ACTA ARITHMETICA
XCV.1 (2000)

Exponential sums with rational function entries

by

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

1. Introduction. In this paper we extend the results of [6] to pure and mixed exponential sums of the type

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

with rational function entries. Here p^m is a prime power with $m\ge 2$, χ is a multiplicative character $(\bmod p^m)$, $e_{p^m}(\cdot)$ is the additive character,

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

and $f=f_1/f_2$ is a rational function with $f_1,f_2\in\mathbb{Z}[X]$, and $(f_1,f_2)=1$ in $\mathbb{Z}[X]$. It is understood that in the two sums x is to take on only values with $p\nmid f_2(x)$, $p\nmid xf_2(x)$ respectively, and that $f(x)$ means $f_1(x)\overline{f_2(x)}$, where $\overline{f_2(x)}$ denotes the multiplicative inverse of $f_2(x)$ $(\bmod p^m)$. Let $d(f)$ and $d^*(f)$ denote the *total* and *maximal* degrees of f,

$$d(f):=d(f_1)+d(f_2), \qquad d^*(f):=\max\{d(f_1),d(f_2)\}.$$

Let $\widetilde{f}$ denote the image of f in $\mathbb{F}_p(X)$, $\widetilde{f}=\widetilde{f}_1/\widetilde{f}_2$, and let

$$d_p(f)=d(\widetilde{f}), \qquad d_p^*(f)=d^*(\widetilde{f}),$$

the *total* and *maximal* degrees of $\widetilde{f}$ (written in reduced form).

It was established by Bombieri [2], Theorem 5, that for the case $m=1$ we have for any f with $d_p(f)\ge 1$,

$$|S(f,p)|\le (n-2+\deg(\widetilde{f})_\infty)p^{1/2}+1, \tag{1.2}$$

2000 *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 Spring 1998 as a visiting scholar.

where n is the number of poles and $(\widetilde{f})_\infty$ is the divisor of the poles of $\widetilde{f}$ over the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$: $(\widetilde{f})_\infty = \sum_{i=1}^{n} d_i P_i$. Here the P_i are the poles (including ∞ if necessary) and the d_i are their respective multiplicities. The plus 1 on the right-hand side of (1.2) may be omitted if $\widetilde{f}$ has a pole at ∞. Perelmuter [23] extended Bombieri's result to mixed exponential sums and obtained for any multiplicative character χ and any rational function f over $\mathbb{Z}$ with $d_p(f) \geq 1$,

$$|S(\chi, f, p)| \leq (n - 1 + \deg(\widetilde{f})_\infty) p^{1/2}. \tag{1.3}$$

In particular, from (1.2) and (1.3) one obtains the uniform upper bounds

$$|S(f,p)| \leq \begin{cases} (d_p(f)-1)p^{1/2} & \text{if } d_p(f_1) > d_p(f_2), \\ 2(d_p(f_2)-1)p^{1/2}+1 & \text{if } d_p(f_1) \leq d_p(f_2), \end{cases} \tag{1.4}$$

$$|S(\chi,f,p)| \leq \begin{cases} d_p(f)p^{1/2} & \text{if } d_p(f_1) > d_p(f_2), \\ (2d_p(f_2)-1)p^{1/2} & \text{if } d_p(f_1) \leq d_p(f_2). \end{cases} \tag{1.5}$$

For values of $m \geq 2$ little has been said about these sums for rational functions in general, although the case of polynomials has been studied extensively and is discussed at length in our work [6]; see Chalk [4], Chen [5], Ding [8], [9], Hua [12]–[14], Konyagin and Shparlinski [17], Loh [18], [19], Loxton and Smith [20], Loxton and Vaughan [21], Nechaev [22], Smith [26] and Stechkin [27]. The first sums with rational function entries to be studied were the Kloosterman sums with $f(X) = AX + BX^{-1}$. Shparlinski [25] treated the more general case of sparse Laurent polynomials. The basic uniform upper bound for polynomials is the Hua upper bound,

$$|S(f, p^m)| \leq C p^{m(1-1/d)}, \tag{1.6}$$

for any polynomial f of degree d with $d_p(f) \geq 1$. The exponent $m(1-1/d)$ is best possible for a uniform upper bound. The constant C in the original work of Hua depended on d but it has been refined many times over the years. Currently the best value is the absolute constant $C = 4.41$, proven in our recent work [7]. For mixed exponential sums, and polynomial entries, the analogue of (1.6) established in [6] is

$$|S(\chi, f, p^m)| \leq 4dp^{m(1-1/(d+1))}. \tag{1.7}$$

The question arises what parameter plays the role of d in (1.6) and (1.7) when f is a rational function, the total degree, the maximal degree, or some other value. In this paper we show that the maximal degree suffices for pure exponential sums, but for mixed exponential sums one needs a value closer to the total degree.

To state our results, let $\mathrm{ord}_p(x)$ denote the normal exponent valuation on the p-adic field. In particular, for $x \neq 0 \in \mathbb{Z}$, $p^{\mathrm{ord}_p(x)} \,\|\, x$. Put $\mathrm{ord}_p(0) = \infty$.

For any nonzero polynomial $f = f(X) = a_0 + a_1X + \ldots + a_dX^d \in \mathbb{Z}[X]$ let

$$\operatorname{ord}_p(f) := \min_{0\le i\le d}\{\operatorname{ord}_p(a_i)\}, \tag{1.8}$$

and extend the valuation to rational functions over $\mathbb{Z}$ by setting $\operatorname{ord}_p(f_1/f_2) = \operatorname{ord}_p(f_1) - \operatorname{ord}_p(f_2)$.

Pure exponential sums. We start by considering the case of pure exponential sums. Let f be a nonconstant rational function over $\mathbb{Z}$. Set $t = \operatorname{ord}_p(f')$ and let $\mathcal{A} \subset \mathbb{F}_p$ be the set of solutions of the congruence

$$p^{-t}f'(x) \equiv 0 \pmod p. \tag{1.9}$$

We denote by $\mathcal{A}$ the set of critical points associated with the sum $S(f, p^m)$, and for any point $\alpha \in \mathcal{A}$ we let ν_α denote the multiplicity of α as a zero of (1.9). If $\alpha \notin \mathcal{A}$ put $\nu_\alpha = 0$. For any integer α with $p\nmid f_2(\alpha)$, let

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

In Theorem 3.1 we obtain the upper bounds

$$|S_\alpha(f, p^m)| \le \nu_\alpha p^{t/(\nu_\alpha+1)}p^{m(1-1/(\nu_\alpha+1))}, \tag{1.10}$$

$$|S(f, p^m)| \le \Big(\sum_{\alpha\in\mathcal{A}} \nu_\alpha\Big)p^{t/(M+1)}p^{m(1-1/(M+1))}, \tag{1.11}$$

for any nonconstant rational function f over $\mathbb{Z}$, any odd prime p and any exponent m with $m \ge t+2$, where $M = \max_{\alpha\in\mathcal{A}}\{\nu_\alpha\}$. In particular, $S_\alpha = 0$ if $\alpha \notin \mathcal{A}$. For $p = 2$ we obtain the same bounds if $m \ge t + 3$ or $m = 2$ and $t = 0$.

The value M can be as large as $d - 1$, where d is the total degree of f, as evidenced by a function such as $f(X) = X^p/(1 + X^k)$, which has an associated critical point at 0 of multiplicity $p + k - 1$. Thus, one can only deduce from (1.11) a uniform upper bound with exponent $m(1-1/d)$, where d is the total degree of f. In Corollary 3.1 we establish the much stronger upper bound

$$|S(f, p^m)| \le dp^{m(1-1/d^*)}, \tag{1.12}$$

where d^* is the maximal degree of f. This upper bound is valid for any rational function f over $\mathbb{Z}$, any odd prime p with $d_p(f) \ge 1$, and any value of $m \ge 2$. When $p = 2$ we obtain the same upper bound with an extra factor of $\sqrt{2}$ on the right-hand side.

The upper bound in (1.12) is obtained by establishing a new type of local upper bound on exponential sums. For any integer α let

$$\sigma_\alpha := \operatorname{ord}_p(f(pY + \alpha) - f(\alpha)).$$

In Theorem 3.2 we show that if $m \geq t+2$ and $d_p(f) \geq 1$ then

$$|S_\alpha(f, p^m)| \leq \nu_\alpha p^{m(1-1/\sigma_\alpha)}. \tag{1.13}$$

Now $\sigma_\alpha \leq \nu_\alpha + t + 1$, as shown in Lemma 2.2(ii), and thus for $t = 0$ the upper bound in (1.13) is always sharper than (1.10). For $t > 0$, (1.10) is sometimes better. The parameter σ_α has appeared in many papers on exponential sums but we are not aware of an upper bound of the type (1.13) ever appearing before, even for the case of polynomials.

