Canad. Math. Bull. Vol. **28**(4), 1985

THE ESTIMATION OF COMPLETE EXPONENTIAL SUMS

BY

J. H. LOXTON AND R. C. VAUGHAN

In memoriam Robert A. Smith

ABSTRACT. This paper proves a conjecture of Loxton and Smith about the size of the exponential sum $S(f;q)$ formed by summing $\exp(2\pi i f(x)/q)$ over x mod q, where f is a polynomial of degree n with integer coefficients. It is shown that $|S(f;q)| \leq C_f d_n(q) q^{e/(e+1)}$, where e is the maximum of the orders of the complex zeros of f'. An estimate is also obtained for C_f in terms of n, e and the different of f, and a number of examples are given to show that the estimate is best possible.

1. **Introduction**. Let q be a positive integer and let f be a polynomial of degree n with integer coefficients. This paper is concerned with the exponential sum

$$S(f;q) = \sum_{x \bmod q} e(f(x)/q) \tag{1}$$

where x is taken over a complete set of residues modulo q and $e(t) = \exp(2\pi i t)$.

When $n = 1$ the sum is trivial and, after the work of Gauss [6], the case $n = 2$ is completely understood. The first systematic study of (1) for larger n is by Hardy and Littlewood [7, 8]. In the case $f(x) = ax^n$ with $(a,q) = 1$ they obtained the bound

$$|S(ax^n;q)| \leq C_n q^{1-1/n} \quad ((a,q) = 1), \tag{2}$$

and their argument readily gives $C_n = n^{n^6}$ (see Vinogradov [19]). They also showed that

$$S(ax^n;p^{mn}) = p^{m(n-1)} \quad (p > n, p \nmid a), \tag{3}$$

so that (2) is essentially best possible. The bound (2) has been sharpened by Stechkin [16] who obtained $C_n = \exp(C(n/\phi(n))^2)$.

Another special case that has been extensively studied is that of $f(x) = ax^n + bx$ with $(a,q) = 1$. As in the work of Hardy and Littlewood this special case was studied in connection with Waring's problem. Davenport and Heilbronn [4, 5] showed that

$$S(ax^n + bx;q) \ll_\epsilon q^{\theta+\epsilon}(q,b) \quad ((a,q) = 1) \tag{4}$$

with $\theta = 2/3$ when $n = 3$ and $\theta = 3/4$ when $n \geq 4$.

Let $C(f)$ denote the content of $f(x) - f(0)$. When $p \nmid C(f)$ the estimate

Received by the editors November 2, 1984 and, in revised form, February 25, 1985.
This research was supported in part by the Australian Research Grants Scheme.
AMS Subject Classification: 10G10, 12B05.

$$(5) \qquad |S(f;p)| \leq (n-1)p^{1/2} \quad (p \nmid C(f))$$

is a well known consequence of the work of Weil [20] on the Riemann hypothesis for curves over finite fields (see, for example, Schmidt [15]). By making use of (5), Hua [10] showed that it is possible to take

$$(6) \qquad \theta = \tfrac{1}{2}$$

in (4) (see Lemma 4.1 of Vaughan [18]). (The earlier work of Davenport and Heilbronn was based on the ideas underlying Mordell's estimate [12].)

When $p < (n-1)^2$ the bound (5) is worse than trivial. Very probably

$$(7) \qquad |S(f;p)| \ll (np)^{1/2} \quad (p \nmid C(f)).$$

It follows at once from Mordell's argument (see Anderson and Stiffler [1]) that

$$(8) \qquad \max_{f;p\nmid C(f),\deg f \leq n} |S(f;p)| > \left[(n!)^2\binom{p}{n} - p^n\right]^{1/2n}$$

and so (7) would be essentially best possible. It is worth pointing out that

$$\sum_{a=1}^{p-1} |S(ax^n;p)|^2 = p(p-1)((n,p-1)-1)$$

so that when $p \equiv 1 \pmod n$ one obtains the sharper lower bound $((n-1)p)^{1/2}$.

For a general polynomial f of degree n with integer coefficients the principal interest is to obtain an upper bound for $|S(f;q)|$ that is uniform for a large class of f with respect to n and q. Hardy and Littlewood [7] obtained $S(f;q) \ll_\epsilon q^{1-2^{1-n}+\epsilon}$ uniformly for f with leading coefficient coprime with q by adapting a method introduced by Weyl [21] for estimating exponential sums. Hua [9] improved on this by showing that for each fixed $\epsilon > 0$,

$$(9) \qquad S(f;q) \ll q^{1-1/n+\epsilon} \quad ((q,C(f)) = 1),$$

and adumbrates an argument on p. 304 that, after the work of Weil [20], enables one to take $\epsilon = 0$ in (9). Thus Nechaev [13], Chen [2], Nechaev [14], Chen [3] and Stechkin [17] have successively obtained

$$(10) \qquad |S(f;q)| \leq C_n q^{1-1/n} \quad ((q,C(f)) = 1)$$

with $C_n = \exp(2^n)(n \geq 12)$, $\exp(Cn^2)$, $\exp(5n^2/\log n)(n \geq 3)$, $\exp(nD_n)(D_n \leq 6.1, D_n \leq 4(n \geq 10))$ and $\exp(n + O(n/\log n))$ respectively.

Of course it is immediate from (10) that

$$(11) \qquad |S(f;q)| \leq C_n q^{1-1/n}(q,C(f))^{1/n}$$

In view of the example (3) this is essentially best possible. However, in view of (4) (with (6)) and (5) one might hope frequently to do better. Recently Loxton and Smith [11] have obtained a bound for $S(f;q)$ which improves on (11) in nearly all cases. Given a polynomial of degree m,

https://doi.org/10.4153/CMB-1985-053-7 Published online by Cambridge University Press

(12) $$F(x) = a_0x^m + a_1x^{m-1} + \ldots + a_m$$

with integer coefficients, write

(13) $$F(x) = a_0 \prod_{\xi} (x - \xi)^{e_\xi}$$

where the ξ are the distinct zeros of F, and e_ξ is the multiplicity of ξ, so that $\sum_\xi e_\xi = m$. The *semi-discriminant* Δ of F is defined by

(14) $$\Delta(F) = a_0^{2n-2} \prod_{\xi \neq \eta} (\xi - \eta)^{e_\xi e_\eta}$$

where the product is over all ordered pairs ξ, η of zeros of F with $\xi \neq \eta$. Let

(15) $$e(F) = \max_{\xi} e_\xi.$$

Loxton and Smith show that

(16) $$|S(f;q)| \leqslant d_{n-1}(q)q^{1-1/2e}(\Delta, q)^{1/2e}$$

where

(17) $$e = e(f'), \quad \Delta = \Delta(f').$$

This gives a smaller bound than (11) when $e < n/2$ and q is large in terms of f. Also, in the case $f(x) = ax^n + bx$ with $(a,q) = 1$, (16) gives a bound of the same quality as (4) with (6).

