ACTA ARITHMETICA
105.4 (2002)

Some doubly exponential sums over $\mathbb{Z}_m$

by

John B. Friedlander (Toronto), Sergei Konyagin (Moscow) and
Igor E. Shparlinski (Sydney)

1. Introduction. For an integer m we denote by $\mathbb{Z}_m$ the residue ring modulo m and by $\mathcal{U}_m = \mathbb{Z}_m^*$ the group of units of $\mathbb{Z}_m$.

Let $\vartheta \in \mathbb{Z}_m$, $\gcd(\vartheta, m) = 1$. We recall that the *multiplicative order* $\operatorname{ord}_m \vartheta$ of an integer ϑ modulo an integer $m \ge 1$ with $\gcd(\vartheta, m) = 1$ is the smallest positive integer t for which

$$\vartheta^t \equiv 1 \pmod m.$$

Define $\mathbf{e}_d(z) = \exp(2\pi i z/d)$. Given an integer ϑ with multiplicative order $\operatorname{ord}_m \vartheta = t$, for integers a, b, c we define the exponential sum

$$S_{a,b,c}(m,t) = \sum_{x,y=1}^{t} \mathbf{e}_m(a\vartheta^x + b\vartheta^y + c\vartheta^{xy}).$$

We obtain a non-trivial upper bound for these sums. Specifically we prove

$$S_{a,b,c}(m,t) = O(t^{21/16} m^{5/8+\varepsilon})$$

provided that $\gcd(ac, m) = 1$ with a somewhat weaker result for the general case. From this we deduce the uniformity of distribution modulo m of the triples $(\vartheta^x, \vartheta^y, \vartheta^{xy})$, $x, y = 1, \dots, t$, provided that $t \ge m^{10/11+\varepsilon}$. As in [2, 3] we actually study the slightly simpler sums

$$W_{a,c}(m,t) = \sum_{y=1}^{t} \Big| \sum_{x=1}^{t} \mathbf{e}_m(a\vartheta^x + c\vartheta^{xy}) \Big|$$

for which obviously $|S_{a,b,c}| \le \min\{W_{a,c}, W_{b,c}\}$.

2000 *Mathematics Subject Classification*: 11L07, 11K45, 11Y16.

Research of J. B. Friedlander supported in part by NSERC grant A5123.

Research of S. Konyagin supported in part by RFBR grants 02-01-00248 and 00-15-96109.

Research of I. E. Shparlinski supported in part by ARC grant A69700294.

Note that in the above sums (and in several more yet to come) we have suppressed in the notation the dependence on ϑ. This does not mean we are claiming that such sums are the same for all ϑ having the same order t. However in all of our results the bounds obtained are uniform for all such ϑ.

For an integer $n \geq 1$ we define the *Carmichael function* $\lambda(n)$ as the largest multiplicative order occurring among elements of the unit group in the residue ring modulo n. More explicitly, for a prime power p^k we have

$$\lambda(p^k) = \begin{cases} p^{k-1}(p-1) & \text{if } p \geq 3 \text{ or } k \leq 2, \\ 2^{k-2} & \text{if } p = 2 \text{ and } k \geq 3, \end{cases}$$

and finally,

$$\lambda(n) = \operatorname{lcm}(\lambda(p_1^{k_1}), \dots, \lambda(p_\nu^{k_\nu})),$$

where

$$n = p_1^{k_1} \dots p_\nu^{k_\nu}$$

is the prime number factorization of n. Thus $\lambda(m)$ is a close relative of the better known Euler function $\varphi(m)$ which denotes the cardinality of the unit group $\mathcal{U}_m$.

We also use our method, combined with some estimates from [10], to estimate the related sums

$$V_{a,c}(m) = \sum_{u \in \mathcal{U}_m} \sum_{y=1}^{\lambda(m)} \mathbf{e}_m(au + cu^y)$$

as well as a number of similar sums.

These sums are generalizations to arbitrary modulus of sums which have been estimated in [2, 3] for the case of $m = p$ prime. However some crucial ingredients of the methods of [2, 3] do not hold for a general composite modulus, so we need to find alternative arguments to deal with such m.

We derive a variety of applications of these to problems from both number theory and complexity theory, as were treated for special moduli using the results of [2, 3]. In particular we extend to arbitrary moduli the results of [6–8, 11–13, 16, 21], which had been obtained only for moduli of special arithmetic structure, such as primes, products of two primes, high powers of small primes. These applications include an upper bound for the discrepancy of the power generator of pseudorandom numbers (which, even for general composite m, may have cryptographic applications) and lower bounds for the communication complexity of modular exponentiation. As in the case of the exponential sum bounds, the extension of these applications also requires some new ideas which may be of independent interest.

Throughout the paper the implied constants in symbols "O", "$\gg$" and "$\ll$" may, where obvious, depend on the small positive parameter ε. A few

other dependencies, on the positive integer parameters n, ν, occur in Section 3 alone and are mentioned in the relevant statements (we recall that $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$).

Acknowledgements. We thank Carl Pomerance for informing us about his recent unpublished results with Greg Martin concerning the normal size of the iterations of the Carmichael function.

2. Preliminaries. In this section we collect known results and some easy consequences of them that we shall need.

LEMMA 1. *Assume $d \ge 1$ is a divisor of an integer $m > 1$. Then for any integer g with $\gcd(g, m) = 1$, $\varphi(d)/\mathrm{ord}_d\, g$ divides $\varphi(m)/\mathrm{ord}_m\, g$ and so $d/\mathrm{ord}_d\, g \le m/\mathrm{ord}_m\, g$. Also $\lambda(d)/d \ge \lambda(m)/m$.*

Proof. The first and third statements are contained in Lemma 2.2 of [10]. The second statement which is implicit in the same lemma follows at once from the first using the inequality $\varphi(m)/\varphi(d) \le m/d$. ∎

We also need the following statement which follows from Lemma 2.1 of [10].

LEMMA 2. *Let $s \ge 2$ be an integer divisor of m. Then $\lambda(s)$ divides $\lambda(m)$. Moreover, for any divisor $d \mid \lambda(s)$ the number of integers $g \in \mathcal{U}_m$ with $\mathrm{ord}_s\, g = \lambda(s)/d$ does not exceed $m\varphi(s)/ds$.*

Proof. The first statement follows easily from the explicit evaluation above for the function λ. For the second part we note that it follows directly from Lemma 2.1 of [10] that there are at most $\varphi(s)/d$ such values $s \in \mathcal{U}_s$. Each such value gives rise to at most m/s values in $\mathcal{U}_m$. ∎

We shall need the basic orthogonality property of characters of $\mathbb{Z}_m$; see for example Exercise 11.a in Chapter 3 of [24].

LEMMA 3. *For any integers u and $m \ge 1$,*

$$\sum_{l=0}^{m-1} \mathbf{e}_m(lu) = \begin{cases} m & \text{if } u \equiv 0 \pmod m, \\ 0 & \text{if } u \not\equiv 0 \pmod m. \end{cases}$$

For integers a and $k \ge 1$ we define the exponential sum

$$\sigma_k(a) = \sum_{x=1}^{t} \mathbf{e}_m(a\vartheta^{kx}).$$

The following estimate is a very straightforward extension of some previously known results; see [14, Lemma 2] or [18, Theorem 8.2].

LEMMA 4. *Assume that $\gcd(a, m) = \delta$ and that $\gcd(k, t) = \gamma$. Then*

$$|\sigma_k(a)| \le \gamma\delta^{1/2}m^{1/2}. \tag{1}$$

Proof. In case $\gamma = \delta = 1$ the result is well known. We reduce the general case to this one. Put $g = \vartheta^k$. For $\delta > 1$, we denote by $\tau_\mu = \operatorname{ord}_\mu g$ the multiplicative order of g modulo $\mu = m/\delta$, and $\tau = \operatorname{ord}_m g$ the multiplicative order of g modulo m so that $\tau = t/\gamma$. We also put $a/\delta = \alpha$ so that we have $\gcd(\alpha, \mu) = 1$ and hence

$$\Big|\sum_{x=1}^{t} \mathbf{e}_m(ag^x)\Big| = \gamma\Big|\sum_{x=1}^{\tau} \mathbf{e}_m(ag^x)\Big| = \frac{\gamma\tau}{\tau_\mu}\Big|\sum_{x=1}^{\tau_\mu} \mathbf{e}_\mu(\alpha g^x)\Big| \le \frac{\gamma\tau}{\tau_\mu}\,\mu^{1/2}.$$

The proof now follows from Lemma 1. ∎

For a sequence of N points

$$\Gamma = (\gamma_{0,x}, \dots, \gamma_{n-1,x})_{x=1}^{N} \tag{2}$$

in the n-dimensional unit cube, denote by Δ_Γ its *discrepancy* which we define to be

$$\Delta_\Gamma = \sup_{B \subseteq [0,1)^n} \left|\frac{T_\Gamma(B)}{N} - |B|\right|,$$

where $T_\Gamma(B)$ is the number of points of the sequence Γ which hit the box

$$B = [\alpha_0, \beta_0) \times \ldots \times [\alpha_{n-1}, \beta_{n-1}) \subseteq [0,1)^n$$

and the supremum is taken over all such boxes.

