DEMONSTRATIO MATHEMATICA
Vol. XXXV No 2 2002

Marian Vâjâitu, Alexandru Zaharescu

CHARACTER SUMS AND PAIR CORRELATIONS

Abstract. Let p be a prime number, χ a generator of the group of Dirichlet characters mod p and let $a_q \in \mathbb{C}$, $|a_q| \leq 1$ for any $1 < q < \sqrt{p}$, q prime. We prove that

$$\sum_{|m|<\sqrt{p}} \Big| \sum_{\substack{q<\sqrt{p} \\ q \text{ prime}}} a_q \chi^m(q) \Big|^2 \ll p.$$

1. Introduction

The pair correlation as well as higher correlation measures are studied in connection with the distribution of spacings between the elements of a given sequence of numbers. In recent years substantial progress was made towards understanding the correlations of fractional parts of polynomials and related sequences (see [6], [8], [1], [7]). In all these problems success came from the fact that one was able to estimate certain exponential sums intimately connected to the correlation measures associated to the given sequence. There are also cases when the correlations are not seen as the goal of the investigation but rather as a tool to be used in achieving a different objective. The study [9] of averages of short exponential sums is an example of such a situation where the pair correlation is used as a tool. Let $\epsilon > 0$, let $N \leq M \leq P$ be positive integers and let $r(X) = \frac{f(X)}{g(X)}$ be a rational function which is not a polynomial, with integer coefficients bounded by P^{K_1} and with deg f, deg $g < K_2$, where K_1 and K_2 are some positive constants. Then it is shown in [9] that for almost all pairs (p, m) with p prime, $p \in [P, 2P]$ and $m \in \{1, \ldots, M\}$ one has

$$\Big| \sum_{1 \leq n \leq N}{}' e\Big(\frac{mr(n)}{p}\Big) \Big| \ll_{\epsilon, K_1, K_2} N^{\frac{1}{2}} P^{\epsilon}. \tag{1.1}$$

1991 *Mathematics Subject Classification*: 11L40, 11A07.

Here almost all means that the exceptional set has density $< P^{-\epsilon}$, $r(n)$ is computed modulo p and $\sum'$ denotes a sum over values of n for which $g(n) \not\equiv 0 \pmod{p}$. In order to prove this result one brings into play the pair correlation of the sets

$$\mathcal{N}_p = \Big\{ \frac{r(n) \pmod{p}}{p} : 1 \le n \le N \Big\}$$

and use them to provide upper bounds for the short moments

$$\sum_{1 \le m \le M} \Big| \sum_{1 \le n \le N}{}' e\Big(\frac{mr(n)}{p}\Big) \Big|^2 \tag{1.2}$$

for each p individually. Such a method can only succeed if one has an alternative way of estimating the pair correlations. This was achieved in [9] by performing an average over p. The result is the following inequality:

$$\sum_{P \le p \le 2P} \sum_{1 \le m \le M} \Big| \sum_{1 \le n \le N}{}' e\Big(\frac{mr(n)}{p}\Big) \Big|^2 \ll_{\epsilon, K_1, K_2} NMP^{1+\epsilon} \tag{1.3}$$

from which (1.1) follows for almost all pairs (p, m).

In this paper we consider averages of character sums of the form

$$\sum_{|m| < \sqrt{p}} \Big| \sum_{\substack{q < \sqrt{p} \\ q \text{ prime}}} \chi^m(q) \Big|^2 \tag{1.4}$$

where p is a prime number and χ is a generator of the group of Dirichlet characters $\pmod{p}$. Usually when dealing with short averages of short character sums we don't know how to obtain best possible upper bounds. The classical inequality of Polya and Vinogradov (see [3]) gives square root cancellation in long character sums, while the well known results of Burgess [2] give nontrivial cancellation in short character sums of length $> p^{\frac{1}{4}}$. One easily obtains square root cancellation in long averages of short character sums, for example

$$\sum_{m \pmod{p-1}} \Big| \sum_{\substack{q < \sqrt{p} \\ q \text{ prime}}} \chi^m(q) \Big|^2 \ll \frac{p^{\frac{3}{2}}}{\log p}, \tag{1.5}$$

while the delicate estimates for higher moments of character sums due to Montgomery [5] give nontrivial cancellation in short averages of short character sums. Our idea in dealing with a sum as in (1.4) is to use a map $x \mapsto g^x \pmod{p}$, where g is a primitive root mod p, in order to transform the character sums from (1.4) in exponential sums and then provide upper bounds in terms of pair correlations as was done in [9] with the sums from

(1.2). The method also works if one has weights in the sums from (1.4). We will prove the following inequality, which is essentially best possible.