Loxton and Smith further conjecture that

(18) $$|S(f;q)| \leqslant c_f d_{n-1}(q)q^{e/(e+1)}$$

and this fits very well with the evidence of (2), (3), (4) with (6), (5) and (8). The object of this paper is to prove this conjecture and obtain a good estimate for c_f.

The quantity Δ appearing in (16) is used as a measure of the local separation of the zeros of f'. However, it is somewhat inefficient for this purpose and in some cases can be excessively large. For example, when $p > n$, the argument of Lemma 4.1 of Vaughan [18] gives

(19) $$S(x^n - nxp^{m(n-1)}; p^{mn}) = p^{m(n-1)},$$

whereas (16) only gives

(20) $$|S(x^n - nxp^{m(n-1)}; p^{mn})| \leqslant np^{mn/2+(n-2)(n-1)m/2}$$

which is worse than trivial when $n \geqslant 4$.

In order to give a better measure of the local spacing of the zeros of f' we instead build on the *different* $\mathfrak{D}$ introduced in Theorems 2 and 3 of Loxton and Smith. Let F be as in (12) and let K denote the algebraic number field generated by the roots of F. Let ord_p denote any extension to K of the additive p-adic valuation, normalized so that $\text{ord}_p\, p = 1$. For a given prime p define

(21) $$\delta(F;\xi) = \delta_p(F;\xi) = \mathrm{ord}_p\,(F^{(e_\xi)}(\xi)/e_\xi!),$$

(22) $$\delta(F) = \delta_p(F) = \max_\xi \delta_p(F;\xi).$$

Note that

(23) $$\frac{F^{(e_\xi)}(\xi)}{e_\xi!} = a_0 \prod_{\eta,\,\eta\neq\xi} (\xi - \eta)^{e_\eta}$$

where the product is over all distinct roots η of F with $\eta \neq \xi$. Now define $\mathfrak{D}(F)$ to be the intersection of the fractional ideals generated by the numbers $F^{(e_\xi)}(\xi)/e_\xi!$. Then

(24) $$\delta(F) = \mathrm{ord}_p\, \mathfrak{D}(F).$$

Note that $\mathfrak{D}(F)$ is an integral ideal because at least one of the numbers (23) is a p-adic integer.

The bulk of this paper is taken up with establishing

THEOREM 1. *Let f be a polynomial of degree $n \geq 2$ with integer coefficients, let* $\delta = \mathrm{ord}_p\,(\mathfrak{D}(f'))$, *and let*

$$\tau = \begin{cases} 1 & \text{when } p \leq n, \\ 0 & \text{when } p > n. \end{cases}$$

Then

$$|S(f;p^\alpha)| \leq (n - 1)p^{(\alpha e+\delta+\tau)/(e+1)}.$$

In the special case $f(x) = x^n - nxp^{m(n-1)}$, $p > n$, the above theorem gives

(25) $$|S(x^n - nxp^{m(n-1)};p^{mn})| \leq (n - 1)p^{m(n-1)}.$$

Indeed, by inspecting the proof for the particular polynomial in question, it is possible to replace the right hand side of this inequality by $p^{m(n-1)}$. This can be compared with (19) and (20).

For a given positive rational integer q we define

(26) $$(\mathfrak{D}(F), q) = \prod_p p^{\min(\mathrm{ord}_p \mathfrak{D}(F),\, \mathrm{ord}_p(q))}.$$

Note that fractional exponents may occur.

Also, whenever $(q_1, q_2) = 1$ we have

(27) $$S(f;q_1q_2) = S(u_1f, q_1)S(u_2f, q_2)$$

where $u_1q_2 + u_2q_1 \equiv 1 \pmod{q_1q_2}$. The following theorem is an immediate consequence of Theorem 1, (26) and (27).

THEOREM 2. *Suppose that f is a polynomial of degree $n \geq 2$ with integer coefficients. Then*

https://doi.org/10.4153/CMB-1985-053-7 Published online by Cambridge University Press

$$|S(f;q)| \leqslant \exp\left(\frac{\vartheta(n)}{e+1}\right)(n-1)^{\omega(q)}(\mathscr{D}(f'),q)^{1/(e+1)}q^{e/(e+1)}$$

where $\vartheta(n) = \sum_{p \leqslant n} \log p$ *and* $\omega(q) = \sum_{p|q} 1$.

We remark that in some circumstances δ can still be too large, particularly when the maximum in (22) occurs for a ξ for which $e_\xi < e$. By following up the remark after Lemma 1 below it is possible to prove Theorem 1 with δ replaced by

$$\delta^* = \delta_p^* = \max_{i \geqslant 0} \max_{\xi} (\delta_p(f',\xi) + i(e_\xi - e)) \tag{28}$$

and Theorem 2 with $(\mathscr{D}(f'),q)$ replaced by

$$\prod_p p^{\min(\delta_p^*, \operatorname{ord}_p q)}. \tag{29}$$

In §2 we give a construction, related to the p-adic approximation to the roots of f', which is basic to the proof of Theorem 1, and establish some properties of the approximations. In §3 we show how the p-adic approximations relate to $S(f;p^\alpha)$, and estimate the sum in certain special cases. We complete the proof of Theorem 1 in §4.

In §5 we give some examples which show that in many situations Theorem 1 is essentially best possible.

2. **The sequences of p-adic approximations**. Let p be a prime and f be a polynomial with $p \nmid C(f)$. We define a sequence of polynomials f_i and a sequence of non-negative integers x_i inductively, as follows.

