PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 7, Pages 1995–1998
S 0002-9939(99)04776-0
Article electronically published on March 17, 1999

NOTE ON HEATH-BROWN'S ESTIMATE FOR HEILBRONN'S EXPONENTIAL SUM

HONG BING YU

(Communicated by David E. Rohrlich)

ABSTRACT. We show that $S_h(a) = \sum_{n=1}^{p} e(\frac{an^{hp}}{p^2}) \ll (h, p-1)p^{11/12}$, which generalizes Heath-Brown's estimate for Heilbronn's exponential sum $S_1(a)$. We also give a simple proof of a crucial lemma in Heath-Brown's work.

1. INTRODUCTION

Let p be a prime, and set $e(x) = \exp(2\pi ix)$. Write

$$S_h(a) = \sum_{n=1}^{p} e(\frac{an^{hp}}{p^2}), \tag{1}$$

where $h \geq 1$ and a is any integer coprime to p. It is a long-standing problem to show that Heilbronn's exponential sum $S_1(a) = o(p)$ as $p \to \infty$ (cf. Odoni [2]). Recently Heath-Brown [1] proved, by an ingenious version of Stepanov's method, that $S_1(a) \ll p^{11/12}$ uniformly in a. In correspondence with D. R. Heath-Brown, he pointed out to me that, when h is a fixed positive integer, one can get exactly the same bound for the sum (1), since Lemma 1 of [1] still holds. Heath-Brown has provided me a proof of this. In fact, his argument leads to the following lemma with $(h, p-1)^{5/4}$ instead of $(h, p-1)$ in (2) below.

Lemma A. *Let*

$$f(x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots + \frac{x^{p-1}}{p-1} \in \mathbb{Z}_p[x],$$

and let

$$S_r = \{k \in \mathbb{Z}_p - \{0, 1\} : \ f(k) = r\},$$

$$N_r = \#S_r.$$

Then there is a value of r for which

$$S_h(a) \ll (h, p-1)p^{3/4}N_r^{1/4}. \tag{2}$$

Received by the editors August 13, 1997 and, in revised form, October 23, 1997.
1991 *Mathematics Subject Classification.* Primary 11L03.
Supported by the National Science Foundation of China.

This together with the estimate ([1, Lemma 4])

$$N_r \ll p^{2/3} \quad \text{uniformly in } r \tag{3}$$

gives at once

Theorem. *If $p \nmid a$, then $S_h(a) \ll (h, p-1)p^{11/12}$, uniformly in a.*

To prove (3), Heath-Brown used ideas of Stepanov [3] and constructed an auxiliary polynomial which vanishes to high order at the points of interest. As is usual in such arguments, it is important to show that the auxiliary polynomial does not vanish identically. Lemma 3 of Heath-Brown [1] serves this purpose. However, the proof of Lemma 3 given in [1] is somewhat difficult and complicated. We take this opportunity to record a simple proof of it in the following more general formulation, which is crucial to our argument.

Lemma B. *Suppose that $g_0(x), \cdots, g_n(x)$ are polynomials in $\mathbb{Z}_p[x]$, $g_n(x)$ does not vanish identically, with deg $g_i(x) \le k_i$ $(0 \le i \le n)$, where n and k_i are non-negative integers satisfying $k_0 \ge k_1 \ge \cdots \ge k_n$ and $m = k_0 + k_1 + \cdots + k_n < p - n$. Then*

$$F_n(x) = \sum_{i=0}^{n} g_i(x) f^i(x)$$

satisfies $x^{m+n+1} \nmid F_n(x)$.

2. Proof of Lemma A

Lemma A can be proved by modifying the argument of [1, Lemma 1]. Let

$$S'_h(a) = \sum_{n=1}^{p-1} e(\frac{an^{hp}}{p^2}),$$

so that $S_h(a) = 1 + S'_h(a)$. Note that if $m \equiv n \pmod p$, then $m^p \equiv n^p \pmod{p^2}$, and that the values assumed by $n^h \pmod p$ are the same as the values assumed by $n^d \pmod p$, where $d = (h, p-1)$. Thus $S'_h(a) = S'_d(a)$, so that we may suppose that $h|(p-1)$.

