Canad. Math. Bull. Vol. **41** (2), 1998 pp. 187–195

EXPONENTIAL SUMS ON REDUCED RESIDUE SYSTEMS

W. K. A. LOH

ABSTRACT. The aim of this article is to obtain an upper bound for the exponential sums $\sum e(f(x)/q)$, where the summation runs from $x = 1$ to $x = q$ with $(x, q) = 1$ and $e(\alpha)$ denotes $\exp(2\pi i\alpha)$.

We shall show that the upper bound depends only on the values of q and s, where s is the number of terms in the polynomial $f(x)$.

1. Introduction.

Let $f(x)$ denote the polynomial

$$f(x) = a_1x^{k_1} + a_2x^{k_2} + \cdots + a_sx^{k_s} \tag{1}$$

with $s \geq 2, k_s > k_{s-1} > \cdots > k_1 \geq 1, k_i \in N$ and $a_i \in \mathbb{Z} \setminus \{0\}$.

Suppose that p is any prime and α is an integer with

$$p^\alpha \mid (a_1, \ldots, a_s), \quad p^{\alpha+1} \nmid (a_1, \ldots, a_s),$$

then define α to be the p-content of the function $f(X)$.

In this paper, we wish to estimate the exponential sum

$$\tilde{S}(q, f) = \sum_{\substack{x=1 \\ (q,x)=1}}^{q} e\big(f(x)/q\big), \tag{2}$$

where $q \geq 1$ and $e(\alpha)$ denotes $\exp(2\pi i\alpha)$.

Since such sums are multiplicative, it suffices to estimate

$$\tilde{S}(p^l, f) = \sum_{\substack{x=1 \\ (p,x)=1}}^{p^l} e\big(f(x)/p^l\big). \tag{3}$$

By using an idea of Loxton and Vaughan [10], we are able to obtain the the following results:

THEOREM 1. *Let f be as in (1) and suppose $p > k_s$ and p does not divide the content of f. Then*

$$|\tilde{S}(p^l, f)| \leq (k_s - 1)p^{(1-\frac{1}{s})l}.$$

Received by the editors December 1, 1995.
AMS subject classification: 11L07.

https://doi.org/10.4153/CMB-1998-028-5 Published online by Cambridge University Press

THEOREM 2. *Let f be as in (1) and suppose $p \le k_s$ and p does not divide the content of f. Then*

$$|\tilde{S}(p^l, f)| \le m(p^{-\tau_0} f')p^{\frac{\tau_0+1}{s}} p^{(1-\frac{1}{s})l},$$

where p^{τ_0} is the largest power of p dividing the content of f and $m(f)$ denote the total number of roots of the congruence

$$f(X) \equiv 0 \pmod p. \tag{4}$$

THEOREM 3. *Let f be as in (1) and suppose q is coprime to the content of f. Then*

$$|\tilde{S}(q, f)| \le q^{(1-\frac{1}{s})+\epsilon},$$

for large q.

COROLLARY 1. *Let*

$$f(x) = a_1 x^{k_1} + a_2 x^{k_2} + \cdots + a_s x^{k_s},$$

and suppose that $q > 0$ is an integer and $(q, a_1, a_2, \ldots, a_s) = q_1$. Then, for large q,

$$|\tilde{S}(q, f)| \le \begin{cases} q_1^{1/s} q^{(1-\frac{1}{s})+\epsilon} & \text{if } 1 \le q_1 < q, \\ \phi(q) & \text{if } q_1 = q. \end{cases}$$

