Canad. Math. Bull. Vol. **44** (1), 2001 pp. 87–92

# On a New Exponential Sum

Daniel Lieman and Igor Shparlinski

*Abstract.* Let $p$ be prime and let $\vartheta \in \mathbb{Z}_p^*$ be of multiplicative order $t$ modulo $p$. We consider exponential sums of the form

$$S(a) = \sum_{x=1}^{t} \exp(2\pi i a \vartheta^{x^2}/p)$$

and prove that for any $\varepsilon > 0$

$$\max_{\gcd(a,p)=1} |S(a)| = O(t^{5/6+\varepsilon} p^{1/8}).$$

Let $p$ be a large prime and let $\vartheta \in \mathbb{Z}_p^*$ be of multiplicative order $t$ modulo $p$. We put

$$\mathbf{e}(z) = \exp(2\pi i z/p).$$

We estimate exponential sums of the form

$$S(a) = \sum_{x=1}^{t} \mathbf{e}(a\vartheta^{x^2}).$$

The question has been motivated by some results of [1] and in fact in the proof we use some estimates from that paper, see Lemma 2 below.

We remark that the similarly looking sums

$$T(a) = \sum_{x=1}^{t} \mathbf{e}(a\vartheta^{x})$$

have been studied in many papers by many authors and have numerous applications, see [4, 5, 6, 7, 8] and references therein.

Throughout the paper the implied constants in symbols '$O$' and '$\ll$' may occasionally, where obvious, depend on the small positive parameter $\varepsilon$ and are absolute otherwise (we recall that $A \ll B$ is equivalent to $A = O(B)$).

In particular, the following bounds have been obtained in [4],

$$\max_{\gcd(a,p)=1} |T(a)| \ll \begin{cases} p^{1/2}, & \text{if } t \geq p^{2/3}; \\ p^{1/4}t^{3/8}, & \text{if } p^{1/2} \leq t \leq p^{2/3}; \\ p^{1/8}t^{5/8}, & \text{if } p^{1/3} \leq t \leq p^{1/2}. \end{cases}$$

Received by the editors March 9, 1999.

The first author was supported in part by the National Science Foundation. The second author was supported in part by the Australian Research Council.

AMS subject classification: Primary: 11L07, 11T23, 11B50; secondary: 11K31, 11K38.

We note that the first bound has been known (with the implied constant $c = 1$) for long time [5, 6, 7, 8] but the second and the third estimates are due to [4] and have been obtained by a different method.

We also remark the papers [2, 3] in which, motivated by some cryptographic applications, the sums

$$U(a) = \sum_{x=1}^{\tau} \mathbf{e}(a\vartheta^{e^x}),$$

where $e$ is some integer and $\tau$ is the period of the sequence $\vartheta^{e^x}$, $x = 1, 2, \dots$ modulo $p$, have been estimated. In particular, it is shown in [3] that if the sequence $\vartheta^{e^x}$, $x = 1, 2, \dots$ is purely periodic modulo $p$ then for any integer $\nu \geq 1$

$$\max_{\gcd(a,p)=1} |U(a)| = O(\tau^{1-(2\nu+1)/2\nu(\nu+1)} p^{(3\nu+2)/4\nu(\nu+1)+\varepsilon}).$$

Nevertheless it is not clear how to use methods of the above works in order to estimate sums $S(a)$. Thus here we use quite different arguments.

Let $\tau(k)$ and $\varphi(k)$ denote the number of distinct positive divisors and the Euler function of an integer $k \geq 1$, respectively. We use the following well known bounds

$$\tau(k) = O(k^{\varepsilon}), \quad \varphi(k) \gg \frac{k}{\ln \ln(k+2)}, \tag{1}$$

see Theorems 5.1 and 5.2 in Chapter 5 of [9].