THEOREM 1. *Let p be a prime number, χ a generator of the group of Dirichlet characters mod p and let $a_q \in \mathbb{C}$, $|a_q| \leq 1$ for any $1 < q < \sqrt{p}$, q prime. Then*

$$\sum_{|m|<\sqrt{p}} \Big| \sum_{\substack{q<\sqrt{p} \\ q \text{ prime}}} a_q \chi^m(q) \Big|^2 \ll p.$$

As a consequence of this result, if we choose an integer b and set $a_q = \chi^b(q)$ for any q, we obtain the following corollary.

COROLLARY 2. *Let p be a prime number and χ a generator of the group of Dirichlet characters mod p. Then for any integer b one has*

$$\sum_{|m-b|<\sqrt{p}} \Big| \sum_{\substack{q<\sqrt{p} \\ q \text{ prime}}} \chi^m(q) \Big|^2 \ll p. \tag{1.6}$$

Note that by adding the inequalities (1.6) for $b = 0$, $[\sqrt{p}]$, $2[\sqrt{p}], \ldots,$ $[\sqrt{p}]^2$ one obtains an upper bound for the long average over $m \pmod{p-1}$ which is essentially as good as (1.5). Thus what Corollary 2 says is that one can localize the long sum from (1.5) to intervals of length $\approx \sqrt{p}$ without any loss of information.

Acknowledgements. The authors are grateful to the referee for pointing out the relationship between Lemma 3 below and the Large Sieve Inequality.

2. Exponential sums and pair correlations

Let $\mathcal{N} = \{x_n : 1 \leq n \leq N\}$ be a finite sequence of real numbers and let M be a positive integer. In [9] it is proved that

$$\sum_{1\leq m\leq M} \Big| \sum_{1\leq n\leq N} e(mx_n) \Big|^2 \ll M\, E(\mathcal{N}, M) \tag{2.1}$$

where

$$E(\mathcal{N}, M) = \Big| \Big\{ 1 \leq n, n' \leq N : \|x_n - x_{n'}\| \leq \frac{1}{M} \Big\} \Big|$$

and $\|\cdot\|$ denotes the distance function to the nearest integer. Here we consider an extension of the above inequality in which we associate weights $a_1, \ldots, a_N \in \mathbb{C}$ to the points $x_1, \ldots, x_N$. The result is the following

LEMMA 3. *For any real numbers $x_1, \cdots, x_N$, any complex numbers $a_1, \cdots, a_N$ and any positive integer M one has*

$$\sum_{|m|\le M} \Big| \sum_{1\le n\le N} a_n e(mx_n)\Big|^2 \ll M \sum_{\substack{1\le n,n'\le N \\ \|x_n - x_{n'}\|\le \frac{1}{2M}}} |a_n a_{n'}|. \tag{2.2}$$

Proof. We follow the proof of (2.1) given in [9]. Let $x_1, \ldots, x_N$, $a_1, \ldots, a_N$ and M be as in the statement of the lemma. Let h be the periodic function mod 1 which on $[-\frac{1}{2}, \frac{1}{2}]$ is given by

$$h(t) = \begin{cases} 2M(1-2M|t|) & \text{if } |t| \le \frac{1}{2M} \\ 0 & \text{if } \frac{1}{2M} \le |t| \le \frac{1}{2}. \end{cases}$$

Expand h in a Fourier series

$$h(t) = \sum_{m\in\mathbb{Z}} c_m e(mt),$$

where the Fourier coefficients are given by

$$c_m = \begin{cases} \frac{4M^2}{\pi^2 m^2} \sin^2\left(\frac{\pi m}{2M}\right) & \text{if } m \ne 0, \\ 1 & \text{if } m = 0. \end{cases}$$

