ACTA ARITHMETICA
LXXXIII.3 (1998)

Explicit evaluations of some Weil sums

by

Robert S. Coulter (St. Lucia, Qld.)

1. Introduction. In this article we will explicitly evaluate exponential sums of the form

$$\sum_{x\in\mathbb{F}_q} \chi(ax^{p^\alpha+1})$$

where χ is a non-trivial additive character of the finite field $\mathbb{F}_q$ with $q = p^e$ odd and $a \in \mathbb{F}_q$. The case $a = 0$ is trivial and so we assume throughout that $a \neq 0$. These sums form a subset of a much larger class of exponential sums of the form

$$\sum_{x\in\mathbb{F}_q} \chi(f(x))$$

where $f \in \mathbb{F}_q[X]$. These sums are also known as *Weil sums*. The problem of explicitly evaluating these sums is quite often difficult. Results giving estimates for the absolute value of the sum are more common and such results have been regularly appearing for many years. The book [5] by Lidl and Niederreiter gives an overview of this area of research in the concluding remarks of Chapter 5.

As with previous explicit evaluations, the special form of our polynomial will play an integral part. In [1] Carlitz obtained explicit evaluations of Weil sums with $f(X) = aX^{p+1} + bX$. His methods involved first obtaining evaluations when $b = 0$ and then proceeding to the general case. This article is largely a generalisation of the methods used by Carlitz in the first part of [1]. A further article dealing with the second part of Carlitz' evaluation method is under preparation.

The polynomials studied in this article are of the form $f(X) = aX^{p^\alpha+1}$ where α is an arbitrary natural number. These monomials are a subset of the class of polynomials known as Dembowski–Ostrom polynomials (or D–O polynomials). We may define a *D–O polynomial* to be any polynomial which, when reduced, has the shape

1991 *Mathematics Subject Classification*: Primary 11T24.

$$f(X) = \sum_{i,j=0}^{e-1} a_{ij} X^{p^i+p^j}.$$

D–O polynomials play an important role in the study of planar functions (see [4, 2]). This article was motivated by the connection between bent polynomials and planar polynomials recently identified in a joint article by the author and Matthews [3]. In that article bent polynomials were defined in terms of character sums and shown to be the multivariate equivalent of planar polynomials over a finite field.

Throughout this article $\mathbb{F}_q$ will denote the finite field of q elements with $q = p^e$ odd, α will denote any natural number and $d = \gcd(\alpha, e) = (\alpha, e)$. We denote the non-zero elements of $\mathbb{F}_q$ by $\mathbb{F}_q^*$. We shall denote by Tr the absolute trace function. The canonical additive character of $\mathbb{F}_q$, denoted by χ_1, is given by

$$\chi_1(x) = e^{2\pi i \mathrm{Tr}(x)/p}$$

for all $x \in \mathbb{F}_q$. Note that $\chi_1(x^p) = \chi_1(x)$ for all $x \in \mathbb{F}_q$. Any additive character χ_a of $\mathbb{F}_q$ can be obtained from χ_1 by $\chi_a(x) = \chi_1(ax)$ for all $x \in \mathbb{F}_q$. Due to this fact we only explicitly evaluate the Weil sums with $\chi = \chi_1$ as it is possible to evaluate the Weil sums for any non-trivial additive character simply by manipulating the results obtained using this identity. We denote our Weil sum by $S_\alpha(a)$. That is,

$$S_\alpha(a) = \sum_{x \in \mathbb{F}_q} \chi_1(a x^{p^\alpha+1}).$$

The evaluation splits into two sections: one for e/d odd and one for e/d even. Our two main results are given in the following two theorems.

THEOREM 1. *Let e/d be odd. Then*

$$S_\alpha(a) = \begin{cases} (-1)^{e-1}\sqrt{q}\,\eta(a) & \text{if } p \equiv 1 \bmod 4, \\ (-1)^{e-1} i^e \sqrt{q}\,\eta(a) & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Here η denotes the multiplicative quadratic character of $\mathbb{F}_q$.