***Lemma 1*** *For any integer $t \geq 1$ the number $N(t)$ of solutions $1 \leq x, y \leq t$ of the congruence $x^2 \equiv y^2 \pmod t$ is bounded by*

$$N(t) \leq 4t\tau(t).$$

**Proof** For each pair of integers $u, v$ the system of congruences

$$x + y \equiv u \pmod t, \quad x - y \equiv v \pmod t$$

has at at most 4 solutions in $1 \leq x, y \leq t$. Indeed, from the above congruences we conclude that

$$2x \equiv u + v \pmod t, \quad 2y \equiv u - v \pmod t.$$

Thus, $x$ and $y$ are uniquely defined modulo $t/\gcd(2,t)$. Therefore $N(t) \leq 4M(t)$, where $M(t)$ is the number of solutions of the congruence

$$uv \equiv 0 \pmod t, \quad 1 \leq u, v \leq t.$$

For $M(t)$ we have

$$M(t) = \sum_{u=1}^{t} \gcd(t,u) = \sum_{d|t} d \sum_{\substack{u=1 \\ \gcd(u,t)=d}}^{t} 1 \leq \sum_{d|t} d\varphi(t/d) \leq t\tau(t)$$

and the desired result follows. ∎

We also need the following estimate which is essentially Theorem 8 of [1].

https://doi.org/10.4153/CMB-2001-010-1 Published online by Cambridge University Press

***Lemma 2*** *For any integers a and b such that* $\gcd(a, b, p) = 1$*, the bound*

$$\sum_{v=1}^{t}\Big|\sum_{u=1}^{t}\mathbf{e}(a\vartheta^{u}+b\vartheta^{uv})\Big| = O(t^{5/3}p^{1/4})$$

*holds.*

Now we are ready to prove our main result.

***Theorem 1*** *The bound*

$$\max_{\gcd(a,p)=1}|S(a)| = O(t^{5/6+\varepsilon}p^{1/8})$$

*holds.*

**Proof** For an integer $x$ let us denote by $Q(x)$ the number of solutions $1 \le y \le t$ of the congruence $x \equiv y^2 \pmod t$.

Let $\mathcal{Q}$ denote the set of squares modulo $t$ which are relatively prime to $t$. That is,

$$\mathcal{Q} = \{z \mid 1 \le z \le t, \gcd(z,t) = 1, Q(z) \ge 1\}.$$

We remark that

$$\sum_{x=1}^{t} Q(x) = t, \quad \sum_{z\in\mathcal{Q}} Q(z) = \varphi(t), \quad \sum_{x=1}^{t} Q^2(x) = N(t). \tag{2}$$

From the Cauchy-Schwarz inequality and from (2) we conclude

$$\varphi(t)^2 = \Big(\sum_{z\in\mathcal{Q}} Q(z)\Big)^2 \le |\mathcal{Q}|\sum_{z\in\mathcal{Q}} Q^2(z) \le |\mathcal{Q}|\sum_{z=1}^{t} Q^2(z) = |\mathcal{Q}|N(t),$$

Accordingly,

$$|\mathcal{Q}| \ge \varphi(t)^2 N(t)^{-1}. \tag{3}$$

Obviously $Q(x) = Q(xz)$ for any integer $x$ and any $z \in \mathcal{Q}$. Therefore

$$S(a) = \sum_{x=1}^{t} Q(x)\mathbf{e}(a\vartheta^{x}) = \frac{1}{|\mathcal{Q}|}\sum_{z\in\mathcal{Q}}\sum_{x=1}^{t} Q(xz)\mathbf{e}(a\vartheta^{xz}) = \frac{1}{|\mathcal{Q}|}W(a), \tag{4}$$

where

$$W(a) = \sum_{x=1}^{t} Q(x)\sum_{z\in\mathcal{Q}}\mathbf{e}(a\vartheta^{xz}).$$

From the Cauchy-Schwarz inequality and (2) we derive

$$\begin{aligned}|W(a)|^2 &\le \sum_{x=1}^{t} Q^2(x) \sum_{x=1}^{t} \Big| \sum_{z\in\Omega} \mathbf{e}(a\vartheta^{xz}) \Big|^2 \\ &= N(t) \sum_{z_1,z_2\in\Omega} \sum_{x=1}^{t} \mathbf{e}\big(a(\vartheta^{xz_1} - \vartheta^{xz_2})\big) \\ &\le N(t) \sum_{\substack{z_1,z_2=1\\ \gcd(z_1z_2,t)=1}}^{t} \Big| \sum_{x=1}^{t} \mathbf{e}\big(a(\vartheta^{xz_1} - \vartheta^{xz_2})\big) \Big|.\end{aligned}$$

Substituting $u \equiv xz_1 \pmod t$ and $v \equiv z_2/z_1 \pmod t$ and then extending the summation over all $v = 1, \dots, t$, we obtain

$$|W(a)|^2 \le N(t)\varphi(t) \sum_{v=1}^{t} \Big| \sum_{u=1}^{t} \mathbf{e}\big(a(\vartheta^{u} - \vartheta^{uv})\big) \Big|.$$