We will use the fact that the coefficients c_m are nonnegative and $|c_m| \gg 1$ uniformly for $|m| < M$. We also use the positivity of h and the fact that $\frac{h}{2M}$ is bounded by the characteristic function of the interval $[-\frac{1}{2M}, \frac{1}{2M}]$. In order to make our positivity argument work, let us note first that it is enough to prove (2.2) when $a_1, \ldots, a_N$ are nonnegative real numbers. Indeed, for any $a_1, \ldots, a_N \in \mathbb{C}$ the left hand side of (2.2) is

$$\le 2 \sum_{|m|\le M} \Big(\Big| \sum_{1\le n\le N} (Re\, a_n) e(mx_n)\Big|^2 + \Big| \sum_{1\le n\le N} (Im\, a_n)\, e(mx_n)\Big|^2 \Big),$$

while the right hand side of (2.2) is

$$\ge M \sum_{\substack{1\le n,n'\le N \\ \|x_n - x_{n'}\|\le \frac{1}{2M}}} (|Re\, a_n\, Re\, a_{n'}| + |Im\, a_n\, Im\, a_{n'}|).$$

Thus the general case of (2.2) follows from the case when $a_1, \ldots, a_N \in \mathbb{R}$. Suppose we are in this case. Then the left hand side of (2.2) is

$$\le 2 \sum_{|m|\le M} \Big(\Big| \sum_{\substack{1\le n\le N \\ a_n>0}} a_n\, e(mx_n)\Big|^2 + \Big| \sum_{\substack{1\le n\le N \\ a_n<0}} a_n\, e(mx_n)\Big|^2 \Big)$$

while the right hand side of (2.2) is

$$\geq M\Big(\sum_{\substack{1\leq n,n'\leq N\\ \|x_n-x_{n'}\|\leq\frac{1}{2M}\\ a_n,a_{n'}>0}} a_n\,a_{n'}+\sum_{\substack{1\leq n,n'\leq N\\ \|x_n-x_{n'}\|\leq\frac{1}{2M}\\ a_n,a_{n'}<0}} a_n\,a_{n'}\Big).$$

This shows that the general case of (2.2) reduces to the case $a_1,\dots,a_N \geq 0$. Assume we are in this case, then we have on one hand

$$\sum_{1\leq n,n'\leq N} a_n\,a_{n'}\,h(x_n-x_{n'}) \leq 2M \sum_{\substack{1\leq n,n'\leq N\\ \|x_n-x_{n'}\|\leq\frac{1}{2M}}} a_n\,a_{n'}. \tag{2.3}$$

On the other hand one has

$$\begin{aligned}\sum_{1\leq n,n'\leq N} a_n\,a_{n'}\,h(x_n-x_{n'}) &= \sum_{1\leq n,n'\leq N} a_n\,a_{n'}\sum_{m\in\mathbb{Z}} c_m\,e(m(x_n-x_{n'}))\\ &= \sum_{m\in\mathbb{Z}} c_m \sum_{1\leq n,n'\leq N} a_n\,a_{n'}\,e(m(x_n-x_{n'}))\\ &= \sum_{m\in\mathbb{Z}} c_m\Big|\sum_{1\leq n\leq N} a_n\,e(mx_n)\Big|^2.\end{aligned} \tag{2.4}$$

Since $c_m \geq 0$ for any m and $|c_m| \gg 1$ for $|m| \leq M$, one has

$$\sum_{|m|\leq M}\Big|\sum_{1\leq n\leq N} a_n\,e(mx_n)\Big|^2 \ll \sum_{m\in\mathbb{Z}} c_m\Big|\sum_{1\leq n\leq N} a_n\,e(mx_n)\Big|^2. \tag{2.5}$$

Now (2.2) follows from (2.3), (2.4) and (2.5), and the lemma is proved.

As was pointed out by the referee, the above lemma implies the dual of the Large Sieve Inequality with worse constants than usually given. The Large Sieve Inequality (see Montgomery [4]) gives an upper bound of the form

$$\sum_{j=1}^{R}|S(\alpha_j)|^2 \leq \Delta(N,\delta)\sum_{n=M+1}^{M+N}|a_n|^2 \tag{2.6}$$

for any trigonometric polynomial with complex coefficients

$$S(\alpha)=\sum_{n=M+1}^{M+N} a_n e(n\alpha)$$

and any real numbers $\alpha_1,\dots,\alpha_R$ which are well spaced (mod 1) in the sense that $\|\alpha_j-\alpha_s\| \geq \delta$ for $j \neq s$. Here one can take $\Delta(N,\delta)=N-1+\delta^{-1}$. By

duality, (2.6) is equivalent to having (see [4], p. 551)

$$\sum_{n=M+1}^{M+N} \Big| \sum_{r=1}^{R} y_r e(n\alpha_r) \Big|^2 \leq \Delta(N,\delta) \sum_{r=1}^{R} |y_r|^2 \tag{2.7}$$