THEOREM 2. *Let e/d be even with $e = 2m$. Then*

$$S_\alpha(a) = \begin{cases} p^m & \text{if } a^{(q-1)/(p^d+1)} \neq (-1)^{m/d} \text{ and } m/d \text{ even}, \\ -p^m & \text{if } a^{(q-1)/(p^d+1)} \neq (-1)^{m/d} \text{ and } m/d \text{ odd}, \\ p^{m+d} & \text{if } a^{(q-1)/(p^d+1)} = (-1)^{m/d} \text{ and } m/d \text{ odd}, \\ -p^{m+d} & \text{if } a^{(q-1)/(p^d+1)} = (-1)^{m/d} \text{ and } m/d \text{ even}. \end{cases}$$

While Theorem 1 can be established easily using known results the proof of Theorem 2 is long and involved, taking up the majority of this article.

2. Preliminaries. Let g be a fixed primitive element of $\mathbb{F}_q$. Then for each $j = 0, \dots, q-2$ we define a multiplicative character λ_j of $\mathbb{F}_q$ by

$$\lambda_j(g^k) = e^{2\pi ijk/(q-1)}$$

for $k = 0, \dots, q-2$. We shall use η to denote the quadratic character of $\mathbb{F}_q$, that is, $\eta = \lambda_{(q-1)/2}$. For any additive character χ and any multiplicative character λ of $\mathbb{F}_q$ we can define the classical Gaussian sum $G(\lambda, \chi)$ by

$$G(\lambda, \chi) = \sum_{x \in \mathbb{F}_q^*} \lambda(x)\chi(x).$$

We have the following results on Gaussian sums which appear in [5].

LEMMA 2.1 ([5, Theorem 5.12]). *For any finite field we have*

(i) $G(\lambda^p, \chi_b) = G(\lambda, \chi_{bp})$,
(ii) $G(\lambda, \chi_{ab}) = \overline{\lambda(a)}G(\lambda, \chi_b)$.

LEMMA 2.2 ([5, Theorem 5.15]). *For $\mathbb{F}_q$ a finite field of odd characteristic we have*

$$G(\eta, \chi_1) = \begin{cases} (-1)^{e-1}\sqrt{q} & \text{if } p \equiv 1 \bmod 4, \\ (-1)^{e-1}i^e\sqrt{q} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

There is one more result on Gaussian sums relevant to our work (see [5, Theorem 5.16]).

LEMMA 2.3 (Stickelberger's Theorem). *Let q be a prime power, let λ be a non-trivial multiplicative character of $\mathbb{F}_{q^2}$ of order k dividing $q+1$ and let χ_1 be the canonical additive character of $\mathbb{F}_{q^2}$. Then*

$$G(\lambda, \chi_1) = \begin{cases} q & \text{if } k \text{ is odd or } (q+1)/k \text{ is even}, \\ -q & \text{if } k \text{ is even and } (q+1)/k \text{ is odd}. \end{cases}$$

The following result on Weil sums will also be required.

LEMMA 2.4 ([5, Theorem 5.30]). *Let $n \in \mathbb{N}$ and λ be a multiplicative character of $\mathbb{F}_q$ of order $d = (n, q-1)$. Then*

$$\sum_{x \in \mathbb{F}_q} \chi(ax^n + b) = \chi(b) \sum_{j=1}^{d-1} \overline{\lambda^j(a)} G(\lambda^j, \chi)$$

for any $a, b \in \mathbb{F}_q$ with $a \neq 0$.

We have the following simple theorem on Weil sums.

