ACTA ARITHMETICA
XCVII.3 (2001)

Estimates of character sums with exponential function

by

Hong Bing Yu (Hefei)

1. Introduction. In [3] Dobrowolski and Williams proved, among other things, the following interesting result:

$$\left|\sum_{x=1}^{X}\left(\frac{ag^x+b}{p}\right)\right| \le \frac{\sqrt{p-1}\,\log(p-1)}{2\log 2}+3\sqrt{p-1}, \tag{1.1}$$

where p is an odd prime, g is a primitive root mod p, $\left(\frac{x}{p}\right)$ is the Legendre symbol, and a,b,X are integers satisfying $p\nmid ab$ and $1\le X\le p-1$.

The purpose of this paper is to extend (1.1) in two directions. We first prove the following result, which may be compared with the classical inequality of Pólya–Vinogradov for character sums with linear polynomial (cf. Davenport [2, §23]).

Theorem 1. *Let $n\ge 2$ and λ be integers with $(n,\lambda)=1$ and λ belonging to the exponent d modulo n. Let χ be a primitive Dirichlet character modulo n. Write*

$$S_n(\chi,\lambda,X)=\sum_{x=1}^{X}\chi(a\lambda^x+b), \tag{1.2}$$

where a,b and X are integers satisfying $(ab,n)=1$ and $1\le X\le d$. Then

$$|S_n(\chi,\lambda,X)|<\sqrt{n}\left(\frac{2}{\pi}\log n+\frac{7}{5}\right). \tag{1.3}$$

We note that for an imprimitive χ no non-trivial bound for $|S_n(\chi,\lambda,X)|$ can be obtained. Consider, for instance, the case where $n=p^k$ (p odd prime and $k\ge 2$) and χ being induced by a (primitive) character modulo p. Let $\lambda\equiv 1 \pmod p$, $\lambda\not\equiv 1 \pmod{p^2}$, $a+b\equiv 1\pmod p$ and $p\nmid ab$. Then it is easily seen that λ belongs to exponent p^{k-1} modulo n and that $S_n(\chi,\lambda,X)=X$ for $X\ge 1$.

2000 *Mathematics Subject Classification*: Primary 11L40.

Project supported by the National Natural Science Foundation of China.

Furthermore, we show that in certain cases the inequality (1.3) is essentially best possible.

Theorem 2. *Let $n = p^k$, p an odd prime, $k \geq 2$. Let χ be a primitive character modulo n, g be a primitive root modulo n, and a, b be integers with $p \nmid ab$. Let $S_n(\chi, g, X)$ be as in* (1.2). *Then*

$$\max_{1 \leq X \leq \varphi(n)} |S_n(\chi, g, X)| \gg \sqrt{n}, \tag{1.4}$$

where the implicit constant is absolute.

Our second purpose is to generalize (1.1) to general finite fields. As usual, let F_q denote the finite field of $q = p^k$ elements (p prime and $k \geq 1$), and let F_q^* be the multiplicative group of non-zero elements of F_q. Let $\widehat{F_q^*}$ be the set of all multiplicative characters of F_q^*, and $\varepsilon \in \widehat{F_q^*}$ be the trivial character. For any $\psi \in \widehat{F_q^*}$ it is convenient to extend the definition of ψ by setting $\psi(0) = 0$.

Theorem 3. *Let $\lambda \in F_q^*$ belong to the exponent d. Let $\chi \in \widehat{F_q^*}$ and $\chi \neq \varepsilon$. Write*

$$T_q(\chi, \lambda, X) = \sum_{x=1}^{X} \chi(a\lambda^x + b), \tag{1.5}$$

where $a, b \in F_q^*$, X is integer with $1 \leq X \leq d$. Then

$$|T_q(\chi, \lambda, X)| < \sqrt{q}\left(\frac{2}{\pi}\log q + \frac{7}{5}\right). \tag{1.6}$$

By Theorem 3 and an argument similar to that used in Burgess [1, §6], we have the following result which may be of independent interest.

Corollary. *Let g be a primitive root of F_q, and $a, b \in F_q^*$. For integers X, Y with $1 \leq Y < Y + X \leq q - 1$, we denote by $H(X, Y)$ the number of primitive roots in the set*

$$\{ag^x + b \mid Y \leq x \leq Y + X - 1,\ (x, q-1) = 1\}.$$

Then

$$H(X, Y) = \frac{\varphi(q-1)}{q-1}\left(\frac{\varphi(q-1)}{q-1}X + \theta 4^{\omega(q-1)}\sqrt{q}\log q\right),$$

where $\omega(q-1)$ is the number of different prime divisors of $q-1$, and $|\theta| \leq 4$.

Finally, we show that the inequality (1.6) is also close to best possible.