for all y_r. Clearly the parameter M is irrelevant in (2.6) and (2.7). Note that if the real numbers $x_1, \dots, x_N$ from Lemma 3 are such that $\|x_n - x_{n'}\| \geq \delta$ for $1 \leq n \neq n' \leq N$, then for any $1 \leq n \leq N$ there are at most $[\frac{1}{M\delta}] + 1$ values of n' for which $\|x_n - x_{n'}\| \leq \frac{1}{2M}$. Therefore in this case the right side of (2.2) is bounded by $(M + \delta^{-1}) \sum_{1 \leq n \leq N} |a_n|^2$. So we see that Lemma 3 implies indeed (2.7), with its right hand side multiplied by an absolute constant.

3. Proof of Theorem 1

Let p, χ and the a_q's be as in the statement of the theorem. Let g be the unique primitive root mod p for which $\chi(g) = e(\frac{1}{p-1})$, and consider the one-to-one map $L : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}/(p-1)\mathbb{Z}$ given by $g^{L(x)} \equiv x \pmod p$ for any $0 \neq x \in \mathbb{Z}/p\mathbb{Z}$. Thus $\chi(y) = e(\frac{L(y)}{p-1})$ for any $0 \neq y \in \mathbb{Z}/p\mathbb{Z}$. Let $\mathcal{H}$ be the set of prime numbers $< \sqrt{p}$ and denote by $\mathcal{U}$ the image of $\mathcal{H}$ in $\mathbb{Z}/(p-1)\mathbb{Z}$ through L. Set $\mathcal{N} = \{\frac{u}{p-1} : u \in \mathcal{U}\}$. Since $\mathcal{U}$ is well defined mod $p-1$, $\mathcal{N}$ will be defined mod 1. For any $x \in \mathcal{N}$ we set

$$a_x := a_u := a_q$$

where u is the unique element of $\mathcal{U}$ which corresponds to x and q is the unique element of $\mathcal{H}$ which corresponds to u, that is $x = \frac{u}{p-1}$ and $u = L(q)$. Then one has

$$\begin{aligned} \sum_{|m|<\sqrt{p}} \Big| \sum_{q \in \mathcal{H}} a_q \chi^m(q) \Big|^2 &= \sum_{|m|<\sqrt{p}} \Big| \sum_{u \in \mathcal{U}} a_u \, e\Big(\frac{mu}{p-1}\Big) \Big|^2 \\ &= \sum_{|m|<\sqrt{p}} \Big| \sum_{x \in \mathcal{N}} a_x \, e(mx) \Big|^2. \end{aligned} \tag{3.1}$$

From Lemma 3 applied with $M = [\sqrt{p}]$ and our assumptions on the weights a_q it follows that

$$\begin{aligned} &\sum_{|m|<\sqrt{p}} \Big| \sum_{x \in \mathcal{N}} a_x \, e(mx) \Big|^2 \\ &\qquad \ll \sqrt{p} \sum_{\substack{x,x' \in \mathcal{N} \\ \|x-x'\| \leq \frac{1}{2[\sqrt{p}]}}} |a_x \, a_{x'}| \\ &\qquad \leq \sqrt{p} \, \# \Big\{ (x,x') \in \mathcal{N} \times \mathcal{N} : \|x - x'\| \leq \frac{1}{2[\sqrt{p}]} \Big\}. \end{aligned} \tag{3.2}$$

As we mentioned in the Introduction, the method is only successful if one has an alternative way of dealing with the pair correlation of the set $\mathcal{N}$. Here we do not have an extra average over p as in [9], but we take advantage of the special shape of the set $\mathcal{N}$. We derive

$$(3.3)\quad \#\left\{(x,x')\in\mathcal{N}\times\mathcal{N}:\|x-x'\|\le\frac{1}{2[\sqrt{p}]}\right\}=$$
$$\#\left\{(u,u')\in\mathcal{U}\times\mathcal{U}:u\equiv u'-s\ (\mathrm{mod}\,p-1);\ |s|\le\frac{p-1}{2[\sqrt{p}]}\right\}=$$
$$\#\left\{(q,q')\in\mathcal{H}\times\mathcal{H}:q\equiv q'g^{-s}\ (\mathrm{mod}\,p);\ |s|\le\frac{p-1}{2[\sqrt{p}]}\right\}.$$