If $\gcd(a, p) = 1$ then from Lemma 2 we conclude

$$|W(a)|^2 \ll N(t)\varphi(t)t^{5/3}p^{1/4}.$$

Substituting this bound in (4) and using the inequality (3) we derive

$$|S(a)| \ll N(t)^{3/2}\varphi(t)^{-3/2}t^{5/6}p^{1/8}.$$

Now the desired result follows from Lemma 1 and the bounds (1). ■

Let us denote by $D(a)$ the discrepancy of the following sequence of fractional parts

$$\left\{ \frac{a\vartheta^{x^2}}{p} \right\}, \quad x = 1, \dots, t, \tag{5}$$

that is,

$$D(a) = \sup_{0\le\alpha\le 1} \left| \frac{A_a(\alpha)}{t} - \alpha \right|,$$

where $A_a(\alpha)$ is the number of fractions (5) which hit the interval $[0, \alpha)$.

Applying Corollary 3.11 of [8] we immediately obtain the following bound.

***Theorem 2*** *For any integer $a$ such that $\gcd(a, p) = 1$, the bound*

$$D(a) = O(t^{5/6+\varepsilon}p^{1/8})$$

*holds.*

https://doi.org/10.4153/CMB-2001-010-1 Published online by Cambridge University Press

It is easy to see that the bounds of Theorems 1 and 2 are non-trivial for $t \geq p^{3/4+\varepsilon}$. It would be useful to reduce the exponent $3/4$. In particular it has been explained in [1] why it is important to obtain non-trivial estimates in the range $t \geq p^{2/3}$.

We believe that our method can be applied to sums

$$S_n(a) = \sum_{x=1}^{t} \mathbf{e}(a\vartheta^{x^n})$$

as well.

Unfortunately we still do not know how to estimate more general sums

$$S(a,b) = \sum_{x=1}^{p-1} \mathbf{e}(a\vartheta^{x^2} + b\vartheta^x)$$

which are related to statistical properties of the Diffie-Hellman pairs $(\vartheta^x, \vartheta^{x^2})$ modulo $p$; we refer to [1] for more details.

Sums

$$S(f;a) = \sum_{x=1}^{t} \mathbf{e}(a\vartheta^{f(x)})$$

with arbitrary polynomials $f(X) \in \mathbb{Z}[X]$ are of interest as well.

Finally we remark that the sequence

$$u_x \equiv \vartheta^{x^2} \pmod{p}$$

satisfies the following simple recurrence relation

$$u_{x+3} \equiv u_{x+2}^3 u_{x+1}^{-3} u_x \pmod{p}.$$

Thus, this and our uniformity of distribution results, can probably make this sequence useful for pseudo-random number generation.

**Acknowledgment** A part of this work was done during a visit by D. L. to Macquarie University, whose hospitality and support are gratefully acknowledged.

## References

[1] R. Canetti, J. B. Friedlander, S. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski, *On the statistical properties of the Diffie-Hellman distribution*. Israel J. Math., (to appear).

[2] J. B. Friedlander, D. Lieman and I. E. Shparlinski, *On the distribution of the RSA generator*. Proc. Intern. Conf. on Sequences and their Applications (SETA '98), Singapore, (eds. C. Ding, T. Helleseth and H. Niederreiter), Springer-Verlag, London, 1999, 205–212.

[3] J. B. Friedlander and I. E. Shparlinski, *On the distribution of the Power generator*. Math. Comp., to appear.

[4] S. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*. Cambridge Univ. Press, Cambridge, 1999.

[5] N. M. Korobov, *On the distribution of digits in periodic fractions*. Math. USSR-Sb. **18**(1972), 659–676.

[6] ______, *Exponential sums and their applications*. Kluwer Acad. Publ., Dordrecht, 1992.
[7] H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*. Bull. Amer. Math. Soc. **84**(1978), 957–1041.
[8] H. Niederreiter, *Random number generation and Quasi-Monte Carlo methods*. SIAM Press, 1992.
[9] K. Prachar, *Primzahlverteilung*. Springer-Verlag, Berlin, 1957.

*Department of Mathematics*
*University of Missouri*
*Columbia, Missouri 65211*
*USA*
*e-mail: lieman@math.missouri.edu*

*Department of Computing*
*Macquarie University*
*NSW 2109*
*Australia*
*e-mail: igor@comp.mq.edu.au*