For an integer vector $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$ we define

$$|\mathbf{a}| = \max_{i=1,\dots,n} |a_i|, \qquad r(\mathbf{a}) = \prod_{i=1}^{n} \max\{|a_i|, 1\}. \tag{3}$$

One of our basic tools to study the uniformity of distribution is the *Koksma–Szüsz inequality*. This statement provides a very important link between the discrepancy and exponential sums. In the case of dimension $n = 1$ it is very well known as the Erdős–Turán inequality. We present it in the following form; see also Theorem 1.21 of [4].

Lemma 5. *There exists an absolute constant $C > 0$ such that, for any integer $L > 1$, for the discrepancy of a sequence of points* (2) *we have the bound*

$$\Delta_\Gamma < C^n\Big(\frac{1}{L+1} + \frac{1}{N}\sum_{0<|\mathbf{a}|\le L} \frac{1}{r(\mathbf{a})}\Big|\sum_{x=1}^{N} \mathbf{e}\Big(\sum_{j=0}^{n-1} a_j\gamma_{j,x}\Big)\Big|\Big),$$

where $|\mathbf{a}|$, $r(\mathbf{a})$ are defined by (3) *and the sum is taken over all integer vectors $\mathbf{a} = (a_0, \dots, a_{n-1}) \in \mathbb{Z}^n$ with $0 < |\mathbf{a}| \le L$.*

Let $\tau(k)$ denote the number of positive integer divisors of an integer $k \ge 1$. We use the well known bounds

$$\varphi(k) \gg \frac{k}{\log\log 3k} \tag{4}$$

and

$$\log \tau(k) \ll \frac{\log k}{\log\log 3k}; \tag{5}$$

see for example Theorems 5.1 and 5.2 of Chapter 1 of [19].

3. Exponential congruences. We define

$$\alpha_\nu = \frac{1}{2^{\nu-2}}, \quad \beta_\nu = \frac{\nu-1}{2^{\nu-2}}, \quad \gamma_\nu = \frac{\nu-2}{2^{\nu-2}}, \quad \nu = 2, 3, \dots$$

The following result is a generalization of a bound from [20], which applied only to congruences modulo a prime power.

LEMMA 6. *Suppose that* $\gcd(a_1 \dots a_n, m) = 1$ *and* $\gcd(\vartheta_1 \dots \vartheta_n, m) = 1$. *Let*

$$\varrho = \max_{1 \le i \le n} \min_{j \ne i} \varrho(i, j)$$

where $\varrho(i, j)$ *denotes the smallest integer* $s \ge 1$ *such that* $\vartheta_i^s \equiv \vartheta_j^s \pmod m$, $1 \le i, j \le n$. *Then for any* $n \ge 2$, *the number of solutions*, $T_n(N, m)$, *to the congruence*

$$a_1\vartheta_1^x + \dots + a_n\vartheta_n^x \equiv 0 \pmod m, \quad 1 \le x \le N, \tag{6}$$

satisfies the bound

$$T_n(N, m) \ll (N^{1-\alpha_n} + N\varrho^{-\beta_n} m^{\gamma_n}) m^\varepsilon,$$

where the implied constant is allowed to depend on n *as well as* ε.

Proof. We prove the bound by induction on n. Without loss of generality we can assume that

$$\varrho = \min_{2 \le j \le n} \varrho(1, j).$$

It is easy to see that for $n = 2$ we have $T_n(N, m) \le N/\varrho + 1$.

Assume now that $n \ge 3$ and that the statement holds for congruences with fewer than n terms. Observe that $T_n(N, m)^2$ is equal to the number of solutions to the system of congruences

$$\begin{aligned} a_1\vartheta_1^x + \dots + a_n\vartheta_n^x &\equiv 0 \pmod m, \\ a_1\vartheta_1^{x+y} + \dots + a_n\vartheta_n^{x+y} &\equiv 0 \pmod m, \end{aligned}$$

where

$$1 \le x \le N, \quad 1 - x \le y \le N - x,$$

and therefore it is bounded by the number of solutions to the system of congruences

$$\begin{aligned} a_1\vartheta_1^x + \dots + a_n\vartheta_n^x &\equiv 0 \pmod m, \\ a_1\vartheta_1^{x+z} + \dots + a_n\vartheta_n^{x+z} &\equiv 0 \pmod m, \end{aligned}$$

where

$$1 \le x \le N, \quad -N \le z \le N.$$

Eliminating the term $a_n\vartheta_n^{x+z}$ from the second congruence we obtain

$$a_1\vartheta_1^x(\vartheta_1^z-\vartheta_n^z)+\ldots+a_{n-1}\vartheta_{n-1}^x(\vartheta_{n-1}^z-\vartheta_n^z)\equiv 0 \pmod m. \tag{7}$$

For $\delta \mid m$ we define r_δ to be the smallest integer $r>0$ such that $\vartheta_1^r \equiv \vartheta_n^r \pmod\delta$. In particular we have $\varrho \le r_m$. From Lemma 1 we see

$$r_\delta \ge \frac{\delta r_m}{m} \ge \frac{\delta\varrho}{m}.$$

Define

$$\mathcal{Q}_\delta = \{z : -N \le z \le N,\ \gcd(\vartheta_1^z-\vartheta_n^z,\ldots,\vartheta_{n-1}^z-\vartheta_n^z,m)=\delta\},$$
$$\mathcal{P}_\delta = \{z : -N \le z \le N,\ \vartheta_{n-1}^z-\vartheta_n^z \equiv 0 \pmod\delta\}.$$

Obviously $\mathcal{Q}_\delta \subseteq \mathcal{P}_\delta$.

Let $\eta = m/\varrho$. For $\delta > \eta$ we use the estimate

$$|\mathcal{Q}_\delta| \le |\mathcal{P}_\delta| \le 2\left\lfloor \frac{N}{r_\delta}\right\rfloor + 1 \le 2\,\frac{N\eta}{\delta}+1 \tag{8}$$

while for $\delta \le \eta$ we can use the estimate

$$|\mathcal{Q}_\delta| \le 2N+1. \tag{9}$$

Let R_δ denote the smallest integer $s \ge 1$ with $\vartheta_i^s \equiv \vartheta_1^s \pmod{m/\delta}$ for at least one i, $2 \le i \le n$. Obviously $R_1 \ge \varrho$. Also, as before we obtain $R_\delta \ge R_1/\delta \ge \varrho/\delta$.

For any $z \in \mathcal{Q}_\delta$ by the inductive hypothesis we see that the number of x which satisfy the congruence (7) is

$$O((N^{1-\alpha_{n-1}} + NR_\delta^{-\beta_{n-1}}(m/\delta)^{\gamma_{n-1}})m^\varepsilon)$$
$$= O((N^{1-\alpha_{n-1}} + N\varrho^{-\beta_{n-1}}m^{\gamma_{n-1}}\delta^{\beta_{n-1}-\gamma_{n-1}})m^\varepsilon).$$

Alternatively this number can be estimated trivially as being at most N.

Combining the above estimates with (8) and (9), we derive that

$$T_n(N,m)^2 \ll (S_1+S_2)m^\varepsilon$$

where

$$S_1 = N\sum_{\substack{\delta\mid m\\ \delta\le\eta}} \min\{N^{1-\alpha_{n-1}} + N\varrho^{-\beta_{n-1}}m^{\gamma_{n-1}}\delta^{\beta_{n-1}-\gamma_{n-1}}, N\},$$

$$S_2 = \sum_{\substack{\delta\mid m\\ \delta>\eta}} \min\{N^{1-\alpha_{n-1}} + N\varrho^{-\beta_{n-1}}m^{\gamma_{n-1}}\delta^{\beta_{n-1}-\gamma_{n-1}}, N\}\left(\frac{N\eta}{\delta}+1\right).$$

We have

$$S_1 \le N\tau(m)(N^{1-\alpha_{n-1}} + N\varrho^{-\beta_{n-1}}m^{\gamma_{n-1}}\eta^{\beta_{n-1}-\gamma_{n-1}})$$
$$= N\tau(m)(N^{1-\alpha_{n-1}} + N\varrho^{-2\beta_{n-1}+\gamma_{n-1}}m^{\beta_{n-1}})$$
$$= N^2\tau(m)(N^{-2\alpha_n} + \varrho^{-2\beta_n}m^{2\gamma_n}).$$

Furthermore,

$$\begin{aligned} S_2 &\le \sum_{\substack{\delta \mid m \\ \delta \ge \eta}} \left(\frac{N^{2-\alpha_{n-1}}\eta}{\delta} + \frac{N^2 m^{\gamma_{n-1}}\eta}{\delta^{1-\beta_{n-1}+\gamma_{n-1}}\varrho^{\beta_{n-1}}} + N \right) \\ &\le \tau(m)(N^{2-\alpha_{n-1}} + N^2\varrho^{-2\beta_{n-1}+\gamma_{n-1}}m^{\beta_{n-1}} + N) \\ &\le 2N^2\tau(m)(N^{-2\alpha_n} + \varrho^{-2\beta_n}m^{2\gamma_n}). \end{aligned}$$

Taking (5) into account we obtain the lemma. ∎

The following statements are analogous to those in [3]. Although as in [2, 3] we use them with $\nu = 2$, we present them in general form which may be of independent interest.