2. *p*-adic Sequences. First of all we establish a reduction procedure along the lines developed in Loxton and Vaughan (1985). We define sequences of polynomials $\{f_i\}$ and associated sequences of integers $\{\tau_i\}$, $\{\omega_i\}$, $\{n_i\}$, $\{x_i\}$ as follows. Let

$$f_0 = f.$$

Given f_i choose τ_i so that the polynomial $p^{-\tau_i} f_i'$ has integer coefficients but p does not divide its content. If the congruence,

$$p^{-\tau_i} f_i'(x) \equiv 0 \pmod p, \tag{5}$$

has no root ω_i, then the sequences terminate with f_i, τ_i, ω_{i-1}, n_{i-1}, x_{i-1}. If it has such a root ω_i choose n_i so that

$$p^{-n_i}\big(f_i(\omega_i + px) - f_i(\omega_i)\big),$$

has integer coefficients but p does not divide its content. Clearly,

$$n_i \ge 2 + \tau_i. \tag{6}$$

Let

$$f_{i+1}(x) = p^{-n_i}\big(f_i(\omega_i + px) - f_i(\omega_i)\big). \tag{7}$$

At each stage of the construction there may be several choices for ω_i modulo p and so it may be possible to construct many such sequences. Let

$$x_i = \omega_0 + p\omega_1 + \cdots + p^{i-1}\omega_{i-1}, \tag{8}$$

https://doi.org/10.4153/CMB-1998-028-5 Published online by Cambridge University Press

and let $\mathcal{A}$ denote the set of all sequences $X = \{x_i\}$ which can be constructed in this way and write $f_i(x_i, X)$, $\tau_i(X)$, $n_i(X)$, $m_i(X)$ for the associated quantities arising in the construction.

We further define

$$\mu_0(X) = 0, \quad \mu_i(X) = \sum_{l=0}^{i-1} n_l(X), \tag{9}$$

Now the polynomials $f_i(x, X)$ are given by

$$f_i(x, X) = p^{-\mu_i}\big(f(x_i + p^i x) - f(x_i)\big). \tag{10}$$

For each $t \in N$ we define subsets $\mathcal{B}_k$, $\mathcal{C}_k$, $\mathcal{E}_k$ of $\mathcal{A}$ as follows. Let $\mathcal{B}_k$ denote the subset of $\mathcal{A}$ formed from those sequences X with at least k elements and satisfying

$$\mu_{k-1} + \tau_{k-1} + 2 \le t \quad \text{and} \quad \mu_k \ge t.$$

Let $\mathcal{C}_k$ denote the subset of $\mathcal{A}$ formed from those sequences X with at least k elements and satisfying

$$\mu_{k-1} + \tau_{k-1} + 2 \le t \quad \text{and} \quad \mu_k < t < \mu_k + \tau_k + 2.$$

Finally let $\mathcal{E}_k$ denote the subset of $\mathcal{A}$ formed from those sequences X with at least k elements and satisfying

$$\mu_k + \tau_k + 2 \le t.$$

Since $\mu_i + \tau_i$ increases with i, the sets $\mathcal{B}_k$ and $\mathcal{C}_k$ are disjoint and $\mathcal{E}_k$ is the union of the $\mathcal{B}_j$ and $\mathcal{C}_j$ with $j > k$. Let $\mathcal{D}_k = \mathcal{B}_k \cup \mathcal{C}_k$. Note that $n_i(X) \le k$, since if $f_i(x) = \sum_{m=0}^{k} a_m x^m$, then $f_i(x_i + px) - f_i(x_i) = \sum_{m=0}^{k} b_m p^m x^m$ with $b_m = a_m$, $b_{m-1} = a_{m-1} + a_m\binom{m}{m-1}x_i$, and so on. Hence the sets $\mathcal{B}_k$, $\mathcal{C}_k$, $\mathcal{D}_k$, $\mathcal{E}_k$ are empty for all sufficiently large k. Let

$$N_k(X) = \begin{cases} \max\big(1, \deg_p(p^{-\tau_k} f_k'), \deg_p(f_k) - 1\big) & \text{when } \tau_{k-1} = 0, \\ \max\big(1, \deg_p(p^{-\tau_k} f_k')\big) & \text{otherwise.} \end{cases} \tag{11}$$

3. Preliminary Lemmata.

LEMMA 1. *Suppose p does not divide the content of f and let $N_k(X)$ be as in (13). Then*

$$\sum_{k=1}^{\infty} \sum_{X \in \mathcal{D}_k} N_k(X) \le \deg_p(p^{-\tau_0} f').$$

PROOF. See Loxton and Vaughan (1985), Lemma 2.