THEOREM 2.5. *Let $f(X) = aX^n \in \mathbb{F}_q[X]$ with $q = p^e$ odd and $(n, q-1) = 2$. Then*

$$\sum_{x \in \mathbb{F}_q} \chi_1(f(x)) = \begin{cases} (-1)^{e-1}\sqrt{q}\,\eta(a) & \text{if } p \equiv 1 \bmod 4, \\ (-1)^{e-1}i^e\sqrt{q}\,\eta(a) & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

P r o o f. The theorem is established directly from Lemmas 2.2 and 2.4. ∎

Finally, we will need the following lemma on greatest common divisors.

LEMMA 2.6. *Let $d = (\alpha, e)$ and p be odd. Then*

$$(p^\alpha + 1, p^e - 1) = \begin{cases} 2 & \text{if } e/d \text{ is odd,} \\ p^d + 1 & \text{if } e/d \text{ is even.} \end{cases}$$

Proof. It is well known that $(p^{2\alpha} - 1, p^e - 1) = p^{(2\alpha, e)} - 1$. Now

$$\begin{aligned}(p^{2\alpha} - 1, p^e - 1) &= (p^\alpha - 1, p^e - 1)\left(p^\alpha + 1, \frac{p^e - 1}{(p^\alpha - 1, p^e - 1)}\right) \\ &= (p^d - 1)\left(p^\alpha + 1, \frac{p^e - 1}{p^d - 1}\right).\end{aligned}$$

Further, $(p^\alpha + 1, p^\alpha - 1) = (p^\alpha + 1, p^d - 1) = 2$ and $(p^e - 1)/(p^d - 1) = 1 + p^d + \ldots + p^{((e/d)-1)d}$. Thus

$$(1) \qquad (p^{2\alpha} - 1, p^e - 1) = \begin{cases} \dfrac{p^d - 1}{2}(p^\alpha + 1, p^e - 1) & \text{if } e/d \text{ is odd,} \\ (p^d - 1)(p^\alpha + 1, p^e - 1) & \text{if } e/d \text{ is even.} \end{cases}$$

It is a simple matter to show

$$(2\alpha, e) = \begin{cases} d & \text{if } e/d \text{ is odd,} \\ 2d & \text{if } e/d \text{ is even} \end{cases}$$

and from this and (1) the lemma is established. ∎

3. The case e/d odd. For e/d odd we avoid following the methods that Carlitz applies in [1]. This case can be dealt with simply by using some of the preliminary results given in the previous section.

THEOREM 1. *Let e/d be odd. Then*

$$S_\alpha(a) = \begin{cases} (-1)^{e-1}\sqrt{q}\,\eta(a) & \text{if } p \equiv 1 \bmod 4, \\ (-1)^{e-1} i^e \sqrt{q}\,\eta(a) & \text{if } p \equiv 3 \bmod 4, \end{cases}$$

where η denotes the multiplicative quadratic character.

Proof. For e/d odd we have $(p^\alpha + 1, q - 1) = 2$ by Lemma 2.6. Theorem 2.5 can now be applied to complete the proof. ∎

We note that, at first glance, the results Carlitz achieves in [1] do not appear to be the same as Theorem 1 with $\alpha = 1$. It can be checked, however, that they are indeed equivalent. The different ways in which they are stated can be attributed to the different methods used to prove the results.

4. The solvability of the equation $a^{p^\alpha} x^{p^{2\alpha}} + ax = 0$. We are left with the case e/d even. Clearly $e = 2m$ for some integer m. The following result is of central importance to the remainder of this article.

THEOREM 4.1. *For $e = 2m$ the equation*

$$a^{p^\alpha} x^{p^{2\alpha}} + ax = 0$$

is solvable for $x \in \mathbb{F}_q^*$ if and only if e/d is even and

$$a^{(q-1)/(p^d+1)} = (-1)^{m/d}.$$

In such cases there are $p^{2d} - 1$ non-zero solutions.