Mixed exponential sums. We now turn our attention to the case of mixed exponential sums. Suppose that p is an odd prime. Let a denote a fixed primitive root $(\mathrm{mod}\, p)$ chosen so that $a > 0$ and

$$a^{p-1} = 1 + rp \quad \text{with} \quad p \nmid r. \tag{1.14}$$

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

$$\chi(a^k) = e\left(\frac{ck}{p^{m-1}(p-1)}\right), \tag{1.15}$$

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 rational function f over $\mathbb{Z}$ we define

$$t_1 = t_1(f) := \mathrm{ord}_p(rXf'(X) + c). \tag{1.16}$$

If $p > d_p^*(f) \geq 1$ then $t = t_1 = 0$. In Lemma 4.1 it is shown that $t_1 = \min\{t, \mathrm{ord}_p(c)\} \leq m-1$. The set of *critical points* $\mathcal{A} \subset \mathbb{F}_p$ associated with the sum $S(\chi, f, p^m)$ is defined to be the set of nonzero residues $(\mathrm{mod}\, p)$ satisfying the congruence

$$p^{-t_1}(rxf'(x) + c) \equiv 0 \pmod{p}. \tag{1.17}$$

It is easy to check that this congruence does not depend on the choice of the primitive root a. For any $\alpha \in \mathcal{A}$ we again let ν_α denote the multiplicity of α as a zero of the congruence (1.17) and for $\alpha \notin \mathcal{A}$, let $\nu_\alpha = 0$. Let

$$S_\alpha = S_\alpha(\chi, f, p^m) := \sum_{\substack{x=1 \\ x \equiv \alpha \,(\mathrm{mod}\, p)}}^{p^m} \chi(x) e_{p^m}(f(x)). \tag{1.18}$$

In Theorem 4.1 we establish the upper bounds

$$|S_\alpha(\chi, f, p^m)| \leq \nu_\alpha p^{t/(\nu_\alpha+1)} p^{m(1-1/(\nu_\alpha+1))}, \tag{1.19}$$

$$|S(\chi, f, p^m)| \leq \Big(\sum_{\alpha \in \mathcal{A}} \nu_\alpha\Big) p^{t/(M+1)} p^{m(1-1/(M+1))}, \tag{1.20}$$

for any rational function f and any value $m \geq t+2$. Here $M = \max_{\alpha \in \mathcal{A}}\{\nu_\alpha\}$. If $\nu_\alpha = 1$ then we obtain an explicit formula for S_α and show that we have equality in (1.19). Similar estimates are obtained when $p = 2$ in Theorem 4.2.

Now, since

$$rXf'(X) + c = (rX[f_2f_1' - f_1f_2'] + cf_2^2)/f_2^2,$$

it is apparent that the value M can be no larger than

$$D = D(f, \chi) := \max\{d(f_1) + d(f_2), 2d(f_2)\}.$$

Thus we are able to deduce in Corollary 4.1 the upper bound

$$|S(\chi, f, p^m)| \leq 4Dp^{m(1-1/(D+1))}, \tag{1.21}$$

for any rational function f over $\mathbb{Z}$, any prime p with $d_p(f) \geq 1$, any $m \geq 2$ and any multiplicative character $\chi \pmod{p^m}$. If χ is a primitive character and $p \leq D$ then a sharper exponent is available using the inequality $M < p$, which is proven in a remark at the end of Section 4.

One would hope to be able to obtain a sharper upper bound, say of the type (1.12), for mixed exponential sums, but no such sharpening is available. In Example 6.1 we show that for any positive integer d_1, there is a rational function $f = f_1/f_2$ with $d(f_1) = d(f_2) = d_1$ such that for infinitely many pairs χ, m we have $|S(\chi, f, p^m)| = p^{m(1-1/(D+1))}$. In a similar manner one can show that for the rational function $f(X) = 1/(X-b)$ with $p \nmid b$, and any value of $m \geq 2$, there exist multiplicative characters $\chi \pmod{p^m}$ with

$$|S(\chi, f, p^m)| = p^{m(1-1/3)} = p^{m(1-1/(D+1))}.$$

There is still room for improvement in (1.21) when $d_1 \neq d_2$. The basic question that must be answered is: for given values of d_1, d_2, what is the maximum possible value of M?

Kloosterman and Salié sums. In Section 5 we apply our results to the particular case of Kloosterman and Salié type sums, where $f(X) = AX + BX^{-1}$, $p \nmid AB$. We obtain for p odd and $m \geq 2$,

$$\Big|\sum_{x=1}^{p^m} \chi(x) e_{p^m}(Ax + Bx^{-1})\Big| \tag{1.22}$$
$$\leq \begin{cases} 2p^{m/2} & \text{if } \chi_2(4ABr^2 + c^2) = 1, \\ 0 & \text{if } \chi_2(4ABr^2 + c^2) = -1, \\ 0 & \text{if } p \,\|\, (4ABR^2 + c^2),\ m \geq 3, \\ 2p^{2m/3} & \text{if } p^2 \mid (4ABR^2 + c^2), \end{cases}$$

where r is as in (1.14), and R is the p-adic integer $R := p^{-1}\log(1 + rp) \equiv r \pmod{p}$. In the first case the sum can be explicitly evaluated (see (5.2), (5.3), (5.7)). Similar bounds are given when $p = 2$ (see (5.8)). For the Kloosterman and Salié sums one takes χ to be the principal character and Jacobi symbol

respectively. In these cases the upper bound $2p^{m/2}$ is well known, and has found many applications, such as in the study of automorphic forms (see Iwaniec [15]) and in the work of Duke, Friedlander and Iwaniec [10] on bilinear forms with Kloosterman fractions. In Example 5.1 we show that the exponent $2m/3$ in the last case of (1.22) is best possible by exhibiting an infinite class of such sums for which $|S(\chi, f, p^m)| = p^{2m/3}$.

2. Preliminary lemmas. Let p be a prime, $\mathbb{Z}_p$, $\mathbb{Q}_p$ denote the p-adic integers and p-adic rationals respectively and let Ω_p be a complete algebraically closed field containing $\mathbb{Q}_p$ (see for example Koblitz [16]). Let $f = f_1/f_2$ be a rational function over $\mathbb{Z}$ with $(f_1, f_2) = 1$ in $\mathbb{Z}[X]$, and $\mathrm{ord}_p(f_2) = 0$. Thus $\mathrm{ord}_p(f) = \mathrm{ord}_p(f_1)$. In this section we shall view f in two ways, first as an analytic function $f = f(x)$ defined on Ω_p, and second as a formal rational function $f = f(X)$ in the indeterminate X.

Let α be a fixed integer with $p \nmid f_2(\alpha)$. Then, over $\mathbb{Q}_p$, f admits a Taylor series expansion about α,

$$f(x) = \sum_{i=0}^{\infty} a_i (x-\alpha)^i, \tag{2.1}$$

with p-adic integer coefficients a_i, $i \geq 0$, given by $a_i = f^{(i)}(\alpha)/i!$, and with the series converging pointwise to $f(x)$ at any value of x with $\mathrm{ord}_p(x-\alpha) > 0$. We also find that for any x with $\mathrm{ord}_p(x-\alpha) > 0$,

$$f'(x) = \sum_{i=0}^{\infty} i a_i (x-\alpha)^{i-1}. \tag{2.2}$$

Define $t = \mathrm{ord}_p(f')$, as before. The integer α is called a zero of $f \pmod p$ of multiplicity ν if, letting $\widetilde{f_1}$ be the image of f_1 in $\mathbb{F}_p[X]$, we can write $\widetilde{f_1}(X) = (X - \widetilde{\alpha})^{\nu} \widetilde{g}(X)$ for some polynomial $\widetilde{g}(X) \in \mathbb{F}_p[X]$ with $\widetilde{g}(\widetilde{\alpha}) \neq 0$. (Note that in this definition we have assumed $p \nmid f_2(\alpha)$, so that $X - \widetilde{\alpha}$ is not a factor of $\widetilde{f_2}(X)$.)

LEMMA 2.1. *For any rational function f over $\mathbb{Z}$ as given above and any integer α with $p \nmid f_2(\alpha)$ we have*:

(i) *The coefficients $\{a_i\}_{i=1}^{\infty}$ in (2.1) satisfy*

$$\mathrm{ord}_p(f) = \min_{i \geq 0} \{\mathrm{ord}_p(a_i)\}.$$

(ii) *If α is a zero of $f \pmod p$ of multiplicity ν then $p \mid a_i$, $1 \leq i < \nu$, $p \nmid a_\nu$ and $p^t \mid \nu$.*

(iii) *If $d_p^*(f) \geq 1$ then*

$$p^t \leq d_p^*(f) := \max\{d_p(f_1), d_p(f_2)\}. \tag{2.3}$$

If, in addition, f is a polynomial, then $p^t \mid d_p(f)$.

P r o o f. Suppose first that $f = f(X)$ is a polynomial. Then viewing p as a prime in the unique factorization domain $\mathbb{Z}[X]$ we see that the condition $p^k \parallel f(X)$ is equivalent to saying $k = \mathrm{ord}_p(f)$. Now $p^k \parallel f(X)$ if and only if $p^k \parallel f(X+\alpha)$, and thus since the latter polynomial is just $\sum_{i=1}^{d} a_i X^i$ we obtain the result of part (i).

Suppose now that $f = f_1/f_2$ is a rational function over $\mathbb{Z}$. Let $f_1,\ f_2$ have Taylor expansions about α given by

$$f_1(x) = \sum_{i=0}^{d_1} b_i (x-\alpha)^i, \qquad f_2(x) = \sum_{i=0}^{d_2} c_i (x-\alpha)^i.$$

We work now in the ring of formal power series $\mathbb{Z}_p[[T]]$, and define

$$F(T) = \sum_{i=0}^{\infty} a_i T^i, \qquad F_1(T) = \sum_{i=0}^{d_1} b_i T^i, \qquad F_2(T) = \sum_{i=0}^{d_2} c_i T^i.$$

Then $F_1(T) = F(T)F_2(T)$. Since $p \nmid f_2(\alpha)$ we have $p \nmid F_2(T)$ in $\mathbb{Z}_p[[T]]$, and thus $p^k \parallel F_1(T)$ if and only if $p^k \parallel F(T)$ or in other words,

$$\min_{0 \le i \le d_1} \{\mathrm{ord}_p(b_i)\} = \min_{i \ge 0} \{\mathrm{ord}_p(a_i)\}.$$

But we have already established (in the case of polynomials) that the left-hand side is just $\mathrm{ord}_p(f_1) = \mathrm{ord}_p(f)$. This completes the proof of part (i).

