Rev. Mat. Iberoam. **28** (2012), no. 1, 231–238
DOI 10.4171/RMI/675

On the restricted divisor function in arithmetic progressions

Igor E. Shparlinski

Abstract. We obtain several asymptotic estimates for the sums of the restricted divisor function

$$\tau_{M,N}(k) = \#\big\{1 \leqslant m \leqslant M,\ 1 \leqslant n \leqslant N : mn = k\big\}$$

over short arithmetic progressions, which improve some results of J. Truelsen. Such estimates are motivated by the links with the pair correlation problem for fractional parts of the quadratic function αk^2, $k = 1, 2, \ldots$ with a real α.

1. Introduction

There is a long history of studying the distribution of the divisor function over short arithmetic progressions, see [2], [3], [5], [6], [7] and references therein. Recently, Truelsen [14] has introduced the restricted divisor function

$$\tau_{M,N}(k) = \#\{1 \leqslant m \leqslant M,\ 1 \leqslant n \leqslant N : mn = k\}$$

and shown its relevance to the *pair correlation problem* for fractional parts of the quadratic function αk^2, $k = 1, 2, \ldots$, with a real α, see also [10] and [12] for various results and conjectures concerning this problem. In particular, it is conjectured in [14] (see Conjecture 1.2) that for any fixed $\varepsilon, \delta, c_1, c_2 > 0$, if positive integers N, M, R and q satisfy

$$N \geqslant q^{1/2+\varepsilon} \quad c_1 N \leqslant M \leqslant c_2 N \quad R \geqslant N^{\delta},$$

then, uniformly over all integers a with $\gcd(a, q) = 1$, we have

$$\sum_{r=1}^{R} \sum_{k \equiv ar \pmod q} \tau_{M,N}(k) \sim \frac{MNR}{q}. \tag{1.1}$$

Mathematics Subject Classification (2010): 11N37.
Keywords: Divisor function, congruences, character sums.

It is also shown in [14] that the asymptotic formula (1.1) yields explicit examples of real α for which distribution of spacings between the fractional parts of αk^2 is *Poissonian*.

Towards the conjecture (1.1), several asymptotic formulas and estimates are derived in [14].

In particular, as in [14], for positive integer q, M, N and a divisor $d \mid q$, we consider the sums

$$\Delta_q(d; M, N) = \sum_{\substack{a=1\\ \gcd(a,q)=d}}^{q} \left| \sum_{k \equiv a \pmod q} \tau_{M,N}(k) - \frac{MN}{q^2}\Phi(q,d) \right|^2, \tag{1.2}$$

where

$$\Phi(q,d) = \sum_{e \mid d} e \sum_{f \mid q/e} f\mu\left(\frac{q}{ef}\right) = \sum_{e \mid d} e\varphi(q/e) \tag{1.3}$$

(see equation (1.5) in [14]), and $\mu(k)$ is the Möbius function. Also as in [14], for positive integer q, M, N and R, we consider the sums

$$\Gamma_q(M, N, R) = \sum_{a=1}^{q-1} \left| \sum_{r \leqslant R} \sum_{k \equiv ar \pmod q} \tau_{M,N}(k) - \frac{MNR}{q} \right|^2. \tag{1.4}$$

Here, in Section 3.1, we show that a result of [13] almost instantly implies the estimate of Theorem 1.8 of [14] on the sums $\Delta_q(d; M, N)$, and in fact, in a slightly stronger form. Furthermore, using a different technique of multiplicative character sums, in Section 3.2 we obtain a new estimate on the sums $\Gamma_q(M, N, R)$, which for some parameter ranges improves that of Theorem 1.9 in [14]. We present our argument only in the case of prime q but combining it with elementary (but somewhat cluttered) sieving it can also be used for arbitrary q.

2. Preliminaries

2.1. General notation and facts

Throughout the paper, any implied constants in symbols O, $\ll$ and $\gg$ may occasionally depend on the positive parameters ε and δ and are absolute otherwise. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that $|U| \leqslant cV$ holds with some constant $c > 0$.

We always assume that the variables which appear in congruences and as arguments of standard arithmetic functions are integer.

