ACTA ARITHMETICA
XCI.3 (1999)

Pure and mixed exponential sums

by

Todd Cochrane (Manhattan, KS) and Zhiyong Zheng (Guangzhou)

1. Introduction. In this paper we evaluate and estimate pure and mixed exponential sums of the type

$$S(f,p^m)=\sum_{x=1}^{p^m} e_{p^m}(f(x)), \qquad S(\chi,f,p^m)=\sum_{\substack{x=1\\ p\nmid x}}^{p^m}\chi(x)e_{p^m}(f(x)), \tag{1.1}$$

where p^m is a prime power with $m\ge 2$, χ is a multiplicative character (mod p^m), $e_{p^m}(\cdot)$ is the additive character,

$$e_{p^m}(x)=e(x/p^m)=e^{2\pi ix/p^m},$$

and f is a polynomial with integer coefficients. Let $d=d(f)$ denote the ordinary degree of f and $d_p(f)$ denote the degree of f read (mod p). We focus our attention on mixed exponential sums in this section and take up a discussion of pure exponential sums in Section 2.

If $m=1$ it is a well known consequence of the work of Weil [21] on the Riemann Hypothesis for curves over a finite field (see e.g. Schmidt [18]) that if $d_p(f)\ge 1$, then for any multiplicative character $\chi \pmod p$,

$$|S(\chi,f,p)|\le d_p(f)p^{1/2}. \tag{1.2}$$

(We note that when $p\,|\,d_p(f)$ the upper bound in (1.2) is trivial.)

For values of $m\ge 2$ it has been conjectured by authors such as E. Bombieri, M. C. Liu, and W. M. Schmidt that an upper bound analogous to the upper bound (2.3) of Hua for pure exponential sums may be available.

1991 *Mathematics Subject Classification*: 11L07, 11L03.
Key words and phrases: exponential sums.
Research of the second author was supported by the National Science Fund of The People's Republic of China for Distinguished Young Scholars. The second author also expresses his thanks to Kansas State University, where he spent a semester as a visiting scholar.

Bombieri, in communication with the second author, has stated his conjecture as follows: For any $f(X) \in \mathbb{Z}[X]$ of degree d with $d_p(f) \geq 1$ we have

$$|S(\chi, f, p^m)| \ll \max\{p^{m/2}, p^{m(1-1/d)}\}. \tag{1.3}$$

We establish here that this upper bound does in fact hold for all but a very exceptional class of polynomials f and characters χ. For this exceptional class one needs exponent $m(1-1/(d+1))$; see Example 9.2. In Corollary 1.1 we establish a uniform upper bound with the exponent $m(1-1/(d+1))$. In many cases, as our main theorem, Theorem 1.1, makes it plain, we obtain an even better upper bound than (1.3).

To state our main theorem, let $\mathrm{ord}_p(x)$ denote the normal exponent valuation on the p-adic field. In particular, for $x \neq 0 \in \mathbb{Z}$, $p^{\mathrm{ord}_p(x)} \parallel x$. For convenience, we set $\mathrm{ord}_p(0) = \infty$. For any nonzero polynomial $f = f(X) = a_0 + a_1X + \ldots + a_dX^d \in \mathbb{Z}[X]$ we define

$$\mathrm{ord}_p(f) := \min_{0 \leq i \leq d} \{\mathrm{ord}_p(a_i)\}. \tag{1.4}$$

Suppose now that p is an odd prime. Throughout this paper the letter a denotes a fixed primitive root (mod p) chosen so that $a > 0$ and

$$a^{p-1} = 1 + rp \quad \text{with } p \nmid r. \tag{1.5}$$

In particular a is a primitive root (mod p^m) for any exponent m. Let χ be a multiplicative character (mod p^m) and let $c = c(\chi, a)$ be the unique integer with $0 < c \leq p^{m-1}(p-1)$ and

$$\chi(a^k) = e\left(\frac{ck}{p^{m-1}(p-1)}\right) \tag{1.6}$$

for every integer k. Thus for instance, if $\chi = \chi_0$, the principal character, then $c = p^{m-1}(p-1)$ and if χ is the quadratic character, then $c = p^{m-1}(p-1)/2$. A character χ is primitive if and only if $p \nmid c$.

For any polynomial f over $\mathbb{Z}$ we define

$$t = t(f) := \mathrm{ord}_p(f'(X)), \quad t_1 = t_1(f) := \mathrm{ord}_p(rXf'(X) + c), \tag{1.7}$$

where $f' = f'(X)$ denotes the derivative of $f(X)$. If $p > d_p(f) \geq 1$ then $t = t_1 = 0$. Also, since $p \nmid r$ it is plain that $t_1 = \min\{t, \mathrm{ord}_p(c)\} \leq m-1$. We define the set of *critical points* associated with the sum $S(\chi, f, p^m)$ to be the set

$$\mathcal{A} = \mathcal{A}(\chi, f, p) := \{\alpha_1, \ldots, \alpha_D\} \tag{1.8}$$

of nonzero residues (mod p) satisfying the congruence

$$p^{-t_1}(rxf'(x) + c) \equiv 0 \pmod{p}. \tag{1.9}$$

It is easy to check that this congruence does not depend on the choice of the primitive root a. Strictly speaking, $\mathcal{A}$ is a set of points in the finite field

$\mathbb{F}_p$, but at times it will be convenient for us to regard $\mathcal{A}$ as a specific set of integer representatives for the points in this set. To keep our notation simple, for any integer α, we shall simply write $\alpha \in \mathcal{A}$ if the residue class of $\alpha \pmod p$ is in $\mathcal{A}$. For any $\alpha \in \mathcal{A}$ let $\nu = \nu_\alpha$ denote the multiplicity of α as a zero of the congruence (1.9). Since the polynomial in (1.9) is nonzero $\pmod p$ we have $\sum_{\alpha\in\mathcal{A}} \nu_\alpha \le d$.

Write

$$S(\chi, f, p^m) = \sum_{\alpha=1}^{p-1} S_\alpha,$$

where for any integer α with $p\nmid\alpha$,

$$S_\alpha = S_\alpha(\chi, f, p^m) := \sum_{\substack{x=1\\ x\equiv\alpha \pmod p}}^{p^m} \chi(x) e_{p^m}(f(x)). \tag{1.10}$$

THEOREM 1.1. *Let p be an odd prime, f be any polynomial over $\mathbb{Z}$ and t, t_1 be as defined in* (1.7). *Suppose that $m \ge t_1 + 2$. Then for any integer α with $p\nmid\alpha$ we have*:

(i) *If $\alpha \notin \mathcal{A}$, then $S_\alpha(\chi, f, p^m) = 0$.*

(ii) *If α is a critical point of multiplicity $\nu \ge 1$ then $t = t_1$ and*

$$|S_\alpha(\chi, f, p^m)| \le \nu p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}. \tag{1.11}$$

(iii) *If α is a critical point of multiplicity one then*

$$S_\alpha(\chi, f, p^m) = \begin{cases} \chi(\alpha^*) e_{p^m}(f(\alpha^*)) p^{(m+t)/2} & \text{if } m-t \text{ is even},\\ \chi(\alpha^*) e_{p^m}(f(\alpha^*)) \chi_2(A_\alpha) \mathcal{G}_p p^{(m+t-1)/2} & \text{if } m-t \text{ is odd}, \end{cases}$$

where α^* is the unique lifting of α to a solution of the congruence

$$p^{-t}(Rxf'(x) + c) \equiv 0 \pmod{p^{[(m-t+1)/2]}},$$

and

$$A_\alpha \equiv 2\alpha p^{-t}(f'(\alpha) + \alpha f''(\alpha)) \pmod p.$$

In particular, we have equality in (1.11).

Here $\mathcal{G}_p$ is the classical Gauss sum,

$$\begin{aligned} \mathcal{G}_p &:= \sum_{x=0}^{p-1} e_p(x^2) = \sum_{x=1}^{p-1} \chi_2(x) e_p(x) \\ &= \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4,\\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4, \end{cases} \end{aligned} \tag{1.12}$$

χ_2 is the quadratic character $\pmod p$, and R is the p-adic integer

$$R := p^{-1}\log(1 + rp) = p^{-1}\sum_{i=1}^{\infty} \frac{(-1)^{i+1}(rp)^i}{i} \equiv r \pmod p.$$

It follows immediately that under the hypotheses of the theorem

$$|S(\chi,f,p^m)| \le \Big(\sum_{\alpha\in\mathcal{A}}\nu_\alpha\Big)p^{t/(M+1)}p^{m(1-1/(M+1))}, \tag{1.13}$$

where M is the maximum multiplicity of the critical points. Also, if all of the critical points are of multiplicity one then we obtain an explicit formula for the sum $S(\chi,f,p^m)$. The proof of Theorem 1.1 is given in Sections 6 and 7, and the case $p=2$ is dealt with in Section 8. Our strategy for estimating the mixed exponential sum S_α is to "untwist" the sum and express it explicitly in terms of a pure exponential sum (see Proposition 6.1). In order to estimate the resulting pure exponential sum we prove a conjecture of Chalk regarding a local type upper bound on pure exponential sums. This will be discussed in Section 2. The proof is "elementary" and self-contained aside from an appeal to the upper bound of Weil, (2.2), for pure exponential sums.

Remarks. 1. The proof we give here actually yields a result more akin to the Riemann Hypothesis. If $m \ge t_1+2$ and α is a critical point of multiplicity ν then we find that $S_\alpha(\chi,f,p^m)$ can be expressed as a sum $z_1+\ldots+z_k$ of complex numbers z_j of moduli $p^{w_j/2}$, $1\le j\le k$, where the weights w_j are nonnegative integers satisfying

$$\frac{w_j}{2} \le m\bigg(1-\frac{1}{\nu+1}\bigg)+\frac{t}{\nu+1}.$$

If $t=0$ then $k\le\nu$ and so the upper bound in (1.11) is an immediate consequence. Moreover, we see that the exponent in (1.11) as well as in (1.13) can be replaced by the greatest half integer less than or equal to it. For values of $t\ge 1$ we have $k\le 3\nu$. This implies a slightly weaker upper bound than (1.11).

2. If $t>\mathrm{ord}_p(c)$ then $t_1=\mathrm{ord}_p(c)$ and there are no critical points. Thus, if $t>\mathrm{ord}_p(c)$ and $t_1\le m-2$, then $S(\chi,f,p^m)=0$. In particular, if χ is a primitive character (so that $\mathrm{ord}_p(c)=0$), $m\ge 2$ and t is any positive integer then $S(\chi,f,p^m)=0$.

3. If $t_1=m-1$ one can have a situation where $\alpha\notin\mathcal{A}$ and yet $S_\alpha\ne 0$; consider for example the Heilbronn sum

$$\sum_{x=1}^{p^2}\chi_0(x)e_{p^2}(x^p) = p\sum_{x=1}^{p-1}e_{p^2}(x^p), \tag{1.14}$$

which has no associated critical points and yet is nonzero in general. Here $t_1=t=1$. It is still desirable to find a good upper bound when $t_1=m-1$. Heath-Brown [9] has taken a step in this direction for the particular case of the Heilbronn sum.