Proof. We wish to solve

$$x^{p^{2\alpha}-1} = -a^{1-p^\alpha} \tag{2}$$

with $x \in \mathbb{F}_q^*$. Suppose there exists a solution to (2). By raising both sides of (2) by $(q-1)/(p^d-1)$ it is clear that e/d must be even since

$$(x^{p^{2\alpha}-1})^{(q-1)/(p^d-1)} = (-a^{p^\alpha-1})^{(q-1)/(p^d-1)}$$

implies

$$1 = (-1)^{(q-1)/(p^d-1)} (a^{q-1})^{(p^\alpha-1)/(p^d-1)} = (-1)^{e/d}.$$

For e/d even $(q-1)/(p^{2d}-1)$ is an integer. If we now raise both sides of (2) by $(q-1)/(p^{2d}-1)$ we obtain the condition

$$(-a^{p^\alpha-1})^{(q-1)/(p^{2d}-1)} = 1$$

or equivalently

$$a^{(q-1)(p^\alpha-1)/(p^{2d}-1)} = (-1)^{m/d}.$$

Now $(p^\alpha - 1, q-1) = p^d - 1$ and $(p^\alpha-1)/(p^d-1)$ is odd when α/d is odd. So we can simplify the condition by noticing that in such cases

$$(a^{(q-1)/(p^d+1)})^{(p^\alpha-1)/(p^d-1)} = ((-1)^{m/d})^{(p^\alpha-1)/(p^d-1)}$$

or equivalently $a^{(q-1)/(p^d+1)} = (-1)^{m/d}$. So if equation (2) is solvable then e/d is even and $a^{(q-1)/(p^d+1)} = (-1)^{m/d}$.

Now let e/d be even with $e = 2m$. Let g be a primitive element of $\mathbb{F}_q$ and $a = g^t$ satisfy $a^{(q-1)/(p^d+1)} = (-1)^{m/d}$. If m/d is even then $t = s(p^d+1)$ and if m/d is odd then $t = (2s+1)(p^d+1)/2$. We wish to show that there exists some $x \in \mathbb{F}_q^*$ satisfying (2). Equivalently, we wish to prove that for any integer s there exists some integer r, with $x = g^r$, satisfying

$$g^{r(p^{2\alpha}-1)} = g^{(q-1)/2} g^{s(p^d+1)(1-p^\alpha)}$$

when m/d is even, or

$$g^{r(p^{2\alpha}-1)} = g^{(q-1)/2} g^{(2s+1)(p^d+1)(1-p^\alpha)/2}$$

when m/d is odd. In both cases we wish to prove the result without conditions on s.

Recall $iu \equiv v \bmod n$ has a solution i if and only if $(u,n) \mid v$. Suppose first that m/d is even. Then there exists an integer r satisfying

$$g^{r(p^{2\alpha}-1)} = g^{(q-1)/2} g^{s(p^d+1)(1-p^\alpha)}$$

for any s if and only if $(p^{2\alpha}-1, q-1) = p^{2d}-1$ divides

$$s(p^d+1)(1-p^\alpha) + (q-1)/2.$$

This is satisfied without conditions on s as $p^{2d}-1$ divides both $(p^d+1)(1-p^\alpha)$ and $(q-1)/2$ when m/d is even.

Now suppose m/d is odd. Then there exists an integer r satisfying

$$g^{r(p^{2\alpha}-1)} = g^{(q-1)/2} g^{(2s+1)(p^d+1)(1-p^\alpha)/2}$$

for any s if and only if $p^{2d}-1$ divides

$$\frac{(2s+1)(p^d+1)(1-p^\alpha)}{2} + \frac{q-1}{2}$$

or equivalently if and only if

$$\frac{(2s+1)(1-p^\alpha)}{p^d-1} + \frac{q-1}{p^{2d}-1}$$

is even. As m/d is odd so too is $(q-1)/(p^{2d}-1)$. Also, as e/d is even we have α/d is odd and so $(2s+1)(1-p^\alpha)/(p^d-1)$ is odd for any s. Thus under our assumptions equation (2) is solvable without conditions on s. Let x_0 be any such solution. Then for any $w \in \mathbb{F}_{p^{2d}}$ the element $x = wx_0$ will be a solution of the equation. Thus it is clear that there will be $(p^{2\alpha}-1, q-1) = p^{2d}-1$ non-zero solutions. ∎