LEMMA 7. *For integers $r, s \ge 1$ dividing m and an integer $\nu \ge 2$ denote by $Q_\nu(r,s)$ the number of solutions to the system of congruences*

$$\begin{aligned} \vartheta^{x_1} + \ldots + \vartheta^{x_\nu} &\equiv \vartheta^{x_{\nu+1}} + \ldots + \vartheta^{x_{2\nu}} \pmod r, \\ \vartheta^{x_1 y} + \ldots + \vartheta^{x_\nu y} &\equiv \vartheta^{x_{\nu+1} y} + \ldots + \vartheta^{x_{2\nu} y} \pmod s \end{aligned}$$

where $x_1, \ldots, x_{2\nu}$, $y = 1, \ldots, t$. Then

$$Q_\nu(r,s) \ll t^{2\nu-\beta_{2\nu}} m^{1+\beta_{2\nu}+\varepsilon} r^{-1} s^{-\alpha_{2\nu}},$$

where the implied constant is allowed to depend on ν as well as ε.

Proof. Defining $t_s = \operatorname{ord}_s \vartheta$ and $t_r = \operatorname{ord}_r \vartheta$, by Lemma 1 we have

$$t_s \ge \frac{ts}{m} \quad \text{and} \quad t_r \ge \frac{tr}{m}.$$

We shall group the solutions to the above pair of congruences in accordance with the value of d where

$$d = \max_{1 \le i < j \le 2\nu} \gcd(x_i - x_j, t_s).$$

For at least one of the $\nu(2\nu-1)$ choices of $1 \le i < j \le 2\nu$, we have $x_i \equiv x_j \pmod d$. Since d divides t_s and hence divides t the number of solutions to the congruence

$$\begin{aligned} &\vartheta^{x_1} + \ldots + \vartheta^{x_\nu} \equiv \vartheta^{x_{\nu+1}} + \ldots + \vartheta^{x_{2\nu}} \pmod r, \\ &1 \le x_1, \ldots, x_{2\nu} \le t, \quad x_i \equiv x_j \pmod d \end{aligned}$$

is bounded by

$$\frac{t^{2\nu}}{dt_r} \le \frac{t^{2\nu-1}m}{dr}. \tag{10}$$

It is very tempting to suggest that using exponential sums one can improve the bound (10) and make it of order $t^{2\nu}/dr$, which would immediately improve all other estimates. In particular, for prime $m = p$ this approach has successfully been used in [2]. However for composite m it does not seem to work.

Applying Lemma 6 with $n = 2\nu$, we see that for each such 2ν-tuple $(x_1, \dots, x_{2\nu})$ there are at most

$$O((t^{1-\alpha_{2\nu}} + t(d/t_s)^{\beta_{2\nu}} s^{\gamma_{2\nu}})s^{\varepsilon/2}) = O((t^{1-\alpha_{2\nu}} + t^{1-\beta_{2\nu}} d^{\beta_{2\nu}} m^{\beta_{2\nu}} s^{\gamma_{2\nu}-\beta_{2\nu}})s^{\varepsilon/2})$$

values of $y = 1, \dots, t$ which satisfy the second congruence

$$\vartheta^{x_1 y} + \dots + \vartheta^{x_\nu y} \equiv \vartheta^{x_{\nu+1} y} + \dots + \vartheta^{x_{2\nu} y} \pmod{s}.$$

Thus, summing over d we obtain

$$\begin{aligned} Q_\nu(r,s) &\ll \sum_{d \mid t_s} \frac{t^{2\nu-1} m}{dr} (t^{1-\alpha_{2\nu}} + t^{1-\beta_{2\nu}} d^{\beta_{2\nu}} m^{\beta_{2\nu}} s^{\gamma_{2\nu}-\beta_{2\nu}})s^{\varepsilon/2} \\ &\ll \tau(t_s) t^{2\nu-1} \frac{m}{r} (t^{1-\alpha_{2\nu}} + t^{1-\beta_{2\nu}} m^{\beta_{2\nu}} s^{\gamma_{2\nu}-\beta_{2\nu}})s^{\varepsilon/2}. \end{aligned}$$

Taking into account that $\beta_{2\nu} - \gamma_{2\nu} = \alpha_{2\nu}$ and (5), we obtain

$$Q_\nu(r,s) \ll t^{2\nu} m^{1+\varepsilon} r^{-1} (t^{-\alpha_{2\nu}} + t^{-\beta_{2\nu}} m^{\beta_{2\nu}} s^{-\alpha_{2\nu}})$$

and, remarking that

$$t^{-\alpha_{2\nu}} \le t^{-\beta_{2\nu}} m^{\beta_{2\nu}-\alpha_{2\nu}} \le t^{-\beta_{2\nu}} m^{\beta_{2\nu}} s^{-\alpha_{2\nu}},$$

we obtain the result. ∎

LEMMA 8. *Let $\mathcal{U}$ be a subset of $\mathcal{U}_m$ having U elements. For positive integers r, s with $r \le m$ and $s \mid m$ and an integer $\nu \ge 2$ denote by $R_\nu(r,s)$ the number of solutions to the system of congruences*

$$\begin{aligned} u_1 + \dots + u_\nu &\equiv u_{\nu+1} + \dots + u_{2\nu} \pmod{r}, \\ u_1^y + \dots + u_\nu^y &\equiv u_{\nu+1}^y + \dots + u_{2\nu}^y \pmod{s}, \end{aligned}$$

where $u_1, \dots, u_{2\nu} \in \mathcal{U}$, $y = 1, \dots, \lambda(m)$. Then

$$R_\nu(r,s) \ll U^{2\nu-2} r^{-1} s^{-\alpha_{2\nu}} \lambda(m)^{1-\beta_{2\nu}} m^{2+\beta_{2\nu}+\varepsilon},$$

where the implied constant is allowed to depend on ν as well as ε.

Proof. We shall group the solutions to the above pair of congruences in accordance with the value of d where d is defined by

$$\frac{\lambda(s)}{d} = \min_{1 \le i < j \le 2\nu} \operatorname{ord}_s(u_i/u_j).$$

For at least one of the $\nu(2\nu-1)$ choices of $1 \le i < j \le 2\nu$, we have $\operatorname{ord}_s(u_i/u_j) = \lambda(s)/d$. Using Lemma 2, we see that for $1 \le i < j \le 2\nu$ the number of solutions to the congruence

$$\begin{aligned} &u_1 + \dots + u_\nu \equiv u_{\nu+1} + \dots + u_{2\nu} \pmod{r}, \\ &u_1, \dots, u_{2\nu} \in \mathcal{U}, \quad \operatorname{ord}_s(u_i/u_j) = \lambda(s)/d, \end{aligned}$$

is bounded by

$$U^{2\nu-2} \frac{m\varphi(s)}{ds} \left(\frac{m}{r} + 1\right) \le 2 \frac{U^{2\nu-2} m^2}{dr}. \tag{11}$$

Using Lemma 6 with $n = 2\nu$ and the last statement in Lemma 1 we see that for each such fixed 2ν-tuple $(u_1, \dots, u_{2\nu})$ there are at most

$$O((\lambda(m)^{1-\alpha_{2\nu}} + \lambda(m)(d/\lambda(s))^{\beta_{2\nu}} s^{\gamma_{2\nu}}) s^{\varepsilon/2}) \\ = O((\lambda(m)^{1-\alpha_{2\nu}} + \lambda(m)^{1-\beta_{2\nu}} d^{\beta_{2\nu}} m^{\beta_{2\nu}} s^{\gamma_{2\nu}-\beta_{2\nu}}) s^{\varepsilon/2})$$

values of $y = 1, \dots, \lambda(m)$ which satisfy the second congruence

$$u_1^y + \dots + u_\nu^y \equiv u_{\nu+1}^y + \dots + u_{2\nu}^y \pmod{s}.$$

Combining this with (11) and summing over d we obtain

$$R_\nu(r,s) \ll U^{2\nu-2} \sum_{d|\lambda(s)} \frac{m^2}{dr} (\lambda(m)^{1-\alpha_{2\nu}} + \lambda(m)^{1-\beta_{2\nu}} d^{\beta_{2\nu}} m^{\beta_{2\nu}} s^{\gamma_{2\nu}-\beta_{2\nu}}) s^{\varepsilon/2} \\ \ll \tau(\lambda(s)) U^{2\nu-2} \frac{m^2}{r} (\lambda(m)^{1-\alpha_{2\nu}} + \lambda(m)^{1-\beta_{2\nu}} m^{\beta_{2\nu}} s^{\gamma_{2\nu}-\beta_{2\nu}}) s^{\varepsilon/2}.$$