4. Theorem 1.1 holds identically for rational functions defined over $\mathbb{Z}$. The proof follows the same line of argument given here but the details will

be provided in [4]. If we take $f(X) = aX + bX^{-1}$, and $\chi = \chi_0$ then the formula in Theorem 1.1(iii) is just the classical formula of Salié [17] for the Kloosterman sum. Our method also extends easily to mixed exponential sums in several variables.

If $d_p(f) \geq 1$ then $p^t \leq d_p(f) \leq d(f)$ and so we obtain as an immediate consequence of (1.13), Theorem 8.1 (for the case $p = 2$), and (1.2) (for the case $m = 1$) the following uniform upper bound for $S(\chi, f, p^m)$.

COROLLARY 1.1. *Let f be a polynomial over $\mathbb{Z}$ of degree $d \geq 1$. Then for any prime p with $d_p(f) \geq 1$, any positive integer $m \geq 2$, and any multiplicative character $\chi \pmod{p^m}$, we have*

$$|S(\chi, f, p^m)| \leq 2d^{1+1/(M+1)} p^{m(1-1/(M+1))}, \tag{1.15}$$

where M is the maximum multiplicity of the critical points associated with the sum. In particular, since $M \leq d$ we have uniformly for any $m \geq 1$,

$$|S(\chi, f, p^m)| \leq 4dp^{m(1-1/(d+1))}. \tag{1.16}$$

(The upper bound in (1.15) is trivial when $t_1 = m - 1$, the case when Theorem 1.1 does not apply.) To see that the exponent on the right-hand side of (1.16) is best possible as a uniform upper bound, one only needs to consider special cases where there is a single critical point of multiplicity d. We do so in Example 9.2. In general, even when there is a critical point of multiplicity d, a sharper upper bound than (1.16) is available by applying our result for pure exponential sums, Theorem 2.1, directly to the untwisted sum given in Proposition 6.1. It is quite possible that the constant $4d$ in (1.16) can be replaced with an absolute constant, analogous to what Stechkin [20] has been able to establish for pure exponential sums.

If χ is any character with $\mathrm{ord}_p(c) > t$ then the critical points are just the solutions of the congruence $p^{-t} f'(x) \equiv 0 \pmod{p}$, and so $M < d$ and $\sum_{\alpha \in \mathcal{A}} \nu_\alpha \leq d - 1$. Thus for any χ with $\mathrm{ord}_p(c) \geq m/2$, such as χ_0, the quadratic character ($p \neq 2$), a cubic character ($3 \mid (p-1)$), etc., and any polynomial f with $d_p(f) \geq 1$ we have the uniform upper bound

$$|S(\chi, f, p^m)| \leq 6(d-1)p^{m(1-1/d)} \quad \text{for } (m, d) \neq (1, 1), \tag{1.17}$$

the desired analogue of Hua's theorem. We need only note that when $t \geq m/2$ then the upper bound in (1.17) is trivial.

In closing we mention that sums of the type

$$S(\chi, f, q) = \sum_{x=1}^{q} \chi(x) e_q(f(x)),$$

where q is an arbitrary modulus can be evaluated or estimated using Theorem 1.1 together with the following multiplicative property of exponential sums. Suppose that $q = p_1^{e_1} \dots p_k^{e_k}$, and that χ is a multiplicative character

(mod q) given by $\chi = \chi_1 \dots \chi_k$ where for $1 \le i \le k$, χ_i is a multiplicative character (mod $p_i^{e_i}$). Set $q_i = q/p_i^{e_i}$, $1 \le i \le k$, and let $a_1, \dots, a_k$ be integers such that $\sum_i a_i q_i = 1$. Then for any polynomial f over $\mathbb{Z}$ we have

$$S(\chi, f, q) = \prod_{i=1}^{k} S(\chi_i, a_i f, p_i^{e_i}).$$

It follows from (1.16) that for any q with $d_p(f) \ge 1$ for all primes $p \,|\, q$, we have

$$|S(\chi, f, q)| \le (4d)^{\omega(q)} q^{1-1/(d+1)}, \tag{1.18}$$

where $\omega(q)$ is the number of distinct prime factors of q. One can also state the analogue of (1.17).

2. Pure exponential sums. There are many known results on the estimation of pure exponential sums of the type

$$S(f, p^m) = \sum_{x=1}^{p^m} e_{p^m}(f(x)), \tag{2.1}$$

where f is a polynomial over $\mathbb{Z}$ of degree d. If $m = 1$, p is odd and $d_p(f) \ge 1$ then by the work of Weil [21] (see also Bombieri [1]), we have

$$|S(f, p)| \le (d_p(f) - 1) p^{1/2}. \tag{2.2}$$

For $m \ge 2$, Hua [10]–[12] showed that if $d_p(f) \ge 1$ then

$$|S(f, p^m)| \le d^3 p^{m(1-1/d)}. \tag{2.3}$$

On the other hand, it was already known from the work of Hardy and Littlewood [7], [8] that if $d \,|\, m$, $p \nmid a$ and $p > d \ge 2$ then

$$S(aX^d, p^m) = p^{m(1-1/d)}, \tag{2.4}$$

and thus as a uniform upper bound the exponent in Hua's bound is best possible. We generalize the example of Hardy and Littlewood in Example 9.1, and show in particular that the constraint $p > d$ is not needed. Chen [3], Chalk [2], Ding [5], [6], Loh [13], Nechaev [16] and Stechkin [20] have made further improvements in the constant on the right-hand side of (2.3). Stechkin [20] showed that the value d^3 can actually be replaced with an absolute constant, although he did not indicate how large it must be.

In order to improve on Hua's estimate, two different approaches have been taken. Smith [19], Loxton and Smith [14], and Loxton and Vaughan [15] considered the factorization of $f'(x)$ over the complex plane and in the latter paper it was shown that

$$|S(f, p^m)| \le (d-1) p^{(\delta+\tau)/(e+1)} p^{m(1-1/(e+1))}, \tag{2.5}$$

where e is the maximum multiplicity of any of the complex zeros of f', $\tau = 0$ if $d < p$, $\tau = 1$ if $d \geq p$, and $\delta = \operatorname{ord}_p(\mathcal{D}(f'))$, where $\mathcal{D}(f')$ is the different of f'.

The result of Loxton and Vaughan may be considered a global type of result. Chalk [2] proceeded in a different manner considering local information instead, and it is this type of result that we have found essential for the proof of Theorem 1.1. Let $\mathcal{A} = \mathcal{A}(f,p)$ be the set of zeros of the congruence

$$p^{-t}f'(x) \equiv 0 \pmod{p}, \tag{2.6}$$

where $t = \operatorname{ord}_p(f')$, and for $\alpha \in \mathcal{A}$ let $\nu = \nu_\alpha$ denote its multiplicity. Again, we call $\mathcal{A}$ the set of critical points associated with the sum $S(f,p^m)$. Chalk [2] established that if $\mathcal{A}$ is empty and $m \geq 2t+2$ then $S(f,p^m) = 0$, and that if $\mathcal{A}$ is nonempty then for $m \geq 2$,

$$|S(f,p^m)| \leq d\Big(\sum_{\alpha\in\mathcal{A}} \nu_\alpha\Big) p^{t/(M+1)} p^{m(1-1/(M+1))}, \tag{2.7}$$

where M is the maximum multiplicity of the critical points. He suggested that one may be able to obtain the upper bound in (2.7) with the constant d on the right-hand side eliminated altogether, thus making the upper bound depend purely on local information. Ding [5] reduced the value d to $\sqrt{d}$, and then in [6] succeeded in eliminating the value d altogether under the assumption $m \geq t+2$. Loh [13], independently, also succeeded in eliminating the value d under the assumption $m \geq t+2$.

In this paper, we prove a more precise version of the local type upper bound suggested by Chalk and obtain an explicit formula for $S(f,p^m)$ in the case where all of the critical points are of multiplicity one. Write

$$S(f,p^m) = \sum_{\alpha=0}^{p-1} S_\alpha,$$

where for any integer α,

$$S_\alpha = S_\alpha(f,p^m) := \sum_{\substack{x=1 \\ x\equiv\alpha \pmod p}}^{p^m} e_{p^m}(f(x)). \tag{2.8}$$

THEOREM 2.1. *Let p be an odd prime and f be a nonconstant polynomial defined over $\mathbb{Z}$. If $m \geq t+2$ then for any integer α we have*:

(i) *If $\alpha \notin \mathcal{A}$ then $S_\alpha(f,p^m) = 0$.*

(ii) *If α is a critical point of multiplicity ν then*

$$|S_\alpha(f,p^m)| \leq \nu p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}. \tag{2.9}$$

(iii) *If α is a critical point of multiplicity one then*

$$S_\alpha(f,p^m)=\begin{cases} e_{p^m}(f(\alpha^*))p^{(m+t)/2} & \text{if } m-t \text{ is even},\\ \chi_2(A_\alpha)e_{p^m}(f(\alpha^*))\mathcal{G}_p p^{(m+t-1)/2} & \text{if } m-t \text{ is odd},\end{cases}$$

where α^* is the unique lifting of α to a solution of the congruence $p^{-t}f'(x)\equiv 0 \pmod{p^{[(m-t+1)/2]}}$, and $A_\alpha \equiv 2p^{-t}f''(\alpha^*) \pmod p$. In particular, we have equality in (2.9).

(iv) *If $p=2$, then for $m\ge t+3$, if $\alpha\notin\mathcal{A}$ then $S_\alpha=0$, and if $\alpha\in\mathcal{A}$ then*

$$|S_\alpha(f,2^m)|\le \nu 2^{t/(\nu+1)}2^{m(1-1/(\nu+1))}, \tag{2.10}$$

with equality if $\nu=1$.

In particular, under the hypotheses of the theorem we have

$$|S(f,p^m)|\le \Big(\sum_{\alpha\in\mathcal{A}}\nu_\alpha\Big)p^{t/(M+1)}p^{m(1-1/(M+1))}, \tag{2.11}$$

where M is the maximum multiplicity of the critical points. If $d_p(f)\ge 1$ then $p^t\le d$, $M\le d-1$ and $\sum_{\alpha\in\mathcal{A}}\nu_\alpha\le d-1$ and so we deduce easily from (2.11) and Weil's bound (for the case $m=1$) the following uniform upper bound.

Corollary 2.1. *Let f be a polynomial over $\mathbb{Z}$ of degree $d\ge 1$. Then for any prime p with $d_p(f)\ge 1$ and any $m\ge 1$ we have*

$$|S(f,p^m)|\le 3(d-1)p^{m(1-1/d)}. \tag{2.12}$$

With a little more work we can replace the constant $3(d-1)$ on the right side of (2.12) with d, for odd p. Remarks 1 and 4 following Theorem 1.1 hold for Theorem 2.1 as well. (We remark that this paper was completed before the authors became aware of the work of Loh [13] and Ding [6] and so there is a certain amount of repetition in the results stated in Theorem 2.1. We feel it is important to keep all of the details for our proof of Theorem 2.1 here because they are used in our proof of Theorem 1.1.)