We make the following observations in regard to Theorem 4.1. Let $f(X) = a^{p^\alpha} X^{p^{2\alpha}} + aX$. The polynomial f belongs to the well known class of polynomials called *linearised* (*or affine*) *polynomials*. These polynomials have been extensively studied (see [5] for some of their properties). In particular, a linearised polynomial is a permutation polynomial if and only if $x = 0$ is its only root in $\mathbb{F}_q$ (see [5, Theorem 7.9]). Theorem 4.1 thus tells us that f is a permutation polynomial over $\mathbb{F}_q$ with $q = p^e$ and $e = 2m$ if and only if either e/d is odd or e/d is even and $a^{(q-1)/(p^d+1)} \neq (-1)^{m/d}$.

5. The absolute value of $S_\alpha(a)$ with $e = 2m$. The proof of Theorem 2 will involve two steps. In this section we shall prove that $S_\alpha(a)$ is a real number and calculate its absolute value. This will leave us only with the task of determining the sign, which we deal with in the following section. We note that throughout this section we only require that $e = 2m$. It is only in determining the sign that we will need to assume e/d is even.

LEMMA 5.1. *For $e = 2m$ there exists some $x \in \mathbb{F}_q$ satisfying $x^{p^\alpha+1} = -1$.*

Proof. The equation $x^{p^\alpha+1} = -1$ is solvable in $\mathbb{F}_q$ if and only if $(p^\alpha + 1, q-1)$ divides $(q-1)/2$. If e/d is odd then by Lemma 2.6 this is equivalent to $4 \mid q-1$, which is always true as $e = 2m$. If e/d is even then the equation is solvable if and only if $p^d + 1 \mid (q-1)/2$. This is equivalent to $(q-1)/(p^d+1)$ being even, which will occur if and only if e/d is even. ∎

LEMMA 5.2. *For $e = 2m$ we have $S_\alpha(a) = S_\alpha(-a) = \overline{S_\alpha(a)}$.*

Proof. From the previous lemma there exists $z \in \mathbb{F}_q$ satisfying $z^{p^\alpha+1} = -1$. From the definition

$$\begin{aligned} S_\alpha(a) &= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1}) = \sum_{x\in\mathbb{F}_q} \chi_1(a(zx)^{p^\alpha+1}) \\ &= \sum_{x\in\mathbb{F}_q} \chi_1(-ax^{p^\alpha+1}) = S_\alpha(-a). \end{aligned}$$

To prove the second equality note that

$$S_\alpha(a) = \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1}) = \sum_{x\in\mathbb{F}_q} \chi_1(-ax^{p^\alpha+1}) = \sum_{x\in\mathbb{F}_q} \overline{\chi_1(ax^{p^\alpha+1})},$$

which can only occur if $S_\alpha(a)$ is real, i.e. only when $S_\alpha(a) = \overline{S_\alpha(a)}$. ∎

The immediate consequence relevant to our discussion is that we now know that if $e = 2m$ then $S_\alpha(a)$ is a real number and so $S_\alpha^2(a) = |S_\alpha(a)|^2$. We have now established enough background material to prove our first result on $S_\alpha(a)$ with e/d even. Note that at this stage we only require e to be even.