The next lemma plays an important role in the proof of the Theorems.

LEMMA 2. *Suppose that $f \in \mathbb{Z}[X]$ and p does not divide the content of f, $p \ge 3$ and $t \ge \tau_0 + 2$ or $p = 2$ and $t \ge \tau_0 + 3$. Then*

$$\tilde{S}(f; p^t) = \sum_{k=1}^{\infty} \sum_{X \in \mathcal{B}_k} e\big(f(x_k)p^{-t}\big)p^{t-k} + \sum_{k=1}^{\infty} \sum_{X \in \mathcal{C}_k} e\big(f(x_k)p^{-t}\big)p^{\mu_k - k} S_k,$$

where

$$S_k = \sum_{x=1}^{p^{t-\mu_k}} e\big(f_k(x)p^{\mu_k - t}\big).$$

In particular, if $\mathcal{A}$ is empty, then $\tilde{S}(f; p^t) = 0$.

https://doi.org/10.4153/CMB-1998-028-5 Published online by Cambridge University Press

PROOF. This is identical to the proof of Lemma 3 of Loxton and Vaughan (1985).

By making use of the following lemma, we can establish a upper bound for $\tilde{S}(p^l, f)$ which depends on the number of terms in the polynomial $f(x)$.

LEMMA 3. *Let*

$$g(x) = a_1 x^{k_1} + \cdots + a_n x^{k_n},$$

with $1 \le k_1 < \cdots < k_n$ *and* $(a_1, a_2, \ldots, a_n, p) = 1$*, and suppose* z *is a root of*

$$g(x) \equiv 0 \pmod{p},$$

of multiplicity m *and with* $p \not| z$*. Then* $m \le n - 1$.

PROOF. We argue by induction. The lemma is trivial when $n = 1$. Suppose $n > 1$. If $p \mid (a_2, \ldots, a_n)$, then $p \not| a_1$, and the lemma follows from the case $n = 1$. Hence $(a_2, \ldots, a_n, p) = 1$. We have

$$g(z + y) = b_0 + b_1 y + \cdots + b_k y^k,$$

where $k = k_n$ and $b_i \equiv 0 \pmod{p}$ for $0 \le i < m$ and $b_m \not\equiv 0 \pmod{p}$. Then

$$(z + y)^{k_1} \quad \text{is a factor of } b_0 + b_1 y + \cdots + b_k y^k,$$

and

$$\begin{aligned} b_0 + b_1 y + \cdots + b_k y^k &= (z + y)^{k_1}(c_0 + c_1 y + \cdots + c_L y^L), \\ &= \sum_i y^i \sum_{l=0}^{i} c_l \binom{i-l}{k_1} z^{k_1+l-i}. \end{aligned}$$

Since the coefficient of y^i is $c_i z^{k_1} + c_{i-1}\binom{k_1}{1} z^{k_1-1} + \cdots$, it is easily seen by induction on i that $c_0 \equiv c_1 \equiv \cdots \equiv c_{m-1} \equiv 0 \pmod{p}$ and $c_m z^{k_1} \equiv b_m \pmod{p}$ so $p \not| c_m$. Thus $g_1(x) = a_1 + a_2 x^{k_2-k_1} + \cdots + a_n x^{k_n-k_1}$ has a root of multiplicity m at z. Now

$$g_1'(z + y) = c_1 + 2c_2 y + \cdots + L c_L y^{L-1},$$

and so g_1' has a root of multiplicity $m - 1$ at z. But

$$g_1'(x) = (k_2 - k_1) a_2 x^{k-2-k_1-1} + \cdots + (k_n - k_1) a_n x^{k_n-k_1-1},$$

and so by the inductive hypothesis $m - 1 \le n - 2$.