If we denote for any integer s

$$\mathcal{H}_s=\{qg^{-s}\ (\mathrm{mod}\,p):q\in\mathcal{H}\},$$

then the right hand side of (3.3) can be written as

$$(3.4)\qquad \sum_{|s|\le\frac{p-1}{2[\sqrt{p}]}}\#(\mathcal{H}_0\cap\mathcal{H}_s).$$

From (3.1), (3.2), (3.3), and (3.4) we get

$$(3.5)\qquad \sum_{|m|<\sqrt{p}}\Big|\sum_{q\in\mathcal{H}}a_q\,\chi^m(q)\Big|^2\ll\sqrt{p}\sum_{|s|\le\frac{p-1}{2[\sqrt{p}]}}\#(\mathcal{H}_0\cap\mathcal{H}_s).$$

For $s=0$ one has $\#(\mathcal{H}_0\cap\mathcal{H}_0)=\#\mathcal{H}=\pi(\sqrt{p})$. For any other s in (3.5) we claim that $\#(\mathcal{H}_0\cap\mathcal{H}_s)\le 1$. Indeed, let us assume that for some such s there are at least two distinct pairs (q_1,q_2), $(q_3,q_4)\in\mathcal{H}\times\mathcal{H}$ such that

$$(3.6)\qquad q_1\equiv q_2\,g^{-s}\ (\mathrm{mod}\,p)$$

and

$$(3.7)\qquad q_3\equiv q_4\,g^{-s}\ (\mathrm{mod}\,p).$$

Note that since $s\not\equiv 0\ (\mathrm{mod}\,p-1)$ one has $g^{-s}\not\equiv 1\ (\mathrm{mod}\,p)$, hence the numbers q_1 and q_2 are distinct. Also q_1 and q_3 are distinct, otherwise the pairs (q_1,q_2) and (q_3,q_4) would coincide. From (3.6) and (3.7) it follows that

$$q_1\,q_4\equiv q_2\,q_3\ (\mathrm{mod}\,p).$$

But $q_1\,q_4$ and $q_2\,q_3$ are positive integers smaller than p, therefore the above congruence implies the equality $q_1\,q_4=q_2\,q_3$. Since q_1, q_2, q_3, and q_4 are prime numbers, q_1 will coincide with either q_2 or q_3, which is not the case. This proves the claim. Hence the right hand side of (3.5) is bounded by $\sqrt{p}(\pi(\sqrt{p})+\frac{p-1}{[\sqrt{p}]})$, and this completes the proof of the Theorem 1.

References

[1] F. Boca, A. Zaharescu, *Pair correlation of values of rational functions* (mod p), Duke Math. J. 105 no. 2 (2000), 267–307.

[2] D. A. Burgess, *On character sums and L-series II*, Proc. London Math. Soc. (3) 13 (1963), 524–536.

[3] H. Davenport, *Multiplicative Number Theory*, Second Edition, Springer-Verlag, 1980.

[4] H. L. Montgomery, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc. 84 no. 4 (1978), 547–567.

[5] H. L. Montgomery, *Distribution of small powers of a primitive root*, Advances in number theory (Kingston, ON, 1991), 137–149, Oxford Sci. Publ., Oxford Univ. Press, New York, 1993. Amer Math. Soc. 111 no. 2 (1991), 523–531.

[6] Z. Rudnick, P. Sarnak, *The pair correlation function of fractional parts of polynomials*, Comm. Math. Phys. 194 (1998), 61–70.

[7] Z. Rudnick, P. Sarnak, A. Zaharescu, *The distribution of spacings between the fractional parts of* $n^2\alpha$, Invent. Math. 145 no. 1 (2001), 37–57.

[8] Z. Rudnick, A. Zaharescu, *A metric result on the pair correlation of fractional parts of sequences*, Acta Arith. 89 no. 3 (1999), 283–293.

[9] A. Zaharescu, *Averages of short exponential sums*, Acta Arith. 88 no. 3 (1999), 223–231.

M. Vâjâitu
INSTITUTE OF MATHEMATICS OF THE ROMANIAN ACADEMY
P.O. BOX 1-764
70700 BUCHAREST, ROMANIA
E-mail: mvajaitu@stoilow.imar.ro

A. Zaharescu
INSTITUTE OF MATHEMATICS OF THE ROMANIAN ACADEMY
P.O. BOX 1-764
70700 BUCHAREST, ROMANIA
and
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
Altgeld Hall, 1409 W. Green Street
URBANA, IL, 61801, U.S.A.
e-mail: zaharesc@math.uiuc.edu

Received March 26, 2001; revised version July 27, 2001.