$

where $a_i \in \dot{\mathbb{F}}_p$. Clearly, $\pm a_i \in A$, since $-1 \in G$. *First let us assume that these three G-cosets in* $\dot{K}$ *are different*. Since $a_i \neq -a_j$, $\{0, \pm a_i\}$ are seven different elements of A. (In particular, $p \geq 7$ here.) Applying repeatedly the Cauchy–Davenport Theorem in $\mathbb{F}_p$, we see that $|n * A| \geq \min\{p, 6n + 1\}$. It follows that

$$n \geq (p-1)/6 \Rightarrow n * A = \mathbb{F}_p \Rightarrow -1 \in n * A \Rightarrow 2n + 1 \in W_p(m).$$

This yields

$$2\left\lceil \frac{p-1}{6} \right\rceil + 1 \in W_p(m)$$

(where $\lceil \cdot \rceil$ denotes the ceiling function). Writing p in the form $6t \pm 1$, we see easily that

$$2\left\lceil \frac{p-1}{6} \right\rceil = \left\lceil \frac{p-1}{3} \right\rceil.$$

Thus, in this case, we get the stronger conclusion that $[(p-1)/3, \infty)_{\mathbb{Z}} \subseteq W_p(m)$.

From now on, we may assume that the three cosets $\{a_i G\}$ *above are not all different*. If $a_1 G = a_2 G$, then $\zeta^2 - 1 = (\zeta - 1)\zeta^i$ for some i, and so $\zeta^i = \zeta + 1$. Since m is even, this shows that $3 \in W_p(m)$, and so $[2, \infty)_{\mathbb{Z}} \subseteq W_p(m)$. We have certainly no problem in this case (except when $d = 1$, which occurs only when $p = 3$). If $a_2 G = a_3 G$, we can finish similarly. Now assume $a_1G = a_3G$. Here, $\zeta^4 - 1 = (\zeta - 1)\zeta^j$ for some j, so $\zeta^j = \zeta^3 + \zeta^2 + \zeta + 1$. As before, this gives $5 \in W_p(m)$. If $p > 7$, then $d = (p-1)/2 \geq 5$, and we have what we want. Thus we are only left with the cases $p = 3, 5, 7$.

If $p = 3$, we have $d = (p-1)/2 = 1$ (and $m = 3^k - 1$ by (4.3)). In this case the desired conclusion is $[2, \infty)_{\mathbb{Z}} \subseteq W_3(m)$, which is true since $2, 3 \in W_3(m)$.

If $p = 5$, then $d = 2 \in W_5(m)$. In this case we need to show that $3 \in W_5(m)$. If $a_1G = a_2G$, we are done as before. Otherwise, one of these cosets must be the identity coset G (since $[\dot{K}:G] = d = 2$), and this implies again that $3 \in W_5(m)$.

Finally, we treat the case $p = 7$. Here we must show that $[\dot{K}:G] = d = 3$ is in the weight set $W_7(m)$. We first note that

$$\text{If } (\zeta - 1)G = (\zeta^i - 1)G = (\zeta^{i+1} - 1)G \text{ for some } i \geq 1, \text{ then } 3 \in W_7(m). \tag{4.4}$$

Indeed, if we write $\zeta^i - 1 = (\zeta - 1)\zeta^r$ and $\zeta^{i+1} - 1 = (\zeta - 1)\zeta^s$, then $\zeta^r = \zeta^{i-1} + \cdots + \zeta + 1$ and $\zeta^s = \zeta^i + \cdots + \zeta + 1$ imply that $\zeta^s = \zeta^i + \zeta^r$, so $3 \in W_7(m)$. Now let C, C' be the two nonidentity cosets of G in $\dot{K}$. By reasonings we have used before, we may assume that $(\zeta^2 - 1)G = C$ and $(\zeta - 1)G = (\zeta^4 - 1)G = C'$. Noting that 3 is prime to m (since $\gcd(p-1, m) = \gcd(6, m) = 2$), we may also assume, in view of (4.4), that $(\zeta^3 - 1)G = C$. Replacing ζ by ζ^3, we may further assume that $(\zeta^9 - 1)G = C'$. Next, note that since $m \geq 6$, it cannot divide 10, so $\zeta^{10} \neq 1$. Thus, in view of (4.4), we may assume that $(\zeta^5 - 1)G = C$, and hence that $(\zeta^{10} - 1)G = C'$. Now we have $C' = (\zeta - 1)G = (\zeta^9 - 1)G = (\zeta^{10} - 1)G$, so $3 \in W_7(m)$ once more by (4.4) Q.E.D.