Now let $\widetilde{F}(T)$, $\widetilde{F}_1(T)$, $\widetilde{F}_2(T)$ be the images of F, F_1, F_2 in $\mathbb{F}_p[[T]]$. Then, if α is a zero of $f(x) \pmod p$ of multiplicity ν it follows that

$$\widetilde{F}(T) = \sum_{i=0}^{\infty} \widetilde{a}_i T^i, \qquad \widetilde{F}_1(T) = \sum_{i=\nu}^{d_1} \widetilde{b}_i T^i, \qquad \widetilde{F}_2(T) = \sum_{i=0}^{d_2} \widetilde{c}_i T^i.$$

Therefore, from the relationship $\widetilde{F}_1(T) = \widetilde{F}(T)\widetilde{F}_2(T)$ and the fact that $\widetilde{c}_0 \ne 0$ we obtain the first part of (ii). Applying part (i) of the lemma to the function $f'(x)$ we have $t = \min_{i \ge 1}\{\mathrm{ord}_p(i a_i)\}$. In particular, $p^t \mid \nu a_\nu$. Since $p \nmid a_\nu$ it follows that $p^t \mid \nu$.

Suppose now that $d_p(f) \ge 1$. The inequality $p^t \le d_p^*(f)$ in part (iii) is now immediate if f has at least one zero $(\mathrm{mod}\, p)$ of multiplicity $\nu \ge 1$, for then by part (ii), $p^t \le \nu \le d_p(f_1) \le d_p^*(f)$. If f has no zero $(\mathrm{mod}\, p)$ then we let α be any integer where f is defined and replace f with the function $f(X) - f(\alpha)$ to obtain a new rational function vanishing at α and satisfying $t(f(X) - f(\alpha)) = t(f)$. Now since

$$f(X) - f(\alpha) = (f_1(X) - f(\alpha) f_2(X))/f_2(X),$$

we also have $d_p^*(f(X) - f(\alpha)) = d_p^*(f)$, and the result of part (iii) follows. Finally, if f is a polynomial of degree d_p then we also have $p^t \mid d_p a_{d_p}$ with $p \nmid a_{d_p}$, and so $p^t \mid d_p$. ∎

Suppose now that α is a zero of the critical point congruence

$$p^{-t}f'(x) \equiv 0 \pmod{p} \tag{2.4}$$

of multiplicity $\nu \geq 1$. Then it follows from Lemma 2.1(ii) that

$$\operatorname{ord}_p(ia_i) \begin{cases} \geq t+1 & \text{if } 1 \leq i \leq \nu, \\ = t & \text{if } i = \nu+1, \\ \geq t & \text{if } i > \nu+1, \end{cases} \tag{2.5}$$

and consequently for $i \geq 1$,

$$\operatorname{ord}_p(a_i p^i) = \operatorname{ord}_p(ia_i) + i - \operatorname{ord}_p(i) \geq \begin{cases} t+2 & \text{if } p \text{ is odd or } \nu > 1, \\ t+1 & \text{if } p = 2,\ \nu = 1. \end{cases} \tag{2.6}$$

Let σ, $g(Y)$ be defined by

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

and τ, $g_1(Y)$ be defined by

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

Now, by the Taylor expansion for f in (2.1) we have

$$g(Y) = \sum_{i=1}^{\infty} a_i p^{i-\sigma} Y^i \quad \text{and} \quad g_1(Y) = \sum_{i=1}^{\infty} a_i i p^{i-\sigma-\tau} Y^{i-1}.$$

Thus, read $(\operatorname{mod} p)$, both $g(Y)$ and $g_1(Y)$ are polynomials in Y of respective degrees $d_p(g)$, $d_p(g_1)$, and we obtain the same relations as in Lemma 3.1 of [6], which was stated for the case of polynomials.

Lemma 2.2. *For any prime p and zero α of* (2.4) *of multiplicity ν we have*:

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

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

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

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

(v) $$p^{\tau} \leq d_p(g).$$

(vi) *If $d_p(f) \geq 1$ then $\sigma \leq d_p^*(f)$.*

Proof. From (2.1) we obtain

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

and thus by Lemma 2.1(i), $\sigma = \min_{i\ge 1}\{\mathrm{ord}_p(a_i p^i)\}$. The result of part (i) follows from (2.6). Now for the term $i = d_p(g)$ we must have

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

It follows from (2.5) that

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

from which the first inequalities in (iii) follow. The second inequalities in (iii) follow immediately from (ii).

Now since the coefficients of $g_1(Y)$ are p-adic integers, we see upon examining the $i = \nu + 1$ coefficient that

$$\mathrm{ord}_p(a_{\nu+1}(\nu+1)p^{\nu+1-\sigma-\tau}) \ge 0.$$

Thus by (2.5) we obtain (ii). Similarly, upon examining the $i = d_p(g_1) + 1$ coefficient and using (2.5) we obtain (iv). The second inequality in (iv) follows immediately from (ii). Part (v) follows from Lemma 2.1(iii) applied to g.

To prove (vi) we note that the rational function

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

has a zero $(\mathrm{mod}\, p)$ at α of multiplicity say ω with $1 \le \omega \le d_p^*(f)$. Thus $p \nmid a_\omega$ and $\sigma \le \mathrm{ord}_p(a_\omega p^\omega) = \omega \le d_p^*(f)$. ∎

Lemma 2.3. *Let p be a prime, $f = f_1/f_2$ be a rational function over $\mathbb{Z}$ with $(f_1, f_2) = 1$ and $t = \mathrm{ord}_p(f')$ and let t_1 be an integer with $0 \le t_1 \le t$. Suppose that 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 with $p \nmid f_2(y)$ we have (in $\mathbb{Z}_p$)*

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

Proof. Since $p \nmid f_2(y)$, f admits a p-adic Taylor expansion about y of the type $f(y+x) = \sum_{i=0}^{\infty} a_i x^i$ with p-adic integer coefficients a_i, and with the series converging to the function at any value of x with $\mathrm{ord}_p(x) > 0$. Thus if $m \ge t_1 + 2$ then for any integer z,

$$f(y + p^{m-t_1-1}z) = \sum_{i=0}^{\infty} a_i (p^{m-t_1-1}z)^i. \tag{2.7}$$

Now by (2.6), $\mathrm{ord}_p(ia_i) \ge t$ for $i \ge 1$. Thus for any $i \ge 1$,

$$\begin{aligned} \mathrm{ord}_p(a_i p^{(m-t_1-1)i}) &\ge i(m-t_1-1) + t - \mathrm{ord}_p(i) \\ &\ge i(m-t_1-1) + t_1 - \mathrm{ord}_p(i), \end{aligned} \tag{2.8}$$

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

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

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 (2.8) and replace the right side with $i(m - t_1 - 1) = i$ to obtain the result. ∎

In the application of Lemma 2.3 to exponential sums it is convenient for us to extend the domain of the additive character $e_{p^m}(\cdot)$ to $\mathbb{Z}_p$ by setting, for any $x \in \mathbb{Z}_p$,

$$e_{p^m}(x) := e_{p^m}(\widetilde{x}), \tag{2.9}$$

where $\widetilde{x}$ is the residue class of x in $\mathbb{Z}_p/(p^m) \simeq \mathbb{Z}/(p^m)$. With this understanding, for any rational function $f = f_1/f_2$ over $\mathbb{Z}$ and any integer x with $p \nmid f_2(x)$ we have $f(x) \in \mathbb{Z}_p$, and

$$e_{p^m}(f(x)) = e_{p^m}(f_1(x)\overline{f_2(x)}), \tag{2.10}$$

where $\overline{f_2(x)}$ denotes the multiplicative inverse of $f_2(x) \pmod{p^m}$.

3. Pure exponential sums. Let $f = f_1/f_2$ be a rational function over $\mathbb{Z}$ with $(f_1, f_2) = 1$, and $\mathcal{A}$ be the set of critical points associated with the exponential sum $S(f, p^m)$ as defined in the introduction (see (1.9)). For any integer α with $p \nmid f_2(\alpha)$ let

$$S_\alpha = S_\alpha(f, p^m) = \sum_{\substack{x=1 \\ x \equiv \alpha \pmod{p}}} e_{p^m}(f(x)). \tag{3.1}$$

THEOREM 3.1. *Let p be a prime, f be a nonconstant rational function defined over $\mathbb{Z}$, and α be any integer with $p \nmid f_2(\alpha)$. Set $t = \mathrm{ord}_p(f')$.*

(a) *If p is odd and $m \geq t + 2$ then*

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

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

$$|S_\alpha(f, p^m)| \leq \nu p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}, \tag{3.2}$$

with equality if $\nu = 1$.

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

(b) *Let $p = 2$ and suppose that either $m \geq t+3$, or $m = 2$ and $t = 0$. If $\alpha \notin \mathcal{A}$ then $S_\alpha = 0$, and if $\alpha \in \mathcal{A}$ then*

$$|S_\alpha(f, 2^m)| \leq \nu 2^{t/(\nu+1)} 2^{m(1-1/(\nu+1))}, \tag{3.3}$$

with equality if $\nu = 1$.

