ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 34, Number 4, Winter 2004

EXPONENTIAL FUNCTION ANALOGUE OF KLOOSTERMAN SUMS

IGOR E. SHPARLINSKI

ABSTRACT. We consider exponential sums of the form

$$\mathcal{K}_g(a,b) = \sum_{\substack{x=1\\ \gcd(x,t)=1}}^{t} \exp\Big(2\pi i(ag^x + bg^{x^{-1}})/p\Big),$$

where g is of multiplicative order t modulo the prime p. We obtain a nontrivial upper bound on these sums on average over all elements g of multiplicative order t, provided that $t \geq p^{3/4+\delta}$ with an arbitrary fixed $\delta > 0$.

1. Introduction.

Let p be a prime, and let $\mathbf{F}_p$ be a finite field of p elements. For an integer $t \geq 1$ we denote by $\mathbf{Z}_t = \{0, \dots, t-1\}$ the residue ring modulo t and we denote by $\mathbf{Z}_t^*$ the subset of $\mathbf{Z}_t$ consisting of $\varphi(t)$ invertible elements, where $\varphi(t)$ is the Euler function. We also identity $\mathbf{F}_p$ with the set $\{0, \dots, p-1\}$.

Finally we define $\mathbf{e}(z) = \exp(2\pi i z/p)$ and use $\log z$ for the natural logarithm of z.

For a divisor $t|p-1$ we denote by $\mathcal{U}_t$ the set of elements $g \in \mathbf{F}_p^*$ of multiplicative order t, that is,

$$\mathcal{U}_t = \{g \in \mathbf{F}_p^* \mid g^s \neq 1,\ 1 \leq s < t;\ g^t = 1\}.$$

It is easy to see that $\#\mathcal{U}_t = \varphi(t)$.

For $g \in \mathcal{U}_t$, we consider exponential sums

$$\mathcal{K}_g(a,b) = \sum_{x \in \mathbf{Z}_t^*} \mathbf{e}(ag^x + bg^{x^{-1}}),$$

where $a, b \in \mathbf{F}_p$.

Received by the editors on October 16, 2001.

These sums appear to be new and have never been studied in the literature. On the other hand, we remark that these sums can be considered as exponential function analogues of the famous *Kloosterman* sums

$$K(a,b) = \sum_{x \in \mathbf{F}_p^*} \mathbf{e}(ax + bx^{-1}).$$

Unfortunately it is not clear how to obtain "individual" estimates of the sums $\mathcal{K}_g(a,b)$. Here we derive an upper bound on $\mathcal{K}_g(a,b)$ "on average" over all $g \in \mathcal{U}_t$. This bound is nontrivial for $t \ge p^{3/4+\delta}$ for any fixed $\delta > 0$ and sufficiently large p.

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

Our results rely on the following estimate for certain double exponential sums from [**2**]; see the proof of Theorem 8 of that paper. Let $\lambda \in \mathbf{F}_p^*$ be of multiplicative order t. For any $a, b \in \mathbf{F}_p^*$ we have the bound

$$\sum_{u \in \mathbf{Z}_t} \left| \sum_{v \in \mathbf{Z}_t} \mathbf{e}(a\lambda^v + b\lambda^{uv}) \right|^4 \ll pt^{11/3}. \tag{1}$$

2. Main results.

Our main estimate is the following.

Theorem 1. *The bound*

$$\max_{\gcd(a,b,p)=1} \frac{1}{\varphi(t)} \sum_{g \in \mathcal{U}_t} |\mathcal{K}_g(a,b)| \ll p^{1/8+\varepsilon} t^{5/6}$$

holds.

Proof. It is easy to see that $\mathcal{K}_g(a,b) = \mathcal{K}_g(b,a)$. Therefore, without loss of generality, we can assume that $\gcd(a,p) = 1$.

Fix an arbitrary element $\vartheta \in \mathcal{U}_t$. Then

$$\mathcal{U}_t = \{\vartheta^u \mid u \in \mathbf{Z}_t^*\}.$$

Putting

$$\sigma = \sum_{g\in\mathcal{U}_t} |\mathcal{K}_g(a,b)|$$

we obtain

$$\sigma = \sum_{g\in\mathcal{U}_t} |\mathcal{K}_g(a,b)| = \sum_{u\in\mathbf{Z}_t^*} \left| \sum_{x\in\mathbf{Z}_t^*} \mathbf{e}(a\vartheta^{ux} + b\vartheta^{ux^{-1}}) \right|.$$