Let $f_0 = f$. Given f_i we choose a non-negative integer τ_i so that the polynomial $p^{-\tau_i} f_i'$ has integer coefficients but p does not divide its content, and we choose r_i to be any residue class modulo p for which $p^{-\tau_i} f_i'(r_i) \equiv 0 \pmod p$. Now let x_i be the least non-negative integer in r_i for which $\operatorname{ord}_p (\sum_{j=0}^{i} x_j p^j - \xi) \leqslant i + 1$ for each root ξ of f'. If no such x_i (i.e. r_i) exists, then the sequences terminate with f_i and x_{i-1}, with the obvious interpretation if x_0 does not exist. When such an x_i does exist we choose the non-negative integer σ_i so that the polynomial $p^{-\sigma_i}\{f_i(x_i + px) - f_i(x_i)\}$ has integer coefficients but p does not divide its content, and we set

$$f_{i+1}(x) = p^{-\sigma_i}\{f_i(x_i + px) - f_i(x_i)\}.$$

At each stage of the construction there may be several choices for r_i and hence for x_i, so it may be possible to construct many such sequences. We denote by $\mathscr{A}$ the set of all sequences $\mathscr{X} = \{x_i\}$ which can be constructed in this way and we write $f_i(x;\mathscr{X})$, $\sigma_i(\mathscr{X})$ and $\tau_i(\mathscr{X})$ for the associated quantities arising in the construction of $\mathscr{X}$. For convenience we will often suppress the $\mathscr{X}$ in the notation. If there is no x_0 satisfying $p^{-\tau_0} f'(x_0) \equiv 0 \pmod p$, then $\mathscr{A}$ is empty.

We further define

$$\Sigma_0(\mathscr{X}) = 0, \quad \Sigma_i(\mathscr{X}) = \sum_{j=0}^{i-1} \sigma_j(\mathscr{X}) \quad (i \geqslant 1)$$

and

$$X_i(\mathscr{X}) = \sum_{j=0}^{i-1} x_j p^j.$$

Then the polynomials $f_i(x, \mathscr{X})$ are given by

$$f_i(x, \mathscr{X}) = p^{-\Sigma_i}\{f(X_i + p^i x) - f(X_i)\}$$

We first of all establish some bounds for $\sigma_i(\mathscr{X})$, $\tau_i(\mathscr{X})$ and $\Sigma_i(\mathscr{X})$.

LEMMA 1. *Let f be a polynomial of degree $n \geqslant 2$ with integer coefficients and let p be a prime with $p \nmid C(f)$. Let $e = e(f')$ and $\delta = \delta(f')$, and let $\mathscr{X}$ be constructed as above. Then*

(i) $2 \leqslant \sigma_i(\mathscr{X}) \leqslant n$,

(ii) $0 \leqslant \tau_i(\mathscr{X}) \leqslant [\log n/\log p]$,

(iii) $\Sigma_i(\mathscr{X}) + \tau_i(\mathscr{X}) \leqslant i(e + 1) + \delta$.

We remark that the proof of (iii) will enable one to replace the right hand side by $\max_{f'(\xi)=0} (i(e_\xi + 1) + \delta_p(f'; \xi))$ which is sometimes sharper.

PROOF. The first inequality $\sigma_i(\mathscr{X}) \geqslant 2$ is a trivial consequence of the definition of x_i, and the upper bound $\sigma_i(\mathscr{X}) \leqslant n$ follows from the observation that if $f_i(x) = \sum_{k=0}^n a_k x^k$, then $f_i(x_i + px) - f_i(x_i) = \sum_{k=1}^n b_k p^k x^k$ with $b_n = a_n$, $b_{n-1} = a_{n-1} + a_n\binom{n}{n-1}x_i$, and so on.

The inequalities in (ii) follow at once from the fact that for some integer m with $1 \leqslant m \leqslant n$ we have $p^{\tau_i} \mid m$.

The third assertion is the most important and is somewhat more delicate. We define

$$\mu_i = \max_{\xi} \operatorname{ord}_p (X_i - \xi)$$

where the maximum is taken over the distinct roots ξ of f'. Note that by the construction of x_i we have $\mu_i \leqslant i$. Let ϵ_i denote the total multiplicity of the roots ρ for which this maximum is attained. Further, let

$$\lambda_i = \operatorname{ord}_p f^{(\epsilon_i+1)}(\rho)/\epsilon_i!$$

where ρ is used to indicate one of these roots. We have

$$f^{(\epsilon_i+1)}(\rho)/\epsilon_i! = a_0 \prod_{\eta} (\rho - \eta)^{e_\eta} + \dots$$

where η is used to indicate roots η of f' with $\operatorname{ord}_p (X_i - \eta) < \mu_i$, and the terms indicated by the dots have larger p-adic order than the main term. Thus

$$\lambda_i = \operatorname{ord}_p \left(a_0 \prod_{\eta} (\rho - \eta)^{e_\eta}\right) = \operatorname{ord}_p \left(a_0 \prod_{\eta} (X_i - \eta)^{e_\eta}\right)$$

and so is independent of the choice of ρ. Hence

$$\begin{aligned}\operatorname{ord}_p f'(X_i) &= \operatorname{ord}_p\left(a_0 \prod_{\eta} (X_i - \eta)^{e_\eta} \prod_{\rho} (X_i - \rho)^{e\rho}\right)\\ &= \lambda_i + \sum_{\rho} e_\rho \mu_i\\ &= \lambda_i + \epsilon_i \mu_i.\end{aligned}$$

On the other hand

$$\Sigma_i + \tau_i - i = \min_{k \geq 0} \{\operatorname{ord}_p (p^{ik} f^{(k+1)}(X_i)/k!)\}.$$