LEMMA 4. *Suppose that* μ_k, m_k *and* τ_k *are defined as in* §2*. Then*

$$m_{i+1} \le m_i, \tag{12}$$

and

$$\mu_k \le k + \sum_{i=1}^{k-1} m_i + \tau_0 - \tau_k. \tag{13}$$

https://doi.org/10.4153/CMB-1998-028-5 Published online by Cambridge University Press

PROOF. For a given X, let $m_i = m_i(\omega_i)$ denote the multiplicity of the root ω_i of $p^{-\tau_i} f_i'(x) \equiv 0 \pmod p$. In other words, on writing

$$p^{-\tau_i} f_i'(\omega_i + y) = b_0 + b_1 y + \cdots + b_n y^n, \tag{14}$$

with $b_l \in \mathbb{Z}$, we have $b_l \equiv 0 \pmod p$ when $0 \le l \le m_i$ and $b_{m_i} \not\equiv 0 \pmod p$. By (7),

$$p^{-\tau_{i+1}} f_{i+1}'(x) = p^{1-n_i-\tau_{i+1}+\tau_i} p^{\tau-i} f_i'(\omega_i + px), \tag{15}$$

and this polynomial has integer coefficients. By (14),

$$p^{-\tau_{i+1}} f_{i+1}'(x) = p^{1-n_i-\tau_{i+1}+\tau_i}(b_0 + b_1 px + \cdots + b_n p^n x^n), \tag{16}$$

and for $l > m_i$ the coefficient of x^l is divisible by a higher power of p than the coefficient of x^{m_i}. Thus

$$\deg_p\big(p^{-\tau_{i+1}} f_{i+1}'(x)\big) \le m_i,$$

and so for each i,

$$m_{i+1} \le m_i \tag{17}$$

Since the polynomial in (16) has integer coefficients and $p \nmid b_{m_i}$, we have

$$1 - n_i - \tau_{i+1} + \tau_i + m_i \ge 0.$$

Hence

$$n_i \le 1 + m_i - \tau_{i+1} + \tau_i,$$

and so

$$\mu_k = \sum_{i=0}^{k-1} n_i \le k + \sum_{i=0}^{k-1} m_i + \tau_0 - \tau_k.$$

This completes the proof of the lemma.

LEMMA 5. *Suppose* $(q_1, q_2) = 1$. *Then*

$$\sum_{x \bmod q_1 q_2} e\big(f(x)/q_1 q_2\big) = \sum_{y_1 \bmod q_1} e\big(u_1 f(y_1)/q_1\big) \sum_{y_2 \bmod q_2} e\big(u_2 f(y_2)/q_2\big).$$

LEMMA 6. *Suppose* $K > 0$, *then for large* q,

$$K^{\omega(q)} \le q^{\epsilon},$$

where $\omega(q)$ *is the number of distinct prime factor of* q.

https://doi.org/10.4153/CMB-1998-028-5 Published online by Cambridge University Press

PROOF. Let $p_1, p_2, \ldots, p_w$ be the first $\omega(q)$ primes.

$$\vartheta(q) = \sum_{r=1}^{\omega(q)} \log p_r \leq \sum_{p|q} \log p \leq \log q.$$

By the Prime Number Theorem,

$$\vartheta(x) \sim x, \quad \Pi(x) \sim \frac{x}{\log x}.$$

Therefore,

$$p_\omega \leq \log q + o(\log q).$$

Since

$$\begin{aligned}\omega(q) = \Pi(p_w) &\sim \frac{p_\omega}{\log p_\omega} \\ &\leq \frac{\log q}{\log\log q} + o\Big(\frac{\log q}{\log\log q}\Big)\end{aligned}$$

$$\begin{aligned}K^{\omega(q)} &\leq K^{\frac{\log q}{\log\log q} + o(\frac{\log q}{\log\log q})} \\ &\leq \exp\Big(\log q\Big(\frac{\log K}{\log\log q} + o(\frac{\log q}{\log\log q}\Big)\Big) \\ &< \exp(\epsilon \log q)\end{aligned}$$

for large q.