5. The Case $\gcd(p-1, m) = 1$

Throughout this section, we shall assume that $\gcd(p-1, m) = 1$ (and as before, $m \geq 3$). The analysis of the weight set $W_p(m)$ in this case turns out to require the hardest work.

The assumption that $\gcd(p-1, m) = 1$ means that the only mth root of unity in $\mathbb{F}_p$ is 1. Therefore, upon factoring the polynomial $X^m - 1$ modulo p, we have

$$X^m - 1 = (X-1)g_1(X)g_2(X)\ldots, \tag{5.1}$$

where the g_i's are irreducible monic polynomials in $\mathbb{F}_p[X]$, each of degree

≥ 2. Let $l := \min\{\deg(g_i)\}$. This integer l will play an important role in finding the estimates on $W_p(m)$ in this section, so let us first note a few other characterizations of it.

Recall that the cyclotomic polynomial $\Phi_n(X) \in \mathbb{Z}[X]$ factors modulo p into a product of irreducible factors each of degree given by the order of the element p in the unit group $U(\mathbb{Z}/n\mathbb{Z})$ (see, e.g. [Gu]). Since $X^m - 1 = \prod_{n|m} \Phi_n(X)$, it follows that l is the minimum of the orders of p in $U(\mathbb{Z}/n\mathbb{Z})$ for n ranging over the divisors of m greater than 1. From this, we see that l is also the minimum of the orders of p in $U(\mathbb{Z}/q\mathbb{Z})$ for q ranging over the prime divisors of m. It is now an easy exercise to check the following:

$$l = \min\{e \geq 1\colon \gcd(p^e - 1, m) > 1\}. \tag{5.2}$$

This simply means that $\mathbb{F}_{p^l}$ is the field with the smallest extension degree over $\mathbb{F}_p$ which contains an mth root of unity other than 1. This can also be verified directly from the definition of l.

For the rest of this section, let $L := \mathbb{F}_{p^l}$, $m' := \gcd(p^l - 1, m)$, and let H be group of m'th roots of unity in L. By (5.2), $|H| = m' \geq 2$. It will be important to work with the set $T := \mathrm{tr}(H)$, where "tr" denotes the field trace from L to $\mathbb{F}_p$. The next theorem gives a description of $W_p(m)$ in terms of l and the cardinality $t := |T|$ (under the standing assumption that $\gcd(p - 1, m) = 1$).

THEOREM 5.3. *Let l and t be as defined above, and let*

$$n := \left\lceil \frac{p-1}{t-1} \right\rceil .$$

Then $[ln, \infty)_{\mathbb{Z}} \subseteq W_p(m') \subseteq W_p(m)$.

Proof. Applying the Cauchy-Davenport Theorem to the subset T in $\mathbb{F}_p$, we have $|2 * T| \geq \min\{p, 2t - 1\}$, and inductively $|i * T| \geq \min\{p, it - (i - 1)\}$. By the definition of n, we have $n(t - 1) \geq p - 1$, so $nt - (n - 1) \geq p$. Therefore, $|n * T| = p$. In particular, for every $j \geq 0$, there exists an equation $t_1 + \cdots + t_n = -j \in \mathbb{F}_p$, where all $t_i \in T$. Now each $t_i \in \mathrm{tr}(H)$ is a sum of l elements of H, so $t_1 + \cdots + t_n + j \cdot 1 = 0$ is a vanishing sum of m'th roots of unity of weight $ln + j$. This shows that $[ln, \infty)_{\mathbb{Z}} \subseteq W_p(m') \subseteq W_p(m)$, as desired. Q.E.D.

Note that the above theorem is meaningful only if we know that the trace set $T \subseteq \mathbb{F}_p$ has at least two elements. Fortuitously, this is always the case, according to the following result.

TRACE LEMMA 5.4. *In the notations of* (5.3), $t = |T| \geq 2$.

The proof of this lemma will be postponed to the last section (Section 6). We shall first assume this lemma and try to get to the main conclusions of this section. Note that the larger the trace set T is, the better bound on $W_p(m)$ is given by (5.3). Since $t \geq 2$ by (5.4), we have in any case:

COROLLARY 5.5. $[l(p-1), \infty)_{\mathbb{Z}} \subseteq W_p(m') \subseteq W_p(m)$.