Thus

$$\Sigma_i + \tau_i \leq \lambda_i + \epsilon_i \mu_i + i.$$

We also have

$$\frac{f^{(e_\rho+1)}(\rho)}{e_\rho!} = a_0 \prod_{\xi} (\rho - \xi)^{e_\xi}$$

where the product is over the zeros ξ of f' with $\xi \neq \rho$. When $\operatorname{ord}_p (X_i - \xi) = \mu_i$ we have $\operatorname{ord}_p (\rho - \xi) \geq \mu_i$ and when $\operatorname{ord}_p (X_i - \xi) < \mu_i$ we have $\operatorname{ord}_p (\rho - \xi) = \operatorname{ord}_p (X_i - \xi)$. Thus

$$\delta \geq \operatorname{ord}_p \frac{f^{(e_\rho+1)}(\rho)}{e_\rho!} \geq \lambda_i + \mu_i(\epsilon_i - e_\rho) \geq \Sigma_i + \tau_i - i - \mu_i e_\rho.$$

Hence

$$\Sigma_i + \tau_i \leq \delta + i + \mu_i e_\rho \leq \delta + i(1 + e).$$

For a positive integer α with $\alpha \geq \tau + 3$ we define subsets $\mathcal{B}_k = \mathcal{B}_k(\alpha)$, $\mathcal{C}_k = \mathcal{C}_k(\alpha)$ and $\mathcal{E}_k = \mathcal{E}_k(\alpha)$ of the set $\mathcal{A}$, as follows. Let $\mathcal{B}_k$ denote the subset of $\mathcal{A}$ formed from those sequences $\mathcal{X}$ with at least k elements and satisfying

$$\Sigma_{k-1} (\mathcal{X}) + \tau_{k-1}(\mathcal{X}) + 3 \leq \alpha \quad \text{and} \quad \Sigma_k (\mathcal{X}) \geq \alpha.$$

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

$$\Sigma_{k-1} (\mathcal{X}) + \tau_{k-1}(\mathcal{X}) + 3 \leq \alpha \quad \text{and} \quad \Sigma_k (\mathcal{X}) < \alpha < \Sigma_k (\mathcal{X}) + \tau_k(\mathcal{X}) + 3.$$

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

$$\Sigma_k (\mathcal{X}) + \tau_k(\mathcal{X}) + 3 \leq \alpha.$$

Since $\Sigma_i(\mathcal{X}) + \tau_i(\mathcal{X})$ 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 $\mathcal{D}_k = \mathcal{B}_k \cup \mathcal{C}_k$. By Lemma 1, (i), the sets $\mathcal{B}_k$, $\mathcal{C}_k$, $\mathcal{D}_k$, $\mathcal{E}_k$ are empty for all sufficiently large k.

When g is a polynomial with integer coefficients, not all divisible by p, we denote by $\deg_p(g)$ the degree of g modulo p, that is, the largest integer k for which the coefficient of x^k in g is not divisible by p. Set

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

LEMMA 2. *Let p be a prime and let f be a polynomial with integer coefficients and $p \nmid C(f)$. Then*

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

PROOF. We show by induction on K that

$$\sum_{k=1}^{K} \sum_{\mathscr{X} \in \mathscr{D}_k} N_k + \sum_{\mathscr{X} \in \mathscr{E}_k} N_k \leq \deg_p(p^{-\tau_0} f').$$

The lemma then follows because $\mathscr{E}_K$ is empty for large K. The inductive step will follow if we show that

$$\sum_{\mathscr{X} \in \mathscr{D}_{K+1} \cup \mathscr{E}_{K+1}} N_{K+1} \leq \sum_{\mathscr{X} \in \mathscr{E}_K} deg_p(p^{-\tau_K} f_K')$$

and this in turn will follow if we establish the inequality

$$\sum_{\substack{x_i \\ p^{-\tau_i} f_i'(x_i) \equiv 0 \pmod p}} n_{i+1} \leq \deg_p(p^{-\tau_i} f_i') \tag{30}$$

with

$$n_{i+1} = \begin{cases} \max(1, \deg_p(p^{-\tau_{i+1}} f_{i+1}'), \deg_p(f_{i+1}) - 1) & \text{when } \tau_i = 0, \\ \max(1, \deg_p(p^{-\tau_{i+1}} f_{i+1}')) & \text{otherwise.} \end{cases}$$

Moreover the case $i = 0$ of (30) yields the case $K = 1$ of the inductive hypothesis.

We prove (30) by adapting an argument of Hua [9]. Let x_i be a root of $p^{-\tau_i} f_i'(x)$ modulo p with multiplicity m_i. Then we can write

$$p^{-\tau_i} f_i'(x_i + x) = b_0 + b_1 x + \ldots + b_n x^n$$

where the b_j are integers, $b_j \equiv 0 \pmod p$ when $0 \leq j \leq m_i - 1$ and $b_{m_i} \not\equiv 0 \pmod p$. Now

$$f_{i+1}(x) = p^{-\sigma_i}(f_i(x_i + px) - f_i(x_i)).$$

Thus

$$p^{-\tau_{i+1}} f_{i+1}'(x) = p^{1-\sigma_i - \tau_{i+1} + \tau_i} \cdot p^{-\tau_i} f_i'(x_i + px)$$

https://doi.org/10.4153/CMB-1985-053-7 Published online by Cambridge University Press

and this polynomial also has integer coefficients. For $k > m_i$ the coefficient of x^k is divisible by a higher power of p than the coefficient of x^{m_i}, so

$$\deg_p (p^{-\tau_{i+1}} f'_{i+1}) \leqslant m_i .$$

Again the coefficient of x^{m_i} is a p-adic integer, so $1 - \sigma_i - \tau_{i+1} + \tau_i + m_i \geqslant 0$. Note also that $\deg_p (f_{i+1}) \leqslant \sigma_i$ from the equation defining f_{i+1}. Thus, when $\tau_i = 0$ we have

$$\deg_p (f_{i+1}) \leqslant \sigma_i \leqslant m_i + 1.$$

Taken together, these inequalities give

$$n_{i+1} \leqslant m_i .$$

Moreover the sum of the multiplicities m_i, taken over all the roots x_i of $p^{-\tau_i} f'_i(x)$ modulo p, is at most $\deg_p (p^{-\tau_i} f'_i)$ and this establishes the required inequality.