THEOREM 5.3. *For $e = 2m$ we have*

$$S_\alpha(a) = \pm \begin{cases} p^m & \text{if } e/d \text{ odd}, \\ p^m & \text{if } e/d \text{ is even and } a^{(q-1)/(p^d+1)} \neq (-1)^{m/d}, \\ p^{m+d} & \text{if } e/d \text{ is even and } a^{(q-1)/(p^d+1)} = (-1)^{m/d}. \end{cases}$$

Proof. By Lemma 5.2,

$$\begin{aligned} S_\alpha^2(a) &= S_\alpha(a)S_\alpha(-a) \\ &= \sum_{w,y\in\mathbb{F}_q} \chi_1(aw^{p^\alpha+1} - ay^{p^\alpha+1}) \\ &= \sum_{x,y\in\mathbb{F}_q} \chi_1(a(x+y)^{p^\alpha+1} - ay^{p^\alpha+1}) \\ &= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1}) \sum_{y\in\mathbb{F}_q} \chi_1(ax^{p^\alpha}y + axy^{p^\alpha}) \\ &= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1}) \sum_{y\in\mathbb{F}_q} \chi_1((a^{p^\alpha}x^{p^{2\alpha}} + ax)y^{p^\alpha}). \end{aligned} \tag{3}$$

The inner sum is zero unless $a^{p^\alpha}x^{p^{2\alpha}}+ax=0$. By Theorem 4.1, if e/d is odd or e/d is even and $a^{(q-1)/(p^d+1)} \neq (-1)^{m/d}$ then the only solution to this equation is $x=0$, from which the first two cases of the theorem follow. If e/d is even and $a^{(q-1)/(p^d+1)} = (-1)^{m/d}$ then there are a total of p^{2d} solutions to this equation. Moreover, for any such x_0 satisfying $a^{p^\alpha}x^{p^{2\alpha}} + ax = 0$ we have

$$(ax_0^{p^\alpha+1})^{p^\alpha} = a^{p^\alpha}x_0^{p^{2\alpha}}x_0^{p^\alpha} = -ax_0^{p^\alpha+1}$$

so that

$$\chi_1(ax_0^{p^\alpha+1}) = \chi_1((ax_0^{p^\alpha+1})^{p^\alpha}) = \overline{\chi_1(ax_0^{p^\alpha+1})}.$$

As p is odd we have $\chi_1(ax_0^{p^\alpha+1}) = 1$. Combining this with equation (3) yields the final case of our theorem and completes the proof. ∎

We note that the first case of Theorem 5.3 and Theorem 1 with $e = 2m$ coincide.

6. Determining the sign of $S_\alpha(a)$ with e/d even. It remains to determine the sign of $S_\alpha(a)$ with e/d even. So far, for e/d even, we have been generalising arguments used by Carlitz in [1]. We continue in this vein throughout the remainder of this article.

THEOREM 6.1. *Let e/d be even and let $N = N_\alpha(a,q)$ denote the number of solutions $(x,y) \in \mathbb{F}_q \times \mathbb{F}_q$ of the equation*

$$ax^{p^\alpha+1} = y^{p^d} - y.$$

Then

$$N = q + (p^d - 1)S_\alpha(a).$$

Proof. We have

$$\begin{aligned} qN &= \sum_{w\in\mathbb{F}_q}\sum_{x,y\in\mathbb{F}_q}\chi_1(w(ax^{p^\alpha+1} - y^{p^d} + y)) \\ &= q^2 + \sum_{w\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_q}\chi_1(awx^{p^\alpha+1})\sum_{y\in\mathbb{F}_q}\chi_1(w(y - y^{p^d})) \\ &= q^2 + \sum_{w\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_q}\chi_1(awx^{p^\alpha+1})\sum_{y\in\mathbb{F}_q}\chi_1(y^{p^d}(w^{p^d} - w)). \end{aligned}$$

The inner sum is zero unless $w^{p^d} = w$, i.e. $w \in \mathbb{F}_{p^d}$. Simplifying yields

$$N_\alpha(a,q) = q + \sum_{w\in\mathbb{F}_{p^d}^*}\sum_{x\in\mathbb{F}_q}\chi_1(awx^{p^\alpha+1}).$$