3. Preliminary lemmas. Let p be a prime, $f=f(X)$ be a polynomial over $\mathbb{Z}$ of degree $d\ge 1$ and α be any integer. Then f admits a Taylor series expansion about α given by

$$f(X)=\sum_{i=0}^{d}a_i(X-\alpha)^i,$$

where $a_i=f^{(i)}(\alpha)/i!\in\mathbb{Z}$, $0\le i\le d$. Clearly,

$$\operatorname{ord}_p(f)=\min_{0\le i\le d}\{\operatorname{ord}_p(a_i)\}. \tag{3.1}$$

Let $t = t(f) = \operatorname{ord}_p(f')$, and suppose that α is a zero of the critical point congruence

$$p^{-t} f'(x) \equiv 0 \pmod{p}, \tag{3.2}$$

of multiplicity ν. Now f' has a Taylor expansion

$$f'(X) = \sum_{i=1}^{d} i a_i (X-\alpha)^{i-1},$$

and so by (3.1) we have $t = \min_{1\le i\le d}\{\operatorname{ord}_p(ia_i)\}$. Reading the polynomial

$$p^{-t} f'(X) = \sum_{i=1}^{d} p^{-t} i a_i (X-\alpha)^{i-1},$$

over the finite field $\mathbb{F}_p$, it follows that

$$\operatorname{ord}_p(ia_i) \begin{cases} \ge t+1 & \text{if } 1 \le i \le \nu, \\ = t & \text{if } i = \nu+1, \\ \ge t & \text{if } i > \nu+1, \end{cases} \tag{3.3}$$

and consequently for $i \ge 1$,

$$\operatorname{ord}_p(a_i p^i) = \operatorname{ord}_p(ia_i) + i - \operatorname{ord}_p(i) \ge \begin{cases} t+2 & \text{if } p \text{ is odd or } \nu > 1, \\ t+1 & \text{if } p = 2,\ \nu = 1. \end{cases} \tag{3.4}$$

Define

$$\sigma := \operatorname{ord}_p(f(pY+\alpha) - f(\alpha)), \quad g(Y) := p^{-\sigma}(f(pY+\alpha) - f(\alpha)),$$
$$\tau := \operatorname{ord}_p(g'(Y)), \quad g_1(Y) := p^{-\tau} g'(Y).$$

Lemma 3.1. *For any prime p and zero α of* (3.2) *of multiplicity ν we have*:

(i) $$\sigma \ge \begin{cases} t+2 & \text{if } p \text{ is odd or } \nu > 1, \\ t+1 & \text{if } p = 2 \text{ and } \nu = 1. \end{cases}$$

(ii) $$\sigma \le \nu + 1 + t - \tau.$$

(iii) $$d_p(g) \le \begin{cases} \sigma - t + \operatorname{ord}_p(d_p(g)) \le \nu + 1 + \operatorname{ord}_p(d_p(g)), \\ \sigma \le \nu + 1 + t - \tau. \end{cases}$$

(iv) $$d_p(g_1) \le \sigma + \tau - t - 1 \le \nu.$$

(v) $$p^\tau \mid d_p(g).$$

Parts of this lemma can be found in the works of Hua [12], Chalk [2], Ding [5], and Stechkin [20].

Proof. From the Taylor expansion for f we have

$$f(pY+\alpha) - f(\alpha) = \sum_{i=1}^{d} a_i p^i Y^i,$$

and thus (i) follows from (3.4). Now

$$g(Y) = \sum_{i=1}^{d} a_i p^{i-\sigma} Y^i,$$

and so for the term $i = d_p(g)$ we must have

$$\sigma = \operatorname{ord}_p(a_i p^i) = \operatorname{ord}_p(ia_i) + i - \operatorname{ord}_p(i).$$

It follows from (3.3) that

$$i = \sigma + \operatorname{ord}_p(i) - \operatorname{ord}_p(ia_i) \le \sigma + \operatorname{ord}_p(i) - t,$$

from which the first inequality in (iii) follows. The second inequality follows immediately from (ii). Also, by the definition of g_1 we have

$$g_1(Y) = \sum_{i=1}^{d} a_i i p^{i-\sigma-\tau} Y^{i-1}.$$

We see upon examining the $i = \nu + 1$ coefficient and using (3.3) that (ii) is obtained, and upon examining the $i = d_p(g_1) + 1$ coefficient and using (3.3) that (iv) is obtained. The second inequality in (iv) follows immediately from (ii). Finally, to obtain (v) suppose that $i = d_p(g)$ and that the coefficient of X^i in g is A_i. Then $p \nmid A_i$. On the other hand, we have $p^\tau \mid iA_i$. Thus $p^\tau \mid i$. ∎

Lemma 3.2. *Let p be a prime, f be a polynomial over $\mathbb{Z}$ with $t = \operatorname{ord}_p(f')$, and let t_1 be any integer with $0 \le t_1 \le t$. If p is odd and $m \ge t_1 + 2$, or $p = 2$ and $m \ge t_1 + 3$, or $p = 2$, $t_1 = 0$ and $m = 2$, then for any integers z, y we have*

$$f(y + p^{m-t_1-1}z) \equiv f(y) + f'(y)p^{m-t_1-1}z \pmod{p^m}.$$

Proof. The polynomial f admits a Taylor expansion about y,

$$f(X) = \sum_{i=0}^{d} a_i (X - y)^i,$$

with integer coefficients a_i, $0 \le i \le d$. For any integer z,

$$f(y + p^{m-t_1-1}z) = \sum_{i=0}^{d} a_i (p^{m-t_1-1}z)^i.$$

Now, since $\operatorname{ord}_p(f') = t$ it follows that $\operatorname{ord}_p(ia_i) \ge t$ for $i \ge 1$. Thus for any $i \ge 1$,

$$\begin{aligned} \operatorname{ord}_p(a_i p^{(m-t_1-1)i}) &\ge i(m - t_1 - 1) + t - \operatorname{ord}_p(i) \\ &\ge i(m - t_1 - 1) + t_1 - \operatorname{ord}_p(i), \end{aligned} \tag{3.5}$$

and for $i \geq 2$ the quantity on the right side is $\geq m$ if and only if

$$m \geq t_1 + \frac{i + \operatorname{ord}_p(i)}{i-1}.$$

It is easy to check that the latter inequality holds for all $i \geq 2$ if p is odd and $m \geq t_1 + 2$ or if $p = 2$ and $m \geq t_1 + 3$. If $p = 2$, $m = 2$ and $t_1 = 0$ then we return to (3.5) and replace the right side with $i(m - t_1 - 1) = i$ to obtain the result. ∎

4. Proof of Theorem 2.1. We begin by deriving a recursion formula for complete exponential sums of the type

$$S(f, p^m) = \sum_{x=1}^{p^m} e_{p^m}(f(x)).$$

Let p be any prime and f be a nonconstant polynomial over $\mathbb{Z}$. As defined earlier, let $t = \operatorname{ord}_p(f')$, $\mathcal{A}$ denote the set of solutions of the congruence $p^{-t} f'(x) \equiv 0 \pmod p$ and write

$$S(f, p^m) = \sum_{\alpha=0}^{p-1} S_\alpha \quad \text{with} \quad S_\alpha = S_\alpha(f, p^m) = \sum_{\substack{x=1 \\ x \equiv \alpha \,(\mathrm{mod}\, p)}}^{p^m} e_{p^m}(f(x)).$$

Suppose that $m \geq t + 2$. Write $x = p^{m-1-t} z + y$ with y running from 1 to p^{m-1-t} and z running from 1 to p^{t+1}, and consequently x running through a complete set of residues (mod p^m). Under the hypotheses of Lemma 3.2, with $t_1 = t$, we have

$$\begin{aligned} S_\alpha &= \sum_{y \equiv \alpha \,(\mathrm{mod}\, p)} \sum_{z} e_{p^m}(f(p^{m-t-1} z + y)) \\ &= \sum_{y \equiv \alpha \,(\mathrm{mod}\, p)} \sum_{z} e_{p^m}(f(y) + f'(y) z p^{m-t-1}) \\ &= \sum_{y \equiv \alpha \,(\mathrm{mod}\, p)} e_{p^m}(f(y)) \sum_{z=1}^{p^{t+1}} e_{p^{t+1}}(z f'(y)) \\ &= p^{t+1} \sum_{\substack{y \equiv \alpha \,(\mathrm{mod}\, p) \\ p^{t+1} \mid f'(y)}} e_{p^m}(f(y)). \end{aligned}$$

We see in particular that $S_\alpha = 0$ unless $\alpha \in \mathcal{A}$, proving Theorem 2.1(i) and the first part of Theorem 2.1(iv).

If $\alpha \in \mathcal{A}$ and chosen so that $0 \le \alpha < p$ then we can proceed by writing

$$\begin{aligned} S_\alpha &= p^{t+1} \sum_{s=1}^{p^{m-2-t}} e_{p^m}(f(\alpha + sp)) \\ &= p^{t+1} e_{p^m}(f(\alpha)) \sum_{s=1}^{p^{m-2-t}} e_{p^m}(f(\alpha + sp) - f(\alpha)) \\ &= p^{\sigma-1} e_{p^m}(f(\alpha)) \sum_{s=1}^{p^{m-\sigma}} e_{p^{m-\sigma}}(g_\alpha(s)), \end{aligned}$$

where

$$\sigma := \operatorname{ord}_p(f(pY + \alpha) - f(\alpha)), \qquad g_\alpha(Y) := p^{-\sigma}(f(pY + \alpha) - f(\alpha)), \tag{4.1}$$

and the latter sum is taken to be $p^{m-\sigma}$ if $m \le \sigma$. Thus we obtain

Proposition 4.1 (The Recursion Relationship). *Suppose that p is an odd prime and $m \ge t + 2$, or $p = 2$ and $m \ge t + 3$, or $p = 2$, $t = 0$ and $m = 2$. Then*:

(i) *If $\alpha \notin \mathcal{A}$ then $S_\alpha = 0$.*

(ii) *If $\alpha \in \mathcal{A}$ and $0 \le \alpha < p$ then*

$$S_\alpha(f, p^m) = e_{p^m}(f(\alpha)) p^{\sigma-1} S(g_\alpha, p^{m-\sigma}), \tag{4.2}$$

where

$$S(g_\alpha, p^{m-\sigma}) = \begin{cases} \displaystyle\sum_{s=1}^{p^{m-\sigma}} e_{p^{m-\sigma}}(g_\alpha(s)) & \text{if } m \ge \sigma, \\ p^{m-\sigma} & \text{if } m < \sigma. \end{cases} \tag{4.3}$$

The stage is now set for proving Theorem 2.1(ii) by induction on m. We defer the proof of part (iii) to Section 5, but we shall assume here that it has already been proven so that we may assume $\nu \ge 2$ in the course of the proof. The precise statement that we shall prove here is the following:

Let p be an odd prime, f be a nonconstant polynomial over $\mathbb{Z}$ and let $d_1 = d_p(p^{-t} f')$. Then

(A) *If $m = 1$ and $d_p(f) \ge 1$ then*

$$|S(f, p)| \le (d_p(f) - 1) p^{1/2}. \tag{4.4}$$

(B) *If $m \ge t + 2$ then*

$$|S(f, p^m)| \le d_1 p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}. \tag{4.5}$$

(C) *If $m \ge t + 2$ and α is a critical point of multiplicity ν then*

$$|S_\alpha(f, p^m)| \le \nu p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}. \tag{4.6}$$

P r o o f. When $m = 1$ this is just the result of Weil. Suppose now that $m \geq t+2$ and that the result is true for all smaller values of m. Let α be a critical point of multiplicity ν with $0 \leq \alpha < p$, and let σ, g_α be as defined in (4.1) and τ, g_1 be defined by

$$\tau = \operatorname{ord}_p(g'_\alpha(Y)), \qquad g_1(Y) = p^{-\tau} g'_\alpha(Y).$$

We consider four cases: $\sigma \geq m$, $\sigma = m-1$, $m-1-\tau \leq \sigma \leq m-2$ and $\sigma \leq m-2-\tau$. A trivial estimate will suffice for the first and third cases, Weil's upper bound will handle the second case and the induction assumption will take care of the last case.

