PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 3, July 1980

ESTIMATES FOR EXPONENTIAL SUMS

ROBERT A. SMITH

ABSTRACT. If f is a polynomial over $\mathbf{Z}$ of degree $n+1$ with $n \geqslant 1$, then for each integer $q \geqslant 1$, $|\Sigma_{1 \leqslant x \leqslant q} \exp(2\pi i f(x)/q)| \leqslant q^{1/2}(D, q)d_n(q)$, *provided* the discriminant D of the derivative of f does not vanish identically, where $d_n(q)$ is the number of representations of q as a product of n factors.

For each positive integer q and for each nonlinear polynomial $f \in \mathbf{Z}[X]$ of degree $n+1$, i.e., $n = \deg f - 1 \geqslant 1$, we define

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

where "$x \bmod q$" means that x runs through a complete set of residues mod q, and $e_q(t) = \exp(2\pi i t/q)$ for each $t \in \mathbf{Z}$. In 1948, A. Weil [6] proved as a consequence of his work in algebraic geometry that the exponential sum in (1) satisfies the following inequality when q is a prime p and $f \notin p\mathbf{Z}[X]$:

$$|S(f; p)| \leqslant (\deg f - 1)p^{1/2}. \tag{2}$$

For certain applications to number theory (e.g., cf. [4]), it is absolutely essential to have upper bounds for (1) with q an arbitrary positive integer (and not just a prime). In 1977, Jing-Run Chen [1] proved that if the content of $f - f(0)$ is relatively prime to q, then (1) satisfies

$$|S(f; q)| \leqslant e^{7(n+1)}q^{1-1/(n+1)},$$

an improvement of an estimate originally due to L. K. Hua [3]. This inequality is essentially best possible (cf. [2, p. 19]). The purpose of this paper is to show that if the discriminant $D(f')$ of f' does not vanish identically, where f' denotes the derivative of f, then a substantial improvement in this estimate can be deduced from Weil's estimate in (2).

We begin by giving a new interpretation of the well-known fact that $S(f; q)$ is multiplicative in q (cf. [4, p. 2]). We observe that we may assume $f(0) = 0$ without loss of generality.

THEOREM 1. *Suppose q_1 and q_2 are positive integers which are relatively prime. Then there exist integers m_1 and m_2 such that*

$$m_1q_1 + m_2q_2 = 1.$$

For each polynomial $f \in \mathbf{Z}[X]$ satisfying $f(0) = 0$, then

$$S(f; q_1q_2) = S(m_2f; q_1)S(m_1f; q_2).$$

Received by the editors June 5, 1979 and, in revised form, September 10, 1979.
AMS (MOS) subject classifications (1970). Primary 10G05.

Proof. Since the map $(x + q_1\mathbf{Z}, y + q_2\mathbf{Z}) \mapsto m_2q_2x + m_1q_1y + q_1q_2\mathbf{Z}$ defines a bijection between $\mathbf{Z}/q_1\mathbf{Z} \times \mathbf{Z}/q_2\mathbf{Z}$ and $\mathbf{Z}/q_1q_2\mathbf{Z}$, then (1) can be rewritten as

$$S(f; q_1q_2) = \sum_{\substack{x \bmod q_1 \\ y \bmod q_2}} e_{q_1q_2}(f(m_2q_2x + m_1q_1y)).$$

For any $x, y \in \mathbf{Z}$, then modulo q_1q_2, we have

$$\begin{aligned} f(m_2q_2x + m_1q_1y) &\equiv f(m_2q_2x) + f(m_1q_1y) \\ &\equiv (m_2q_2 + m_1q_1)(f(m_2q_2x) + f(m_1q_1y)) \\ &\equiv m_2q_2f(m_2q_2x) + m_1q_1f(m_1q_1y) \end{aligned}$$

(since $f(0) = 0$ implies $f(qx) \equiv 0 \bmod q$ for all $x \in \mathbf{Z}$)

$$\begin{aligned} &\equiv m_2q_2f((1 - m_1q_1)x) + m_1q_1f((1 - m_2q_2)y) \\ &\equiv m_2q_2f(x) + m_1q_1f(y). \end{aligned}$$

This completes the proof of Theorem 1.