4. Proof of Theorems.

PROOF OF THEOREM 1. When $t = 1$, we use Weil's estimate,

$$|\tilde{S}(p^l, f)| \leq \big(\deg_p(f') - 1\big)p^{\frac{1}{2}} \leq \big(\deg_p(f') - 1\big)p^{t(1-\frac{1}{s})},$$

since $s \geq 2$. Suppose that $t \geq 2$. Since $p > k_1$, we have

$$\tau_i = 0 \quad \text{for each } i, \tag{18}$$

because differentiating f_i one introduces a factor $< p$ in the coefficients. If $X \in B$, then by Lemma 3 we have $m_0 \leq s - 1$. Thus, by (17), $m_i \leq s - 1$ for each i. Now, by (13), $\mu_k \leq sk$ and so $k \geq t/s$. Thus the first double sum in Lemma 2 is bounded by

$$\sum_{k=1}^{\infty} \sum_{X \in B_k} p^{(1-\frac{1}{s})t}. \tag{19}$$

If $X \in C_k$, then $\mu_{k-1} + 2 \leq t = \mu_k + 1$. Hence, by the Weil estimate,

$$|S_k| \leq \big(\deg_p(f_k) - 1\big)p^{\frac{1}{2}},$$

https://doi.org/10.4153/CMB-1998-028-5 Published online by Cambridge University Press

for which see Chapter II of Schmidt (1976). Moreover $t-1 \le sk$. Thus the second double sum in Lemma 2 is bounded by

$$\sum_{k=1}^{\infty} \sum_{X \in C_k} p^{t-\frac{1}{2}-k}\big(\deg_p(f_k)-1\big).$$

This is

$$\le \sum_{k=1}^{\infty} \sum_{X \in C_k} p^{(1-\frac{1}{s})t}\big(\deg_p(f_k)-1\big). \tag{20}$$

The theorem follows from (19), (20) and Lemma 1.

PROOF OF THEOREM 2. First of all, when $t = 1$. Trivially,

$$|\tilde{S}(p^l, f)| = p^{\frac{1}{s}} p^{(1-\frac{1}{s})} = p^{\frac{1}{s}} p^{t(1-\frac{1}{s})}$$

Secondly, suppose $2 \le t \le \tau_0 + 1$. By using the trivial estimate, we have

$$|\tilde{S}(p^l, f)| \le p^t \le p^{\frac{\delta+1}{s}} p^{t(1-\frac{1}{s})}.$$

Thirdly, suppose $t \ge \tau_0 + 2$, we use Lemma 3. By (13),

$$\mu_k = \sum_{i=0}^{k} n_i \le k + \sum_{i=0}^{k-1} m_i + \tau_0 - \tau_k,$$

with all $m_i \le s-1$. Therefore,

$$\mu_k \le sk + \tau_0 - \tau_k.$$

If $X \in B_k$, then

$$\mu_{k-1} + \tau_{k-1} + 2 \le t \le \mu_k.$$

Hence,

$$t \le sk + \tau_0 - \tau_k \le sk + \tau_0. \tag{21}$$

The first double sum in Lemma 2 is bounded by

$$\sum_{k=1}^{\infty} \sum_{X \in B_k} p^{\frac{\tau_0+1}{s}} p^{(1-\frac{1}{s})t}$$

If $X \in C_k$, then

$$\mu_k < t \le \mu_k + \tau_k + 1. \tag{22}$$

Again by (13),

$$t \le sk + \tau_0 - \tau_k + \tau_k + 1 \le sk + \tau_0 + 1.$$

Let $t = \mu_k + \theta$, hence $1 \le \theta \le \tau_k + 1$. Therefore,

$$\begin{aligned} p^{\mu_k - k}|S_k| &\le p^{\mu_k - k} p^{\theta} \\ &= p^{t-k} \\ &\le p^{t-((t-\tau_0-1)/s)} \\ &= p^{\frac{\tau_0+1}{s}} p^{t(1-\frac{1}{s})} \end{aligned}$$

https://doi.org/10.4153/CMB-1998-028-5 Published online by Cambridge University Press