Taking into account that $\beta_{2\nu} - \gamma_{2\nu} = \alpha_{2\nu}$ together with (5), we obtain

$$R_\nu(r,s) \ll U^{2\nu-2} \lambda(m) r^{-1} (\lambda(m)^{-\alpha_{2\nu}} + \lambda(m)^{-\beta_{2\nu}} m^{\beta_{2\nu}} s^{-\alpha_{2\nu}}) m^{2+\varepsilon}.$$

Remarking that

$$\lambda(m)^{-\alpha_{2\nu}} \le \lambda(m)^{-\beta_{2\nu}} m^{\beta_{2\nu}-\alpha_{2\nu}} \le \lambda(m)^{-\beta_{2\nu}} m^{\beta_{2\nu}} s^{-\alpha_{2\nu}},$$

we derive the desired result. ∎

4. Distribution of triples $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ and pairs (u, u^y). Now we are prepared to prove our main results.

THEOREM 9. *Let a, c be integers with $\gcd(a, m) = \delta_a$. Then*

$$\sum_{y=1}^{t} \Big| \sum_{x=1}^{t} \mathbf{e}_m(a\vartheta^x + c\vartheta^{xy}) \Big|^4 \ll \delta_a t^{9/4} m^{5/2+\varepsilon}.$$

Proof. We proceed along the lines of [2, 3], getting

$$\sum_{y=1}^{t} \Big| \sum_{x=1}^{t} \mathbf{e}_m(a\vartheta^x + c\vartheta^{xy}) \Big|^4 = \sum_{y=1}^{t} \frac{1}{t} \sum_{z=1}^{t} \Big| \sum_{x=1}^{t} \mathbf{e}_m(a\vartheta^{x+z} + c\vartheta^{(x+z)y}) \Big|^4 \\ = t^{-1} \sum_{y=1}^{t} \sum_{z=1}^{t} \Big| \sum_{x=1}^{t} \mathbf{e}_m(a\vartheta^z \vartheta^x + c\vartheta^{zy} \vartheta^{xy}) \Big|^4 \\ \le t^{-1} \sum_{y=1}^{t} \sum_{\lambda=0}^{m-1} \sum_{\mu=0}^{m-1} \Big| \sum_{x=1}^{t} \mathbf{e}_m(a\lambda\vartheta^x + \mu\vartheta^{xy}) \Big|^4$$

since for each fixed $y = 1, \dots, t$ the pairs $(\vartheta^z, c\vartheta^{zy})$, $z = 1, \dots, t$, are all distinct modulo m.

Using Lemmas 3 and 7 with $\mu_a = m/\delta_a$, we obtain

$$\sum_{y=1}^{t}\sum_{\lambda=0}^{m-1}\sum_{\mu=0}^{m-1}\Big|\sum_{x=1}^{t}\mathbf{e}_m(a\lambda\vartheta^x+\mu\vartheta^{xy})\Big|^4 \le m^2\,Q_2(\mu_a,m)$$
$$\ll \delta_a m^2\, t^{4-\beta_4} m^{2+\beta_4-\alpha_4+\varepsilon}$$
$$\ll \delta_a t^{13/4} m^{5/2+\varepsilon}$$

and the result follows. ∎

Although for some applications it is Theorem 9 that is needed sometimes the following consequence suffices.

THEOREM 10. *Let a, c be integers with $\gcd(a,m)=\delta_a$ and $\gcd(c,m)=\delta_c$. Then for any $\varepsilon>0$ we have*

$$W_{a,c}(m,t) \ll \begin{cases} \delta_c^{1/2} t m^{1/2+\varepsilon} & \text{if } \delta_a = m,\\ \delta_a^{1/4} t^{21/16} m^{5/8+\varepsilon} & \text{if } \delta_a < m. \end{cases}$$

Proof. If $\delta_a = m$, then using Lemma 4 we have

$$W_{a,c}(m,t) = \sum_{y=1}^{t}\Big|\sum_{x=1}^{t}\mathbf{e}_m(c\vartheta^{xy})\Big|$$
$$\le \delta_c^{1/2} m^{1/2}\sum_{y=1}^{t}\gcd(y,t)$$
$$= \delta_c^{1/2} m^{1/2}\sum_{d\mid t} d \sum_{\substack{y=1\\ \gcd(y,t)=d}}^{t} 1$$
$$\le \delta_c^{1/2} m^{1/2}\sum_{d\mid t} dt/d = \delta_c^{1/2} m^{1/2} t\tau(t).$$

Now we consider the case $\delta_a < m$. We apply the Hölder inequality getting

$$W_{a,c}^4(m,t) \le t^3\sum_{y=1}^{t}\Big|\sum_{x=1}^{t}\mathbf{e}_m(a\vartheta^x + c\vartheta^{xy})\Big|^4$$

and the result follows from Theorem 9. ∎

We remark that if $\delta_a = 1$ then the bound of Theorem 10 is nontrivial for $t \ge m^{10/11+\varepsilon}$. Also, as noted already in the introduction, the theorem provides trivially a bound for the sum $S_{a,b,c}(m,t)$. This is just slightly stronger than the bound stated in the introduction.

We now give the analogue of Theorem 9 for the corresponding sum over subgroups $\mathcal{U}$ of $\mathcal{U}_m$.

THEOREM 11. *Let $\mathcal{U}$ be a subgroup of $\mathcal{U}_m$ having U elements. Let a, c be integers with $\gcd(a, m) = \delta_a$. Then*

$$\sum_{y=1}^{\lambda(m)} \Big| \sum_{u\in\mathcal{U}} \mathbf{e}_m(au + cu^y)\Big|^4 \ll \delta_a U \lambda(m)^{1/4} m^{7/2+\varepsilon}.$$

Proof. We have

$$\sum_{y=1}^{\lambda(m)} \Big| \sum_{u\in\mathcal{U}} \mathbf{e}_m(au + cu^y)\Big|^4 = \sum_{y=1}^{\lambda(m)} \frac{1}{U} \sum_{z\in\mathcal{U}} \Big| \sum_{u\in\mathcal{U}} \mathbf{e}_m(azu + cz^y u^y)\Big|^4$$
$$\le \frac{1}{U} \sum_{y=1}^{\lambda(m)} \sum_{z,w\in\mathbb{Z}_m} \Big| \sum_{u\in\mathcal{U}_m} \mathbf{e}_m(azu + wu^y)\Big|^4$$

since the pairs (z, cz^y), $z \in \mathbb{Z}_m$, are distinct modulo m. Using Lemmas 3 and 8 with $\mu_a = m/\delta_a$, we obtain

$$\sum_{y=1}^{\lambda(m)} \sum_{z,w\in\mathbb{Z}_m} \Big| \sum_{u\in\mathcal{U}} \mathbf{e}_m(azu + wu^y)\Big|^4 \le m^2 R_2(\mu_a, m)$$
$$\ll \delta_a U^2 \lambda(m)^{1-\beta_4} m^{3+\beta_4-\alpha_4+\varepsilon}$$

and the result follows. ∎

THEOREM 12. *Let a, c be integers with $\gcd(a, m) = \delta_a$ and $\gcd(c, m) = \delta_c$. Then for any $\varepsilon > 0$ we have the bound*

$$|V_{a,c}(m)| \ll \begin{cases} \delta_c^{1/2} m^{3/2+\varepsilon} & \text{if } \delta_a = m, \\ \delta_a^{1/4} \lambda(m)^{13/16} m^{9/8+\varepsilon} & \text{if } \delta_a < m. \end{cases}$$

Proof. If $\delta_a = m$ then

$$|V_{a,c}(m)| \le \sum_{u\in\mathcal{U}_m} \Big| \sum_{y=1}^{\lambda(m)} \mathbf{e}_m(cu^y)\Big|.$$

Let d be a divisor of $\lambda(m)$. For each $u \in \mathcal{U}_m$ of multiplicative order $t = \lambda(m)/d$, by Lemma 4 we obtain

$$\Big| \sum_{y=1}^{\lambda(m)} \mathbf{e}_m(cu^y)\Big| = d \Big| \sum_{y=1}^{\lambda(m)/d} \mathbf{e}_m(cu^y)\Big| \le d\delta_c^{1/2} m^{1/2}.$$

From Lemma 2 we see that there are at most $\varphi(m)/d$ such values of y. Therefore, the total contribution from all such y does not exceed $\delta_c^{1/2} m^{1/2} \varphi(m)$ and thus from (5) we derive $|V_{a,c}(m)| \ll \delta_c^{1/2} m^{3/2+\varepsilon}$.