Now consider any field $K = \mathbb{F}_{p^k}$ containing the group G of all mth roots of unity. Clearly, $L \subseteq K$, and $H = \dot{L} \cap G$. Let $d = (p^k - 1)/m$ and $d' = (p^l - 1)/m'$. We now proceed to the proof of the following, which is a stronger version of Theorem 1.3 in the case treated in this section.

THEOREM 5.6. *Assume that* $\gcd(p-1, m) = 1$. *Then* $[d', \infty)_{\mathbb{Z}} \subseteq W_p(m')$ *and* $[d, \infty)_{\mathbb{Z}} \subseteq W_p(m)$ *except in the following two special cases*: (A) $d' = p - 1$; (B) $p = 2$, $d' = 3$, *and* $m' = 5$. *In these special cases, we have* $[d'+1, \infty)_{\mathbb{Z}} \subseteq W_p(m')$ *and* $[d+1, \infty)_{\mathbb{Z}} \subseteq W_p(m)$.

Proof. Since $d' = [\dot{L} : H] = [\dot{L}G : G]$ divides $d = [\dot{K} : G]$ and $m' \mid m$, it suffices to prove the theorem for $W_p(m')$. Let

$$s = (p^{l-1} + \cdot \cdot \cdot + p + 1)/m', \tag{5.7}$$

so that $d' = s(p-1)$. *First let us treat the special case* (A), *where we have* $s = 1$. Here we are supposed to prove that $[p, \infty)_{\mathbb{Z}} \subseteq W_p(m')$. Since now $[\dot{L} : H] = p - 1$ (and $H \cap \mathbb{F}_p = \{1\}$), we have $\dot{L} = H \cdot \dot{\mathbb{F}}_p$. Therefore, fixing a primitive m'th root of unity $\alpha \in H$, we have $\alpha - 1 = b^{-1}\alpha^i$ for some integer i and some $b \in \dot{\mathbb{F}}_p$. For convenience, let us think of b as an integer in $[1, p-1]$. Multiplying $b \cdot 1 + (p-b) \cdot 1 = 0 \in \mathbb{F}_p$ by α and using the relation $b\alpha = b + \alpha^i$, we get

$$0 = b\alpha + (p-b)\alpha = b \cdot 1 + \alpha^i + (p-b)\alpha,$$

which is a vanishing sum of weight $p + 1$. Multiplying this by α again and repeating the argument, we get vanishing sums (of m'th roots of unity) of weight $p + i$ for any $i > 0$. Coupled with $p \in W_p(m')$, this gives $[p, \infty)_{\mathbb{Z}} \subseteq W_p(m')$, as desired. *For the rest of the proof, we may asume that* $s > 1$. We claim the following:

LEMMA 5.8. $s > 1$ *implies that* $s \geq l$, *except perhaps when* $p = 2$ *and* $l = 4, 6, 8, 9$.

Thus, leaving aside the four special cases, we have $d' = s(p-1) \geq l(p-1)$, so the desired conclusion for $W_p(m')$ in (5.6) follows from (5.5). The four special cases will have to be treated later.

Proof of Lemma 5.8. We go into the following two cases.

Case 1. l is prime. We claim that $l \le q$ for any prime $q \mid s$ (and therefore $l \le s$). In fact, from (5.7), we get $p^{l-1} + \cdots + p + 1 \equiv 0 \pmod q$, so $p^l \equiv 1 \pmod q$. If $p \not\equiv 1 \pmod q$, then p has order l in $U(\mathbb{Z}/q\mathbb{Z})$ (since l is prime), and so $l \mid (q-1)$. In this case $l \le q - 1 < q$. If $p \equiv 1 \pmod q$, then from $p^{l-1} + \cdots + p + 1 \equiv l \equiv 0 \pmod q$, we have in fact $l = q$.