Case (i). Suppose that $\sigma \geq m$. Then by (4.2) and (4.3),

$$|S_\alpha| \leq p^{m-1} = p^{(m-\nu-1)/(\nu+1)} p^{m(1-1/(\nu+1))} \leq p^{t/(\nu+1)} p^{m(1-1/(\nu+1))},$$

the last inequality following from Lemma 3.1(ii).

Case (ii). Suppose that $\sigma = m-1$. We start by noting that by the inequality $\sigma \leq \nu + t + 1 - \tau$ of Lemma 3.1(ii) we have trivially

$$|S_\alpha| \leq p^{m-1} \leq \nu p^{t/(\nu+1)} p^{m(1-1/(\nu+1))},$$

unless $\tau = 0$ and $p > \nu^{\nu+1}$, and so we may assume that $p > \nu^{\nu+1}$.

Let $d_p = d_p(g_\alpha)$. We note that since f is nonconstant, $d_p(g_\alpha) \geq 1$. By Lemma 3.1(iii) we have

$$d_p \leq \nu + 1 + \operatorname{ord}_p(d_p). \tag{4.7}$$

Suppose that $\operatorname{ord}_p(d_p) \geq 1$. If $d_p = p$ then by (4.7), $p \leq \nu + 2$, contradicting our assumptions that $p > \nu^{\nu+1}$ and $\nu \geq 2$. Otherwise $d_p \geq 2p$ and thus since $\operatorname{ord}_p(d_p) \leq d_p/2$ we see by (4.7) that

$$p \leq \tfrac{1}{2} d_p \leq d_p - \operatorname{ord}_p(d_p) \leq \nu + 1,$$

again contradicting our assumptions.

Thus we must have $\operatorname{ord}_p(d_p) = 0$ and so by (4.7), $d_p \leq \nu + 1$. It follows from (4.2) and the upper bound of Weil, (4.4), that

$$\begin{aligned} |S_\alpha| &= p^{\sigma-1} |S(g_\alpha, p)| \leq (d_p - 1) p^{\sigma - 1/2} \\ &\leq \nu p^{1/(\nu+1) - 1/2} p^{(\sigma-\nu-1)/(\nu+1)} p^{m(1-1/(\nu+1))}, \end{aligned}$$

and so by Lemma 3.1(ii) we obtain (4.6).

Case (iii). Suppose that $m-1-\tau \leq \sigma \leq m-2$. In particular, we must have $\tau \geq 1$. Then we have the trivial estimate

$$\begin{aligned} |S_\alpha| &\leq p^{m-1} = p^{(m-\nu-1)/(\nu+1)} p^{m(1-1/(\nu+1))} \\ &\leq p^{1/(\nu+1)} p^{(\sigma+\tau-\nu-1)/(\nu+1)} p^{m(1-1/(\nu+1))} \\ &\leq p^{1/(\nu+1)} p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}, \end{aligned} \tag{4.8}$$

the latter inequality following from Lemma 3.1(ii). Now, by Lemma 3.1(v), $p^\tau \mid d_p(g_\alpha)$. Since $\tau \ge 1$ and $d_p(g_\alpha) \ge 1$, it follows from Lemma 3.1(iii) that

$$p - 1 \le p^\tau - \tau \le d_p(g_\alpha) - \mathrm{ord}_p(d_p(g_\alpha)) \le \nu + 1.$$

Thus for $\nu \ge 2$ we have $p^{1/(\nu+1)} \le (\nu+2)^{1/(\nu+1)} \le \nu$ and so (4.6) follows from (4.8).

Case (iv). Suppose finally that $\sigma \le m - 2 - \tau$. In this case we can apply the induction assumption to the sum $S(g_\alpha, p^{m-\sigma})$ and deduce from (4.2) and (4.5) that

$$|S_\alpha| = p^{\sigma-1}|S(g_\alpha, p^{m-\sigma})| \le d_2 p^{\sigma-1} p^{\tau/(d_2+1)} p^{(m-\sigma)(1-1/(d_2+1))},$$

where $d_2 = d_p(p^{-\tau} g'_\alpha)$. Now from Lemma 3.1(iv) we have $d_2 \le \nu$ and thus since $m - \sigma - \tau > 0$ we obtain

$$|S_\alpha| \le \nu p^{\sigma-1} p^{\tau/(\nu+1)} p^{(m-\sigma)(1-1/(\nu+1))} \le \nu p^{(\tau+\sigma-\nu-1)/(\nu+1)} p^{m(1-1/(\nu+1))},$$

and thus (4.6) follows from Lemma 3.1(ii).

Having established (4.6) in every case, we can easily deduce the inequality in (4.5):

$$\begin{aligned} |S(f,p^m)| &\le \sum_{\alpha\in\mathcal{A}} |S_\alpha(f,p^m)| \le \sum_{\alpha\in\mathcal{A}} \nu_\alpha p^{t/(\nu_\alpha+1)} p^{m(1-1/(\nu_\alpha+1))} \\ &\le \Big(\sum_{\alpha\in\mathcal{A}} \nu_\alpha\Big) p^{t/(d_1+1)} p^{m(1-1/(d_1+1))} \le d_1 p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}, \end{aligned}$$

where $d_1 = d_p(p^{-t} f')$. This completes the proof of Theorem 2.1(ii) for $\nu \ge 2$. ∎

We now turn to part (iv) of Theorem 2.1. When $p = 2$ we shall prove by induction on m that for any nonconstant polynomial f over $\mathbb{Z}$, if $m \ge t + 3$, then with $d_1 := d_p(p^{-t} f')$, we have

(A)

$$|S(f, 2^m)| \le d_1 2^{t/(d_1+1)} 2^{m(1-1/(d_1+1))}. \tag{4.9}$$

(B) For any critical point α of multiplicity ν,

$$|S_\alpha(f, 2^m)| \le \nu 2^{t/(\nu+1)} 2^{m(1-1/(\nu+1))}. \tag{4.10}$$

Indeed, as we just observed for the case of odd p, the upper bound in (4.9) is an immediate consequence of (4.10) and so we may restrict our attention to (4.10). The case $\nu = 1$ is treated in Section 5 (see (5.3)). If $\nu \ge 2$ then the upper bound in (4.10) is trivial for $m \le 2\nu + t + 2$. Thus we may assume that $m > 2\nu + t + 2$, $\nu \ge 2$, and that (4.9) and (4.10) are valid for all smaller values of m. By the inequality $\sigma \le \nu + t + 1 - \tau$ of Lemma 3.1(ii) it follows that $m - \sigma \ge \tau + 3$. Thus we can apply the recursion relationship of

Proposition 4.1 and obtain, as in Case (iv) above,

$$|S_\alpha| = 2^{\sigma-1}|S(g_\alpha, 2^{m-\sigma})| \le d_2 2^{\sigma-1} 2^{\tau/(\nu+1)} 2^{(m-\sigma)(1-1/(\nu+1))}$$
$$\le \nu 2^{t/(\nu+1)} 2^{m(1-1/(\nu+1))},$$

which establishes (4.10). ∎

5. Evaluation of pure exponential sums. Let p be an odd prime, and f be a polynomial over $\mathbb{Z}$ with $t = \operatorname{ord}_p(f')$. Suppose first that $m-t$ is even and that $m-t \ge 2$. Write $x = p^{(m-t)/2}z + y$ with y running from 1 to $p^{(m-t)/2}$ and z running from 1 to $p^{(m+t)/2}$. Then with S_α as defined in (2.8), we have

$$S_\alpha = \sum_{y \equiv \alpha \,(\mathrm{mod}\, p)} e_{p^m}(f(y)) \sum_{z=1}^{p^{(m+t)/2}} e_{p^m}(p^{(m-t)/2} f'(y) z)$$
$$= p^t \sum_{y \equiv \alpha \,(\mathrm{mod}\, p)} e_{p^m}(f(y)) \sum_{z=1}^{p^{(m-t)/2}} e_{p^{(m-t)/2}}(p^{-t} f'(y) z),$$

and thus we obtain

$$S_\alpha = p^{(m+t)/2} \sum_{\substack{y \equiv \alpha \,(\mathrm{mod}\, p) \\ p^{-t} f'(y) \equiv 0 \,(\mathrm{mod}\, p^{(m-t)/2})}} e_{p^m}(f(y)), \tag{5.1}$$

where, in the sum, y runs from 1 to $p^{(m-t)/2}$.

If α is a critical point of multiplicity one then it has a unique lifting to a solution of the congruence $p^{-t} f'(y) \equiv 0 \pmod{p^{(m-t)/2}}$. This establishes the first identity in Theorem 2.1(iii).

Suppose next that $m-t$ is odd and that $m-t \ge 3$. Let $x = p^{(m-t+1)/2}z + y$ with y running from 1 to $p^{(m-t+1)/2}$ and z running from 1 to $p^{(m+t-1)/2}$. Then proceeding as above we obtain

$$S_\alpha = p^t \sum_{y \equiv \alpha \,(\mathrm{mod}\, p)} e_{p^m}(f(y)) \sum_{z=1}^{p^{(m-t-1)/2}} e_{p^{(m-t-1)/2}}(p^{-t} f'(y) z),$$

and thus

$$S_\alpha = p^{(m+t-1)/2} \sum_{\substack{y \equiv \alpha \,(\mathrm{mod}\, p) \\ p^{-t} f'(y) \equiv 0 \,(\mathrm{mod}\, p^{(m-t-1)/2})}} e_{p^m}(f(y)), \tag{5.2}$$

where, in the sum, y runs from 1 to $p^{(m-t+1)/2}$.