In the case $\delta_a < m$ we first interchange variables and only then use the triangle inequality

$$|V_{a,c}(m)| \le \sum_{y=1}^{\lambda(m)} \Big| \sum_{u \in \mathcal{U}_m} \mathbf{e}_m(au + cu^y) \Big|.$$

Applying the Hölder inequality we derive

$$|V_{a,c}(m)|^4 \le \lambda(m)^3 \sum_{y=1}^{\lambda(m)} \Big| \sum_{u \in \mathcal{U}_m} \mathbf{e}_m(au + cu^y) \Big|^4$$

and the result follows from the case $\mathcal{U} = \mathcal{U}_m$ of Theorem 11. ∎

As with Theorem 11, the latter estimate above generalizes to an arbitrary subgroup $\mathcal{U}$ of $\mathcal{U}_m$ in which case the factor $m^{9/8}$ is replaced by $U^{1/4}m^{7/8}$.

One verifies that the bound of Theorem 12 is nontrivial for $\lambda(m) > \delta_a^2 m^{2/3+\varepsilon}$. Moreover, since it has been shown in [5] that $\lambda(m) = m^{1+o(1)}$ for almost all m it follows that almost all m are covered by our results.

Denote by D_t the discrepancy of the triples of the fractional parts

$$\left(\left\{ \frac{\vartheta^x}{m} \right\}, \left\{ \frac{\vartheta^y}{m} \right\}, \left\{ \frac{\vartheta^{xy}}{m} \right\} \right), \qquad x, y = 1, \dots, t.$$

THEOREM 13. *For any fixed $\varepsilon > 0$ we have the bound*

$$D_t \ll t^{-11/16} m^{5/8+\varepsilon}.$$

Proof. Using Lemma 5 with $n = 3$, $L = m - 1$ and $N = t^2$, we obtain

$$D_t \ll \frac{1}{m} + \frac{1}{t^2} \sum_{\substack{-m<a,b,c<m \\ a^2+b^2+c^2>0}} \frac{|S_{a,b,c}|}{\max\{|a|,1\} \max\{|b|,1\} \max\{|c|,1\}}.$$

From Theorem 10 and the bound (5) we see that the contribution to the last sum from the terms with $a = b = 0$ is

$$\begin{aligned}
\sum_{0<|c|<m} \frac{W_{0,c}(m,t)}{|c|} &= \sum_{\delta \mid m} \sum_{\substack{0<|c|<m \\ \gcd(c,m)=\delta}} \frac{W_{0,c}(m,t)}{|c|} \\
&\ll t^{1+\varepsilon/2} m^{1/2} \sum_{\delta \mid m} \delta^{1/2} \sum_{\substack{0<|c|<m \\ \gcd(c,m)=\delta}} \frac{1}{|c|} \\
&\ll t^{1+\varepsilon/2} m^{1/2} \sum_{\delta \mid m} \delta^{1/2} \sum_{0<|c|<m/\delta} \frac{1}{\delta|c|} \\
&\ll t^{1+\varepsilon/2} m^{1/2} \log m \sum_{\delta \mid m} \delta^{-1/2} \ll t m^{1/2+\varepsilon}.
\end{aligned}$$

Now fix a divisor $\delta \mid m$ with $\delta < m$. From Theorem 10 we see that the contribution to the last sum from those terms with $\gcd(a,m) = \delta$ is

$$\begin{aligned}
&\sum_{\substack{-m<a,b,c<m\\ \gcd(a,m)=\delta}} \frac{W_{a,c}(m,t)}{|a|\max\{|b|,1\}\max\{|c|,1\}} \\
&\quad \ll \delta^{1/4} t^{21/16} m^{5/8+\varepsilon/2} \sum_{\substack{-m<a,b,c<m\\ \gcd(a,m)=\delta}} \frac{1}{|a|\max\{|b|,1\}\max\{|c|,1\}} \\
&\quad \ll \delta^{1/4} t^{21/16} m^{5/8+\varepsilon/2} \sum_{0<|a|<m/\delta} \frac{1}{\delta|a|} \sum_{-m<b,c<m} \frac{1}{\max\{|b|,1\}\max\{|c|,1\}} \\
&\quad \ll \delta^{-3/4} t^{21/16} m^{5/8+\varepsilon/2} \log^3 m.
\end{aligned}$$

The same contribution comes from the terms with $\gcd(b,m) = \delta$. Ignoring that these terms overlap we find that the total contribution over $|a| + |b| > 0$ is

$$t^{21/16} m^{5/8+\varepsilon/2} \log^3 m \sum_{\delta \mid m} \delta^{-3/4} \ll t^{21/16} m^{5/8+\varepsilon}.$$

Taking into account that $t^2 m^{-1} + t m^{1/2} \ll t^{21/16} m^{5/8}$, we obtain the result. ∎

It is easy to see that this theorem implies the statement in the introduction concerning the uniform distribution of the triples.

Similarly we denote by Δ_m the discrepancy of the points

$$\left(\left\{\frac{u}{m}\right\}, \left\{\frac{u^y}{m}\right\}\right), \qquad u \in \mathcal{U}_m,\ y = 1, \dots, \lambda(m).$$

Using Theorem 12 in place of Theorem 10, we derive the following upper bound.

THEOREM 14. *For any $\varepsilon > 0$, we have the bound*

$$\Delta_m \ll \lambda(m)^{-3/16} m^{1/8+\varepsilon}.$$

Recalling that $\lambda(m) = m^{1+o(1)}$ for almost all m (see [5]), we derive that $\Delta_m \ll m^{-1/16+\varepsilon}$ for almost all m.

5. Distribution of exponential functions with nonlinear exponents. In this and the following sections we give a number of applications of Theorem 9. In many cases we could use Theorem 11 in place of Theorem 9 but the result would be a little weaker. The main interest of Theorem 11 is that it applies to subgroups of $\mathcal{U}_m$ which are not necessarily cyclic and thus in particular to $\mathcal{U}_m$ itself.

In this section we obtain analogues of the results of [6] which corresponded to the case when $m = p$ is a prime. Unfortunately the method

of [6] does not seem to extend to arbitrary composite numbers and instead we adapt the method of [8, 16]. Thus, although we can now obtain nontrivial estimates for any integer modulus m the results are weaker than those of [6, 13] which held less generally.

We say a sequence $\mathcal{Z} = (z_1, \dots, z_T)$ of T elements from $\mathbb{Z}_t$ is $\mathcal{K}$-*invariant* if $\mathcal{K} \subseteq \mathcal{U}_t$ has the property that the sequence $kz_1, \dots, kz_T$, taken modulo t, is a permutation of the original sequence $z_1, \dots, z_T$ for each $k \in \mathcal{K}$. We lose nothing by assuming that $\mathcal{K}$ is a subgroup since it is clear that if the sequence $\mathcal{Z}$ is invariant with respect to a subset $\mathcal{K}$ of $\mathcal{U}_t$ then it is also invariant with respect to the subgroup generated by $\mathcal{K}$.

As before we suppose that $\vartheta \in \mathcal{U}_m$ is of multiplicative order $t \geq 1$. We estimate exponential sums of the form

$$S_a(m, \mathcal{Z}, t) = \sum_{s=1}^{T} \mathbf{e}_m(a\vartheta^{z_s})$$

for $\mathcal{K}$-invariant sequences $\mathcal{Z}$.

THEOREM 15. *Let $\mathcal{Z} = (z_1, \dots, z_T)$ be a $\mathcal{K}$-invariant sequence of elements of $\mathbb{Z}_t$ for a subgroup $\mathcal{K} < \mathcal{U}_t$ of cardinality $|\mathcal{K}| = K$. Let N denote the number of solutions of the congruence $z_r \equiv z_s \pmod t$, $1 \leq r, s \leq T$. Then, for any integer a with $\gcd(a, m) = \delta_a < m$,*

$$|S_a(m, \mathcal{Z}, t)| \ll N^{1/2} K^{-1/8} \delta_a^{1/8} t^{9/32} m^{5/16+\varepsilon}.$$

Proof. Define $Q(x)$ as the number of elements $z \in \mathcal{Z}$ with $z \equiv x \pmod t$. Note that

$$\sum_{x \in \mathbb{Z}_t} Q(x) = T \quad \text{and} \quad \sum_{x \in \mathbb{Z}_t} Q(x)^2 = N.$$