Case 2. l is composite. Let q be the smallest prime divisor of l and write $l = qt$. Then $1 < t < l$ and (5.2) implies that $\gcd(p^t - 1, m) = 1$. Since $(p^t - 1) \mid (p^l - 1)$, we see that $p^t - 1$ divides $(p^l - 1)/m' = s(p-1)$. Thus, $s \ge (p^t - 1)/(p-1)$. We shall now exploit the following elementary fact which is easy to prove using calculus:

LEMMA 5.9. $p^x \ge (p-1)x^2 + 1$ *for every* $x \in [2, \infty)_{\mathbb{Z}}$ *with the exception of* $p = 2$ *and* $x = 2, 3, 4$.

Applying this lemma to $x = t$, we get the desired conclusion

$$s \ge \frac{p^t - 1}{p - 1} \ge t^2 \ge qt = l,$$

except when $p = 2$ and $t = 2, 3, 4$. If $t = 2$, we have $q = 2$ so $l = 4$. If $t = 3$, we have $q = 2, 3$, so $l = 6$ or 9. Finally, if $t = 4$, we have $q = 2$ so $l = 8$. This proves (5.8), but we still have to complete the proof of (5.6) in the four special cases noted.

In these cases, $d' = (2^l - 1)/m'$, so both m', d' are odd (and >1). *We may assume that* $d' < m'$. (For, if $d' \ge m'$, we have $[m', \infty)_{\mathbb{Z}} \subseteq W_2(m')$ since m' is odd, and hence $[d', \infty)_{\mathbb{Z}} \subseteq W_2(m')$.) We simply have to check the four outstanding cases individually.

(1) $l = 4$. Here $2^l - 1 = 15$, so $d' = 3$, $m' = 5$, and we are in the case (B) of (5.6). The desired conclusion in this case is $[4, \infty)_{\mathbb{Z}} \subseteq W_2(m')$, which is true since $5 = m' \in W_2(m')$. In fact, by (2.6), we have $W_2(5) = 2\mathbb{N} + 5\mathbb{N} = \{0, 2\} \cup [4, \infty)_{\mathbb{Z}}$. In particular, $3 \notin W_2(5)$, so this case is truly exceptional.

(2) $l = 6$. Here $2^l - 1 = 63$, so we have either $d' = 7$, $m' = 9$ or $d' = 3$, $m' = 21$. In both cases, $[2, \infty)_{\mathbb{Z}} \subseteq W_2(m')$ (since $2, 3 \in W_2(m')$), so there is no problem. (Actually, in the case $d' = 7$, we are in the good case $s = d' \ge l$ already.)

(3) $l = 8$. Here $2^l - 1 = 255$, so we have either $d' = 5$, $m' = 51$ or $d' = 15$, $m' = 17$. The latter case presents no problems, since we are once more in the good case $s = d' \ge l$. In the former case, $3 \mid m'$ implies that $W_2(m') = [2, \infty)_{\mathbb{Z}}$, so again there is no problem.

(4) $l = 9$. Here $2^l - 1 = 511$, so $d' = 7$, $m' = 73$. We have shown in (2.5) that $W_2(73) = \{0\} \cup [2, \infty)_{\mathbb{Z}}$, so there is no problem.

This finally completes the proof of Theorem 5.6.

6. TRACES OF mth ROOTS OF UNITY

In Section 5, we stated without proof the Trace Lemma 5.4, which was crucial for the proofs of (5.5) and (5.6). In this section, we return to the trace set $T = \text{tr}(H)$ and ofer a general analysis of T which we believe to be of independent interest. The proof of the Trace Lemma is an easy by-product of this general analysis.

The notations (and hypotheses) introduced at the beginning of Section 5 will remain in force. In particular, H is the group of m'th roots of unity in $L = \mathbb{F}_{p^l}$, and "tr" is the field trace from L to $\mathbb{F}_p$. To enumerate the elements in T, let

$$X^{m'} - 1 = (X - 1)h_1(X) \cdot \cdot \cdot h_r(X) \tag{6.1}$$

be the factorization of $X^{m'} - 1$ into (monic) irreducibles over $\mathbb{F}_p$. Then $\deg h_i \geq l$ by the definition of l (and the fact that $(X^{m'} - 1) \mid (X^m - 1)$). On the other hand, since L contains all m'th roots of unity, each $h_i(X)$ splits completely in L, so $\deg h_i \leq [L : \mathbb{F}_p] = l$. Therefore, $\deg h_i = l$ for all i. Let

$$h_i(X) = X^l - a_i X^{l-1} + \cdot \cdot \cdot , \tag{6.2}$$

and let $\{\alpha_{ij}\}$ be all the roots of $h_i(X)$ in L. For each h_i, we can identify the field $\mathbb{F}_p[X]/(h_i(X))$ with L by the correspondence $\overline{X} \leftrightarrow \alpha_{ij}$ (for any j). Therefore, $\text{tr}(\alpha_{ij}) = \sum_k \alpha_{ik} = a_i$ for all i, j. We have thus

$$T = \{\text{tr}(1), a_1, . . . , a_r\} = \{l, a_1, . . . , a_r\}, \tag{6.3}$$

with possible duplications.