Proof. The proof is identical to the proof of Theorem 2.1 in [6]. One starts by showing that under the hypotheses of Lemma 2.3 with $t_1 = t$, we have

$$S_\alpha = p^{t+1} \sum_{\substack{y \equiv \alpha \,(\mathrm{mod}\, p) \\ p^{t+1} | f'(y)}} e_{p^m}(f(y)), \tag{3.4}$$

and thus $S_\alpha = 0$ unless $\alpha \in \mathcal{A}$, proving part (a)(i) and the first part of (b). Suppose now that $\alpha \in \mathcal{A}$. Then defining

$$\begin{aligned} \sigma = \sigma_\alpha &:= \mathrm{ord}_p(f(pY + \alpha) - f(\alpha)), \\ g_\alpha(Y) &:= p^{-\sigma}(f(pY + \alpha) - f(\alpha)), \end{aligned} \tag{3.5}$$

one obtains the following recursion relationship: If p is odd and $m \geq t+2$, or $p = 2$ and $m \geq t+3$ then

$$S_\alpha(f, p^m) = e_{p^m}(f(\alpha)) p^{\sigma-1} S(g_\alpha, p^{m-\sigma}), \tag{3.6}$$

where the latter sum $S(g_\alpha, p^{m-\sigma})$ is taken to be $p^{m-\sigma}$, in case $m < \sigma$. The inequalities in (3.2) and (3.3) can then be proven by induction on m. The proof is identical to that in [6] since the relations given in Lemma 2.2 of the present paper are identical to those of Lemma 3.1 of [6]. We note that when $m - \sigma = 1$ (leaving the sum $S(g_\alpha, p)$), we need only appeal to the upper bound of Weil [28] for the case of polynomials, since g_α is a polynomial when read $(\mathrm{mod}\, p)$. The identity in part (a)(iii) and the equality in (3.2) and (3.3), when $\nu = 1$, are also proven identically as in Section 5 of [6]. ∎

A particular consequence of this theorem is that if there are no critical points associated with the sum $S(f, p^m)$ then the sum is zero. As an example we state

Corollary 3.1. *Let $f(X) = (aX + b)/(cX + d)$ be a rational function over $\mathbb{Z}$ with $d^* = 1$, that is, $ad - bc \neq 0$. Let p be any prime with $p \nmid (ad - bc)$. Then if $m \geq 2$ or $m = 1$ and $p \mid c$ then $S(f, p^m) = 0$. If $m = 1$ and $p \nmid c$ then $S(f, p) = -e_p(a\bar{c})$.*

Proof. If p is a prime with $p \nmid (ad - bc)$ then $t = t(f) = 0$ and there are no critical points associated with the sum $S(f, p^m)$. Thus if $m \geq 2$ it follows from parts (i) and (iv) of Theorem 3.1 that $S(f, p^m) = 0$. The case $m = 1$ can be dealt with in an elementary manner. ∎

Next we give a variant of the inequality in (3.2) in terms of the parameter σ.

THEOREM 3.2. *Let p be a prime, f be a nonconstant rational function defined over $\mathbb{Z}$, and $t = \mathrm{ord}_p(f')$. Suppose that α is critical point of multiplicity ν with σ as defined in* (3.5).

(a) *If p is odd and $m \geq t+2$ then*

$$|S_\alpha(f, p^m)| \leq \nu p^{m(1-1/\sigma)}. \tag{3.7}$$

(b) *If $p = 2$ and $m \geq t+3$ then*

$$|S_\alpha(f, 2^m)| \leq \sqrt{2}\nu 2^{m(1-1/\sigma)}. \tag{3.8}$$

COROLLARY 3.2. *Let p be a prime and f be a rational function over $\mathbb{Z}$ of total degree d and maximal degree d^* with $d_p(f) \geq 1$. If p is odd then for any $m \geq 2$ we have*

$$|S(f, p^m)| \leq dp^{m(1-1/d^*)}. \tag{3.9}$$

If $p = 2$ then we obtain the same inequality with an extra factor of $\sqrt{2}$ on the right-hand side.

Proof. From the inequality $\sigma_\alpha \leq d_p^*(f)$ of Lemma 2.2(vi) we obtain, under the hypotheses of Theorem 3.2,

$$|S(f, p^m)| \leq \Big(\sum_{\alpha \in \mathcal{A}} \nu_\alpha\Big) p^{m(1-1/d_p^*(f))} \leq d_p(f_1) p^{m(1-1/d_p^*(f))}, \tag{3.10}$$

with an extra factor of $\sqrt{2}$ on the right-hand side in case $p = 2$. Here, $f_1 = p^{-t} f'$. Since $d_p(f_1) \leq d-1$ and $d_p^*(f) \leq d^*(f)$ we deduce the upper bound in (3.9).

Suppose now that p is odd and $m \leq t+1$. By (2.3) we have $p^t \leq d^*$. In particular, since $m \geq 2$ we have $d^* \geq p \geq 3$. Thus we obtain the trivial upper bound

$$|S(f, p^m)| \leq p^m \leq p^t p \leq dp \leq dp^{m(1-1/d^*)}.$$

Suppose next that $p = 2$ and $m \leq t+2$. If $d^* = 1$ then the inequality in (3.9) follows from Corollary 3.1. If $d^* \geq 2$ then since $2^t \leq d^*$ we have

$$2^m \leq 4d^* \leq (\sqrt{2}d^*)^{d^*} \leq (\sqrt{2}d)^{d^*},$$

and so $2^{m/d^*} \leq \sqrt{2}d$. It follows that

$$|S(f, 2^m)| \leq 2^m \leq \sqrt{2}d 2^{m(1-1/d^*)}. \ \blacksquare$$

Proof of Theorem 3.2. The proof is by induction on m. Suppose first that p is odd. We shall prove the inequality in (3.7) together with the inequality in (3.10), which is always an immediate consequence of (3.7). If $m = 2$, then since $\sigma \geq 2$ we have trivially that $|S_\alpha| \leq p \leq \nu p^{m(1-1/\sigma)}$, establishing (3.7).

Suppose now that m is an arbitrary positive integer with $m \geq t+2$ and that the theorem has been proven for all smaller values of m. Let f be a rational function over $\mathbb{Z}$, and let α be an associated critical point of multiplicity ν. We first dispense with the case $\nu = 1$. In this case, by Theorem 3.1(iii), we have $|S_\alpha| = p^{(m+t)/2}$. Now, using the assumption $m \geq t+2$ and then the inequality $\sigma \geq t+2$ of Lemma 2.2(i), we have

$$t \leq m\left(1 - \frac{2}{t+2}\right) \leq m\left(1 - \frac{2}{\sigma}\right),$$

whence it follows that

$$(m+t)/2 \leq m(1 - 1/\sigma),$$

which establishes (3.7). Henceforth we shall assume that $\nu \geq 2$. We consider four cases.

Case (i). If $\sigma \geq m$ then we have trivially,

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

Case (ii). Suppose next that $\sigma = m-1$. The trivial estimate $|S_\alpha| \leq p^{m-1} \leq \nu p^{m(1-1/\sigma)}$ holds provided that $p \leq \nu^\sigma$. Suppose now that $p > \nu^\sigma$. Let $d_p = d_p(g_\alpha)$ where g_α is as defined in (3.5). If $p = d_p$, then by Lemma 2.2(iii), $p \leq \nu+2$, and thus $\nu^\sigma < \nu+2$, contradicting our assumption that $\nu \geq 2$. If $d_p \geq 2p$ then since $\mathrm{ord}_p(d_p) \leq d_p/2$ we have

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

which again leads to a contradiction. Thus we must have $\mathrm{ord}_p(d_p) = 0$ and so by Lemma 2.2(iii), $d_p - 1 \leq \nu$. Then by the recursion relationship (3.6) and upper bound of Weil, we have

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

Case (iii). Define τ and g_1 as in Section 2,

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

Suppose that $m - 1 - \tau \leq \sigma \leq m-2$. In particular, $\tau \geq 1$. Then we have the trivial upper bound

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

if and only if $p^{m-\sigma} \leq \nu^\sigma$. Now $m - \sigma \leq \tau + 1$, and so the trivial bound holds if $p^{\tau+1} \leq \nu^\sigma$. By Lemma 2.2(v) and (iii), $p^\tau \leq d_p(g) \leq \sigma$ and so $p^{\tau+1} \leq p^{2\tau} \leq \sigma^2$. Thus it suffices to have $\sigma^2 \leq \nu^\sigma$ which is always the case unless $\sigma = 3$ and $\nu = 2$.

Suppose now that $\sigma = 3$, $\nu = 2$. Then since $p^\tau \leq \sigma$ we must have $p = 3$, $\tau = 1$ and $m = 5$. Suppose that f has Taylor expansion $f(x) = \sum_{i=0}^{\infty} a_i (x-\alpha)^i$ about α, with p-adic integer coefficients a_i. By Lemma 2.2(i) we obtain $t \leq \sigma - 2 = 1$. Since $\nu = 2$ it follows from (2.5) that $t =$

$\mathrm{ord}_p(3a_3) = 1 + \mathrm{ord}_p(a_3)$. Thus we must have $t = 1$ and $\mathrm{ord}_p(a_3) = 0$. From the recursion relationship (3.6) we have

$$|S_\alpha| = p^2 |S(g_\alpha, p^2)|,$$

where

$$g_\alpha(Y) = p^{-3} \sum_{i=1}^{\infty} a_i (pY)^i.$$

Since $\tau = 1$ it follows that $p^3 \mid a_1$ and $p^2 \mid a_2$, and thus we can write

$$g_\alpha(Y) = a_3 Y^3 + p(a_4 Y^4 + b_2 Y^2 + b_1 Y) + p^2(\text{stuff}),$$

for some p-adic integers b_1, b_2. It is clear that the value of $g_\alpha(y) \pmod 9$ depends only on the residue class of $y \pmod 3$, and so

$$|S(g_\alpha, p^2)| = 3 \sum_{y=-1}^{1} e_9(g_\alpha(y)).$$

Now since $g_\alpha(0) = 0$ and $3 \nmid a_3$, the latter sum is bounded above by

$$|1 + e_9(1) + e_9(-1)| = 2.532\ldots < 2.884\ldots = 2 \cdot 3^{1/3}.$$

Altogether, we obtain

$$|S_\alpha| = 3^2 |S(g_\alpha, 3^2)| \le 3^3 \cdot 2 \cdot 3^{1/3} = \nu 3^{5(1-1/\sigma)}.$$

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 the recursion relationship (3.6) and (3.10) that

$$|S(f, p^m)| \le p^{\sigma-1} d_p(g_1) p^{(m-\sigma)(1-1/d_p(g_\alpha))}.$$

Now by Lemma 2.2(iv), $d_p(g_1) \le \nu$ and by Lemma 2.2(iii), $d_p(g_\alpha) \le \sigma$. Thus

$$|S(f, p^m)| \le p^{\sigma-1} \nu p^{(m-\sigma)(1-1/\sigma)} = \nu p^{m(1-1/\sigma)}.$$