Suppose now that α is a critical point of multiplicity one and let α^* be the unique lifting of α to a solution of the congruence $p^{-t} f'(y) \equiv 0$

$(\mathrm{mod}\ p^{(m-t+1)/2})$. Then $p^m \mid f'(\alpha^*)p^{(m-t-1)/2}$, and so we obtain

$$\begin{aligned} S_\alpha &= p^{(m+t-1)/2} \sum_{u=0}^{p-1} e_{p^m}(f(\alpha^* + p^{(m-t-1)/2}u)) \\ &= p^{(m+t-1)/2} \sum_{u=0}^{p-1} e_{p^m}\left(f(\alpha^*) + f'(\alpha^*)p^{(m-t-1)/2}u + \frac{f''(\alpha^*)}{2}p^{m-t-1}u^2\right) \\ &= p^{(m+t-1)/2} e_{p^m}(f(\alpha^*)) \sum_{u=0}^{p-1} e_p(p^{-t}2^{-1}f''(\alpha^*)u^2). \end{aligned}$$

The second identity in Theorem 2.1(iii) follows from the standard formula for quadratic Gauss sums.

Finally, we consider the prime $p = 2$. Let α be a critical point of multiplicity one. Suppose first that $m-t \geq 3$ and that $m-t$ is even. Then letting $x = 2^{(m-t+2)/2}z + y$ with z running from 1 to $2^{(m+t-2)/2}$ and y running from 1 to $2^{(m-t+2)/2}$ we obtain

$$S_\alpha = 2^{(m+t-2)/2} \sum_{\substack{y \equiv \alpha \,(\mathrm{mod}\, 2) \\ 2^{-t}f'(y) \equiv 0 \,(\mathrm{mod}\, 2^{(m-t-2)/2})}} e_{2^m}(f(y)) = 2^{(m+t-2)/2} T_\alpha,$$

say. Now, since α admits a unique lifting to a solution α^* of the congruence $2^{-t}f'(y) \equiv 0 \pmod{2^{(m-t-2)/2}}$ we can write $y = \alpha^* + k2^{(m-t-2)/2}$ with $k = 0, 1, 2, 3$ and obtain

$$T_\alpha = e_{2^m}(f(\alpha^*)) \sum_{k=0}^{3} e_8(Ak^2 + 2Bk),$$

for some integers A, B with A odd. Since the value of $Ak^2 + 2Bk \pmod 8$ is invariant if k is replaced with $k+4$, the latter sum is just half the value of a complete Gauss sum (mod 8), which is well known to be of modulus 4. Thus we obtain

$$|S_\alpha(f, 2^m)| = 2^{(m+t)/2}. \tag{5.3}$$

If $m-t$ is odd and $m-t \geq 3$ then writing $x = 2^{(m-t+1)/2}z + y$ with y running from 1 to $2^{(m-t+1)/2}$ and z running from 1 to $2^{(m+t-1)/2}$, we obtain

$$\begin{aligned} S_\alpha(f, 2^m) &= 2^{(m+t-1)/2}(e_{2^m}(f(\alpha^*)) + e_{2^m}(f(\alpha^* + 2^{(m-t-1)/2}))) \\ &= 2^{(m+t-1)/2} e_{2^m}(f(\alpha^*))(1 + e_4(B)), \end{aligned}$$

for some odd integer B, where α^* is the unique lifting of α to a solution of the congruence $p^{-t}f'(y) \equiv 0 \pmod{2^{(m-t+1)/2}}$. Thus we again obtain (5.3). The equality in (5.3) establishes (2.10) for the case $\nu = 1$.

6. Proof of Theorem 1.1. Let p be an odd prime, $m \geq 2$ a positive integer, f a polynomial over $\mathbb{Z}$, χ a multiplicative character (mod p^m) with $c = c(\chi, a)$ as defined in (1.6), and t, t_1 be as defined in (1.7),

$$t := \operatorname{ord}_p(f'(X)), \quad t_1 := \operatorname{ord}_p(rXf'(X) + c).$$

Let $\mathcal{A}$ be the set of critical points associated with the sum $S(\chi, f, p^m)$, that is, the nonzero (mod p) solutions of the congruence

$$p^{-t_1}(rxf'(x) + c) \equiv 0 \pmod{p}. \tag{6.1}$$

We note that $t_1 = \min\{t, \operatorname{ord}_p(c)\}$ and that if $t_1 < t$ then $\mathcal{A}$ is empty.

Suppose that $m \geq t_1 + 2$. Write $k = jp^{m-t_1-2}(p-1) + l$, with j running from 0 to $p^{t_1+1} - 1$, l running from 0 to $p^{m-t_1-2}(p-1) - 1$, and consequently k running from 0 to $p^{m-1}(p-1) - 1$. Let α be an integer of the type $\alpha = a^{l_\alpha}$ with $0 \leq l_\alpha < p - 1$. Then we have

$$\begin{aligned} S_\alpha = S_\alpha(\chi, f, p^m) &:= \sum_{x \equiv \alpha \,(\mathrm{mod}\, p)}^{p^m} \chi(x) e_{p^m}(f(x)) \\ &= \sum_{k \equiv l_\alpha \,(\mathrm{mod}\, p-1)}^{p^{m-1}(p-1)-1} \chi(a^k) e_{p^m}(f(a^k)) \\ &= \sum_{\substack{l=0 \\ l \equiv l_\alpha \,(\mathrm{mod}\, p-1)}}^{p^{m-t_1-2}(p-1)-1} \sum_{j=0}^{p^{t_1+1}-1} e\left(\frac{c(jp^{m-t_1-2}(p-1) + l)}{p^{m-1}(p-1)}\right) e\left(\frac{f(a^k)}{p^m}\right). \end{aligned}$$

Now for any choice of j and l we see from (1.5) that

$$a^k \equiv a^l(1 + rp)^{p^{m-t_1-2}j} \equiv a^l(1 + jrp^{m-t_1-1}) \pmod{p^{m-t_1}},$$

and thus since $m \geq t_1 + 2$, it follows from Lemma 3.2 and the fact that $p^t \mid f'(X)$ that

$$f(a^k) \equiv f(a^l + a^l jrp^{m-t_1-1}) \equiv f(a^l) + f'(a^l)a^l jrp^{m-t_1-1} \pmod{p^m}.$$

We obtain

$$\begin{aligned} S_\alpha = &\sum_{\substack{l=0 \\ l \equiv l_\alpha \,(\mathrm{mod}\, p-1)}}^{p^{m-t_1-2}(p-1)-1} e\left(\frac{cl}{p^{m-1}(p-1)} + \frac{f(a^l)}{p^m}\right) \\ &\times \sum_{j=0}^{p^{t_1+1}-1} e\left(\frac{cj}{p} + \frac{f'(a^l)a^l jr}{p}\right) \\ = p^{t_1+1} &\sum_{\substack{l \equiv l_\alpha \,(\mathrm{mod}\, p-1) \\ c + rf'(a^l)a^l \equiv 0 \,(\mathrm{mod}\, p^{t_1+1})}}^{p^{m-t_1-2}(p-1)-1} e\left(\frac{cl}{p^{m-1}(p-1)} + \frac{f(a^l)}{p^m}\right). \end{aligned} \tag{6.2}$$

Thus $S_\alpha = 0$ unless $\alpha \in \mathcal{A}$ in which case we must have $t = t_1$ and we can proceed by writing $l = l_\alpha + (p-1)y$ with y running from 0 to $p^{m-t-2}-1$, to obtain

$$S_\alpha = p^{t+1} \sum_{y=0}^{p^{m-t-2}-1} e\left(\frac{c(l_\alpha + (p-1)y)}{p^{m-1}(p-1)} + \frac{f(\alpha(1+rp)^y)}{p^m}\right) \tag{6.3}$$

$$= p^{t+1}\chi(\alpha) e_{p^m}(f(\alpha)) \sum_{y=0}^{p^{m-t-2}-1} e_{p^m}(F_1(y)),$$

where

$$F_1(y) = f(\alpha(1+rp)^y) - f(\alpha) + pcy. \tag{6.4}$$

Our next step is to make a change of variables in order to transform the function $F_1(y)$ into a polynomial that we can deal with. Let $\log(1+pu)$ denote the p-adic logarithm

$$\log(1+pu) = \sum_{i=1}^{\infty} \frac{(-1)^{i+1}(pu)^i}{i},$$

and set

$$R := p^{-1}\log(1+pr) = r - \frac{r^2 p}{2} + \frac{r^3 p^2}{3} - \dots \tag{6.5}$$

We note that $\log(1+pu)$ is a p-adic integer for any $u \in \mathbb{Z}_p$, and that R is a p-adic unit (since $p \nmid r$) with $R \equiv r \pmod p$. Set

$$y = \frac{1}{Rp}\log(1+pu), \tag{6.6}$$

and note that as u runs through a complete set of residues modulo any given power of p, so does y (in $\mathbb{Z}_p$). This is most readily seen from the inverse relationship

$$(1+rp)^y = e^{y\log(1+rp)} = e^{yRp} = 1 + pu. \tag{6.7}$$

Thus if

$$y_1 = \frac{1}{Rp}\log(1+pu_1), \quad y_2 = \frac{1}{Rp}\log(1+pu_2), \quad y_1 \equiv y_2 \pmod{p^k}$$

then

$$e^{y_1 Rp} \equiv e^{y_2 Rp} \pmod{p^{k+1}}$$

and consequently $u_1 \equiv u_2 \pmod{p^k}$. In order to deal with the resulting exponential sum in the variable u we extend the domain of the additive character $e_{p^m}(\cdot)$ to the ring of p-adic integers $\mathbb{Z}_p$ by setting, for any $x \in \mathbb{Z}_p$,

$$e_{p^m}(x) := e_{p^m}(\widetilde{x}), \tag{6.8}$$

where $\widetilde{x}$ is the residue class of x in $\mathbb{Z}_p/(p^m) \simeq \mathbb{Z}/(p^m)$.