3. **The reduction of the exponential sum and a special case.**

LEMMA 3. *Let p be a prime and let f be a polynomial with integer coefficients and $p \nmid C(f)$. If $\alpha \geqslant \tau_0 + 3$, then*

$$S(f;p^\alpha) = \sum_{k=1}^{\infty} \sum_{\mathscr{X} \in \mathscr{B}_k} e(f(X_k)p^{-\alpha})p^{\alpha-k} + \sum_{k=1}^{\infty} \sum_{\mathscr{X} \in \mathscr{C}_k} e(f(X_k)p^{-\alpha})p^{\Sigma_k - k} S(f_k; p^{\alpha - \Sigma_k}).$$

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

PROOF. We show by induction on K that

$$S(f;p^\alpha) = \sum_{k=1}^{K} \sum_{\mathscr{X} \in \mathscr{B}_k} e(f(X_k)p^{-\alpha})p^{\alpha-k} + \sum_{k=1}^{K} \sum_{\mathscr{X} \in \mathscr{C}_k} e(f(X_k)p^{-\alpha}(p^{\Sigma_k - k} S(f_k;p^{\alpha-\Sigma_k})$$

$$+ \sum_{\mathscr{X} \in \mathscr{E}_K} e(f(X_K)p^{-\alpha})p^{\Sigma_K - K} S(f_K;p^{\alpha-\Sigma_K}).$$

We first establish the case $K = 1$. We have

$$S(f;p^\alpha) = \sum_{\substack{x \bmod p^\alpha \\ p^{\tau_0+1} | f'(x)}} e(f(x)p^{-\alpha}) + \sum_{\substack{x \bmod p^\alpha \\ p^{\tau_0+1} \nmid f'(x)}} e(f(x)p^{-\alpha}).$$

The second sum here is

$$\sum_{\substack{u \bmod p^{\alpha-\tau_0-1} \\ p \nmid p^{-\tau_0} f'(u)}} \sum_{v \bmod p^{\tau_0+1}} e(f(u + p^{\alpha-\tau_0-1}v)p^{-\alpha})$$

and this can be rewritten as

$$\sum_{u,v} e\Big(f(u)p^{-\alpha} + p^{-\tau_0} f'(u) v p^{-1} + \dots$$

$$+ p^{-\tau_0} f^{(k)}(u) \frac{v^k}{k!} p^{(k-1)(\alpha-\tau_0-2)+k-2} + \dots\Big).$$

For $k \geqslant 2$ we have $\operatorname{ord}_p(k!) \leqslant 2k - 3$. Moreover the polynomials $p^{-\tau_0} f^{(k)}(x)$ have integer coefficients. Hence when $\alpha \geqslant \tau_0 + 3$ the double sum above is

$$\sum_{\substack{u \bmod p^{\alpha-\tau_0-1} \\ p \nmid p^{-\tau_0} f'(u)}} e(f(u)p^{-\alpha}) \sum_{v \bmod p^{\tau_0+1}} e(p^{-\tau_0} f'(u) v p^{-1}) = 0.$$

When $\mathscr{A}$ is empty there are no solutions to $p^{-\tau_0} f'(x) \equiv 0 \pmod p$ and so $S(f; p^\alpha) = 0$. This establishes the second part of the lemma. Otherwise

$$S(f; p^\alpha) = \sum_{x_0} \sum_{\substack{x \bmod p^\alpha \\ x \equiv x_0 (\bmod p)}} e(f_0(x) p^{-\alpha})$$

$$= \sum_{x_0} e(f(x_0)p^{-\alpha}) \sum_{x \bmod p^{\alpha-1}} e(f_1(x) p^{\sigma_0 - \alpha}).$$

The terms with $\Sigma_1 = \sigma_0 \geqslant \alpha$ contribute

$$\sum_{\mathscr{X} \in \mathscr{B}_1} e(f(X_1)p^{-\alpha}) p^{\alpha-1}$$

The terms with $\Sigma_1 < \alpha$ are of two kinds, those with $\mathscr{X} \in \mathscr{C}_1$ and those with $\mathscr{X} \in \mathscr{E}_1$. For each kind the summand is

$$e(f(X_1)p^{-\alpha}) p^{\Sigma_1 - 1} S(f_1; p^{\alpha - \Sigma_1}).$$

This establishes the case $K = 1$ of the inductive hypothesis. Now suppose that the inductive hypothesis holds for some $K \geqslant 1$. Consider the sum

$$\sum_{\mathscr{X} \in \mathscr{E}_K} e(f(X_K)p^{-\alpha}) p^{\Sigma_K - K} S(f_K; p^{\alpha - \Sigma_K}).$$

By repeating the argument used above, we see that for $\mathscr{X} \in \mathscr{E}_K$ we have $S(f_K; p^{\alpha - \Sigma_K}) = 0$ unless there is an x_K such that $p^{-\tau_K} f_K'(x_K) \equiv 0 \pmod p$. In that case the summand corresponding to $\mathscr{X}$ in the above sum is

$$\sum_{x_K} e(f(X_{K+1})p^{-\alpha}) p^{\alpha - K - 1} \quad \text{or} \quad \sum_{x_K} e(f(X_{K+1})p^{-\alpha}) p^{\Sigma_{K+1} - K - 1} S(f_{K+1}; p^{\alpha - \Sigma_{K+1}})$$

according as $\Sigma_{K+1} \geqslant \alpha$ or $\Sigma_{K+1} < \alpha$. This leads to the desired conclusion.

The reduction step can also be made to work in the case $\alpha = \tau_0 + 2$.

LEMMA 4. *Let p be a prime and let f be a polynomial with integer coefficients and $p \nmid C(f)$. If $\alpha = \tau_0 + 2$, then*

$$|S(f; p^\alpha)| \leqslant p^{\alpha-1} \deg_p (p^{-\tau_0} f').$$

PROOF. Suppose first that $p > 2$. When $k \geqslant 3$ we have $\operatorname{ord}_p(k!) \leqslant k - 2$. Moreover $\operatorname{ord}_p(2!) = 0$. Hence, by the argument used in the first part of the proof of Lemma 3 we have

$$S(f;p^\alpha) = \sum_{\substack{u \bmod p \\ p \mid p^{-\tau_0} f'(u)}} p^{\tau_0+1} e(f(u)p^{-\alpha}).$$

The congruence $p^{-\tau_0} f'(u) \equiv 0 \pmod p$ has at most $\deg_p (p^{-\tau_0} f')$ solutions. This gives the desired conclusion.