Theorem 4. *Let g be a primitive root of $F_q, a, b \in F_q^*$, and $T_q(\chi, \lambda, X)$ be as in* (1.5). *Then*

$$\max_{1\le X\le q-1} |T_q(\chi,g,X)| \gg \sqrt{q}, \tag{1.7}$$

where the implicit constant is absolute.

2. Proof of Theorem 1. Our argument is a modification of that used in the proof of the Pólya–Vinogradov inequality mentioned above.

Write $e_n(y)=e^{2\pi iy/n}$ as usual. For any Dirichlet character ψ modulo n, the Gaussian sum $G(\psi)$ is defined by

$$G(\psi)={\sum_{y=1}^{n}}' \psi(y)e_n(y), \tag{2.1}$$

where the accent indicates that we only consider those y coprime to n.

For reference purposes, we state the following well known result in the form of a lemma (cf. Davenport [2, §9]).

Lemma 1. (i) *If* $(m,n)=1$, *then*

$$\psi(m)G(\overline{\psi})={\sum_{y=1}^{n}}' \overline{\psi}(y)e_n(my). \tag{2.2}$$

(ii) *If* ψ *is a primitive character modulo* n, *then* (2.2) *holds for any* m.

(iii) *For any character* ψ *modulo* n *we have* $|G(\psi)|\le\sqrt{n}$, *and the equality holds if and only if* ψ *is primitive.*

We now prove Theorem 1. Since χ is a primitive character modulo n, we have by Lemma 1(ii) and (1.2),

$$\begin{aligned} S_n(\chi,\lambda,X) &= \frac{1}{G(\overline{\chi})}{\sum_{y=1}^{n}}' \overline{\chi}(y)e_n(by)\sum_{x=1}^{X} e_n(ay\lambda^x) \\ &= \frac{1}{G(\overline{\chi})}{\sum_{y=1}^{n}}' \overline{\chi}(y)e_n(by)S_y(X), \end{aligned} \tag{2.3}$$

say. Further, since $(ay\lambda^x,n)=1$, it follows that $e_n(ay\lambda^x)$ can be expanded into a finite Fourier series with respect to the Dirichlet characters ψ modulo n. We have (using (2.1)), for $x=1,\ldots,X$,

$$e_n(ay\lambda^x)=\frac{1}{\varphi(n)}\sum_{\psi} G(\overline{\psi})\psi(ay\lambda^x)$$

and so

$$S_y(X)=\frac{1}{\varphi(n)}\sum_{\psi} G(\overline{\psi})\psi(ay)\sum_{x=1}^{X}\psi(\lambda^x).$$

Substituting this in (2.3) and using Lemma 1(i) (noting that $(b,n)=1$), we get

$$S_n(\chi,\lambda,X)=\frac{1}{G(\overline{\chi})\varphi(n)}\sum_{\psi}G(\overline{\psi})\psi(a)\sideset{}{'}\sum_{y=1}^{n}\overline{\chi}(y)\psi(y)e_n(by)\sum_{x=1}^{X}\psi(\lambda^x) \tag{2.4}$$
$$=\frac{1}{G(\overline{\chi})\varphi(n)}\sum_{\psi}G(\overline{\psi})G(\overline{\chi}\psi)\psi(a)\chi\overline{\psi}(b)\sum_{x=1}^{X}\psi(\lambda^x).$$

Recall that λ belongs to the exponent d modulo n. Thus each dth root of unity $e_d(j)$ $(0\le j\le d-1)$ occurs exactly $\varphi(n)/d$ times as a value of $\psi(\lambda)$. Therefore, by (2.4) and Lemma 1(iii), we have (cf. the proof of Niederreiter [6, Theorem 8.3])

$$\begin{aligned}|S_n(\chi,\lambda,X)| &\le \frac{\sqrt{n}}{\varphi(n)}\sum_{\substack{\psi\\ \psi(\lambda)\ne 1}}\frac{2}{|1-\psi(\lambda)|}+\frac{X}{\varphi(n)}\cdot\frac{\varphi(n)}{d}\sqrt{n}\\ &=\frac{2\sqrt{n}}{\varphi(n)}\cdot\frac{\varphi(n)}{d}\sum_{j=1}^{d-1}\frac{1}{|1-e_d(j)|}+\frac{X}{d}\sqrt{n}\\ &=\frac{\sqrt{n}}{d}\sum_{j=1}^{d-1}\frac{1}{|\sin(\pi j/d)|}+\frac{X}{d}\sqrt{n}\\ &\le\frac{\sqrt{n}}{d}\left(\frac{2}{\pi}d\log d+\frac{2}{5}d\right)+\frac{X}{d}\sqrt{n},\end{aligned}$$

where we have used Lemma 2 of Niederreiter [5] in the last step. Theorem 1 then follows, since $X\le d<n$.