Set $F_2(u) = F_1(y)$, and let f have Taylor expansion about α given by

$$f(X) = \sum_{i=0}^{d} a_i (X-\alpha)^i,$$

with rational integer coefficients a_i, $0 \le i \le d$. Then for any $u \in \mathbb{Z}_p$ we have

$$\begin{aligned} F_2(u) &= f(\alpha(1+pu)) - f(\alpha) + cR^{-1}\log(1+pu) \\ &= \sum_{i=1}^{d} a_i \alpha^i p^i u^i + cR^{-1} \sum_{i=1}^{\infty} \frac{(-1)^{i+1}(pu)^i}{i} \\ &= \sum_{i=1}^{d} (Ria_i\alpha^i + (-1)^{i+1}c)\frac{p^i}{Ri} u^i + \frac{c}{R} \sum_{i=d+1}^{\infty} \frac{(-1)^{i+1}p^i}{i} u^i. \end{aligned} \tag{6.9}$$

Define

$$G(X) := p^{-t}(RXf'(X) + c),$$

and let $G(X)$ have Taylor expansion about α,

$$G(X) = \sum_{i=0}^{d} b_i (X-\alpha)^i,$$

with p-adic integer coefficients b_i, $0 \le i \le d$. Then we have

$$\begin{aligned} p^t G(X) &= R(X-\alpha)\sum_{i=0}^{d} a_i i (X-\alpha)^{i-1} + R\alpha \sum_{i=0}^{d} a_i i (X-\alpha)^{i-1} + c \\ &= Ra_d d (X-\alpha)^d + R\sum_{i=1}^{d-1} (a_i i + \alpha a_{i+1}(i+1))(X-\alpha)^i \\ &\quad + R\alpha a_1 + c, \end{aligned}$$

and so we see that $b_0 = p^{-t}(R\alpha a_1 + c)$, $b_d = p^{-t} R a_d d$ and for $1 \le i \le d-1$,

$$b_i = p^{-t} R(ia_i + \alpha(i+1)a_{i+1}). \tag{6.10}$$

It follows that for $1 \le i \le d$,

$$a_i = (-1)^{i+1}(Ri\alpha^i)^{-1}\Big(\sum_{j=0}^{i-1}(-1)^j p^t b_j \alpha^j - c\Big). \tag{6.11}$$

Thus by (6.9) and (6.11) we obtain

$$\begin{aligned} F_2(u) = &\sum_{i=1}^{d} (-1)^{i+1}\Big(\sum_{j=0}^{i-1}(-1)^j b_j \alpha^j\Big)\frac{p^{i+t}}{Ri} u^i \\ &+ \frac{c}{R}\sum_{i=d+1}^{\infty} \frac{(-1)^{i+1}p^i}{i} u^i. \end{aligned} \tag{6.12}$$

Let $F_2(U)$ be the formal power series over $\mathbb{Z}_p$ obtained by replacing u with the indeterminate symbol U in (6.9) or (6.12) and let $F_\alpha(U)$ be a polynomial with rational integer coefficients chosen so that in $\mathbb{Z}_p[[U]]$,

$$F_\alpha(U) \equiv F_2(U) \pmod{p^{m+t+d}}, \tag{6.13}$$

that is, the corresponding coefficients are congruent (mod p^{m+t+d}). Since the coefficients of $F_2(U)$ are all eventually zero (mod p^{m+t+d}) such a polynomial $F_\alpha(U)$ exists. The absolute degree of $F_\alpha(U)$ is of no particular concern since we are only interested in local information regarding $F_\alpha(U)$. We have taken a larger modulus in (6.13) than necessary in order to preserve the multiplicity of p dividing certain coefficients of $F_2(U)$ and thus make the statement of Lemma 6.1 below more transparent.

Now, since α is a critical point, we know $p \mid b_0$ and $p^t \mid c$. Thus for any integer u it follows from (6.12) that $p^{t+2} \mid F_2(u)$ (in $\mathbb{Z}_p$) and consequently $p^{t+2} \mid F_1(y)$ for any integer y. Thus from (6.3) we obtain

$$\begin{aligned} S_\alpha &= p^{-1}\chi(\alpha)e_{p^m}(f(\alpha))\sum_{y=1}^{p^m} e_{p^m}(F_1(y)) \\ &= p^{-1}\chi(\alpha)e_{p^m}(f(\alpha))\sum_{u=1}^{p^m} e_{p^m}(F_2(u)) \\ &= \chi(\alpha)e_{p^m}(f(\alpha))\sum_{u=1}^{p^{m-1}} e_{p^m}(F_\alpha(u)). \end{aligned} \tag{6.14}$$

We have established

Proposition 6.1 (Untwisting a mixed exponential sum). *Suppose that p is an odd prime, f is a polynomial over $\mathbb{Z}$, χ is a multiplicative character (mod p^m) and that $m \geq t_1 + 2$. Let $\mathcal{A}$ be the set of critical points associated with the sum $S(\chi, f, p^m)$ and suppose that representatives have been chosen so that for any $\alpha \in \mathcal{A}$, $\alpha = a^{l_\alpha}$ with $0 \leq l_\alpha < p-1$. Then*

$$S(\chi, f, p^m) = \sum_{\alpha \in \mathcal{A}} \chi(\alpha)e_{p^m}(f(\alpha))S(F_\alpha, p^{m-1}),$$

where F_α is as defined in (6.13).

We now proceed to prove Theorem 1.1(ii) for the case where $\nu \geq 2$. The case $\nu = 1$ is treated in Section 7. Let

$$\begin{aligned} \sigma &:= \operatorname{ord}_p(F_\alpha(U)), \quad & g_\alpha(U) &:= p^{-\sigma}F_\alpha(U), \\ \tau &:= \operatorname{ord}_p(g'_\alpha(U)), \quad & g_1(U) &:= p^{-\tau}g'_\alpha(U). \end{aligned}$$

LEMMA 6.1 *We have the same relationships as in Lemma* 3.1:

(i) $$\sigma \geq t+2.$$

(ii) $$\sigma \leq \nu + 1 + t - \tau.$$

(iii) $$d_p(g_\alpha) \leq \sigma - t + \mathrm{ord}_p(d_p(g_\alpha)) \leq \nu + 1 + \mathrm{ord}_p(d_p(g_\alpha)).$$

(iv) $$d_p(g_1) \leq \sigma + \tau - t - 1 \leq \nu.$$

(v) $$p^\tau \mid d_p(g_\alpha).$$

P r o o f. Part (i) follows immediately from (6.12) and our observations above that $p \mid b_0$ and $p^t \mid c$. From (6.12) we also obtain

$$F_2'(U) = p^t R^{-1} \sum_{i=1}^{d} (-1)^{i+1} \Big(\sum_{j=0}^{i-1} (-1)^j b_j \alpha^j \Big) p^i U^{i-1} + cR^{-1} \sum_{i=d+1}^{\infty} (-1)^{i+1} p^i U^i. \tag{6.15}$$

Since α is a critical point of multiplicity $\nu \geq 1$ we have $p \mid b_i$ for $i < \nu$, and $p \nmid b_\nu$. By definition, $p^{\sigma+\tau}$ divides every coefficient of $F_2'(U)$ and thus examining the $i = \nu + 1$ coefficient in (6.15) we obtain (ii). Some care needs to be taken when $\nu = d$. In this case we must have $p^t \parallel c$ for otherwise the critical point congruence is just $p^{-t} x f'(x) \equiv 0 \pmod p$ and so the multiplicity of α is at most $d-1$. Part (iii) comes from the fact that p^σ is the maximum power of p dividing the $i = d_p(g_\alpha)$ coefficient in (6.12) and part (iv) from the fact that $p^{\sigma+\tau}$ is the maximum power of p dividing the $i = d_p(g_1) + 1$ coefficient in (6.15). Part (v) follows as in Lemma 3.1. ∎

We can now complete the proof of Theorem 1.1(ii) by considering the same four cases as in the proof of Theorem 2.1(ii): $\sigma \geq m$, $\sigma = m-1$, $m - 1 - \tau \leq \sigma \leq m - 2$ and $\sigma \leq m - 2 - \tau$. In each case we establish the inequality

$$|S_\alpha| \leq \nu p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}. \tag{6.16}$$

The trivial estimate $|S_\alpha| \leq p^{m-1}$ suffices for the first and third cases identically as before under the assumption that $\nu \geq 2$. For the other two cases we use (6.14), which can be written as

$$|S_\alpha| = p^{\sigma-1} |S(g_\alpha, p^{m-\sigma})|. \tag{6.17}$$

In the second case, an application of Weil's bound to the sum $S(g_\alpha, p)$ holds identically as before for $\nu \geq 2$. In the fourth case, instead of using an induction assumption as we did in the proof of Theorem 2.1(ii), we simply apply the result of Theorem 2.1(ii), specifically (2.11), and the proof follows as before: Letting $d_2 = d_p(g_1)$ we obtain from (6.17) and (2.11),

$$|S_\alpha| \leq d_2 p^{\sigma-1} p^{\tau/(d_2+1)} p^{(m-\sigma)(1-1/(d_2+1))}.$$

Now by Lemma 6.1(iv) we have $d_2 \le \nu$ and thus since $m-\sigma-\tau>0$ we obtain

$$|S_\alpha| \le \nu p^{\sigma-1} p^{\frac{\tau}{\nu+1}} p^{(m-\sigma)(1-\frac{1}{\nu+1})} = \nu p^{\frac{\tau+\sigma-\nu-1}{\nu+1}} p^{m(1-\frac{1}{\nu+1})}.$$

The inequality in (6.16) now follows from Lemma 6.1(ii). This completes the proof of Theorem 1.1(ii) for $\nu \ge 2$. In the next section we take care of the case $\nu = 1$ and establish part (iii) of the theorem.

7. Evaluation of mixed exponential sums. Having established Proposition 6.1 one can attempt to evaluate a mixed exponential sum by untwisting the sum first and then applying either the recursion relationship of Proposition 4.1 or Theorem 2.1(iii) to the resulting pure exponential sum. A more direct approach is to proceed as follows. Suppose first that $m-t$ is even and that $m-t \ge 2$. Let r, R be as defined earlier, $a^{p-1} = 1+rp$ with $p \nmid r$, $R = p^{-1}\log(1+rp)$, and define ϱ by

$$a^{p^{(m-t)/2-1}(p-1)} = 1 + \varrho p^{(m-t)/2}. \tag{7.1}$$

Then it is easy to see that

$$\varrho \equiv r \pmod p \quad \text{and} \quad \varrho \equiv R \pmod{p^{(m-t)/2}}. \tag{7.2}$$

Write $k = jp^{(m-t)/2-1}(p-1)+l$, with j running from 0 to $p^{(m+t)/2}-1$, l running from 0 to $p^{(m-t)/2-1}(p-1)-1$, and consequently k running from 0 to $p^{m-1}(p-1)-1$. Then we have

$$\begin{aligned} &S(\chi, f, p^m) \\ &\quad = \sum_{k=0}^{p^{m-1}(p-1)-1} \chi(a^k) e_{p^m}(f(a^k)) \\ &\quad = \sum_{l=0}^{p^{(m-t)/2-1}(p-1)-1} \sum_{j=0}^{p^{(m+t)/2}-1} e\left(\frac{c(jp^{(m-t)/2-1}(p-1)+l)}{p^{m-1}(p-1)}\right) e\left(\frac{f(a^k)}{p^m}\right). \end{aligned}$$

Now for any choice of j and l we have

$$a^k \equiv a^l(1+\varrho p^{(m-t)/2})^j \equiv a^l(1+j\varrho p^{(m-t)/2}) \pmod{p^{m-t}},$$

and thus since $p^t \mid f'(X)$,

$$f(a^k) \equiv f(a^l + a^l j\varrho p^{(m-t)/2}) \equiv f(a^l) + f'(a^l)a^l j\varrho p^{(m-t)/2} \pmod{p^m}.$$

It follows that

$$S(\chi, f, p^m)$$
$$= \sum_l e\left(\frac{cl}{p^{m-1}(p-1)} + \frac{f(a^l)}{p^m}\right) \sum_{j=0}^{p^{(m+t)/2}-1} e\left(\frac{cj}{p^{(m+t)/2}} + \frac{f'(a^l)a^l j\varrho}{p^{(m+t)/2}}\right)$$
$$= p^{(m+t)/2} \sum_{\substack{l=0 \\ c+f'(a^l)a^l\varrho \equiv 0 \,(\mathrm{mod}\, p^{(m+t)/2})}}^{p^{(m-t)/2-1}(p-1)-1} e\left(\frac{cl}{p^{m-1}(p-1)} + \frac{f(a^l)}{p^m}\right).$$

Thus

$$S(\chi, f, p^m) = p^{(m+t)/2} \sum_{\alpha \in \mathcal{A}^*} \chi(\alpha) e_{p^m}(f(\alpha)), \tag{7.3}$$

where $\mathcal{A}^*$ is a set of integer representatives for the set of reduced residues (mod $p^{(m-t)/2}$) satisfying the congruence

$$p^{-t}(Rxf'(x) + c) \equiv 0 \pmod{p^{(m-t)/2}}. \tag{7.4}$$

We note that for $\alpha \in \mathcal{A}^*$ the value of $\chi(\alpha)e_{p^m}(\alpha)$ does not depend on the choice of the integer representative for α, and thus the sum in (7.3) is well defined. If α is a critical point of multiplicity one then it admits a unique lifting to a solution of the congruence (7.4). This establishes the first formula in Theorem 1.1(iii).