Suppose now that $p = 2$. Then

$$S(f;2^\alpha) = \sum_{u \bmod 2} \sum_{v \bmod 2^{\tau_0+1}} e(f(u+2v)2^{-\tau_0-2})$$

$$= \sum_{u \bmod 2} e(f(u)2^{-\tau_0-2}) \sum_{v \bmod 2^{\tau_0+1}} e\Big(\sum_{k \geq 1} 2^{-\tau_0} f^{(k)}(u) v^k 2^{k-2}/k!\Big).$$

The exact power of 2 dividing $k!$ is $k - 1$ when k is a power of 2 and less than $k - 1$ in all other cases. Consequently, the terms in the sum over k are all integers except possibly for those in which k is a power of 2, and these have denominator at most 2. The summand over v is always 1 when v is even and it is $(-1)^{\chi(u)}$ with

$$\chi(u) = \sum_{\substack{k=2^\ell \\ \ell \geq 0}} 2^{-\tau_0} f^{(k)}(u) 2^{k-1}/k!$$

when v is odd. Thus

$$S(f;2^\alpha) = \sum_{\substack{u \bmod 2 \\ 2 \mid \chi(u)}} 2^{\tau_0+1} e(f(u)2^{-\tau_0-2}).$$

When $\deg_2 (2^{-\tau_0} f') \geq 2$ the conclusion is trivial. When $\deg_2 (2^{-\tau_0} f') = 1$ we have $2^{-\tau_0} f'(x) \equiv a + x \pmod 2$ where a is a constant. Thus $\chi(u) \equiv a + u + 1 \pmod 2$. Hence the summation condition is satisfied by only one choice of u. Thus

$$|S(f;2^\alpha)| \leq 2^{\alpha-1} \deg_2 (2^{-\tau_0} f')$$

as required. When $\deg_2 (2^{-\tau_0} f') = 0$ we have $2^{-\tau_0} f'(x) \equiv 1 \pmod 2$ and the summation condition is never satisfied. Thus $S(f;2^\alpha) = 0 = 2^{\alpha-1} \deg_2 (2^{-\tau_0} f')$ which proves the lemma in this case also.

4. **The proof of Theorem 1**. It clearly suffices to establish the theorem in the case $p \nmid C(f)$.

The argument is divided into a number of cases. First of all we suppose that $\alpha = 1$. By (5) we have

$$|S(f;p^\alpha)| \leq (n-1)p^{1/2} \leq (n-1)p^{\alpha e/(e+1)}.$$

This establishes the case $\alpha = 1$.

Next suppose that $2 \leq \alpha \leq \tau_0 + 1$. Since $\tau_0 \leq (\log n)/(\log p)$ and $\tau_0 \leq \delta$, we have $\tau = 1$ and $\alpha \leq \delta + \tau$. Hence a trivial estimate gives

$$|S(f;p^\alpha)| \leq p^\alpha \leq p^{\alpha-(\alpha-\delta-\tau)/(e+1)}.$$

Thirdly we suppose that $\alpha = \tau_0 + 2$. Then $\alpha \leqslant \delta + 2$ and Lemma 4 gives

$$|S(f;p^\alpha)| \leqslant (n-1)p^{\alpha-1} \leqslant (n-1)p^{\alpha-(\alpha-\delta)/(e+1)}.$$

In the fourth case $\alpha \geqslant \tau_0 + 3$, we use Lemma 3. For a sequence $\mathscr{X}$ in $\mathscr{B}_k$ we have $\alpha \leqslant \Sigma_k$. Hence, by Lemma 1 the contribution from $\mathscr{X}$ is bounded by

$$|e(f(X_k)p^{-\alpha})p^{\alpha-k}| \leqslant p^{\alpha-(\alpha-\delta)/(e+1)}.$$

The contribution from a sequence $\mathscr{X}$ in $\mathscr{C}_k$ is

$$C_k \text{ (say)} = e(f(X_k)p^{-\alpha})p^{\Sigma_k-k}\, S(f_k; p^{\alpha-\Sigma_k})$$

and we have $0 < \alpha - \Sigma_k \leqslant \tau_k + 2$. We now argue in a similar manner to the previous cases.

When $\alpha - \Sigma_k = 1$ and $\tau_{k-1} > 0$ we have $\tau = 1$. Thus, again by Lemma 1, we have

$$|C_k| \leqslant p^{\alpha-k} \leqslant p^{\alpha-(\alpha-\delta-\tau)/(e+1)}.$$

When $\alpha - \Sigma_k = 1$ and $\tau_{k-1} = 0$, Lemma 1 gives $k \geqslant (\alpha - \delta - 1)/(e+1)$. We have $p \nmid C(f_k)$. Hence, by (5) with f replaced by f_k we have

$$\begin{aligned}|C_k| &\leqslant (\deg_p(f_k) - 1)p^{\alpha-k-1/2}\\ &\leqslant (\deg_p(f_k) - 1)p^{\alpha-(\alpha-\delta)/(e+1)}.\end{aligned}$$

When $2 \leqslant \alpha - \Sigma_k \leqslant \tau_k + 1$ we have, by Lemma 1, $\alpha \leqslant \Sigma_k + \tau_k + 1 \leqslant k(e+1) + \delta + 1$ and $\tau = 1$ so that trivially we have

$$|C_k| \leqslant p^{\alpha-k} \leqslant p^{\alpha-(\alpha-\delta-1)/(e+1)}.$$

Finally, when $\alpha - \Sigma_k = \tau_k + 2$, Lemma 1 gives $\alpha \leqslant k(e+1) + \delta + 2$. Hence, by Lemma 4 with f replaced by f_k and α by $\alpha - \Sigma_k$, we have

$$|C_k| \leqslant \deg_p(p^{-\tau_k}f_k')p^{\alpha-k-1} \leqslant \deg_p(p^{-\tau_k}f_k')p^{\alpha-(\alpha-\delta)/(e+1)}.$$

On combining the contributions of all the sequences we obtain

$$|S(f;p^\alpha)| \leqslant \sum_{k=1}^{\infty} \sum_{\mathscr{X}\in\mathscr{D}_k} N_k(\mathscr{X})p^{\alpha-(\alpha-\delta-\tau)/(e+1)}.$$

Hence, by Lemma 2,

$$|S(f;p^\alpha)| \leqslant (n-1)p^{(\alpha e+\delta+\tau)/(e+1)}$$

which establishes the theorem.