It is now easy to prove the Trace Lemma 5.4, which asserted that $|T| \geq 2$. Assume, for the moment, that T is a singleton. Then, by (6.3), $a_i = l$ for all i. Summing all roots of the polynomial in (6.1) (and recalling that $m' \geq 2$), we get

$$0 = 1 + a_1 + \cdot \cdot \cdot + a_r = 1 + rl = m' \in \mathbb{F}_p,$$

contradicting the fact that m' is prime to p.

Equation (6.3) gives an upper bound $|T| \leq 1 + r$, and this becomes an equality iff the elements listed in (6.3) are distinct. *This is the case, for instance if* $l = 2$. To see this, note that the constant term of each $h_i(X)$ in (6.1) is 1, since it is an mth root of unity in $\mathbb{F}_p$, and we are assuming that $\gcd(p - 1, m) = 1$. Therefore, if $l = 2$, we have $h_i(X) = X^2 - a_i X + 1$. Since the h_i's are distinct, so are the a_i's, and of course $a_i \neq 2$ (since otherwise $h_i(X) = (X - 1)^2$). Therefore, $|T| = 1 + r$, and (5.3) gives the pretty good estimate

$$[2n, \infty)_{\mathbb{Z}} \subseteq W_p(m') \subseteq W_p(m) \qquad \text{with} \qquad n = \left\lceil \frac{p-1}{r} \right\rceil .$$

For a simple example of this, let $p = 5$, and $m = 3$. Here $m' = 3$, $l = 2$, $r = 1$, $L = \mathbb{F}_{25}$, and $|T| = 2$. By (2.6), $W_5(3)$ is the set

$$3\mathbb{N} + 5\mathbb{N} = \{0, 3, 5, 6\} \cup [8, \infty)_{\mathbb{Z}}.$$

Since $2n = 8$, the conclusion in (5.3) is sharp here.

In general, $t := |T|$ may be less than $1 + r$, since there may be duplications among the elements of T listed in (6.3). For an example where interesting duplications occur, take $p = 7$ and $m = 19$. Here $m' = 19$ and $l = 3$, $r = 6$. *Mathematica* gives a factorization

$$\begin{aligned} X^{19} - 1 = &(X - 1)(X^3 + 2X + 6)(X^3 + 4X^2 + X + 6) \\ &(X^3 + 4X^2 + 4X + 6) \cdot (X^3 + 5X^2 + 6) \\ &(X^3 + 3X^2 + 3X + 6)(X^3 + 6X^2 + 3X + 6) \in \mathbb{F}_7[X]. \end{aligned}$$

Since $-4 = 3 = \mathrm{tr}(1)$ in $\mathbb{F}_7$, T has only five (two less than $1 + r = 7$) distinct elements $\{0, 1, 2, 3, 4\}$. In this case, the number n in (5.3) is $\left\lceil \frac{7-1}{5-1} \right\rceil = 2$, and (5.3) shows that $[6, \infty)_{\mathbb{Z}} \subseteq W_7(19)$. Note that, in spite of the trace duplications, this is still much sharper than what is given in (5.6).

In general, we cannot hope to improve upon the lower bound $|T| \geq 2$. For one thing, $\mathbb{F}_p$ may have only two elements to begin with. Also, we may have $r = 1$, in which case (5.4) and (6.3) show that $|T| = 2$. Even if $p \geq 3$ and $r \geq 2$, there are many cases in which T is just a doubleton. Let us illustrate the situation $r = 2$ by taking m to be an odd prime q (so that $m' = q$ too), and assuming that p is also odd and has order $l = (q - 1)/2$ in the group $U(\mathbb{Z}/q\mathbb{Z})$. In this case, $r = 2$, and (6.1) becomes

$$X^q - 1 = (X - 1)h_1(X)h_2(X), \tag{6.4}$$

where h_1, h_2 are monic irreducible (over $\mathbb{F}_p$) of degree l. Following a standard notation in number theory, let us define q^* to be q if $q \equiv 1 \pmod 4$, and q^* to be $-q$ if $q \equiv 3 \pmod 4$. Then the size of the trace set $T = \mathrm{tr}(H)$ is determined as follows.