Remarking that, for $u \in \mathbf{Z}_t^*$, ux runs through $\mathbf{Z}_t^*$ together with x, we obtain

$$\sigma = \sum_{g\in\mathcal{U}_t} |\mathcal{K}_g(a,b)| = \sum_{u\in\mathbf{Z}_t^*} \left| \sum_{x\in\mathbf{Z}_t^*} \mathbf{e}(a\vartheta^{u^2x} + b\vartheta^{x^{-1}}) \right|.$$

Let $N(v)$ be the number of solutions of the convergence $u^2 \equiv v \pmod t$. Then

$$\sigma = \sum_{v\in\mathbf{Z}_t^*} N(v) \left| \sum_{x\in\mathbf{Z}_t^*} \mathbf{e}(a\vartheta^{vx} + b\vartheta^{x^{-1}}) \right|.$$

It has been shown in Lemma 5 of [**5**] that

$$\sum_{v\in\mathbf{Z}_t^*} N(v) = O(t^{1+\varepsilon}). \tag{2}$$

Using the Cauchy inequality and the bound (2), we derive

$$\begin{aligned}\sigma^2 &= \sum_{v\in\mathbf{Z}_t^*} N(v)^2 \sum_{x,y\in\mathbf{Z}_t^*} \mathbf{e}(b(\vartheta^{x^{-1}} - \vartheta^{y^{-1}})) \\ &\quad\times \sum_{v\in\mathbf{Z}_t^*} \mathbf{e}(a(\vartheta^{vx} - \vartheta^{vy})) \\ &\ll t^{1+\varepsilon} \sum_{x,y\in\mathbf{Z}_t^*} \left| \sum_{v\in\mathbf{Z}_t^*} \mathbf{e}(a(\vartheta^{vx} - \vartheta^{vy})) \right|.\end{aligned}$$

Substituting xy instead of y, we obtain

$$\sigma^2 \ll t^{1+\varepsilon} \sum_{x,y\in\mathbf{Z}_t^*} \left| \sum_{v\in\mathbf{Z}_t^*} \mathbf{e}(a(\vartheta^{vx} - \vartheta^{vxy})) \right|.$$

By the Hölder inequality we have

$$\sigma^8 \ll t^{10+4\varepsilon} \sum_{x,y\in \mathbf{Z}_t^*} \left| \sum_{v\in \mathbf{Z}_t^*} \mathbf{e}(a(\vartheta^{vx} - \vartheta^{vxy}))\right|^4.$$

For each $x \in \mathbf{Z}_t^*$ we apply (1) with $\lambda = \vartheta^x$ getting

$$\sigma^8 \ll pt^{44/3+4\varepsilon}.$$

Recalling that

$$\#\mathcal{U}_t = \varphi(t) \gg \frac{t}{\log\log(t+2)},$$

see Theorem 5.1 of [**9**, Chapter 1], we derive the desired result. $\square$

It is easy to see that the bound of Theorem 1 is nontrivial for $t \ge p^{3/4+\delta}$ with an arbitrary fixed $\delta > 0$. In particular, if $t = p-1$, that is, for the average value of over primitive roots, we obtain

$$\max_{\gcd(a,b,p)=1} \frac{1}{\varphi(p-1)} \sum_{g\in\mathcal{U}_{p-1}} |\mathcal{K}_g(a,b)| \ll p^{23/24+\varepsilon}.$$

Given a set $\mathcal{M}$ of N points $(u_\nu, v_\nu) \in [0,1]^2$, $\nu = 1,\dots,N$, of the unit square, we define the *discrepancy* $D(\mathcal{M})$ of this set as

$$D(\mathcal{M}) = \sup_B \left| \frac{A_N(B)}{N} - \mu(B)\right|,$$

where the supremum is taken over all boxes $B = [\alpha,\beta]\times[\gamma,\delta] \in [0,1]^2$, $\mu(B) = (\beta-\alpha)(\delta-\gamma)$ and $A_N(B)$ is the number of points of this set which hit B.

For $g \in \mathcal{U}_t$, we denote by D_g the discrepancy of the following set of pairs of fractional parts

$$\left(\left\{\frac{g^x}{p}\right\}, \left\{\frac{g^{x^{-1}}}{p}\right\}\right), \quad x \in \mathbf{Z}_t^*.$$

Theorem 2. *The bound*

$$\frac{1}{\varphi(t)} \sum_{g \in \mathcal{U}_t} D_g \ll p^{1/8+\varepsilon} t^{-1/6}$$

holds.