5. **Some examples**. We give here some examples which show that Theorem 1 is essentially best possible.

When $p \geqslant 3$ it is classical that

$$\left|\sum_{x=1}^{p^\alpha} e(x^2/p^\alpha)\right| = p^{\alpha/2}$$

so that the theorem is certainly best possible when $e = 1$ and $n = 2$. For $e = 1$ and $n \geqslant 2$ consider $f(x) = x^n - nx$. Then $f'(x) = n(x^{n-1} - 1)$ and $f''(x) = n(n-1)x^{n-2}$. Following the definitions of §2 (except that we replace the condition $\text{ord}_p\,(\sum_{j=0}^{i} x_j p^j - \xi) \leqslant i + 1$, which is only used in Lemma 1, by the condition $-p/2 < x_i \leqslant p/2$) and assuming that $p > p_0(n)$ and $(p-1, n-1) = (2, n-1)$ we find that $X_i = 1$ when $n - 1$ is odd and $X_i = \pm 1$ when $n - 1$ is even. Moreover $f(X_i) = -X_i(n-1) = \mp(n-1)$, $f'(X_i) = 0$, $f''(X_i) = X_i n(n-1) = \pm n(n-1)$, $\tau_i = 0$, $\Sigma_i = 2i$.

Now, by Lemma 3, given $\alpha \geqslant 3$ we see that $S(f; p^\alpha)$ is the sum of one or two terms of the form

$$e(f(X_k)p^{-\alpha})p^k S(f_k; p^{\alpha-2k})$$

where $k = [(\alpha-1)/2]$ and $f_k(x) = p^{-2k}(f(X_k + p^k x) - f(X_k))$. For $\alpha \geqslant 6$ we have $f_k(x) \equiv \pm\binom{n}{2}x^2 \pmod{p^{\alpha-2k}}$. Hence for $\alpha \geqslant 6$ and α even it follows that $S(f; p^\alpha)$ is the sum of one or two terms of the form $e(\mp(n-1)p^{-\alpha})p^{\alpha/2}$. Thus for $p > p_0(n)$ and $(p-1, n-1) = (2, n-1)$ we obtain, for even $\alpha \geqslant 6$,

$$|S(f; p^\alpha)| > \tfrac{1}{2}p^{\alpha/2}.$$

By a slightly more careful analysis this example can be extended to all even α, and to odd $\alpha \geqslant 3$ when either n is even or $2 \| n - 1$ and $p \equiv 1 \pmod 4$.

In the next example we suppose that $p > p_0(n)$ and $n > e \geqslant 2$ and take

$$f(x) = n! \int_0^x y^e(y-1)\ldots(y-n+e+1)\,dy$$

This time in considering the definitions of §2 we assume that $0 \leqslant x_i < p$. Now there are $n - e$ sequences $\mathscr{X}$, each of the form $\mathscr{X} = (j, 0, 0, \ldots)$ $(0 \leqslant j \leqslant n - e - 1)$. Moreover when $x_0 = 0$ we have $\sigma_i = e + 1$ $(i = 0, 1, \ldots)$, $\tau_i = 0$ $(i = 0, 1, \ldots)$ and when $x_0 = j$ with $1 \leqslant j \leqslant n - e - 1$ we have $\sigma_i = 2$ $(i = 0, 1, \ldots)$, $\tau_i = 0$ $(i = 0, 1, \ldots)$. Now Lemmas 2, 3, 4 and the argument of §4 show that when $e + 1 | \alpha$ we have

$$S(f; p^\alpha) = p^{\alpha e/(e+1)} + \theta(n-1)p^{\alpha/2}$$

with $|\theta| \leqslant 1$. Thus

$$|S(f; p^\alpha)| > \tfrac{1}{2}p^{\alpha e/(e+1)}$$

once more.

Our final example shows that if $e(\geqslant 2)$ is small compared with n, then even the factor $n - 1$ in Theorem 1 cannot be materially reduced.

Let

$$P(x) = \prod_{r=0}^{m} (x - r), \quad f(x) = P(x)^{e+1},$$

so that $n = (m + 1)(e + 1)$. The function $P'(x)$ has all of its m roots real and interlacing, but not coinciding with, the $m + 1$ roots of $P(x)$. Let K denote the algebraic number field generated by the roots of P'. For a given prime p let ord_p denote any additive non-Archimedean valuation on K which coincides with the additive p-adic valuation on $\mathbb{Q}$ (normalized so that $\text{ord}_p\, p = 1$). We assume throughout that p is so large that $\text{ord}_p(\xi - \xi') = 0$ for each pair ξ, ξ' of distinct roots of $P'(x)$. We again construct sequences as prescribed in §2. We assume that $p > p_0(n)$. There are at least $m + 1$ and at most $2m + 1$ possible choices for x_0, namely

$$x_0 \equiv r \quad (0 \leqslant r \leqslant m) \tag{31}$$

together with any possible solutions of

$$P'(x_0) \equiv 0 \pmod p. \tag{32}$$

Since $P'(x) = \sum_{s=0}^{m} \prod_{\substack{r=0\\ r\neq s}}^{m} (x - r)$ it follows that the solutions of (32) are distinct from those of (31). For sequences arising from (31) we assume that $0 \leqslant x_i < p$, so that $x_0 = r$. For any arising from (32), however, we suppose that $\max \text{ord}_p (X_i - \xi) \leqslant i$ where the maximum is taken over the roots ξ of P'. When $x_0 = r$ $(0 \leqslant r \leqslant m)$ it follows that $x_i = 0$ $(i \geqslant 1)$, $\tau_i = 0$ $(i \geqslant 0)$, $\sigma_i = e + 1$ $(i \geqslant 0)$, $f(X_i) = 0$. On the other hand, when x_0 satisfies (32) it follows that X_i (if it exists) satisfies $p^i \mid f'(X_i)$. Moreover there is at most one root, ξ_0 of P' such that $\text{ord}_p (X_i - \xi_0) > 0$, for otherwise $\text{ord}_p (\xi - \xi') > 0$ for two distinct roots ξ, ξ' of P'. Hence $i \leqslant \text{ord}_p P'(X_i) = \text{ord}_p (m + 1) + \sum_\xi \text{ord}_p (X_i - \xi) = \text{ord}_p (X_i - \xi_0) \leqslant i$. Thus $\text{ord}_p P'(X_i) = i$. It follows that $\tau_i = 0$ $(i \geqslant 0)$, $\sigma_i = 2$ $(i \geqslant 0)$.