It is possible to remove w from the inner sum and so simplify the equation further. If $w \in \mathbb{F}_{p^d}^*$ then the equation $wz_w^{p^\alpha+1} = 1$ is solvable for $z_w \in \mathbb{F}_q$

provided $(p^\alpha+1, q-1) = p^d+1$ divides $(q-1)/(p^d-1)$. If e/d is even then this is always true and so

$$N_\alpha(a,q) = q + \sum_{w\in\mathbb{F}^*_{p^d}} \sum_{x\in\mathbb{F}_q} \chi_1(awx^{p^\alpha+1}) = q + \sum_{w\in\mathbb{F}^*_{p^d}} \sum_{x\in\mathbb{F}_q} \chi_1(aw(z_w x)^{p^\alpha+1})$$
$$= q + \sum_{w\in\mathbb{F}^*_{p^d}} \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1}) = q + (p^d-1)S_\alpha(a). \ \blacksquare$$

We are now ready to prove Theorem 2 using a counting argument concerning $N_\alpha(a,q)$ and comparing our results with those obtained in Theorem 6.1.

THEOREM 2. *Let e/d be even with $e = 2m$. Then*

$$S_\alpha(a) = \begin{cases} p^m & \text{if } a^{(q-1)/(p^d+1)} \neq (-1)^{m/d} \text{ and } m/d \text{ even}, \\ -p^m & \text{if } a^{(q-1)/(p^d+1)} \neq (-1)^{m/d} \text{ and } m/d \text{ odd}, \\ p^{m+d} & \text{if } a^{(q-1)/(p^d+1)} = (-1)^{m/d} \text{ and } m/d \text{ odd}, \\ -p^{m+d} & \text{if } a^{(q-1)/(p^d+1)} = (-1)^{m/d} \text{ and } m/d \text{ even}. \end{cases}$$

Proof. Consider the equation $ax^{p^\alpha+1} = y^{p^d} - y$. If (x,y) is a solution with $x \neq 0$ then (wx, y) is also a solution where $w^{p^d+1} = 1$. Thus the solutions of this equation with $x \neq 0$ occur in batches of size p^d+1. In addition there are p^d solutions with $x = 0$. So according to this counting argument we have

$$N \equiv p^d \bmod p^d+1 \equiv -1 \bmod p^d+1.$$

Theorem 6.1 gives us an alternative evaluation of N, and combining it with the above equation obtained through our counting argument we obtain

$$2 - 2S_\alpha(a) \equiv 0 \bmod p^d+1. \tag{4}$$

Suppose that $p > 3$ or that $p = 3$ and $d > 1$. There are two cases to consider.

We consider the case $a^{(q-1)/(p^d+1)} \neq (-1)^{m/d}$ first. For this case $S_\alpha(a) = \varepsilon p^m$ where $\varepsilon = \pm 1$. Recalling

$$p^m - 1 = (p^d+1)(p^{(m/d-1)d} - p^{(m/d-2)d} + \ldots - 1)$$

if m/d is even and

$$p^m + 1 = (p^d+1)(p^{(m/d-1)d} - p^{(m/d-2)d} + \ldots + 1)$$

if m/d is odd, it is clear that

$$p^m \bmod p^d+1 = \begin{cases} -1 & \text{if } m/d \text{ odd}, \\ 1 & \text{if } m/d \text{ even}. \end{cases}$$

Combining this with (4) and Theorem 6.1 gives us the first two cases of Theorem 2.

If $a^{(q-1)/(p^d+1)} = (-1)^{m/d}$ then

$$S_\alpha(a) = \varepsilon p^m p^d \equiv -\varepsilon p^m \bmod p^d + 1$$

and so it is clear we will obtain the opposite signs to those of the first case. This completes the proof for all cases except $p = 3$ and $d = 1$.