3. Proof of Theorem 2. In this section we write $r=\varphi(n)$ and let

$$S(x)=\sum_{0\le y\le x}\chi(ag^y+b) \tag{3.1}$$

for $x\ge 0$. The function $S(rx)$ is of bounded variation, and hence has a convergent Fourier series

$$S(rx)=\sum_{m=-\infty}^{\infty}c_m e^{2\pi imx}\quad\text{for } 0<x<1. \tag{3.2}$$

Clearly

$$c_0=\int_0^1 S(rx)\,dx=\frac{1}{r}\sum_{l=0}^{r-1}S(l).$$

For $m \neq 0$, we have

$$c_m = \int\limits_0^1 S(rx)e^{-2\pi imx}\,dx = \frac{1}{r}\int\limits_0^r S(x)e_r(-mx)\,dx \tag{3.3}$$
$$= \frac{1}{2\pi im}\Big(\sum_{l=0}^{r-1}\chi(ag^l+b)e_r(-lm) - \sum_{l=0}^{r-1}\chi(ag^l+b)\Big).$$

By the hypothesis of Theorem 2 it is easily seen that

$$\sum_{l=0}^{r-1}\chi(ag^l+b) = \sum_{\substack{y=1\\ p\nmid y}}^{p^k}\chi(y+b) = \sum_{\substack{y=1\\ p\nmid y}}^{p^k}\chi(y) - \sum_{y=1}^{p^{k-1}}\chi(b+py) \tag{3.4}$$
$$= -\sum_{y=1}^{p^{k-1}}\chi(b+py) = 0$$

(a proof of the last equality can be found in Davenport [2, p. 66]). Moreover, by the same argument used in Section 2 and using the same notation as there, we arrive at the identity

$$\sum_{l=0}^{r-1}\chi(ag^l+b)e_r(-lm) \tag{3.5}$$
$$= \frac{1}{rG(\overline{\chi})}\sum_{\psi}G(\overline{\psi})G(\overline{\chi}\psi)\psi(a)\chi\overline{\psi}(b)\sum_{l=0}^{r-1}\psi(g^l)e_r(-lm).$$

The inner sum is equal to r if $\psi(g) = e_r(m)$ and equal to 0 otherwise. Clearly, $\psi(g) = e_r(m)$ if and only if $\psi = \psi_m$, where ψ_m is the Dirichlet character modulo n given by

$$\psi_m(x) = e_r(s\,\mathrm{ind}_g x), \qquad 0 < s \le r \text{ and } s \equiv m \pmod{r}. \tag{3.6}$$

Thus by (3.3)–(3.5) we have, for $m \neq 0$,

$$c_m = \frac{1}{2\pi imG(\overline{\chi})}G(\overline{\psi}_m)G(\overline{\chi}\psi_m)\psi_m(a)\chi\overline{\psi}_m(b). \tag{3.7}$$

Since χ is primitive, we may write $\chi(x) = e_r(t\,\mathrm{ind}_g x)$ with $0 < t < r$ and $p \nmid t$. From (3.6) we see that if (and only if) m satisfies $m \not\equiv 0, t \pmod{p}$, then both ψ_m and $\overline{\chi}\psi_m$ are primitive characters modulo n. Thus, by Lemma 1(iii) and (3.7), we have

$$|c_m| = \frac{\sqrt{n}}{2\pi|m|} \qquad \text{for } m \not\equiv 0, t \pmod{p}. \tag{3.8}$$

On applying Parseval's formula to (3.2) and using (3.8), we have

$$\frac{1}{r}\sum_{l=0}^{r-1}|S(l)|^2 = \int_0^1 |S(rx)|^2\,dx = \sum_m |c_m|^2 \gg n.$$

Now, in view of (1.2), (3.1) and (3.4), Theorem 2 follows immediately.

4. Proof of Theorems 3 and 4. We first prove Theorem 3. Our argument is a version of that used in Section 2. We observe that $\chi(a\lambda^x + b)$, considered as a function of b, can be expanded into a finite Fourier series with respect to the multiplicative characters of F_q^*. Thus, for $x = 1, \ldots, X$,

$$\chi(a\lambda^x + b) = \sum_{\psi} c_\psi \overline{\psi}(-b), \tag{4.1}$$

with the Fourier coefficients

$$c_\psi = \frac{1}{q-1}\sum_{y\in F_q^*}\chi(a\lambda^x + y)\psi(-y) = \frac{1}{q-1}\chi\psi(a\lambda^x)J(\chi,\psi), \tag{4.2}$$

where $J(\chi,\psi)$ is a Jacobi sum

$$J(\chi,\psi) = \sum_{u\in F_q}\chi(1+u)\psi(-u)$$

(note that we have defined that $\psi(0) = 0$ for any $\psi \in \widehat{F_q^*}$). By (1.5), (4.1) and (4.2) we have

$$\begin{aligned} T_q(\chi,\lambda,X) &= \frac{1}{q-1}\sum_{\psi} J(\chi,\psi)\chi\psi(a)\overline{\psi}(-b)\sum_{x=1}^{X}\chi\psi(\lambda^x) \\ &= \frac{1}{q-1}\sum_{\psi} J(\chi,\overline{\chi}\psi)\psi(a)\chi\overline{\psi}(-b)\sum_{x=1}^{X}\psi(\lambda^x). \end{aligned} \tag{4.3}$$