Next we consider the prime $p = 2$. Again, first consider the case $\nu = 1$. Suppose that α is a critical point of multiplicity one. Since f' cannot have a zero of multiplicity one $(\mathrm{mod}\, 2)$, we must have $t \ge 1$. Now by Lemma 2.2(i), $\sigma \ge t + 1$. Using in turn the inequality $t \ge 1$ and then the inequalities $\sigma \ge t + 1$, $m \ge t + 3$, we have

$$\frac{t}{2} \le (t+3)\left(\frac{1}{2} - \frac{1}{t+1}\right) + \frac{1}{2} \le m\left(\frac{1}{2} - \frac{1}{\sigma}\right) + \frac{1}{2}.$$

Thus, by the equality in (3.3), we have

$$|S_\alpha(f, 2^m)| = 2^{(m+t)/2} \le \sqrt{2}\, 2^{m(1-1/\sigma)}.$$

Henceforth we shall assume that $\nu \ge 2$. In particular, by Lemma 2.2(i), it follows that $\sigma \ge 2$. We start the induction proof with $m = 3$. In this case we have the trivial bound $|S_\alpha(f, 2^3)| \le 4 \le \sqrt{2}\, 2^{3(1-1/\sigma)}$. Suppose now that

$m \geq t+3$ and that the inequality in (3.8) has been established for all smaller values of m. If $m - \sigma \leq \tau + 2$ then we have the trivial bound

$$|S_\alpha(f, 2^m)| \leq 2^{m-1} \leq \sqrt{2}\nu 2^{m(1-1/\sigma)},$$

since

$$2^{m-\sigma} \leq 2^{\tau+2} \leq 4\sigma \leq (2\sqrt{2})^\sigma \leq (\sqrt{2}\nu)^\sigma.$$

Here, we have used the facts that $\sigma \geq 2$ and $2^\tau \leq d_p(g_\alpha) \leq \sigma$. If $m-\sigma \geq t+3$ then we can apply the induction assumption as in Case (iv) above to obtain the result. ∎

4. Mixed exponential sums. We begin by stating the generalization of Theorem 1.1 in [6] which was stated for the case of polynomials. Let $S(\chi, f, p^m)$, $S_\alpha = S_\alpha(\chi, f, p^m)$, the values a, r, $c = c(\chi, a)$, and the set of critical points $\mathcal{A}$ be as defined in the introduction.

THEOREM 4.1. *Let p be an odd prime, f be any rational function over $\mathbb{Z}$, χ be a multiplicative character (mod p^m), α an integer with $p \nmid \alpha f_2(\alpha)$ and t, t_1 be as defined in* (1.9) *and* (1.16). *Then if $m \geq t_1 + 2$ 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 $\nu \geq 1$ then $t = t_1$ and*

$$|S_\alpha(\chi, f, p^m)| \leq \nu p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}. \tag{4.1}$$

(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 (4.1).

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

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

χ_2 is the quadratic character (mod p), and R is the p-adic integer

$$R := p^{-1} \log(1 + rp) = p^{-1} \sum_{i=1}^{\infty} \frac{(-1)^{i+1}(rp)^i}{i} \equiv r \pmod{p}. \tag{4.2}$$

It follows immediately that under the hypotheses of the theorem

$$|S(\chi,f,p^m)| \le \Big(\sum_{\alpha\in\mathcal{A}}\nu_\alpha\Big)p^{t/(M+1)}p^{m(1-1/(M+1))}, \tag{4.3}$$

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 $S(\chi,f,p^m)$.

For the prime $p=2$ the critical point congruence associated with the sum $S(\chi,f,2^m)$ is just

$$2^{-t_1}(xf'(x)+c)\equiv 0 \pmod 2,$$

where $c=c(\chi)$ is defined by the relations $\chi(5)=e_{2^{m-2}}(c)$, $1\le c\le 2^{m-2}$, and $t_1=\operatorname{ord}_2(Xf'(X)+c)$ (see [6], Section 8). The only allowable critical point is the residue class 1 and it is a critical point if and only if $t=t_1$ and $f'(1)\equiv c \pmod{2^{t+1}}$. We have

THEOREM 4.2. *Suppose that f is a rational function over $\mathbb{Z}$, χ is a multiplicative character (mod 2^m), and $m\ge t_1+3$. 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 $\nu\ge 1$ then $t=t_1$ and*

$$|S(\chi,f,2^m)| \le 2\nu 2^{t/(\nu+1)}2^{m(1-1/(\nu+1))}. \tag{4.4}$$

The proofs of Theorems 4.1 and 4.2 follow the same line of argument given in [6] for the case of polynomials. We shall include here a complete proof of Theorem 4.1 in order to highlight the modifications required for the case of rational functions, but for the sake of brevity we shall omit the proof of Theorem 4.2. It follows identically as the proof of Theorem 8.1 of [6], taking into account these modifications.

In the course of the proof of Theorem 4.1 we need the fact that if the sum $S(\chi,f,p^m)$ has an associated critical point then $t_1=t$. This was a trivial observation for the case of polynomials but appears to be a nontrivial fact for rational functions. It is plain from the definition that $t_1\ge t$ in this case. Equality will follow from Lemma 4.1 below. We also use this lemma to prove

COROLLARY 4.1. *Let $f=f_1/f_2$ be a rational function over $\mathbb{Z}$ with $(f_1,f_2)=1$ and let $D=\max\{d(f_1)+d(f_2),2d(f_2)\}$. Then for any prime p with $d_p(f)\ge 1$, any positive integer $m\ge 2$ and any multiplicative character χ (mod p^m) we have*

$$|S(\chi,f,p^m)| \le 4Dp^{m(1-1/(D+1))}. \tag{4.5}$$

P r o o f. Suppose first that p is odd and $m<t_1+2$. Then, by Lemma 4.1 below, $m\le t+1$. Now, by Lemma 2.1(iii), $p^t\le d^*(f)\le D$, and so we have the trivial upper bound

$$|S(\chi,f,p^m)| \le p^m \le p^t p \le Dp^{m(1-1/(D+1))}.$$

Suppose now that $m \geq t_1 + 2$. If $\mathcal{A}$ is empty then the upper bound is trivial. Otherwise we must have $t = t_1$, as noted above, and $m \geq t + 2$. Then it follows from (4.3) and the facts that $\sum_{\alpha \in \mathcal{A}} \nu_\alpha \leq D$ and $M \leq D$ that

$$|S(\chi, f, p^m)| \leq Dp^{t/(D+1)} p^{m(1-1/(D+1))} \leq D^{1/(D+1)} Dp^{m(1-1/(D+1))},$$

which is sharper than (4.5).

For $p = 2$ we see that trivially, if $m \leq t_1 + 2$, the $|S(\chi, f, 2^m)| \leq 2^{m-1} \leq 2^{t+1} \leq 2D$. Otherwise, by (4.4) we obtain the upper bound in (4.5). ∎

LEMMA 4.1. *Let p be a prime, f a rational function over $\mathbb{Z}$ with* $\mathrm{ord}_p(f) \geq 0$, *c, r any integers with $p \nmid r$ and let t, t_1 be defined by*

$$t = \mathrm{ord}_p(f'), \qquad t_1 = \mathrm{ord}_p(rXf'(X) + c).$$

Then $t_1 = \min\{t, \mathrm{ord}_p(c)\}$.

This lemma follows readily from

LEMMA 4.2. *Let p be a prime and f be a rational function over $\mathbb{Z}$ with* $\mathrm{ord}_p(f) \geq 0$. *Then for any positive integer k, there exists a nonnegative integer l, rational numbers a_i, $i \geq -l$, and a rational function h over $\mathbb{Z}$ such that in the field of formal Laurent series over $\mathbb{Q}$, we have*

$$f(X) = \sum_{i=-l}^{\infty} a_i X^i + p^k h(X), \tag{4.6}$$

with $\mathrm{ord}_p(a_i) \geq 0$, *for $i \geq -l$, and* $\mathrm{ord}_p(h) \geq 0$.

P r o o f. The proof is by induction on k. Suppose first that $k = 1$. Write $f = f_1/f_2$ with $f_1, f_2 \in \mathbb{Z}[X]$, $(f_1, f_2) = 1$ in $\mathbb{Z}[X]$, and $\mathrm{ord}_p(f_2) = 0$. Suppose that when read $(\mathrm{mod}\, p)$, f_2 has a zero at $x = 0$ of multiplicity $l \geq 0$. Then we can write

$$f_2(X) = aX^l g_1(X) + pg_2(X)$$

for some integer a with $p \nmid a$, and polynomials $g_1, g_2 \in \mathbb{Z}[X]$, with $g_1(0) = 1$. Thus,

$$f(X) = \frac{f_1(X)}{f_2(X)} = \frac{f_1(X)}{aX^l g_1(X)} + ph(X) \tag{4.7}$$

for some rational function $h(X)$ over $\mathbb{Z}$ with $\mathrm{ord}_p(h) \geq 0$. Now, since $g_1(0) = 1$, f_1/g_1 admits a power series expansion $f_1/g_1 = \sum_{i=0}^{\infty} b_i X^i$ with integer coefficients b_i, $i \geq 0$. But then by (4.7) we obtain the result of the lemma. The induction step now follows easily by applying the result of the lemma in succession to the function $h(X)$. ∎

Proof of Lemma 4.1. It is sufficient to prove that for any nonnegative integer k,

$$\mathrm{ord}_p(rXf'(X) + c) \geq k$$

if and only if $\mathrm{ord}_p(f') \geq k$ and $\mathrm{ord}_p(c) \geq k$. One direction is trivial: If $\mathrm{ord}_p(f') \geq k$ and $\mathrm{ord}_p(c) \geq k$ then $\mathrm{ord}_p(rXf'(X)+c) \geq k$. Suppose now that $\mathrm{ord}_p(rXf'(X)+c) \geq k$. It suffices to show that $\mathrm{ord}_p(c) \geq k$. This is trivial if $k = 0$. Suppose now that $k \geq 1$ and write f as in (4.6). Then

$$rXf'(X) + c = rX \sum_{i=-l}^{\infty} a_i i X^{i-1} + c + p^k rXh'(X),$$

that is

$$H(X) := X^l(rXf'(X) + c - p^k rXh'(X)) = \sum_{i=-l}^{\infty} ra_i i X^{l+i} + cX^l. \tag{4.8}$$