The previous arguments require the stipulation that if $p = 3$ then $d > 1$ as otherwise ε could be ± 1 and still satisfy (4). For the rest of the proof we thus assume $p = 3$ and $d = 1$. Firstly, by Lemma 2.6, we have $k = (p^\alpha + 1, q - 1) = 4$. Let λ be the multiplicative character of $\mathbb{F}_q$ of order 4. If g is a primitive element of $\mathbb{F}_q$ then we have

$$\lambda(g^t) = \begin{cases} 1 & \text{if } t \equiv 0 \bmod 4, \\ i & \text{if } t \equiv 1 \bmod 4, \\ -1 & \text{if } t \equiv 2 \bmod 4, \\ -i & \text{if } t \equiv 3 \bmod 4. \end{cases}$$

Lemma 2.1 tells us that $G(\lambda^3, \chi_1) = G(\lambda, \chi_1)$. Combining this information with the previous case statement and Lemmas 2.2 and 2.4 we obtain through some manipulation

$$S_\alpha(a) = \begin{cases} 2G(\lambda, \chi_1) + (-1)^{m+1} p^m & \text{if } t \equiv 0 \bmod 4, \\ -2G(\lambda, \chi_1) + (-1)^{m+1} p^m & \text{if } t \equiv 2 \bmod 4, \\ (-1)^m p^m & \text{if } t \equiv 1, 3 \bmod 4, \end{cases} \tag{5}$$

where $a = g^t$.

If m is odd then so too is $(3^m + 1)/4$ and we can apply Stickelberger's Theorem to determine $G(\lambda, \chi_1) = -p^m$. If $a^{(q-1)/4} = -1$ then $a = g^t$ where $t \equiv 2 \bmod 4$ and if $a^{(q-1)/4} \neq -1$ then $t \equiv 0, 1, 3 \bmod 4$. Thus $S_\alpha(a) = 2p^m + p^m = p^{m+1}$ when $a^{(q-1)/4} = -1$. If $t \equiv 1, 3 \bmod 4$ we have $S_\alpha(a) = -p^m$ and if $t \equiv 0 \bmod 4$ we obtain $S_\alpha(a) = -2p^m + p^m = -p^m$. All of these results coincide with our previous results.

Finally, suppose m is even. Then $a^{(q-1)/4} = 1$ if $t \equiv 0 \bmod 4$ and $a^{(q-1)/4} \neq 1$ if $t \equiv 1, 2, 3 \bmod 4$. Suppose firstly that $t \equiv 2 \bmod 4$. By Theorem 5.3

$$S_\alpha(a) = \pm p^m = -2G(\lambda, \chi_1) - p^m$$

and so $G(\lambda, \chi_1) = 0$ or $-p^m$. But $|G(\lambda, \chi_1)| = p^m$ for any non-trivial λ (see [5, Theorem 5.11]), and so $G(\lambda, \chi_1) = -p^m$. Substituting back into (5) in much the same way as we did for m odd completes the proof. ∎

Having evaluated $S_\alpha(a)$ for e/d even we can now return to Theorem 6.1 to obtain explicitly the number of solutions of the equation $ax^{p^\alpha+1} = y^{p^d} - y$. We leave this to the reader. We note that the proof of Theorem 2 includes the proof of the following corollary on Gauss sums.

Corollary 6.2. *Let $q = 3^{2m}$ and denote by λ the multiplicative character of $\mathbb{F}_q$ of order 4. Then $G(\lambda, \chi_1) = -3^m$.*

References

[1] L. Carlitz, *Evaluation of some exponential sums over a finite field*, Math. Nachr. 96 (1980), 319–339.

[2] R. S. Coulter and R. W. Matthews, *Planar functions and planes of Lenz–Barlotti class II*, Des. Codes Cryptogr. 10 (1997), 167–184.

[3] —, —, *Bent polynomials over finite fields*, Bull. Austral. Math. Soc. 56 (1997), 429–437.

[4] P. Dembowski and T. G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. 103 (1968), 239–258.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, Reading, 1983 (now distributed by Cambridge Univ. Press).

School of Information Technology
The University of Queensland
St. Lucia, Queensland 4072
Australia
E-mail: shrub@cs.uq.edu.au

Received on 7.2.1997
and in revised form on 30.7.1997 (3133)