To establish an upper bound for $S(f; q)$, it therefore suffices to assume that $q = p^\alpha$ with $\alpha > 2$ in view of (2). For fixed α, we define

$$\delta = \left[\frac{\alpha}{2}\right] \quad \text{and} \quad \gamma = \alpha - \delta.$$

Since $\alpha > 2$, it follows that

$$2\gamma > \alpha \quad \text{and} \quad \gamma > \delta > 1. \tag{3}$$

Furthermore, we shall assume that f is a polynomial in $\mathbf{Z}[X] - p\mathbf{Z}[X]$ with $D(f') \neq 0$. For each pair of positive integers r and s, then

$$B(p^{r+s}) = p^rB(p^s) \oplus B(p^r), \tag{4}$$

where

$$B(p^r) = \{x \in \mathbf{Z}: 0 < x < p^r\},$$

a set of representatives of the residue classes $\bmod p^r$. Taking $r = \gamma$ and $s = \delta$ in (4), the Taylor expansion of $f(u + p^\gamma v) \bmod p^\alpha$ (cf. (3)) transforms (1) into

$$S(f; p^\alpha) = p^\delta \sum_{\substack{0 < u < p^\gamma \\ f'(u) \equiv 0 \bmod p^\delta}} e_{p^\alpha}(f(u)). \tag{5}$$

For each $F \in \mathbf{Z}[X]$, let

$$N(F; p^m) = \operatorname{card}\{x \bmod p^m: F(x) \equiv 0 \bmod p^m\}.$$

By a theorem of Sándor [5], we know that if $D(F) \neq 0$, then

$$N(F; p^m) < (\deg F)p^{\nu(m,F)} \tag{6}$$

where

$$\nu(m, F) < \begin{cases} \frac{1}{2}\operatorname{ord}_p D(F) & \text{if } m > \operatorname{ord}_p D(F), \\ m - 1 & \text{if } m < \operatorname{ord}_p D(F). \end{cases}$$

If α is even, then $\gamma = \delta > 1$ whence (5) and (6) imply

$$|S(f; p^\alpha)| < n(D(f'), p^\alpha)p^{\alpha/2}. \tag{7}$$

Next suppose that α is odd, so that $\gamma = \delta + 1 > 2$. If $\operatorname{ord}_p D(f') > 1$, then (5) and (6) again imply that (7) holds, since $\frac{1}{2}(1 + \operatorname{ord}_p D(f')) < \operatorname{ord}_p D(f')$. If $\operatorname{ord}_p D(f') = 0$, the decomposition in (4) (with $r = \delta$ and $s = 1$), together with the Taylor expansion of $f(x + p^\delta y) \bmod p^\alpha$, imply that

$$S(f; p^\alpha) = p^\delta \sum_{\substack{0 < x < p^\delta \\ f'(x) \equiv 0 \bmod p^\delta}} e_{p^\alpha}(f(x)) \sum_{0 < y < p} e_p\left(\tfrac{1}{2}f''(x)y^2 + p^{-\delta}f'(x)y\right). \qquad (8)$$

If $p > 2$, the absolute value of the Gaussian sum in (8) is $p^{1/2}$ since $\operatorname{ord}_p D(f') = 0$, whence $|S(f; p^\alpha)| < np^{\alpha/2}$, and similarly for $p = 2$. Therefore, we have proved that for all $\alpha > 2$ and for all $f \in \mathbf{Z}[X] - p\mathbf{Z}[X]$ for which $D(f') \neq 0$, the inequality in (7) holds. We can now prove

THEOREM 2. *Suppose f is a nonlinear polynomial in $\mathbf{Z}[X]$ such that $D(f') \neq 0$. Then for any integer $q > 1$,*

$$|S(f; q)| < q^{1/2}(D(f'), q)d_n(q),$$

where $n = \deg f - 1 > 1$ and $d_n(q)$ denotes the number of representation of q as a product of n factors.