Suppose now that $m - t$ is odd and that $m - t \geq 3$. This time let ϱ be defined by the equation

$$a^{p^{(m-t-1)/2}(p-1)} = 1 + \varrho p^{(m-t+1)/2}. \tag{7.5}$$

Then

$$\varrho \equiv R \pmod{p^{(m-t+1)/2}}. \tag{7.6}$$

For l running from 0 to $p^{(m-t-1)/2}(p-1) - 1$ and j running from 0 to $p^{(m+t-1)/2} - 1$, writing $k = jp^{(m-t-1)/2}(p-1) + l$ and observing that

$$a^k \equiv a^l(1 + \varrho p^{(m-t+1)/2})^j \equiv a^l(1 + j\varrho p^{(m-t+1)/2}) \pmod{p^{m-t+1}},$$

and consequently (since $p^t \mid f'(X)$),

$$f(a^k) \equiv f(a^l) + f'(a^l)a^l\varrho j p^{(m-t+1)/2} \pmod{p^m}, \tag{7.7}$$

we obtain

$$S(\chi, f, p^m) = \sum_{l=0}^{p^{(m-t-1)/2}(p-1)-1} e\left(\frac{cl}{p^{m-1}(p-1)} + \frac{f(a^l)}{p^m}\right) \times \sum_{j=0}^{p^{(m+t-1)/2}-1} e\left(\frac{cj}{p^{(m+t-1)/2}} + \frac{f'(a^l)a^l j\varrho}{p^{(m+t-1)/2}}\right) \tag{7.8}$$

$$= p^{(m+t-1)/2} \sum_{\substack{l=0 \\ c+f'(a^l)a^l\varrho\equiv 0 \,(\mathrm{mod}\, p^{(m+t-1)/2})}}^{p^{(m-t-1)/2}(p-1)-1} e\bigg(\frac{cl}{p^{m-1}(p-1)} + \frac{f(a^l)}{p^m}\bigg).$$

Again we see that if $\alpha \notin \mathcal{A}$ then $S_\alpha = 0$. If $\alpha \in \mathcal{A}$ then

$$S_\alpha = p^{(m+t-1)/2} \sum_{\substack{l=0 \\ a^l\equiv\alpha \,(\mathrm{mod}\, p)}}^{p^{(m-t-1)/2}(p-1)-1} e\bigg(\frac{cl}{p^{m-1}(p-1)} + \frac{f(a^l)}{p^m}\bigg). \tag{7.9}$$

Suppose now that α is a critical point of multiplicity one. Then α admits a unique lifting to a solution of the congruence

$$p^{-t}(Rxf'(x) + c) \equiv 0 \pmod{p^{(m-t+1)/2}}. \tag{7.10}$$

To keep our notation simple we suppose that α is a solution of (7.10) and that

$$\alpha \equiv a^{l_\alpha} \pmod{p^m} \quad \text{with } 0 \le l_\alpha < p^{m-1}(p-1) - 1.$$

Let s be defined by

$$a^{p^{(m-t-3)/2}(p-1)} = 1 + sp^{(m-t-1)/2}. \tag{7.11}$$

Noting that in the sum in (7.9), l is allowed to run through any complete set of residues (mod $p^{(m-t-1)/2}(p-1)$) (subject to the constraint $a^l \equiv \alpha$ (mod p)), we can write $l = l_\alpha + p^{(m-t-3)/2}(p-1)u$ with u running from 0 to $p-1$. Then

$$\begin{aligned} a^l &\equiv \alpha(1 + sp^{(m-t-1)/2})^u \\ &\equiv \alpha\bigg(1 + usp^{(m-t-1)/2} + \binom{u}{2}s^2p^{m-t-1}\bigg) \pmod{p^{m-t}}, \end{aligned}$$

and thus since $p^t \mid f'(X)$ and $m - t \ge 3$ it follows in the same manner as in the proof of Lemma 3.2 that

$$\begin{aligned} f(a^l) \equiv f(\alpha) + f'(\alpha)\alpha\bigg(usp^{(m-t-1)/2} + \binom{u}{2}s^2p^{m-t-1}\bigg) \\ + \overline{2}f''(\alpha)\alpha^2u^2s^2p^{m-t-1} \pmod{p^m}, \end{aligned}$$

where $\overline{2}$ denotes the multiplicative inverse of 2 (mod p^m). Thus

$$\begin{aligned} S_\alpha = \chi(\alpha)e_{p^m}(f(\alpha))p^{(m+t-1)/2} \\ \times \sum_{u=0}^{p-1} e\bigg(\frac{cp^{(m-t-3)/2}(p-1)u}{p^{m-1}(p-1)} + \frac{f'(\alpha)\alpha usp^{(m-t-1)/2}}{p^m} \\ + \frac{f'(\alpha)\alpha\binom{u}{2}s^2p^{m-t-1} + \overline{2}f''(\alpha)\alpha^2u^2s^2p^{m-1}}{p^m}\bigg) \end{aligned} \tag{7.12}$$

$$= \chi(\alpha)e_{p^m}(f(\alpha))p^{(m+t-1)/2}\sum_{u=0}^{p-1} e_p(A_\alpha u^2 + B_\alpha u),$$

where

$$A_\alpha = p^{-t}(\overline{2}f''(\alpha)\alpha^2 s^2 + \overline{2}f'(\alpha)\alpha s^2), \tag{7.13}$$

$$B_\alpha = \frac{c + f'(\alpha)\alpha s}{p^{(m-t-1)/2}} - \overline{2}f'(\alpha)\alpha s^2. \tag{7.14}$$

Now, by definition of ϱ, (7.5), and s, (7.11), we have

$$\varrho = s + \overline{2}(p-1)s^2 p^{(m-t-1)/2} + p^{-1}\binom{p}{3}s^3 p^{m-t-1} + \dots,$$

and thus from (7.14) we get

$$B_\alpha \equiv \frac{c + f'(\alpha)\alpha\varrho}{p^{(m-t-1)/2}} \pmod{p}.$$

Now by (7.6) and our assumption that α satisfies (7.10) we obtain

$$B_\alpha \equiv \frac{c + R\alpha f'(\alpha)}{p^{(m-t-1)/2}} \equiv 0 \pmod{p}.$$

The second formula of Theorem 1.1(iii) now follows from (7.12) and the standard formula for a quadratic Gauss sum.

8. Mixed exponential sums with $p = 2$. The prime $p = 2$ requires special attention because there is no primitive root (mod 2^m) for $m \geq 3$. For $m \geq 3$ the reduced residues (mod 2^m) are of the form $\{\pm 5^k : 0 \leq k \leq 2^{m-1}\}$, and a multiplicative character $\chi \pmod{2^m}$ is determined by the relations

$$\chi(5) = e_{2^{m-2}}(c), \quad \chi(-1) = (-1)^\kappa \tag{8.1}$$

for some integer c with $1 \leq c \leq 2^{m-2}$ and $\kappa = 0$ or 1. Let f be a polynomial with integer coefficients and $d_2(f) \geq 1$, and set

$$t = \operatorname{ord}_2(f'), \quad t_1 = \operatorname{ord}_2(Xf'(X) + c).$$

The critical point congruence associated with the sum $S(\chi, f, 2^m)$ is just $2^{-t_1}(xf'(x)+c) \equiv 0 \pmod 2$. The only allowable critical point is the residue class 1 and it is a critical point if and only if $t = t_1$ and $f'(1) \equiv c \pmod{2^{t+1}}$.

THEOREM 8.1. *Suppose that $m \geq t_1 + 3$, f is a polynomial over $\mathbb{Z}$ and χ is a multiplicative character (mod 2^m) satisfying* (8.1). *Then*:

(i) *If* 1 *is not a critical point then* $S(\chi, f, 2^m) = 0$.

(ii) *If* 1 *is a critical point of multiplicity* $\nu \geq 1$ *then* $t = t_1$ *and*

$$|S(\chi, f, 2^m)| \leq 2\nu 2^{t/(\nu+1)}2^{m(1-1/(\nu+1))}. \tag{8.2}$$

Proof. Let $k = j2^{m-t_1-3} + l$ with j running from 1 to 2^{t_1+1}, and l running from 1 to 2^{m-t_1-3}. Now

$$5^k \equiv 5^l(1+2^2)^{j2^{m-t_1-3}} \equiv 5^l(1+2^{m-t_1-1}j) \pmod{2^{m-t_1}},$$

and so by Lemma 3.2 and the fact that $2^t \mid f'(X)$ we obtain, if $m - t_1 \geq 3$,

$$f(5^k) \equiv f(5^l) + f'(5^l)5^l j2^{m-t_1-1} \pmod{2^m}.$$

A similar relationship holds for $f(-5^k)$. Thus for $m - t_1 \geq 3$ we obtain

$$S(\chi, f, 2^m) = 2^{t+1}T_1 + \chi(-1)2^{t+1}T_2, \tag{8.3}$$

where

$$T_1 = \sum_{c+f'(5^l)5^l \equiv 0 \,(\mathrm{mod}\, 2^{t_1+1})}^{2^{m-t_1-3}} e\left(\frac{cl}{2^{m-2}} + \frac{f(5^l)}{2^m}\right) \tag{8.4}$$

and

$$T_2 = \sum_{c-f'(-5^l)5^l \equiv 0 \,(\mathrm{mod}\, 2^{t_1+1})}^{2^{m-t_1-3}} e\left(\frac{cl}{2^{m-2}} + \frac{f(-5^l)}{2^m}\right).$$

In particular, if 1 is not a critical point then $S(\chi, f, 2^m) = 0$, proving part (i) of the theorem.

Suppose now that 1 is a critical point of multiplicity ν. In particular, $t = t_1$. We note first that the upper bound in (8.2) is trivial if $m - t \leq 3(\nu+1)$ and thus we may assume that $m - t \geq 3\nu + 4 \geq 7$.