The function $H(X)$ is a rational function over $\mathbb{Z}$ with $\mathrm{ord}_p(H) \geq k$ and admitting a power series expansion with p-adic integer coefficients. Now the coefficient of X^l in this expansion is just c and so by Lemma 2.2(i) we must have $\mathrm{ord}_p(c) \geq \mathrm{ord}_p(H) \geq k$. ∎

Proof of Theorem 4.1. For the sake of clarity we repeat here the argument given in [6] together with the necessary modifications. Let p be an odd prime, $m \geq 2$ a positive integer, f a polynomial over $\mathbb{Z}$, χ a multiplicative character $(\mathrm{mod}\, p^m)$ with $c = c(\chi, a)$ as defined in (1.15). Let t, t_1 be as defined in (1.9) and (1.16) and $\mathcal{A}$ be the set of critical points associated with the sum $S(\chi, f, p^m)$. 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 (1.14) 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 2.3 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

$$S_\alpha = \sum_{\substack{l=0 \\ l\equiv l_\alpha \pmod{p-1}}}^{p^{m-t_1-2}(p-1)-1} e\left(\frac{cl}{p^{m-1}(p-1)} + \frac{f(a^l)}{p^m}\right) \tag{4.9}$$
$$\times \sum_{j=0}^{p^{t_1+1}-1} e\left(\frac{cj}{p} + \frac{f'(a^l)a^l jr}{p}\right)$$
$$= p^{t_1+1} \sum_{\substack{l\equiv l_\alpha \pmod{p-1} \\ c+rf'(a^l)a^l\equiv 0 \pmod{p^{t_1+1}}}}^{p^{m-t_1-2}(p-1)-1} e\left(\frac{cl}{p^{m-1}(p-1)} + \frac{f(a^l)}{p^m}\right).$$

Thus $S_\alpha = 0$ unless $\alpha \in \mathcal{A}$ in which case, by the remark before Lemma 4.1, 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

$$S_\alpha = p^{t+1} \sum_{y=0}^{p^{m-t-2}-1} e\left(\frac{c(l_\alpha + (p-1)y)}{p^{m-1}(p-1)} + \frac{f(\alpha(1+rp)^y)}{p^m}\right) \tag{4.10}$$
$$= p^{t+1}\chi(\alpha)e_{p^m}(f(\alpha)) \sum_{y=0}^{p^{m-t-2}-1} e_{p^m}(F_1(y)),$$

where

$$F_1(y) = f(\alpha(1+rp)^y) - f(\alpha) + pcy. \tag{4.11}$$

Let $\log(1+pu)$ denote the p-adic logarithm

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

R be as defined in (4.2) and set

$$y = \frac{1}{Rp}\log(1+pu). \tag{4.12}$$

Then as u runs through a complete set of residues modulo any given power of p, so does y (in $\mathbb{Z}_p$).

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

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

with p-adic integer coefficients a_i. Then for any $u \in \mathbb{Z}_p$ we have

$$F_2(u) = f(\alpha(1+pu)) - f(\alpha) + cR^{-1}\log(1+pu) \tag{4.13}$$

$$= \sum_{i=1}^{\infty} a_i \alpha^i p^i u^i + cR^{-1} \sum_{i=1}^{\infty} \frac{(-1)^{i+1}(pu)^i}{i}$$
$$= \sum_{i=1}^{\infty} (Ria_i\alpha^i + (-1)^{i+1}c)\frac{p^i}{Ri}u^i.$$

Define

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

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

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

with p-adic integer coefficients b_i. Then we have

$$p^t G(X) = R(X-\alpha)\sum_{i=0}^{\infty} a_i i(X-\alpha)^{i-1} + R\alpha \sum_{i=0}^{\infty} a_i i(X-\alpha)^{i-1} + c$$
$$= R\sum_{i=1}^{\infty}(a_i i + \alpha a_{i+1}(i+1))(X-\alpha)^i + R\alpha a_1 + c,$$

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

$$b_i = p^{-t}R(ia_i + \alpha(i+1)a_{i+1}). \tag{4.14}$$

It follows that for $i \geq 1$,

$$a_i = (-1)^{i+1}(Ri\alpha^i)^{-1}\Big(\sum_{j=0}^{i-1}(-1)^j p^t b_j \alpha^j - c\Big). \tag{4.15}$$

Inserting this expression for a_i into (4.13) yields

$$F_2(u) = \sum_{i=1}^{\infty}(-1)^{i+1}\Big(\sum_{j=0}^{i-1}(-1)^j b_j \alpha^j\Big)\frac{p^{i+t}}{Ri}u^i. \tag{4.16}$$

Let $F_2(U)$ be the formal power series over $\mathbb{Z}_p$ obtained by replacing u with the indeterminate U in (4.13) or (4.16) and let $F_\alpha(U)$ be a polynomial with rational integer coefficients chosen so that in $\mathbb{Z}_p[[U]]$,

$$F_\alpha(U) \equiv F_2(U) \pmod{p^{m+t+d}}, \tag{4.17}$$

that is, the corresponding coefficients are congruent $(\mathrm{mod}\, p^{m+t+d})$. Since the coefficients of $F_2(U)$ are all eventually zero $(\mathrm{mod}\, p^{m+t+d})$ 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 $F_\alpha(U)$.

Set

$$\begin{aligned} \sigma &:= \mathrm{ord}_p(F_\alpha(U)), \quad & g_\alpha(U) &:= p^{-\sigma}F_\alpha(U), \\ \tau &:= \mathrm{ord}_p(g'_\alpha(U)), \quad & g_1(U) &:= p^{-\tau}g'_\alpha(U). \end{aligned} \tag{4.18}$$

LEMMA 4.3. *We have the same relationships as in Lemma* 2.2.

(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) $$p^\tau \,|\, d_p(g_\alpha).$$

P r o o f. Part (i) follows immediately from (4.16) and the fact that $p \,|\, b_0$, since α is a critical point. From (4.16) we also obtain

$$F_2'(U) = p^t R^{-1} \sum_{i=1}^{d} (-1)^{i+1} \Big(\sum_{j=0}^{i-1} (-1)^j b_j \alpha^j \Big) p^i U^{i-1} + cR^{-1} \sum_{i=d+1}^{\infty} (-1)^{i+1} p^i U^i. \tag{4.19}$$

Since α is a critical point of multiplicity $\nu \geq 1$ we have $p \,|\, b_i$ 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 (4.19) we obtain (ii). Part (iii) comes from the fact that p^σ is the maximum power of p dividing the $i = d_p(g_\alpha)$ coefficient in (4.16) 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 (4.19). Part (v) follows from Lemma 2.1(iii). ∎

Now, since $\sigma \geq t + 2$ it follows from (4.10) that

$$S_\alpha = p^{t+1} \chi(\alpha) e_{p^m}(f(\alpha)) \sum_{u=0}^{p^{m-t-2}-1} e_{p^m}(F_2(u)). \tag{4.20}$$

Thus, if α is a critical point of the type $\alpha = a^{l_\alpha}$ with $0 \leq l_\alpha < p - 1$ then we have

$$S_\alpha = p^{\sigma-1} \chi(\alpha) e_{p^m}(f(\alpha)) S(g_\alpha, p^{m-\sigma}). \tag{4.21}$$

The inequality in (4.1) can now be established by considering four cases: $\sigma \geq m$, $\sigma = m - 1$, $m - 1 - \tau \leq \sigma \leq m - 2$ and $\sigma \leq m - 2 - \tau$. The trivial estimate $|S_\alpha| \leq p^{m-1}$ suffices for the first and third cases. For the other two cases we appeal to (4.21), and use the upper bound of Weil for case $m - \sigma = 1$ and the upper bound in (3.10) for pure exponential sums for the last case. The details are identical to those given in [6] for the cases of polynomials, since the inequalities in Lemma 4.3 are the same as in [6].

The proof of part (iii) of Theorem 4.1 is identical to the proof given in Section 7 of [6] for the case of polynomials. ∎

REMARK. If χ is primitive it follows from the above argument that the maximum multiplicity M of any critical point satisfies $M \le p-1$. Indeed, by (4.15) we have

$$pa_pR\alpha^p = -\sum_{j=0}^{p-1} p^t b_j \alpha^j + c.$$

If $p \mid b_j$ for $0 \le j \le p-1$ then it follows that $p \mid c$.

5. Kloosterman and Salié sums. We start by considering the case of odd p and deal with $p = 2$ at the end of the section. Let p be an odd prime and $f(X) = AX + BX^{-1}$, with $p \nmid AB$. Then for any multiplicative character $\chi \pmod{p^m}$, $t_1 = t = 0$ and the critical point congruence (1.17) is

$$RAx^2 + cx - BR \equiv 0 \pmod{p}, \tag{5.1}$$

where $R := p^{-1}\log(1+rp) \equiv r \pmod{p}$. We have written the critical point congruence with the parameter R rather than r because this is the value one must use in lifting the critical points to solutions modulo prime powers. There are three cases to consider.

CASE (i). Suppose first that $p \nmid (4ABr^2 + c^2)$, and that $\chi_2(4ABr^2 + c^2) = -1$. Then there are no critical points and so $S(\chi, f, p^m) = 0$ for all values of $m \ge 2$.