It is well known that

$$|J(\chi,\overline{\chi}\psi)| \le \sqrt{q} \quad \text{with equality if } \psi \ne \varepsilon, \chi \tag{4.4}$$

(cf. Lidl and Niederreiter [4, Chapter 5]). Moreover, since λ belongs to the exponent d, it follows that each dth root of unity $e_d(j)$ $(0 \le j \le d-1)$ occurs exactly $(q-1)/d$ times as a value of $\psi(\lambda)$. Hence, by (4.3), (4.4) and the argument used in Section 2, we have

$$\begin{aligned} |T_q(\chi,\lambda,X)| &\le \frac{\sqrt{q}}{q-1}\cdot\frac{q-1}{d}\sum_{j=1}^{d-1}\frac{1}{|\sin(\pi j/d)|} + \frac{X\sqrt{q}}{q-1}\cdot\frac{q-1}{d} \\ &< \sqrt{q}\left(\frac{2}{\pi}\log q + \frac{7}{5}\right). \end{aligned}$$

This completes the proof of Theorem 3.

Proof of Theorem 4. We proceed as in the proof of Theorem 2. Write $r = q - 1$ and let

$$T(x) = \sum_{0 \le y \le x} \chi(ag^y + b)$$

for $x \ge 0$. The function $T(rx)$ has a convergent Fourier series

$$T(rx) = \sum_{m=-\infty}^{\infty} c'_m e^{2\pi i m x} \quad \text{for } 0 < x < 1. \tag{4.5}$$

Clearly

$$c'_0 = \frac{1}{r} \sum_{l=0}^{r-1} T(l);$$

and, for $m \ne 0$, by an argument used in Section 3 we have

$$\begin{aligned} c'_m &= \int_0^1 T(rx) e^{-2\pi i m x}\, dx \\ &= \frac{1}{2\pi i m}\Big(\sum_{l=0}^{r-1} \chi(ag^l + b) e_r(-lm) - \sum_{l=0}^{r-1} \chi(ag^l + b)\Big) \\ &= \frac{1}{2\pi i m} \sum_{l=0}^{r-1} \chi(ag^l + b) e_r(-lm) + \frac{\chi(b)}{2\pi i m} \\ &= \frac{1}{2\pi i m r} \sum_{\psi} J(\chi, \overline{\chi}\psi) \psi(a) \chi\overline{\psi}(-b) \sum_{l=0}^{r-1} \psi(g^l) e_r(-lm) + \frac{\chi(b)}{2\pi i m} \\ &= \frac{1}{2\pi i m} J(\chi, \overline{\chi}\psi_m) \psi_m(a) \chi\overline{\psi}_m(-b) + \frac{\chi(b)}{2\pi i m}, \end{aligned} \tag{4.6}$$

where $\psi_m \in \widehat{F_q^*}$ being defined by $\psi_m(g) = e_r(s)$ with $0 < s \le r$ and $s \equiv m \pmod{r}$.

Let χ be defined by $\chi(g) = e_r(t)$ with $0 < t < r$. Then $\psi_m \ne \varepsilon, \chi$ if and only if $m \not\equiv 0, t \pmod{r}$. Thus, by (4.4) and (4.6) we get

$$|c'_m| \ge \frac{1}{2\pi |m|}(\sqrt{q} - 1) \quad \text{for } m \not\equiv 0, t \pmod{r}.$$

Then, Theorem 4 follows from this, (4.5) and Parseval's formula as in Section 3.

Acknowledgements. The author thanks the referee for his careful reading of the manuscript and suggestions on the revision of the paper.

References

[1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), 179–192.

[2] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer, 1980.

[3] E. Dobrowolski and K. S. Williams, *An upper bound for the sum* $\sum_{n=a+1}^{a+H} f(n)$ *for a certain class of functions* f, Proc. Amer. Math. Soc. 114 (1992), 29–35.

[4] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, 1983.

[5] H. Niederreiter, *On the distribution of pseudo-random numbers generated by the linear congruential method. III*, Math. Comp. 30 (1976), 571–597.

[6] —, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. 84 (1978), 957–1041.

Department of Mathematics
University of Science and Technology of China
Hefei, 230026, Anhui
P.R. China
E-mail: yuhb@ustc.edu.cn

Received on 23.10.1998
and in revised form on 14.8.2000 (3486)