PROOF. First, we shall assume that $q = p^\alpha$, where p is a prime. Clearly, there exists a unique integer $t > 0$ and a unique polynomial $g \in \mathbf{Z}[X] - p\mathbf{Z}[X]$ such that

$$f(X) = p^t g(X). \qquad (9)$$

If $t > \alpha$, then (1) implies $S(f; p^\alpha) = p^\alpha$, which certainly satisfies the inequality (7) since

$$D(vF) = v^{2 \deg F - 1} D(F) \qquad (10)$$

for any $F \in \mathbf{Z}[X]$ and any $v \in \mathbf{Z}$. If $t < \alpha$, then (1) implies that

$$S(f; p^\alpha) = p^t S(g; p^{\alpha - t}). \qquad (11)$$

If $t = \alpha - 1$, then (11), together with (2), imply that $|S(f; p^\alpha)| < np^{t + 1/2}$, i.e., the inequality (7) is again satisfied in view of (10). Thus, we may assume $\alpha - t > 2$. By what has already been proved in (7), we have

$$|S(g; p^{\alpha - t})| < n(D(g'), p^{\alpha - t})p^{(\alpha - t)/2},$$

whence $S(f; p^\alpha)$ again satisfies the inequality (7) in view of (9), (10) and (11). Hence, we have shown that (7) holds under the assumptions of Theorem 2.

Now let $q > 1$ be arbitrary. Without loss of generality, we may assume that $f(0) = 0$. By Theorem 1,

$$S(f; q) = \prod_{p^\alpha \| q} S(m(p^\alpha)f; p^\alpha), \qquad (12)$$

where $m(p^\alpha)$ is a suitable integer satisfying

$$(m(p^\alpha), p) = 1 \qquad (13)$$

for each prime p dividing q. Thus, (12) implies

$$|S(f; q)| < \prod_{p^\alpha \| q} n(D(m(p^\alpha)f'), p^\alpha)p^{\alpha/2} < d_n(q)(D(f'), q)q^{1/2}$$

in view of (10) and (13), together with the fact that

$$\prod_{p|q} n = \prod_{p|q} d_n(p) \leqslant d_n(q).$$

This completes the proof of Theorem 2.

REMARK. If $\delta > \operatorname{ord}_p D(f') \geqslant 1$, we observe that the inequality (7) can be replaced by the stronger inequality (cf. (6))

$$|S(f; p^\alpha)| \leqslant n(D(f'), p^\alpha)^{1/2} p^{\alpha/2}. \tag{14}$$

It is therefore reasonable to ask if (14) holds for $\delta \leqslant \operatorname{ord}_p D(f')$ whenever $\operatorname{ord}_p D(f') \geqslant 1$. It appears that such an improvement would require a very detailed analysis of the auxiliary exponential sum in (5) for those primes p dividing the discriminant of f' (there are only a finite number of such primes!). Thus, if (14) holds for all primes p dividing $D(f')$, then the inequality in Theorem 2 can be strengthened to

$$|S(f; q)| \leqslant q^{1/2}(D(f'), q)^{1/2} d_n(q).$$

REFERENCES

1. Jing-Run Chen, *On Professor Hua's estimate of exponential sums*, Sci. Sinica **20** (1977), 711–719.

2. G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio numerorum": II. Proof that every large number is the sum of at most* 21 *biquadrates*, Math. Z. **9** (1921), 14–27.

3. L. K. Hua, *On an exponential sum*, J. Chinese Math. Soc. **2** (1940), 301–312.

4. ______, *Additive theory of prime numbers*, Transl. Math. Mono., vol. 13, Amer. Math. Soc., Providence, R. I., 1965.

5. G. Sándor, *Über die Anzahl der Lösungen einer Kongruenz*, Acta Math. **87** (1952), 13–17.

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

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, TORONTO M5S 1A1, CANADA