We also have $Q(kx) = Q(x)$ for any $k \in \mathcal{K}$ since repetitions in $\mathcal{Z}$ are preserved under the permutation of $\mathcal{Z}$ generated by multiplication by $k \in \mathcal{K}$. Therefore

$$\begin{aligned} S_a(m, \mathcal{Z}, t) &= \sum_{x \in \mathbb{Z}_t} Q(x) \mathbf{e}_m(a\vartheta^x) \\ &= \frac{1}{K} \sum_{k \in \mathcal{K}} \sum_{x \in \mathbb{Z}_t} Q(kx) \mathbf{e}_m(a\vartheta^{kx}) \\ &= \frac{1}{K} \sum_{k \in \mathcal{K}} \sum_{x \in \mathbb{Z}_t} Q(x) \mathbf{e}_m(a\vartheta^{kx}) \\ &= \frac{1}{K} \sum_{x \in \mathbb{Z}_t} Q(x) \sum_{k \in \mathcal{K}} \mathbf{e}_m(a\vartheta^{kx}). \end{aligned}$$

From the Cauchy–Schwarz inequality we derive

$$\begin{aligned}|S_a(m,\mathcal{Z},t)|^2 &\le \frac{1}{K^2}\sum_{x\in\mathbb{Z}_t} Q^2(x)\sum_{x\in\mathbb{Z}_t}\Big|\sum_{k\in\mathcal{K}}\mathbf{e}_m(a\vartheta^{kx})\Big|^2\\ &= \frac{N}{K^2}\sum_{x\in\mathbb{Z}_t}\Big|\sum_{k\in\mathcal{K}}\mathbf{e}_m(a\vartheta^{kx})\Big|^2\\ &= \frac{N}{K^2}\sum_{x\in\mathbb{Z}_t}\sum_{k_1,k_2\in\mathcal{K}}\mathbf{e}_m(a(\vartheta^{k_1x}-\vartheta^{k_2x}))\\ &= \frac{N}{K^2}\sum_{x\in\mathbb{Z}_t}\sum_{k_1,k_2\in\mathcal{K}}\mathbf{e}_m(a(\vartheta^{k_1x}-\vartheta^{k_1k_2x}))\end{aligned}$$

because $\mathcal{K}$ forms a subgroup of $\mathcal{U}_t$. For each $k_1\in\mathcal{K}$ we substitute $v\equiv k_1x \pmod t$ getting

$$\begin{aligned}|S_a(m,\mathcal{Z},t)|^2 &\le \frac{N}{K^2}\sum_{k_1,k_2\in\mathcal{K}}\sum_{v\in\mathbb{Z}_t}\mathbf{e}_m(a(\vartheta^{v}-\vartheta^{k_2v}))\\ &= \frac{N}{K}\sum_{k\in\mathcal{K}}\sum_{v\in\mathbb{Z}_t}\mathbf{e}_m(a(\vartheta^{v}-\vartheta^{kv})).\end{aligned}$$

By the Hölder inequality we have

$$|S_a(m,\mathcal{Z},t)|^8 \le \frac{N^4}{K}\sum_{k\in\mathcal{K}}\Big|\sum_{v\in\mathbb{Z}_t}\mathbf{e}_m(a(\vartheta^{v}-\vartheta^{kv}))\Big|^4$$

and the result follows from Theorem 9. ∎

As already noted in [6], for each integer $n\ge 1$ both sequences x^n, $x\in\mathbb{Z}_t$, and x^n, $x\in\mathcal{U}_t$, are $\mathcal{K}$-invariant with respect to the subgroup

$$\mathcal{K}=\{x^n \mid x\in\mathcal{U}_t\}.$$

Hence Theorem 15 can be used to derive upper bounds for the sums

$$\sum_{x\in\mathbb{Z}_t}\mathbf{e}_m(a\vartheta^{x^n}) \quad\text{and}\quad \sum_{x\in\mathcal{U}_t}\mathbf{e}_m(a\vartheta^{x^n}).$$

In particular, for the sequence x^n, $x\in\mathcal{U}_t$, the upper bound for the corresponding quantity $N\ll t^{1+\varepsilon}$ was given in Lemma 5 of [6]. Since clearly we also have $K\gg t^{1-\varepsilon}$ we can conclude that

$$\Big|\sum_{x\in\mathcal{U}_t}\mathbf{e}_m(a\vartheta^{x^n})\Big| \ll \delta_a^{1/8}t^{21/32}m^{5/16+\varepsilon}.$$

In the special case $m=p$ one can give a stronger bound (see [6]), and this in turn has found some cryptographic applications in [22].

The sequence x^n, $x\in\mathbb{Z}_t$, is $\mathcal{K}$-invariant with respect to the same subgroup as well. However, the sums over all $x\in\mathbb{Z}_t$ cannot be estimated in such a direct way because the value of N for them is too large (unless $n=2$

or t is cube-free). Nevertheless, using the same technique as in the proof of Theorem 7 of [6] one can estimate these sums as well.

Another basic example occurs when we replace the fixed power above by an exponential function. Let e be an element of $\mathcal{U}_t$ having multiplicative order T. Then the sequence e^s, $s = 0, \dots, T-1$, is $\mathcal{K}$-invariant with respect to the set

$$\mathcal{K} = \{e^s \mid s = 0, \dots, T-1\}.$$

It is obvious that for this sequence $N = K$; thus Theorem 15 implies the bound

$$\Big| \sum_{s=1}^{T} \mathbf{e}_m(a\vartheta^{e^s}) \Big| \ll \delta_a^{1/8} T^{3/8} t^{9/32} m^{5/16+\varepsilon}. \tag{12}$$

If $\delta_a \ll m^{\varepsilon}$ and $T \gg t^{1-\varepsilon}$ then the bound (12) is nontrivial for $t \geq m^{10/11+2\varepsilon}$. Obviously the same bound holds for any sequence $\mathcal{Z}$ with $N \leq K^{1+\varepsilon}$. For example, this holds for the sequence x^n, $x \in \mathcal{U}_t$; see Lemma 5 of [6].

We now apply the bound (12) to study the distribution of the *power generator*

$$u_s \equiv u_{s-1}^e \pmod m, \quad 0 \leq u_s \leq m-1, \quad s = 1, 2, \dots, \tag{13}$$

with the *initial value* $u_0 = \vartheta$ (an integer coprime to m) and *exponent* $e \geq 2$. As before we assume that $\vartheta \in \mathcal{U}_m$ has multiplicative order $t \geq 1$ and that $e \in \mathcal{U}_t$ has multiplicative order T. It is clear that

$$u_s \equiv \vartheta^{e^s} \pmod m, \quad s = 0, 1, \dots,$$

and thus this sequence is purely periodic with period T.

Let $D_m(t, T)$ be the discrepancy of the sequence u_s/m, $s = 0, \dots, T-1$.

THEOREM 16. *For any $\varepsilon > 0$, we have the bound*

$$D_m(t, T) \ll T^{-5/8} t^{9/32} m^{5/16+\varepsilon}.$$

Proof. Using Lemma 5 with $n = 1$, $L = m-1$, $N = T$ and the bound (12), we obtain

$$\begin{aligned} D_m(t, T) &\ll \frac{1}{m} + T^{-5/8} t^{9/32} m^{5/16+\varepsilon/2} \sum_{\delta \mid m} \delta^{1/8} \sum_{\substack{0<|a|<m \\ \gcd(a,m)=\delta}} \frac{1}{|a|} \\ &\ll \frac{1}{m} + T^{-5/8} t^{9/32} m^{5/16+\varepsilon/2} \log m \sum_{\delta \mid m} \delta^{-7/8}. \end{aligned}$$

From the bound (5) we obtain the result. ∎

In the case that t is of order near to m the bound of Theorem 16 is valuable as long as $T > m^{19/20+\varepsilon}$. When T (and hence also t) is of order

near m the bound becomes of the form

$$D_m(t,T) \le T^{-1/32+\varepsilon}. \tag{14}$$

It has been shown in [9, 10] that for almost all $m = pl$ which are products of two distinct primes p and l and for almost all initial values ϑ and exponents e of the power generator (13) the period T is close to m indeed. Thus this result combined with the estimates of [13] implies that $D_m(t,T) \le T^{-1/8+\varepsilon}$ for almost all $m = pl$ and almost all parameters ϑ and e with $\gcd(\vartheta, m) = \gcd(e, \varphi(m)) = 1$.

It is not too difficult to modify the methods of [10] to prove that T is of order exceeding $m^{1-\varepsilon}$ for almost all integers m (of arbitrary arithmetic structure) and almost all admissible parameters ϑ and e. Indeed, Greg Martin and Carl Pomerance (unpublished) have obtained much more precise results of this nature. It follows that the bound (14) also holds for almost all m, ϑ and e with $\gcd(\vartheta, m) = \gcd(e, \varphi(m)) = 1$.

6. Double sums over sparse sets and communication complexity of exponentiation. In this section we consider exponential sums over fairly arbitrary sets and then apply the results to a problem from complexity theory which is related to modular exponentiation.

As before we fix an element $\vartheta \in \mathbb{Z}_m$ of multiplicative order t but now consider the double exponential sum

$$S_a(m,t,\mathcal{X},\mathcal{Y}) = \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} \mathbf{e}_m(a\vartheta^{xy}),$$

where $a \in \mathbb{Z}_m$ and $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{Z}_t$.