CASE (ii). Suppose next that $p \nmid (4ABr^2 + c^2)$ and that $\chi_2(4ABr^2 + c^2) = 1$. Then there are two distinct critical points

$$\alpha_1 = \overline{2RA}(-c + \sqrt{4ABR^2 + c^2}), \quad \alpha_2 = \overline{2RA}(-c - \sqrt{4ABR^2 + c^2}), \tag{5.2}$$

each of multiplicity one. By the formula in Theorem 4.1(iii), we see that if m is even then

$$S(\chi, AX + BX^{-1}, p^m) = p^{m/2} \sum_{i=1}^{2} \chi(\alpha_i) e_{p^m}(f(\alpha_i)), \tag{5.3}$$

where the square root and inverse in (5.2) are taken $\pmod{p^{m/2}}$. If m is odd then

$$S(\chi, AX + BX^{-1}, p^m) = p^{(m-1)/2}\mathcal{G}_p \sum_{i=1}^{2} \chi(\alpha_i)\chi_2(\overline{2}f(\alpha_i)) e_{p^m}(f(\alpha_i)), \tag{5.4}$$

where the square root and inverse are interpreted $\pmod{p^{(m+1)/2}}$.

CASE (iii). Suppose now that $p \mid (4ABr^2 + c^2)$. Then there is a single critical point, $\alpha \equiv -\overline{2RA}c \pmod{p}$, of multiplicity two, and the series $F_2(u)$ in (4.13) is given by

$$F_2(u) = (RA\alpha^2 + c\alpha - RB)\frac{p}{R\alpha}u + p^3(\text{higher order terms}).$$

If $p^2 \nmid (RA\alpha^2+c\alpha-RB)$, that is $p^2 \nmid (4ABR^2+c^2)$, then $\sigma = 2$, the polynomial $g_\alpha(u) \equiv p^{-\sigma} F_2(u) \pmod{p^m}$ is linear $(\mathrm{mod}\, p)$ and thus the sum $S(g_\alpha, p^{m-2})$ is zero for $m \geq 3$. If $p^2 \nmid (4ABR^2 + c^2)$ then we settle for the upper bound of (1.19),

$$|S(\chi, AX + BX^{-1}, p^m)| = |S_\alpha| \leq 2p^{2m/3}, \tag{5.5}$$

for $m \geq 2$. This completes the proof of (1.22). The following example shows that the exponent $2m/3$ in (5.5) is best possible in general.

Example 5.1. Let p be a prime with $p > 3$, m a positive integer divisible by 3, $f = AX - AX^{-1}$ with $p \nmid A$, and χ be a multiplicative character $(\mathrm{mod}\, p^m)$ such that $c \equiv -2RA \pmod{p^{m-1}}$, where $R = p^{-1}\log(1 + rp)$. Then

$$S(\chi, AX - AX^{-1}, p^m) = p^{2m/3}.$$

P r o o f. In this example there is a single critical point of multiplicity two at $\alpha \equiv 1 \pmod{p}$. Since 1 is of the form a^{l_α} with $0 \leq l_\alpha < p - 1$, we can take $\alpha = 1$ in the proof of Theorem 4.1. Now f admits a Taylor expansion about 1 of the form

$$f(X) = A\frac{(X-1)^2 + 2(X-1)}{1 + (X-1)} = A\Big(2(X-1) + \sum_{i=2}^{\infty}(-1)^{i+1}(X-1)^i\Big).$$

Thus by (4.13) we have (working in $\mathbb{Z}_p$),

$$\begin{aligned} F_2(U) &= \sum_{i=1}^{\infty}(Ria_i + (-1)^{i+1}c)\frac{p^i}{Ri}U^i \\ &= (2RA + c)\frac{p}{R}U + \sum_{i=2}^{\infty}(RiA(-1)^{i+1} + (-1)^{i+1}c)\frac{p^i}{Ri}U^i, \end{aligned}$$

and thus

$$F_2(U) \equiv \sum_{i=3}^{\infty}(RiA + c)\frac{(-1)^{i+1}p^i}{Ri}U^i \pmod{p^m}. \tag{5.6}$$

Now, since $p > 3$, p^3 is the maximum power of p dividing the U^3 coefficient in (5.6), and the coefficients of all higher powers are divisible by p^4. Thus $\sigma = 3$ and the polynomial g_α in (4.18) is of the type

$$g_\alpha \equiv kU^3 + pU^3G(U) \pmod{p^m},$$

for some integer k, not divisible by p, and polynomial G with integer coefficients. Now, by Example 9.1 of [6], if $3 \mid m$ then $S(g_\alpha, p^m) = p^{2m/3}$, and so by (4.21) we see that if $3 \mid m$ then

$$S_\alpha = p^{\sigma-1}S(g_\alpha, p^{m-\sigma}) = p^{2m/3}. \ \blacksquare$$

EXAMPLE 5.2. Let χ be a multiplicative character $(\mathrm{mod}\, p^m)$ with $\mathrm{ord}_p(c) \geq [(m+1)/2]$. The Kloosterman sum and Salié sums, obtained by taking χ to be the principal character and quadratic character respectively, are special cases. For any such character, the sum $S(\chi, AX + BX^{-1}, p^m)$ has two distinct critical points $\alpha_1 = \sqrt{B\bar{A}}$, and $\alpha_2 = -\sqrt{B\bar{A}}$, provided AB is a square $(\mathrm{mod}\, p)$. Moreover, these two values are also the solutions of the critical point congruence modulo $p^{[(m+1)/2]}$, provided the square roots and multiplicative inverse are taken modulo that power of p. If we interpret the square roots as square roots $(\mathrm{mod}\, p^m)$ then, with $S = S(\chi, AX+BX^{-1}, p^m)$, the formulae in (5.3) and (5.4) simplify to

$$S = \begin{cases} 0, \\ p^{m/2} \sum_{i=1}^{2} \chi(\alpha_i) e_{p^m}(2(-1)^{i+1}\sqrt{AB}), \\ p^{(m-1)/2} \mathcal{G}_p \sum_{i=1}^{2} \chi_2((-1)^{i+1}\sqrt{AB}) \chi(\alpha_i) e_{p^m}((-1)^{i+1} 2\sqrt{AB}), \end{cases} \tag{5.7}$$

for the three cases, $\chi_2(AB) = -1$; $\chi_2(AB) = 1$, m is even; $\chi_2(AB) = 1$, m is odd, respectively. For the case of the Kloosterman sum the formula in (5.7) has already been obtained by Salié [24], Whiteman [29], Estermann [11], Carlitz [3], and Williams [30].

The case $p = 2$. Let $f = AX + BX^{-1}$ with $2 \nmid AB$. When $p = 2$ the critical point congruence is

$$x^2 + cx - 1 \equiv 0 \pmod 2,$$

where c is defined by $\chi(5) = e_{2^m}(c)$, $1 \leq c \leq 2^{m-2}$. If c is odd then there is no critical point and so $S(\chi, f, 2^m) = 0$ for $m \geq 3$. If c is even then $\alpha = 1$ is a critical point of multiplicity two. In this case we untwist the sum, using the method of [6], to obtain the following upper bound. If $A + B + c \equiv 0 \pmod 4$ and $m \geq 4$ then $S(\chi, f, 2^m) = 0$, otherwise for $m \geq 1$ we have

$$|S(\chi, f, 2^m)| \leq \begin{cases} 2^{(m+3)/2} & \text{if } c \equiv 0 \pmod 4 \text{ and } A \equiv B \pmod 4, \\ 6 \cdot 2^{2m/3} & \text{if } c \equiv 2 \pmod 4 \text{ and } A \equiv -B \pmod 4. \end{cases} \tag{5.8}$$

To prove this inequality we start with the identity (8.3) of [6]: For $m \geq 3$,

$$\begin{aligned} S(\chi, f, 2^m) &= 2e_{2^m}(f(1)) \sum_{y=1}^{2^{m-3}} e_{2^m}(F_1(y)) \\ &\quad + 2\chi(-1) e_{2^m}(f(-1)) \sum_{y=1}^{2^{m-3}} e_{2^m}(F_2(y)) \\ &= S_1 + S_2, \end{aligned} \tag{5.9}$$

say, where

$$F_1(y) = 5cy + f(5^y) - f(1), \qquad F_2(y) = 5cy + f(-5^y) - f(-1).$$

We focus our attention on estimating S_1; the case of S_2 is analogous. Set $R = (\log 5)/4$, $y = \log(1+4u)/(4R)$, and let $f(X) = \sum_{i=0}^{\infty} a_i(X-1)^i$ be the Taylor expansion of f about 1. Then $F_1(y) = H_1(u)$ where

$$H_1(u) = \left(4\frac{c}{R} + 4(A-B)\right)u + \left(-8\frac{c}{R} + 16B\right)u^2 + 4^3(\text{higher order terms}).$$

Let σ be the largest power of 2 dividing all of the coefficients of H_1 and put $g = 2^{-\sigma}H_1$. Then

$$|S_1| = 2^{\sigma-2}|S(g, 2^{m-\sigma})|. \tag{5.10}$$

Case (i). Suppose first that $4 \mid c$ and that $A \equiv B \pmod 4$. It follows that $\sigma = 4$, $\mathrm{ord}_p(g') \le 1$ and that the sum $S(g, 2^{m-\sigma})$ has either no critical point or a single critical point of multiplicity one. Thus for $m \ge 8$ it follows from Theorem 3.1(b) that $|S_1| \le 2^2 2^{(m-4+1)/2}$. If $m \le 5$ then we have trivially $|S_1| \le 2^{m-2} \le 2^{(m+1)/2}$. For the cases $m = 6, 7$ the inequality in (5.8) can be checked numerically.

Case (ii). Suppose next that $4 \mid c$ and $A \equiv -B \pmod 4$, or that $c \equiv 2 \pmod 4$ and $A \equiv B \pmod 4$. Then $\sigma = 3$, and for $m \ge \sigma + 2$ the sum $S(g, 2^{m-\sigma})$ has no associated critical point and therefore is equal to zero. If $m = 4$ then g is linear and so the sum is again zero.

Case (iii). Suppose finally that $c \equiv 2 \pmod 4$ and that $A \equiv -B \pmod 4$. Then σ can be as large as 6. In this case we are content to settle for the upper bound of Theorem 4.2, $|S(\chi, f, 2^m)| \le 6 \cdot 2^{2m/3}$, and observe that examples can be constructed where $|S(\chi, f, 2^m)| = 2^{2m/3}$ in the same manner as in Example 5.1. A more detailed case study may be done here to obtain sharper bounds in general.