PROPOSITION 6.5. *Under the above assumptions* $|T| = 2$ *iff* $p \mid (q^* - 1)$ (*and* $|T| = 3$ *otherwise*).

Proof. Let $E = \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/q}$, and fix a generator t of $U(\mathbb{Z}/q\mathbb{Z})$. Then $\sigma\colon \zeta \mapsto \zeta^t$ is a generator for $\mathrm{Gal}(E/\mathbb{Q})$, and $\sigma^2\colon \zeta \mapsto \zeta^{t^2}$ is a generator for $\mathrm{Gal}(E/F)$, where F is the fixed field E^{σ^2}. Note that $X^{q-1} + \cdots + X + 1$ factors into $f(X)g(X)$ over $F[X]$, where

$$f(X) = X^l - aX^{l-1} + \cdots \qquad \text{and} \qquad g(X) = X^l - bX^{l-1} + \cdots$$

are, respectively, the minimal polynomials of ζ and ζ^t over F. We have

$$a - b = \mathrm{tr}_{E/F}(\zeta) - \mathrm{tr}_{E/F}(\zeta^t) = \sum_{j=0}^{l-1} \zeta^{t^{2j}} - \sum_{j=0}^{l-1} \zeta^{t^{2j+1}} \in F.$$

This is precisely the quadratic Gauss sum (with respect to the Legendre character on $\mathbb{F}_q$), so by [IR, (8.2.2)], $a - b = \sqrt{q^*}$. (Gauss showed that the $\sqrt{q^*}$ here is the one taken in the upper half plane if $q \equiv 3 \pmod 4$, but this will not be needed in the following.) Since we also have $a + b = -1$, it follows that

$$a = (\sqrt{q^*} - 1)/2, \qquad b = -(\sqrt{q^*} +)/2.$$

Incidentally, this proves the well-known fact that $F = \mathbb{Q}(\sqrt{q^*})$.

Let R be the ring of algebraic integers in F. Since p is unramified in E, it is also unramified in F, so $pR = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}, \mathfrak{p}'$ are distinct prime ideals of R, both of residue degree 1. Identifying $R/\mathfrak{p}$ with $\mathbb{F}_p$, we may take the polynomials h_1, h_2 in (6.4) to be $\bar{f}$ and $\bar{g}$ where "bar" means reduction modulo $\mathfrak{p}$. In particular, $T = \{l, \bar{a}, \bar{b}\}$ by (6.3). Here the two elements $\bar{a}, \bar{b}$ are *always* different (for otherwise $\mathfrak{p}$ would contain $(a - b)^2 = q^*$ as well as p). Therefore, T will have only two elements iff $\mathfrak{p}$ also contains

$$4(l - a)(l - b) = (q - \sqrt{q^*})\,(q + \sqrt{q^*}) = q^2 - q^* = q^*(q^* - 1).$$

Since $q^* \notin \mathfrak{p}$, this happens iff $q^* - 1 \in \mathfrak{p}$, that is, iff $p \mid (q^* - 1)$, as claimed. Q.E.D.

COROLLARY 6.6. *Let* $q = 2l + 1$ *and* $p = 2l' + 1$ *be distinct primes such that the order of* p *is* l *modulo* q. *If* $p \mid (q^* - 1)$, *then* $[2ll', \infty)_{\mathbb{Z}} \subseteq W_p(q)$. *Otherwise*, $[ll', \infty)_{\mathbb{Z}} \subseteq W_p(q)$.

Proof. This follows from (5.3) and (6.5), since the number n in (5.3) is $2l'$ in the first case and l' in the second case. Q.E.D.