Proof. From the *Erdös-Turán-Koksm inequality*, (see [**4**, Theorem 1.21]), we derive

$$D_g \ll \frac{1}{p} + \frac{1}{\varphi(t)} \sum_{0<|a|+|b|<p} \frac{1}{\max\{1,|a|\}} \frac{1}{\max\{1,|b|\}} |\mathcal{K}_g(a,b)|.$$

Therefore

$$\sum_{g \in \mathcal{U}_t} D_g \ll \frac{1}{p} + \frac{1}{\varphi(t)} \sum_{0<|a|+|b|<p} \frac{1}{\max\{1,|a|\}} \frac{1}{\max\{1,|b|\}} \sum_{g \in \mathcal{U}_t} |\mathcal{K}_g(a,b)|$$

and from Theorem 1 we derive the desired result. □

3. Remarks. Theorem 2 implies that for almost all $g \in \mathbf{F}_p^*$ of sufficiently large multiplicative order t, g^x and $g^{x^{-1}}$ behave statistically independently modulo p. This may be considered as evidence in favor of a certain cryptographic assumption about pseudorandom behavior modulo p of the pair $(g^x, g^{x^{-1}})$, $x \in \mathbf{Z}_t^*$ (see [**8, 10**]). In particular, security of several cryptographic constructions is based on the *indistinguishability assumption*, which asserts that if t is a large prime, then it is infeasible to distinguish between a stream of pairs of the shape $(g^x, g^{x^{-1}})$ and a stream of pairs of the shape (u, v), where x and (u, v) are chosen uniformly and independently at random from $\mathbf{Z}_t^*$ and $\mathbf{F}_p^* \times \mathbf{F}_p^*$, respectively, see [**8, 10**] for more details and relevant references. We see from Theorem 2 that for almost all $g \in \mathbf{F}_p^*$ these two streams of pairs have very similar statistical properties and thus are unlikely to be distinguished by statistical methods. This certainly does not imply the desired indistinguishability property but the inverse fact (nonuniformity of distribution) would certainly be disastrous for cryptographic applications of this assumption.

Our results can be viewed as analogues of those from [**2, 3**] about the statistical distribution of triples (g^x, g^y, g^{xy}), $x, y \in \mathbf{Z}_t^*$ which are motivated by the *Diffe-Hellman indistinguishability assumption* for the streams of such triples and the triples (u, v, w), $u, v, w \in \mathbf{F}_p^*$. Cryptographic relevance of results of this type has also been discussed in [**1**].

Using the extensions of the bound (1) given in [**6, 7**] to prime power and arbitrary composite moduli, one can extend our results to such moduli as well.

Finally we remark that obtaining a nontrivial upper bound for "individual" sums $\mathcal{K}_g(a, b)$ remains a challenging open question.

REFERENCES

1. D. Boneh, *The decision Diffie-Hellman problem*, Lecture Notes in Comput. Sci., vol. 1423, Springer-Verlag, Berlin, 1998, pp. 48–63.

2. R. Canetti, J.B. Friedlander, S. Konyagin, M. Larsen, D. Lieman and I.E. Shparlinski, *On the statistical properties of Diffie-Hellman distributions*, Israel J. Math. **120** (2000), 23–46.

3. R. Canetti, J.B. Friedlander and I.E. Shparlinski, *On certain exponential sums and the distribution of Diffie-Hellman triples*, J. London Math. Soc. **59** (1999), 799–812.

4. M. Drmota and R.F. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

5. J.B. Friedlander, J. Hansen and I.E. Shparlinski, *On character sums with exponential functions*, Mathematika **47** (2000), 75–85.

6. ———, *On the distribution of the power generator modulo a prime power*, Proc. DIMACS Workshop on Unusual Applications of Number Theory, 2000, Amer. Math. Soc., Providence, RI, 2004, pp. 71–79.

7. J.B. Friedlander, S.V. Konyagin and I.E. Shparlinski, *Some doubly exponential sums over* $\mathbf{Z}_m$, Acta Arith. **105** (2002), 349–370.

8. P. MacKenzie, *On the security of the SPEKE password-authenticated key exchange protocol*, Cryptology ePrint Archive, Report 2001/57, 2001, 1–19. Available from `http://eprint.iacr.org/`.

9. K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957.

10. A.-R. Sadeghi and M. Steiner, *Assumptions related to discrete logarithms: Why subtleties make a real difference*, Lecture Notes in Comput. Sci., vol. 2045, Springer-Verlag, Berlin, 2001, pp. 243–260.

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: `igor@ics.mq.edu.au`