6. Extremal examples

Lemma 6.1. *Let d be a positive integer and $P(X) \in \mathbb{Q}[X]$ the polynomial of degree $D = 2d$ obtained by truncating the series for $-\log(1+X)$,*

$$P(X) = \sum_{i=1}^{D} \frac{(-1)^i}{i} X^i.$$

Then there exist polynomials $f_1, f_2 \in \mathbb{Z}[X]$, each of degree d, such that $p \nmid f_2(0)$ for any prime $p > D$ and

$$\frac{f_1(X)}{f_2(X)} = P(X) + X^{D+1}Q(X) \tag{6.1}$$

for some rational function $Q(X)$ over $\mathbb{Z}$, defined at the origin. In other words, the first D coefficients of the Taylor expansion of f_1/f_2 coincide with the coefficients of $-\log(1+X)$.

P r o o f. Say

$$P(X)=\sum_{i=1}^{D}a_iX^i,\quad f_1(X)=\sum_{j=1}^{d}b_jX^j,\quad f_2(X)=\sum_{k=0}^{d}c_kX^k,$$

where $a_i=(-1)^i/i$, $1\le i\le D$ and the values b_j, c_k are unknowns. We may assume that $c_0=1$. In order to satisfy (6.1) we must have

$$\sum_{i+k=j}a_ic_k=b_j\quad\text{for } 1\le j\le d, \tag{6.2}$$

and

$$\sum_{i=1}^{d}a_{j-i}c_i=-a_j\quad\text{for } d+1\le j\le D. \tag{6.3}$$

The latter system is a nonhomogeneous system of d equations in d unknowns $c_1,\dots,c_d$. After a permutation of columns we see that the coefficient matrix is $[(-1)^{i+j+1}/(i+j-1)]$, which up to signs is just the well known Hilbert matrix $[1/(i+j-1)]$ that arises in numerical analysis (see e.g. [1]). The Hilbert matrix is known to be nonsingular with inverse $[\alpha_{ij}]$ given explicitly by

$$\alpha_{ij}=(-1)^{i+j}(i+j-1)\binom{d+j-1}{d-i}\binom{d+i-1}{d-j}\binom{i+j-2}{i-1}\binom{i+j-2}{j-1}.$$

In particular the entries α_{ij} are integers and consequently so are the entries of the inverse of the coefficient matrix for (6.3), which is given by $[(-1)^{i+j+1}\alpha_{ij}]$. Thus (6.3) has a unique solution in rational numbers c_k, $1\le k\le d_2$. Moreover since the values c_k are integral linear combinations of the values $1/(d+1),1/(d+2),\dots,1/D$, it is clear that the denominators of the fractions c_k, written in reduced form, are comprised of prime factors $p<D$. Having solved for the c_i, (6.2) then uniquely determines the values b_j, $1\le j\le d$. Clearing the denominators in the fraction f_1/f_2 we obtain polynomials f_1 and f_2 with integer coefficients satisfying (6.1), and having the property that $f_2(0)$ is comprised of primes $p\le D$. It follows from the next example that the degrees of f_1, f_2 are exactly d. ∎

As examples we have for $d=1$, $f_1/f_2=-X/(X+2)$, and for $d=2$, $f_1/f_2=(-3X^2-6X)/(X^2+6X+6)$.

Example 6.1. We show that the exponent $m(1-1/(D+1))$ in (1.21) is best possible when $d_1=d_2$. Let d_1 be a given positive integer and set $D=2d_1$. Let L be the least common multiple of the integers from 1 to D, and $P(X)$ be the polynomial in Lemma 6.1 with $d=d_1$. Let $f_1(X),f_2(X)\in\mathbb{Z}[X]$ be polynomials of degrees at most d_1, satisfying (6.1) and put $f(X)=Lf_1(X-1)/f_2(X-1)$. Let p be a prime with $p>D+2$, m a positive

integer with $(D+1)\,|\,m$, and χ be a multiplicative character $(\mathrm{mod}\, p^m)$ such that $c=c(\chi,a)\equiv RL \pmod{p^{m-1}}$, where $R=p^{-1}\log(1+rp)$. Then we claim that

$$S(\chi,f,p^m) = e_{p^m}(f(1))p^{m(1-1/(D+1))}. \tag{6.4}$$

P r o o f. We have

$$\begin{aligned} G(X) &:= RXf'(X)+c = (LRXP'(X-1)+c)+LRX(X-1)^Dq(X)\\ &\equiv c(1-X)^D + cX(X-1)^Dq(X) \pmod{p^m}, \end{aligned}$$

where $q(X)$ is a rational function over $\mathbb{Z}$ given by

$$q(X) = (X-1)Q'(X-1)+(D+1)Q(X-1).$$

Now, since $p>D$, it follows from the condition $p\nmid f_2(0)$ of Lemma 6.1, that $Q(X)$ does not have a pole at $x=0$ when read $(\mathrm{mod}\, p)$ and consequently $q(X)$ does not have a pole at $x=1$ when read $(\mathrm{mod}\, p)$. Thus, there is a single critical point $\alpha=1$ of multiplicity D. Now since the first D coefficients of the Taylor expansion of f about $\alpha=1$ are just the coefficients of $LP(X)$, we deduce for $1\le i\le D$ that the coefficient of U^i in (4.13) is

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

Thus

$$F_2(U)\equiv \sum_{i=D+1}^{\infty}(Ria_i+(-1)^{i+1}c)\frac{p^i}{Ri}U^i \pmod{p^m}.$$

Since $p>D+2$ we see that $\sigma := \mathrm{ord}_p(F_\alpha(U))\ge D+1$, but by Lemma 4.3(ii) we also know that $\sigma\le D+1$. Therefore $\sigma=D+1$. If $m=D+1$ then by (4.21), $S_\alpha=p^D=p^{m(1-1/(D+1))}$. Otherwise $m\ge 2(D+1)$ and the maximum power of p dividing the $(D+1)$st coefficient of $F_2(U)$ is p^σ. Therefore,

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

for some polynomial $h_\alpha(U)$ with integer coefficients. We observe that $g(U)$ is a polynomial of the type considered in Example 9.1 of [6], and thus from (4.20) we conclude that if $(D+1)\,|\,m$, then

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

We note that in order to construct an example of this type it is necessary for p to be larger than D, because for $p\le D$ the maximum multiplicity of a critical point is at most $M\le p-1<D$, as we noted in the remark at the end of Section 4.

References

[1] K. E. Atkinson, *An Introduction to Numerical Analysis*, Wiley, New York, 1978.
[2] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. 88 (1966), 71–105.
[3] L. Carlitz, *A note on multiple Kloosterman sums*, J. Indian Math. Soc. 29 (1965), 197–200.
[4] J. H. H. Chalk, *On Hua's estimate for exponential sums*, Mathematika 34 (1987), 115–123.
[5] J. R. Chen, *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1977), 711–719.
[6] T. Cochrane and Z. Y. Zheng, *Pure and mixed exponential sums*, Acta Arith. 91 (1999), 249–278.
[7] —, —, *On Hua's bound for exponential sums*, preprint.
[8] P. Ding, *An improvement to Chalk's estimation of exponential sums*, Acta Arith. 59 (1991), 149–155.
[9] —, *On a conjecture of Chalk*, J. Number Theory 65 (1997), 116–129.
[10] W. Duke, J. Friedlander and H. Iwaniec, *Bilinear forms with Kloosterman fractions*, Invent. Math. 128 (1997), 23–43.
[11] T. Estermann, *On Kloosterman's sum*, Mathematika 8 (1961), 83–86.
[12] L. K. Hua, *On exponential sums*, J. Chinese Math. Soc. 20 (1940), 301–312.
[13] —, *On exponential sums*, Sci. Record (Peking) (N.S.) 1 (1957), 1–4.
[14] —, *Additive Primzahltheorie*, Teubner, Leipzig, 1959, 2–7.
[15] H. Iwaniec, *Topics in Classical Automorphic Forms*, Grad. Stud. Math. 17, Amer. Math. Soc., Providence, RI, 1991.
[16] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Springer, New York, 1984.
[17] S. V. Konyagin and I. E. Shparlinski, *On the distribution of residues of finitely generated multiplicative groups and their applications*, Macquarie Mathematics Reports, Macquarie University, 1995.
[18] W. K. A. Loh, *Hua's Lemma*, Bull. Austral. Math. Soc. 50 (1994), 451–458.
[19] —, *Exponential sums on reduced residue systems*, Canad. Math. Bull. 41 (1997), 187–195.
[20] J. H. Loxton and R. A. Smith, *On Hua's estimate for exponential sums*, J. London Math. Soc. (2) 26 (1982), 15–20.
[21] J. H. Loxton and R. C. Vaughan, *The estimation of complete exponential sums*, Canad. Math. Bull. 28 (1985), 442–454.
[22] 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).
[23] G. I. Perelmuter, *Estimate of a sum along an algebraic curve*, Mat. Zametki 5 (1969), 373–380 (in Russian).
[24] H. Salié, *Über die Kloostermanschen Summen* $S(u, v; q)$, Math. Z. 34 (1931), 91–109.
[25] I. E. Shparlinski, *On exponential sums with sparse polynomials and rational functions*, J. Number Theory 60 (1996), 233–244.
[26] R. A. Smith, *Estimate for exponential sums*, Proc. Amer. Math. Soc. 79 (1980), 365–368.
[27] 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.

[28] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.
[29] A. L. Whiteman, *A note on Kloosterman's sums*, Bull. Amer. Math. Soc. 51 (1945), 373–377.
[30] K. S. Williams, *Note on the Kloosterman sum*, Proc. Amer. Math. Soc. 30 (1971), 61–62.

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 8.11.1999 (3708)