Unlike the set $\mathcal{Z}$ in the previous section the sets $\mathcal{X}, \mathcal{Y}$ are not required to have any special arithmetic structure but can be quite general. The fact that we are considering a double sum rather than a single sum suffices to produce useful results as long as the two sets are sufficiently dense. In the case $m = p$, a prime, such sums have been estimated in our earlier work [11] and in the next proof we exploit the technique developed there.

THEOREM 17. *For any integer a with $\gcd(a,m) = \delta_a$ and any sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{Z}_t$, we have the bound*

$$|S_a(m,t,\mathcal{X},\mathcal{Y})| \ll |\mathcal{X}|^{1/2}|\mathcal{Y}|^{21/32}\delta_a^{1/8}t^{1/2}m^{5/16+\varepsilon}.$$

Proof. For a divisor $d \mid t$ we denote by $\mathcal{Y}(d)$ the subset of $y \in \mathcal{Y}$ with $\gcd(y,t) = d$. Then

$$|S_a(m,t,\mathcal{X},\mathcal{Y})| \le \sum_{d\mid t} |\sigma_d|,$$

where

$$\sigma_d = \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}(d)} \mathbf{e}_m(a\vartheta^{xy}).$$

Using the Cauchy inequality, we derive

$$\begin{aligned}|\sigma_d|^2 &\le |\mathcal{X}| \sum_{x\in\mathcal{X}} \Big| \sum_{y\in\mathcal{Y}(d)} \mathbf{e}_m(a\vartheta^{xy})\Big|^2\\ &\le |\mathcal{X}| \sum_{x\in\mathbb{Z}_t} \Big| \sum_{y\in\mathcal{Y}(d)} \mathbf{e}_m(a\vartheta^{xy})\Big|^2\\ &= |\mathcal{X}| \sum_{y,z\in\mathcal{Y}(d)} \sum_{x\in\mathbb{Z}_t} \mathbf{e}_m(a(\vartheta^{xy}-\vartheta^{xz})).\end{aligned}$$

By the Hölder inequality we have

$$\begin{aligned}|\sigma_d|^8 &\le |\mathcal{X}|^4|\mathcal{Y}(d)|^6 \sum_{y,z\in\mathcal{Y}(d)} \Big| \sum_{x\in\mathbb{Z}_t} \mathbf{e}_m(a(\vartheta^{xy}-\vartheta^{xz}))\Big|^4\\ &\le |\mathcal{X}|^4|\mathcal{Y}(d)|^6 \sum_{y\in\mathcal{Y}(d)} \sum_{v\in\mathbb{Z}_{t/d}} \Big| \sum_{x\in\mathbb{Z}_t} \mathbf{e}_m(a(\vartheta^{xy}-\vartheta^{xvd}))\Big|^4.\end{aligned}$$

Because each element $y \in \mathcal{Y}(d)$ can be represented in the form $y = dw$ with $\gcd(w, t/d) = 1$ and $\vartheta_d = \vartheta^d$ is of multiplicative order t/d, we see that the double sum over v and x does not depend on y. (Make the change of variables x into xw^{-1}, v into vw.) Therefore,

$$\begin{aligned}|\sigma_d|^8 &\le |\mathcal{X}|^4|\mathcal{Y}(d)|^7 \sum_{v\in\mathbb{Z}_{t/d}} \Big| \sum_{x\in\mathbb{Z}_t} \mathbf{e}_m(a(\vartheta_d^x-\vartheta_d^{xv}))\Big|^4\\ &= |\mathcal{X}|^4|\mathcal{Y}(d)|^7 d^4 \sum_{v\in\mathbb{Z}_{t/d}} \Big| \sum_{x\in\mathbb{Z}_{t/d}} \mathbf{e}_m(a(\vartheta_d^x-\vartheta_d^{xv}))\Big|^4.\end{aligned}$$

By Theorem 9 we obtain

$$|\sigma_d|^8 \ll |\mathcal{X}|^4|\mathcal{Y}(d)|^7\delta_a d^4(t/d)^{9/4}m^{5/2+\varepsilon} = |\mathcal{X}|^4|\mathcal{Y}(d)|^7\delta_a d^{7/4}t^{9/4}m^{5/2+\varepsilon}.$$

Using the bound $|\mathcal{Y}(d)| \le |\mathcal{Y}|$ for $d \le t/|\mathcal{Y}|$ and the bound $|\mathcal{Y}(d)| \le t/d$ for $d > t/|\mathcal{Y}|$, we obtain

$$|\sigma_d|^8 \ll |\mathcal{X}|^4|\mathcal{Y}|^7(t/|\mathcal{Y}|)^{7/4}\delta_a t^{9/4}m^{5/2+\varepsilon} = |\mathcal{X}|^4|\mathcal{Y}|^{21/4}\delta_a t^4 m^{5/2+\varepsilon}.$$

Hence

$$|\sigma_d| \ll |\mathcal{X}|^{1/2}|\mathcal{Y}|^{21/32}\delta_a^{1/8}t^{1/2}m^{5/16+\varepsilon/8}$$

for any divisor $d \,|\, t$. Applying the bound (5), we derive the result. ∎

If the sets $\mathcal{X}$ and $\mathcal{Y}$ both have cardinality at most N and $\gcd(a, m) = 1$ (or even $\gcd(a, m) \ll m^{\varepsilon}$) then the bound of Theorem 17 becomes

$$|S_a(m, t, \mathcal{X}, \mathcal{Y})| \ll N^{37/32}t^{1/2}m^{5/16+\varepsilon}.$$

If $\mathcal{X}$ and $\mathcal{Y}$ are nearly dense in the sense that $N \ge t^{1+o(1)}$ then Theorem 17 is nontrivial starting with $t \ge m^{10/11+\varepsilon}$. In another special case when t is almost of order m, that is, $t = m^{1+o(1)}$, the bound is nontrivial for sets of cardinalities both exceeding $N \ge m^{26/27+\varepsilon}$.

We now define the integer n by the inequalities $2^n \le t \le 2^{n+1} - 1$ and denote by $\mathcal{B}$ the set of n-bit integers,

$$\mathcal{B} = \{x \in \mathbb{Z} : 0 \le x \le 2^n - 1\}.$$

We do not distinguish between an n-bit integer $x \in \mathcal{B}$ and its binary expansion. Thus $\mathcal{B}$ can be considered as the n-dimensional Boolean cube $\mathcal{B} = \{0, 1\}^n$ as well. We now recall the notion of communication complexity. Given a Boolean function $f(x, y)$ of $2n$ variables

$$x = (x_1, \ldots, x_n) \in \mathcal{B} \quad \text{and} \quad y = (y_1, \ldots, y_n) \in \mathcal{B},$$

we assume that there are two collaborating parties and the value of x is known to one of the parties and the value of y is known to the other, but each party has no information about the values of the other. The goal is to create a *communication protocol* $\mathbf{P}$ such that, for any inputs $x, y \in \mathcal{B}$, at the end at least one of the parties can compute the value of $f(x, y)$. The largest number of bits required to be exchanged by a protocol $\mathbf{P}$, taken over all possible inputs $x, y \in \mathcal{B}$, is called the communication complexity $\mathrm{C}(\mathbf{P})$ of this protocol. The smallest possible value of $\mathrm{C}(\mathbf{P})$, taken over all possible protocols, is called the *communication complexity* $\mathrm{C}(f)$ of the function f (see [1, 15]).

Given $x, y \in \mathcal{B}$ we study the communication complexity of computation of ϑ^{xy}. This function ϑ^{xy} is well known as the *Diffie–Hellman secret key* which arises in the Diffie–Hellman key exchange protocol (see [17, 23]). Studying various complexity characteristics of this function is of primal interest for cryptography and complexity theory. Lower bounds for a number of complexity characteristics of this function as well as for the discrete logarithm have been obtained in [21]. In particular, for an odd m one can consider the Boolean function $f(x, y)$ which is defined as the rightmost bit of ϑ^{xy}, that is,

$$f(x_1, \ldots, x_n, y_1, \ldots, y_n) = \begin{cases} 1 & \text{if } \vartheta^{xy} \in \{1, 3, \ldots, m-2\}, \\ 0 & \text{if } \vartheta^{xy} \in \{2, 4, \ldots, m-1\}. \end{cases} \tag{15}$$

In the case when $m = p$ and $t = p - 1$ (that is, when ϑ is a primitive root modulo p) the lower bound $\mathrm{C}(f) \ge n/24 + o(n)$ for the communication complexity of this function f has been given in [21]. Here, using Theorem 17, we derive a linear lower bound for $\mathrm{C}(f)$ for all odd m and all $t \ge m^{10/11+\varepsilon}$. Obviously $\mathrm{C}(f) \le n$, so that up to a constant factor this bound is tight.