Now we take $\alpha = k(e + 1)$. The arguments of Lemma 2 and §§3 and 4 show that

$$S(f;p^\alpha) = (m + 1)p^{\alpha e/(e+1)} + \theta(n - 1)p^{\alpha/2}$$

$$= \frac{n}{e + 1}p^{\alpha e/(e+1)} + \theta(n - 1)p^{\alpha/2}$$

where $|\theta| \leqslant 1$. Thus, given any $e \geqslant 2$ there are arbitrarily large n for which there is an f with degree n such that whenever $p > p_0(n)$ we have

$$|S(f;p^\alpha)| \gg np^{\alpha e/(e+1)}.$$

In each of the above examples we have $\delta = 0$. However if we replace $f(x)$ by $p^\delta f(x)$, then since we have $S(p^\delta f; p^\alpha) = p^\delta S(f; p^{\alpha-\delta})$ for $\alpha \geqslant \delta$ we may proceed as above and obtain the respective lower bounds $\frac{1}{2}p^{(\alpha+\delta)/2}$, $\frac{1}{2}p^{(\alpha e+\delta)/(e+1)}$ and $np^{(\alpha e+\delta)/(e+1)}$ for appropriate choices of the parameters.

We may also modify the examples in a less trivial manner. Let $g(x) = \sum_k a_k p^{(n-k)m} x^k$ where the a_k are defined by $f(x) = \sum_k a_k x^k$. Then, in each case, for α sufficiently large we have $S(g;p^\alpha) = p^{(n-1)m} S(f;p^{\alpha-nm})$. In the first example we find that $|S(g;p^\alpha)| > \frac{1}{2}p^{(\alpha+(n-2)m)/2}$ and $\delta = (n - 2)m$ (c.f. (19)). In the second and third examples we find for suitable choices of the parameters that $|S(g;p^\alpha)| \sim p^\lambda$ and $|S(g;p^\alpha)| \sim$

https://doi.org/10.4153/CMB-1985-053-7 Published online by Cambridge University Press

$np^{\lambda}/(e+1)$ respectively with $\lambda = (\alpha e + nm - em - m)/(e+1)$. In each case we have $\delta = \max_{f'(\xi)=0}(n - e_\xi - 1)m = (n-2)m$ so that Theorem 1 is no longer sharp. However when we replace δ by δ^* (given by (28)), since $\delta^* = (n-e-1)m$, the modified version of Theorem 1 alluded to after Theorem 2 *is* sharp.

References

1. D. R. Anderson and J. T. Stiffler, *Lower bounds for the maximum modulus of certain classes of trigonometric sums*, Duke Math. J., **30** (1963), pp. 171–176.

2. J.-R. Chen, *On the representation of natural numbers as a sum of terms of the form* $[x(x+1)\ldots(x+n-1)]/n!$, Acta Math. Sinica, **9** (1959), pp. 264–270.

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

4. H. Davenport and H. Heilbronn, *On an exponential sum*, Proc. London Math. Soc., (2), **41** (1936), pp. 449–453.

5. H. Davenport and H. Heilbronn, *On Waring's problem: Two cubes and one square*, Proc. London Math. Soc., (2), **43** (1937), pp. 73–104.

6. K. F. Gauss, *Summatio quarundam serierum singularium*, Comment. Soc. Reg. Sci. Gottingen Recentiores **1** (1808/11) (see also, Werke, Band II, Königl. Ges. Wiss. Göttingen, 1863,1876).

7. G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio Numerorum"; I: A new solution of Waring's problem*, Nachrichten von der K. Gesellschaft der Wissenschaften zu Göttingen, Math.-phys. Klasse, (1920), pp. 33–54.

8. G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio Numerorum": VI: Further researches in Waring's Problem*, Math. Z., **23** (1925), pp. 1–37.

9. L.-K. Hua, *On an exponential sum*, J. Chinese Math. Soc., **2** (1940), pp. 301–312 (see also, Sur une somme exponentielle, C. R. Acad. Sci. Paris, **210** (1940), pp. 520–523).

10. L.-K. Hua, *On exponential sums*, Sci. Record (Peking) (N.S.), **1** (1957), pp. 1–4.

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

12. L. J. Mordell, *On a sum analogous to a Gauss's sum*, Quart. J. of Math., **3** (1932), pp. 161–167.

13. V. I. Nechaev, *On the representation of natural numbers as a sum of terms of the form* $(x(x+1)\ldots(x+n-1))/n!$, Izv. Akad. Nauk SSSR Ser. Mat., **17** (1953), pp. 485–498.

14. V. I. Nechaev, *An estimate of a complete rational trigonometric sum*, Mat. Zametki, **17** (1975), pp. 839–849 (English translation, Math. Notes, **17** (1975), pp. 504–511).

15. W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, 536, Springer-Verlag, Berlin, 1976.

16. S. B. Stechkin, *An estimate of Gaussian sums*, Mat. Zametki, **17** (1975), pp. 579–588 (English translation, Math. Notes, **17** (1975), pp. 342–349).

17. S. B. Stechkin, *Estimate of a complete rational trigonometric sum*, Proc. Steklov Inst., **143** (1977), pp. 188–220 (English translation, A.M.S., 1980, Issue 1, pp. 201–220).

18. R. C. Vaughan, *The Hardy–Littlewood method*, C.U.P., 1981, Cambridge.

19. I. M. Vinogradov, *The method of trigonometric sums in the theory of numbers*, Proc. Steklov Inst., **23** (1947), pp. 1–111.

20. A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci., U.S.A., **34** (1948), pp. 204–207.

21. H. Weyl, *On the equidistribution of numbers mod. one*, Math. Ann., **77** (1916), pp. 313–352.

University of New South Wales
Sydney, Australia

Imperial College
London, England