We focus our attention on estimating T_1, the estimate for T_2 being analogous. We can write

$$T_1 = e_{2^m}(f(1)) \sum_{l=1}^{2^{m-t-3}} e_{2^m}(F_1(l)), \tag{8.5}$$

where

$$F_1(l) := 4cl + f(5^l) - f(1). \tag{8.6}$$

Let $\log(1+4u)$ be the 2-adic logarithm and R the 2-adic unit

$$R := \frac{1}{4}\log 5 = \sum_{i=1}^{\infty} \frac{(-1)^{i+1}4^{i-1}}{i}.$$

Set

$$l = \frac{1}{4R}\log(1+4u).$$

Then $5^l = e^{4Rl} = 1 + 4u$, and as u runs through a complete set of residues modulo any given power of 2, so does l in $\mathbb{Z}_2$. Set $F_2(u) = F_1(y)$ and

$$G(X) := 2^{-t}(RXf'(X) + c),$$

say $f(X)=\sum_{i=0}^{d} a_i(X-1)^i$, $G(X)=\sum_{i=0}^{d} b_i(X-1)^i$. Then we have the same relations as in (6.10) and (6.11), and we obtain

$$F_2(u)=\sum_{i=1}^{d}(-1)^{i+1}\Big(\sum_{j=0}^{i-1}(-1)^j b_j\Big)\frac{2^{2i+t}}{Ri}u^i+\frac{c}{R}\sum_{i=d+1}^{\infty}\frac{(-1)^{i+1}4^i}{i}u^i. \tag{8.7}$$

Let σ, τ, g_α and g_1 be as defined in Section 6 (right before Lemma 6.1). Then the analogue of Lemma 6.1 we obtain here is

$$\sigma \ge t+3, \tag{8.8}$$

$$\sigma \le 2\nu+t+2-\tau, \tag{8.9}$$

$$d_2(g_1)\le(\sigma+\tau-t)/2-1\le\nu. \tag{8.10}$$

It follows from (8.9) and our assumption that $m-t\ge 3\nu+4$ that $m-\sigma\ge\tau+3$. Then by (8.5), Theorem 2.1(iv) and (8.10) we obtain

$$\begin{aligned}2^{t+1}|T_1| &= 2^{t+1}\Big|\sum_{u=1}^{2^{m-t-3}} e_{2^m}(F_2(u))\Big| = 2^{\sigma-2}|S(g_\alpha,2^{m-\sigma})|\\ &\le 2^{\sigma-2}d_2 2^{\tau/(d_2+1)}2^{(m-\sigma)(1-1/(d_2+1))},\end{aligned}$$

where $d_2=d_2(g_1)$. Thus by (8.10) and (8.9) we have

$$\begin{aligned}2^{t+1}|T_1| &\le \nu 2^{\sigma-2}2^{\tau/(\nu+1)}2^{(m-\sigma)(1-1/(\nu+1))}\\ &= \nu 2^{(\sigma-2\nu-2+\tau)/(\nu+1)}2^{m(1-1/(\nu+1))}\\ &\le \nu 2^{t/(\nu+1)}2^{m(1-1/(\nu+1))}.\end{aligned}$$

The same upper bound holds for $|T_2|$ and so by (8.3) we obtain the inequality in (8.2). ∎

9. Extremal examples

Example 9.1. In this example we give a class of polynomials for which the exponent $m(1-1/d)$ in the upper bound for pure exponential sums is sharp. Let $d\ge 2$ be a positive integer, p a prime, a an integer with $p\nmid a$ and $h(X)$ be any polynomial over $\mathbb{Z}$. Set $\delta=\operatorname{ord}_p(d)$. Suppose that either p is odd or that $p=2$ and $d\ne 2,4$. Then for any m with $d\mid m$ we have

$$S(aX^d+p^{\delta+1}X^d h(X),p^m)=p^{m(1-1/d)}. \tag{9.1}$$

For the case $p=2$ and $d=2$ or 4 we note that

$$S(X^2,2^2)=2(1+i),\qquad S(X^4,2^4)=2^3(1+e(1/16)).$$

Proof. Suppose that p is odd. The proof is by induction on m starting with $m=d$. Let $f(X)=aX^d+p^{\delta+1}X^d h(X)$ and $t=t(f):=\operatorname{ord}_p(f')$. Then it is easy to see that $t=\delta$ and so the critical point congruence is just

$$p^{-t}f'(x)\equiv a_1x^{d-1}\equiv 0 \pmod p,$$

where $a_1 = p^{-\delta}da$. Thus there is a single critical point, $\alpha = 0$, of multiplicity $d-1$, and so it follows from the recursion relationship (4.2) that if $m \geq \delta+2$ then

$$S(f, p^m) = p^{\sigma-1}S(g, p^{m-\sigma}),$$

where $\sigma = \mathrm{ord}_p(f(pY)) = d$ and

$$g(Y) = p^{-\sigma}f(pY) = aY^d + p^{\delta+1}Y^d h(pY).$$

Now when $m = d$, we have $m-\sigma = 0$ and so $S(f, p^m) = p^{d-1} = p^{d(1-1/d)}$ provided that $d \geq \delta+2$. Since p is odd and $d \geq 2$ the latter condition always holds. If $m > d$ and $d \,|\, m$ then we observe that the polynomial g is of the same type as f and so by the induction assumption we have

$$S(f, p^m) = p^{d-1}S(g, p^{m-d}) = p^{d-1}p^{(m-d)(1-1/d)} = p^{m(1-1/d)}.$$

When $p = 2$ the same argument works only this time we need $d \geq \delta+3$ in order to apply the recursion relationship. This condition holds unless $d = 2$ or 4. ∎

Example 9.2. In this example we show that the exponent $m(1–1/(d+1))$ in the upper bound for mixed exponential sums is best possible. Let $d \geq 1$ be a fixed positive integer, L the least common multiple of the integers from 1 to d, and define $f(X) \in \mathbb{Z}[X]$ by

$$f(X) = \sum_{i=1}^{d} \frac{(-1)^i L}{i}(X-1)^i.$$

Let p be a prime with $p > d+2$, m a positive integer with $d+1 \,|\, m$, and χ be any multiplicative character (mod p^m) such that $c = c(\chi, a) \equiv RL \pmod{p^{m-1}}$, where R is as defined in (6.5). There are $p-1$ such characters χ, all of them primitive. Then

$$S(\chi, f, p^m) = p^{m(1-1/(d+1))}. \tag{9.2}$$

Proof. We have

$$\begin{aligned} G(X) := RXf'(X) + c &\equiv c\Big(X\sum_{i=1}^{d}(-1)^i(X-1)^{i-1} + 1\Big) \\ &\equiv c(1-X)^d \pmod{p^{m-1}}, \end{aligned} \tag{9.3}$$

and so there is a single critical point $\alpha = 1$ of multiplicity d. From (6.9) we see that for $1 \leq i \leq d$ the coefficient of U^i in $F_2(U)$ is

$$(R(-1)^i L + (-1)^{i+1}c)p^i(Ri)^{-1} \equiv 0 \pmod{p^m}.$$

Thus

$$F_2(U) \equiv L\sum_{i=d+1}^{\infty} \frac{(-1)^{i+1}p^i}{i}U^i \pmod{p^m}.$$

Since $p > d+2$ we see that $\sigma := \mathrm{ord}_p(F_\alpha(U)) = d+1$, and that

$$g_\alpha(U) := p^{-\sigma}F_\alpha(U) \equiv (-1)^d L\overline{(d+1)}U^{d+1} + pU^{d+1}h_\alpha(U) \pmod{p^{m-d-1}},$$

for some polynomial $h_\alpha(U)$ with integer coefficients. Here, $\overline{d+1}$ is the inverse of $d+1 \pmod{p^m}$. We observe that $g_\alpha(U)$ is a polynomial of the type considered in Example 9.1, and thus from Proposition 6.1 and (9.1) we obtain, if $d+1 \mid m$,

$$\begin{aligned} S(\chi, f, p^m) &= \chi(1)e_{p^m}(f(1))p^d \sum_{u=0}^{p^{m-d-1}} e_{p^{m-d-1}}(g_\alpha(u)) \\ &= p^d p^{(m-d-1)(1-1/(d+1))} = p^{m(1-1/(d+1))}. \ \blacksquare \end{aligned}$$

References

[1] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. 88 (1966), 71–105.

[2] J. H. H. Chalk, *On Hua's estimate for exponential sums*, Mathematika 34 (1987), 115–123.

[3] J. R. Chen, *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1977), 711–719.

[4] T. Cochrane and Z. Y. Zheng, *Exponential sums with rational function entries*, to appear.

[5] P. Ding, *An improvement to Chalk's estimation of exponential sums*, Acta Arith. 59 (1991), 149–155.

[6] —, *On a conjecture of Chalk*, J. Number Theory 65 (1997), 116–129.

[7] G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio Numerorum" 1: A new solution of Waring's problem*, Nachr. K. Gesellschaft Wiss. Göttingen Math.-Phys. Kl. 1929, 33–54.

[8] —, —, *Some problems of "Partitio Numerorum"*, Math. Z. 23 (1925), 1–37.

[9] D. R. Heath-Brown, *An estimate on Heilbronn's exponential sum*, in: Analytic Number Theory, Vol. 2 (Allerton Park, IL, 1995), Progr. Math. 139, Birkhäuser, Boston, 1996, 451–463.

[10] L. K. Hua, *On exponential sums*, J. Chinese Math. Soc. 20 (1940), 301–312.

[11] —, *On exponential sums*, Sci. Record (Peking) (N.S.) 1 (1957), 1–4.

[12] —, *Additive Primzahltheorie*, Teubner, Leipzig, 1959, 2–7.

[13] W. K. A. Loh, *Hua's Lemma*, Bull. Austral. Math. Soc. (3) 50 (1994), 451–458.

[14] J. H. Loxton and R. A. Smith, *On Hua's estimate for exponential sums*, J. London Math. Soc. (2) 26 (1982), 15–20.

[15] J. H. Loxton and R. C. Vaughan, *The estimation of complete exponential sums*, Canad. Math. Bull. 28 (1985), 442–454.

[16] V. I. Nechaev, *An estimate of a complete rational trigonometric sum*, Mat. Zametki 17 (1975), 839–849 (in Russian); English transl.: Math. Notes 17 (1975).

[17] H. Salié, *Über die Kloostermanschen Summen $S(u, v; q)$*, Math. Z. 34 (1931), 91–109.

[18] W. M. Schmidt, *Equations over Finite Fields*, Lecture Notes in Math. 536, Springer, Berlin, 1976.

[19] R. A. Smith, *Estimate for exponential sums*, Proc. Amer. Math. Soc. 79 (1980), 365–368.
[20] S. B. Stechkin, *Estimate of a complete rational trigonometric sum*, Trudy Mat. Inst. Steklov. 143 (1977), 188–220 (in Russian); English transl.: Proc. Steklov Inst. Math. 1 (1980), 201–220.
[21] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 203–210.

Department of Mathematics
Kansas State University
Manhattan, KS 66506, U.S.A.
E-mail: cochrane@math.ksu.edu

Department of Mathematics
Zhongshan University
Guangzhou, P.R. China
E-mail: addsr03@zsu.edu.cn

Received on 4.1.1999
and in revised form on 20.5.1999 (3539)