The second double sum in Lemma 2 is bounded by

$$\sum_{k=1}^{\infty}\sum_{X\in C_k} p^{\frac{\tau_0+1}{s}} p^{t(1-\frac{1}{s})}.$$

Hence,

$$\begin{aligned}|\tilde{S}(p^l,f)| &\le p^{\frac{\tau_0+1}{s}t(1-\frac{1}{s})}\Big\{\sum_{k=1}^{\infty}\sum_{X\in B_k} 1+\sum_{k=1}^{\infty}\sum_{X\in C_k} 1\Big\},\\ &\le m(p^{-\tau_0}f')p^{\frac{\tau_0+1}{s}}p^{t(1-\frac{1}{s})}.\end{aligned}$$

This completes the proof of the theorem.

PROOF OF THEOREM 3. Let $p = p_1p_2\cdots p_R$. We divide the proof into two cases.

(i) If $p_i > k$ for all i, then by Theorem 1

$$|\tilde{S}(p_i^{t_i},f)| \le (k_s-1)p_i^{(1-\frac{1}{s})t_i}.$$

By Lemma 5, we have

$$|\tilde{S}(q,f)| \le q^{(1-\frac{1}{s})+\epsilon},$$

for large q.

(ii) If $p_r \le k_1$ and $p_{r+1} > k_1$, then

$$\tilde{S}(p_i^{t_i},f) \le \begin{cases} m(p^{-\tau_0}f')k_s^{\frac{\delta+1}{s}}p_i^{(1-\frac{1}{s})t_i}, & \text{if } i\le r,\\ (k_s-1)p_i^{(1-\frac{1}{s})t_i}, & \text{if } i>r.\end{cases}$$

Note that $m(p^{-\tau_0}f')r \le k_s-1$. By Lemma 5, we have

$$|\tilde{S}(q,f)| \le \Big((k_s-1)k_s^{\frac{\delta+1}{s}}\Big)^{\omega(q)}q^{(1-\frac{1}{s})}.$$

By Lemma 6,

$$\Big((k_s-1)k_s^{\frac{\delta+1}{s}}\Big)^{\omega(q)} < q^{\epsilon},$$

if q is large. Therefore,

$$|\tilde{S}(q,f)| \le q^{(1-\frac{1}{s})+\epsilon}.$$

This completes the proof of the theorem.

REFERENCES

1. J. H. H. Chalk, *On Hua's Estimates for Exponential Sums*, Mathematika (2) **34**(1987), 115–123.
2. Ping Ding, *An improvement to Chalk's Estimation of Exponential Sums*, Acta Arith. **LIX.2**(1991), 149–155.
3. ______, *On Chalk's Estimation of Exponential Sums (II)*, Canad. Math. Bull., (1992), in the course of publication.
4. L. K. Hua, *On an exponential sum*, Chinese J. Math. **2**(1940), 301–312.
5. ______, *On exponential sums*, Sci. Record (Peking) (N.S.) **1**(1957), 1–4.

6. ______, *Die Abschắtzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie*, Enzyklopǎdie Math. Wiss., **Bd I2**(1959), H.13, TI §13, S 41.
7. ______, *Additive Theory of Prime Numbers*, Amer. Math. Soc. **1**, Providence, 1965, 2–7.
8. W. K. A. Loh, *Hua's Lemma*, Bull. Austal. Math. Soc. (3) **50**(1994), 451–458.
9. J. H. Loxton and R. A. Smith, *On Hua's estimate of a complete exponential sums*, J. London Math. Soc. (2) **26**(1982), 15–20.
10. J. H. Loxton and R. C. Vaughan, *The Estimation of Complete Exponential Sums*, Canad. J. Math. (4) **28**(1985), 440–454.
11. L. J. Mordell, *On a sum analogous to a Gauss's sum*, Quart. J. Math. **3**(1932), 161–167.
12. A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34**(1948), 204–207.

https://doi.org/10.4153/CMB-1998-028-5 Published online by Cambridge University Press