EXAMPLE 6.7. Let $q = 11$ (with $q^* = -11$). Then the primes 3 and 5 both have order $l = (q-1)/2 = 5$ modulo q, and according to *Mathematica*:

$$X^{11} - 1 = (X-1)(X^5 + X^4 + 2X^3 + X^2 + 2)$$
$$(X^5 + 2X^3 + X^2 + 2X + 2) \in \mathbb{F}_3[X],$$

$$X^{11} - 1 = (X-1)(X^5 + 2X^4 + 4X^3 + X^2 + X + 4)$$
$$(X^5 + 4X^4 + 4X^3 + X^2 + 3X + 4) \in \mathbb{F}_5[X].$$

Thus, for $p = 3$, $T = \{l, -1, 0\} = \{2, 0\}$ in $\mathbb{F}_3$. This is consistent with (6.5) since $p = 3$ divides $q^* - 1 = -12$. Here, $l = 5$, $l' = 1$, so (6.6) gives $[10, \infty)_{\mathbb{Z}} \subseteq W_3(11)$. (In fact, from $0, 2 \in T$, we see easily that $5, 6 \in W_3(11)$, and so $8, 9 \in W_3(11)$ also.) On the other hand, if we choose $p = 5$, then $T = \{l, -2, -4\} = \{0, 3, 1\}$ in $\mathbb{F}_5$, consistently with (6.5) since $p = 5$ does not divide $q^* - 1 = -12$. Here, $l = 5$, $l' = 2$, so (6.6) gives again $[10, \infty)_{\mathbb{Z}} \subseteq W_5(11)$, and $0, 1, 3 \in T$ show further that $5, 7, 9 \in W_5(11)$.

The arguments in the proof of (6.5) can be generalized. However, if the order of p modulo q is smaller than $(q-1)/2$ (in other words $r > 2$), the computations of the trace elements in T will involve Gaussian sums with (higher) character values as coefficients. We shall not go into this analysis here. We should point out, however, that if q is *fixed*, then the prime ideal method (in characteristic 0) used in the proof of (6.5) will suffice to show that the upper bound $|T| \leq 1 + r$ becomes an *equality* for sufficiently large p. Therefore, by (5.3),

$$[ln, \infty)_{\mathbb{Z}} \subseteq W_p(q) \qquad \text{with} \qquad n = \left\lceil \frac{p-1}{r} \right\rceil,$$

for sufficiently large p.

ACKNOWLEDGMENT

We thank the referee of this paper, whose comments enabled us to rewrite more accurately the last paragraph in Section 1 comparing the use of different methods in treating diagonal equations over finite fields.

REFERENCES

[BS] Z. I. Borevich and I. R. Sharfarevich, "Number Theory," Academic Press, New York/ London, 1966.

[Gr] M. J. Greenberg, ‘‘Lectures on Forms in Many Variables,’’ Mathematics Lecture Notes Series, Benjamin, Reading, MA, 1969.

[Gu] W. J. Guerrier, The factorization of the cyclotomic polynomial mod p, *Amer. Math. Monthly* **75** (1968), 46.

[IR] K. Ireland and M. Rosen, ‘‘A Classical Introduction to Modern Number Theory,’’ Graduate Texts in Mathematics, Vol. 84, Springer-Verlag, Berlin/Heidelberg/New York, 1982.

[La] T. Y. Lam, ‘‘The Algebraic Theory of Quadratic Forms,’’ Mathematics Lecture Notes Series, Benjamin, Reading, MA, 1973. (Second printing with revisions, 1980.)

[LL] T. Y. Lam and K. H. Leung, On vanishing sums of roots of unity, preprint series, MSRI, 1995.

[LeV] W. LeVeque, ‘‘Topics in Number Theory, Vol. 1,’’ Addison-Wesley, Reading, MA, 1956.

[Ln] R. Lidl and H. Neidereiter, ‘‘Finite Fields,’’ Encyclopedia of Mathematics and Its Applications, Vol. 20, Addison-Wesley, Reading, MA, 1983.

[Ma] H. B. Mann, ‘‘Addition Theorems,’’ Krieger, Huntington, NY, 1976.

[QY] S. Qi and P.-Z. Yuan, On the number of solutions of diagonal equations over a finite field, *Finite Fields Appl.* **2** (1996), 35–41.

[Sch] W. Schmidt, ‘‘Equations over Finite Fields,’’ Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin/Heidelberg/New York, 1976.

[Sm] C. Small, ‘‘Arithmetic of Finite Fields,’’ Dekker, New York/Basel/Hong Kong, 1991.

[Wi] E. Witt, Theorie der quadratischen Formen über beliebigen Körpern, *J. Reine Angew. Math.* **176** (1937), 31–44.