Since the number of solutions of $n^h \equiv y \pmod p$ can be expressed as $1 + \sum_\chi \chi(y)$, where the summation is extended over the Dirichlet characters $\chi \pmod p$ satisfying $\chi^h = \chi_0$ and $\chi \ne \chi_0$ (note that there are exactly $h-1$ such characters). Hence

$$S'_h(a) = S'_1(a) + \sum_{\chi} \sum_{y=1}^{p-1} \chi(y) e(\frac{ay^p}{p^2}) = S'_1(a) + \sum_{\chi} S(a, \chi), \tag{4}$$

say. Then, by using the argument of Lemma 1 of [1], we have

$$\begin{aligned} |S(a,\chi)|^2 &= (p-1) + \sum_{b=1}^{p-1} \sum_{k=2}^{p-1} \chi(kb)\overline{\chi}((k-1)b) e\left(\frac{ab^p(k^p - (k-1)^p)}{p^2}\right) \\ &= (p-1) + \sum_{k} \chi(k)\overline{\chi}(k-1) S'_1(a(1 - pf(k))) \\ &\le p - 1 + \sum_{k} |S'_1(a(1-pf(k)))| \\ &= (p-1) + \sum_{r=1}^{p} N_r |S'_1(a(1-pr))|, \end{aligned}$$

and so

$$|S(a,\chi)|^4 \ll p^2 + \{\sum_{r=1}^{p} N_r^2\}\{\sum_{r=1}^{p} |S_1'(a(1-pr))|^2\}$$
$$\ll p^3 \max_r N_r.$$

The lemma now follows from (4), Lemma 1 of [1] and Hölder's inequality easily.

3. Proof of Lemma B

We proceed by induction on n. When $n = 0$, the result is trivial. For $n > 0$ we suppose that Lemma B is true with n replaced by l $(0 \le l < n)$. Now we use induction on $I(F_n(x)) = k_0+k_1+\cdots+k_n$. When $I(F_n(x)) = 0$, the $g_i(x)$ $(0 \le i \le n)$ are all constants. Since $x = 0$ is a simple root of $f(x)$, it follows that $x^{n+1} \nmid F_n(x)$. Suppose that the result has been proved when $I(F_n(x)) < m$, where $m > 0$ and $m + n < p$; and, assume that there exists a polynomial $F_n(x)$ with $I(F_n(x)) = m$ such that $x^{m+n+1}|F_n(x)$. Then $x^{m+n}|F_n'(x)$. Let

$$F(x) = \sum_{i=1}^{n}\{(x-1)g_{i-1}'(x) + ig_i(x)\}f^{i-1}(x) + (x-1)g_n'(x)f^n(x).$$

It is easily verified that $F(x) \equiv (x-1)F_n'(x) \pmod{x^{p-1}}$. Hence $x^{m+n}|F(x)$ and so

$$x^{m+n}|(F(x) - rF_n(x)), \tag{5}$$

where $r = \deg g_n(x)$. We note that, since $k_{i-1} \ge k_i$ $(1 \le i \le n)$, the polynomial $(x-1)g_{i-1}'(x)+ig_i(x)-rg_{i-1}(x)$ is either identically zero or its degree is not greater than k_{i-1} $(1 \le i \le n)$. Also, if $(x-1)g_n'(x)-rg_n(x)$ is not identically zero, then its degree is less than $r \le k_n$. Thus $I(F(x)-rF_n(x)) < m$, contradicting the induction hypothesis on $I(F_n(x))$ by (5). Hence

$$(x-1)g_n'(x) - rg_n(x) = 0 \tag{6}$$

identically. Further, by the induction hypothesis on n, we must have the identity

$$(x-1)g_{i-1}'(x) + ig_i(x) - rg_{i-1}(x) = 0,\ 1 \le i \le n. \tag{7}$$

From (6) we have $g_n(x) = a(x-1)^r, a \not\equiv 0 \pmod{p}$. Then, it is easily seen from (7) with $i = n$ that $an \equiv 0 \pmod{p}$, which is impossible. This completes the proof of the lemma.

Acknowledgments

I am grateful to Dr. D. R. Heath-Brown for informing me of his unpublished work, and for his comments on an early draft of the manuscript. I also thank the referee for the suggestion in the revision of the paper.

References

1. D. R. Heath-Brown, An estimate for Heilbronn's exponential sum, Analytic Number Theory, Vol 2. Birkhäuser Boston, PM, 139, 1996, pp. 451–463. MR **97k:**11120
2. R. W. K. Odoni, Trigonometric sums of Heilbronn's type, Math. Proc. Camb. Phil. Soc. **98** (1985), 389–396. MR **86m:**11061

3. S. A. Stepanov, The number of points of a hyperelliptic curve over a prime field, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 1171–1181. MR **40:**5620

Department of Mathematics, University of Science and Technology of China, Hefei 230026, Anhui, The People's Republic of China
E-mail address: yuhb@ustc.edu.cn