THEOREM 18. *For any $\delta > 0$ and sufficiently large $t \ge m^{10/11+\delta}$ the communication complexity of the function $f(x,y)$ given by* (15) *satisfies the bound*

$$\mathrm{C}(f) \ge \left(\frac{11}{32}\,\delta - \varepsilon\right) n.$$

Proof. We define the *combinatorial discrepancy* $\Delta(f)$ of f as

$$\Delta(f) = 2^{-2n} \max_{\mathcal{X},\mathcal{Y}\subseteq\mathcal{B}} |N_1(\mathcal{X},\mathcal{Y}) - N_0(\mathcal{X},\mathcal{Y})|,$$

where the maximum is taken over all sets $\mathcal{X},\mathcal{Y} \subseteq \mathcal{B}$ and $N_\mu(\mathcal{X},\mathcal{Y})$ is the number of pairs $(x,y) \in \mathcal{X}\times\mathcal{Y}$ with $f(x,y) = \mu$.

A link between the discrepancy and the communication complexity is provided by the inequality

$$\mathrm{C}(f) \ge \log_2\left(\frac{1}{\Delta(f)}\right) \tag{16}$$

which forms a part of Lemma 2.2 of [1]. Let $c = (m+1)/2$ be the multiplicative inverse of 2 modulo m. It is easy to see that $N_0(\mathcal{X},\mathcal{Y})$ is just the number of pairs $(x,y) \in \mathcal{X}\times\mathcal{Y}$ for which $c\vartheta^{xy} \in [1,(m-1)/2]$. From Lemma 5 with $n=1$, $L = m-1$ and $N = |\mathcal{X}|\,|\mathcal{Y}|$ we conclude that

$$\left|N_0(\mathcal{X},\mathcal{Y}) - \frac{|\mathcal{X}|\,|\mathcal{Y}|(m-1)}{2m}\right| \ll \frac{|\mathcal{X}|\,|\mathcal{Y}|}{m} + \sum_{0<|a|<m} \frac{|S_a(m,t,\mathcal{X},\mathcal{Y})|}{|a|}.$$

Replacing $|\mathcal{X}|$ and $|\mathcal{Y}|$ with t in the bound of Theorem 17 we obtain

$$\begin{aligned}\left|N_0(\mathcal{X},\mathcal{Y}) - \frac{|\mathcal{X}|\,|\mathcal{Y}|(m-1)}{2m}\right| &\ll \frac{|\mathcal{X}|\,|\mathcal{Y}|}{m} + \sum_{0<|a|<m} \frac{|S_a(m,t,\mathcal{X},\mathcal{Y})|}{|a|}\\ &\ll t^2 m^{-1} + t^{53/32} m^{5/16+\varepsilon/2} \sum_{d\mid m} d^{1/8} \sum_{\substack{0<|a|<m\\ \gcd(a,m)=d}} \frac{1}{|a|}\\ &\ll t^{53/32} m^{5/16+\varepsilon/2} \sum_{d\mid m} d^{1/8} \sum_{0<|a|<m/d} \frac{1}{d|a|}\\ &\ll t^{53/32} m^{5/16+\varepsilon/2} \log m \sum_{d\mid m} d^{-7/8}.\end{aligned}$$

Using (5), we obtain

$$\left|N_0(\mathcal{X},\mathcal{Y}) - \frac{1}{2}\,|\mathcal{X}|\,|\mathcal{Y}|\right| \ll t^{53/32} m^{5/16+3\varepsilon/4}.$$

Similarly

$$\left|N_1(\mathcal{X},\mathcal{Y}) - \frac{1}{2}\,|\mathcal{X}|\,|\mathcal{Y}|\right| \ll t^{53/32} m^{5/16+3\varepsilon/4}.$$

Therefore the discrepancy of f satisfies the bound

$$\begin{aligned}\Delta(f) &\ll 2^{-2n}t^{53/32}m^{5/16+\varepsilon}\\ &\ll t^{-11/32}m^{5/16+\varepsilon} \le m^{-11\delta/32+\varepsilon} \le t^{-11\delta/32+\varepsilon}.\end{aligned} \tag{17}$$

Applying (16) we obtain the result. ∎

For $t = m^{1+o(1)}$ we obtain $\mathrm{C}(f) \ge n/32 + o(n)$. For smaller values of t the bound of Theorem 18 can be slightly improved, for example to

$$\mathrm{C}(f) \ge \left(\frac{121\delta}{320+352\delta} - \varepsilon\right)n$$

if in (17) one uses $m \ge t^{(10/11+\delta)^{-1}}$ instead of $m \ge t$.

Analogous results can also be obtained for the function

$$g(x_1,\dots,x_n,y_1,\dots,y_n) = \begin{cases} 1 & \text{if } \vartheta^{xy} \in [0, m/2),\\ 0 & \text{if } \vartheta^{xy} \in [m/2, m),\end{cases}$$

which can be considered modulo an arbitrary integer (not necessarily odd as for the function f).

It would be interesting to consider also the sums

$$V_a(m,\mathcal{U},\mathcal{Y}) = \sum_{u\in\mathcal{U}}\sum_{y\in\mathcal{Y}} \mathbf{e}_m(au^y),$$

where $a \in \mathbb{Z}_m$ and $\mathcal{U} \subseteq \mathcal{U}_m$ and $\mathcal{Y} \subseteq \mathbb{Z}_{\lambda(m)}$. It is clear that for $m = p$ these sums are equivalent to the sums $S_a(m,t,\mathcal{X},\mathcal{Y})$, however for composite m they are different. It seems quite plausible that the method of proof of Theorem 17 combined with Theorem 11 or its appropriate modification can produce a nontrivial upper bound for these sums. Such a bound would imply an analogue of Theorem 18 for modular powering u^y.

References

[1] L. Babai, N. Nisan and M. Szegedy, *Multiparty protocols, pseudorandom generators for logspace and time-space trade-offs*, J. Comput. System Sci. 45 (1992), 204–232.

[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. Friedlander and I. 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. Tichy, *Sequences, Discrepancies and Applications*, Springer, Berlin, 1997.

[5] P. Erdős, C. Pomerance and E. Schmutz, *Carmichael's lambda function*, Acta Arith. 58 (1991), 363–385.

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

[7] J. B. Friedlander, J. Hansen and I. E. Shparlinski, *On the distribution of the power generator modulo a prime power*, in: Proc. DIMACS Workshop on Unusual Applications of Number Theory, 2000, Amer. Math. Soc., to appear.

[8] J. B. Friedlander, D. Lieman and I. E. Shparlinski, *On the distribution of the RSA generator*, in: Sequences and their Applications (Singapore, 1998), Springer, London, 1999, 205–212.

[9] J. B. Friedlander, C. Pomerance and I. E. Shparlinski, *Small values of the Carmichael function and cryptographic applications*, in: Proc. Workshop on Cryptography and Computational Number Theory (Singapore, 1999), Birkhäuser, 2001, 25–32.

[10] —, —, —, *Period of the power generator and small values of Carmichael's function*, Math. Comp. 70 (2001), 1591–1605.

[11] J. B. Friedlander and I. E. Shparlinski, *Double exponential sums over thin sets*, Proc. Amer. Math. Soc. 129 (2001), 1617–1621.

[12] —, —, *On the distribution of Diffie–Hellman triples with sparse exponents*, SIAM J. Discrete Math. 14 (2001), 162–169.

[13] —, —, *On the distribution of the power generator*, Math. Comp. 70 (2001), 1575–1589.

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

[15] E. Kushilevitz and N. Nisan, *Communication Complexity*, Cambridge Univ. Press, Cambridge, 1997.

[16] D. Lieman and I. E. Shparlinski, *On a new exponential sum*, Canad. Math. Bull. 44 (2001), 87–92.

[17] A. J. Menezes, P. C. van Oorrschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.

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

[19] K. Prachar, *Primzahlverteilung*, Springer, Berlin, 1957.

[20] I. E. Shparlinski, *On prime divisors of recurrence sequences*, Izv. Vyssh. Ucheb. Zaved. Ser. Mat. 1980, no. 1, 100–103 (in Russian).

[21] —, *Communication complexity and Fourier coefficients of the Diffie–Hellman key*, in: Lecture Notes in Comput. Sci. 1776, Springer, Berlin, 2000, 259–268.

[22] —, *Security of most significant bits of* g^{x^2}, Inform. Process. Lett., to appear.

[23] D. R. Stinson, *Cryptography*: *Theory and Practice*, CRC Press, Boca Raton, FL, 1995.

[24] I. M. Vinogradov, *Elements of Number Theory*, Dover Publ., New York, 1954.

Department of Mathematics
University of Toronto
Toronto, Ontario M5S 3G3, Canada
E-mail: frdlndr@math.toronto.edu

Department of Mechanics and Mathematics
Moscow State University
Moscow, 119899, Russia
E-mail: konyagin@ok.ru

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

Received on 18.6.2001
and in revised form on 25.2.2002 (4056)