We recall that for

$$\varphi(s, K) = \sum_{\substack{1 \leqslant k \leqslant K\\ \gcd(k,s)=1}} 1$$

we have the asymptotic formula

$$\varphi(s,K) = \frac{\varphi(s)}{s}K + O(s^{o(1)}), \tag{2.1}$$

(see equation (3.1) in [14]), that follows from the inclusion-exclusion principle and the well-known bounds on the divisor and Euler functions

$$\tau(s) = s^{o(1)} \quad \text{and} \quad \varphi(s) = s^{1+o(1)},$$

see Theorems 317 and 328 in [9], respectively.

2.2. Character sums

Let $\varPhi_s$ be the set of all $\varphi(s)$ multiplicative characters modulo s. We also use χ_0 to denote the principal character and

$$\varPhi_s^* = \varPhi_s \setminus \{\chi_0\}$$

to denote the set of nonprincipal multiplicative characters modulo s.

For an integer Z and $\chi \in \varPhi_s$ we define the sum

$$S_s(Z;\chi) = \sum_{z=1}^{Z} \chi(z). \tag{2.2}$$

The following result is a combination of the Pólya–Vinogradov (for $\nu = 1$) and Burgess (for $\nu \geqslant 2$) bounds, see Theorems 12.5 and 12.6 in [11].

Lemma 2.1. *For a prime s and positive integers $Z \leqslant s$, the bound*

$$\max_{\chi\in\varPhi_s^*} |S_s(Z;\chi)| \leqslant Z^{1-1/\nu} s^{(\nu+1)/4\nu^2+o(1)}$$

holds with an arbitrary fixed integer $\nu \geqslant 1$.

We combine Lemma 2.1 with a bound on the fourth moment of the sums $S_s(Z,t;\chi)$. First we recall the following estimate from [1] (for prime s) and [7] (for arbitrary s), see also [4], [8], which we present in the following slightly relaxed form.

Lemma 2.2. *For positive integers $Z \leqslant s$, the following bound holds:*

$$\sum_{\chi\in\varPhi_s^*} |S_s(Z;\chi)|^4 \leqslant s^{1+o(1)} Z^2.$$

2.3. Sums with $\tau_{M,N}(k)$ and congruences

We note that sums of the restricted divisor function over an arithmetic progression can be expressed via the number of solutions to a certain congruence. For example,

$$\sum_{k\equiv a \pmod q} \tau_{M,N}(k) = T_q(M,N;a), \tag{2.3}$$

where $T_q(M,N;a)$ is number of solutions to the congruence

$$mn \equiv a \pmod q, \quad 1 \leqslant m \leqslant M,\ 1 \leqslant n \leqslant N. \tag{2.4}$$

This interpretation underlines our approach.

To estimate the function $T_s(M,N;a)$ it is more convenient to work with the quantity $T_s^*(X,Y;a)$, which is defined as number of solutions to the congruence

$$xy \equiv a \pmod s, \quad 1 \leqslant x \leqslant X,\ \gcd(x,s)=1,\ 1 \leqslant y \leqslant Y.$$

One of our main tools is the following special case of Theorem 1 in [13], combined with (2.1).

Lemma 2.3. *For positive integers s and $X \leqslant Y$, we have*

$$\sum_{a=1}^{s} \left| T_s^*(X,Y;a) - \frac{\varphi(s)}{s^2} XY \right|^2 \leqslant XY s^{o(1)}.$$

We also define $R_s(X,Y,Z;a)$ as number of solutions to the congruence

$$xy \equiv az \pmod s,$$

with

$$1 \leqslant x \leqslant X, \quad 1 \leqslant y \leqslant Y, \quad 1 \leqslant z \leqslant Z.$$

Lemma 2.4. *For a prime s and positive integers $X,Y,Z < s$ we have*

$$\sum_{a=1}^{s-1} \left| R_s(X,Y,Z;a) - \frac{XYZ}{s-1} \right|^2 \leqslant XYZU^{1-2/\nu} s^{(\nu+1)/2\nu^2+o(1)}$$

where $U = \min\{X,Y,Z\}$ and $\nu \geqslant 1$ is an arbitrary fixed positive integer.

Proof. We note that for every a with $\gcd(a,s)=1$, we obtain

$$R_s(X,Y,Z;a) = \frac{1}{s-1} \sum_{x=1}^{X} \sum_{y=1}^{Y} \sum_{z=1}^{Z} \sum_{\chi \in \Phi_s} \chi\left(a^{-1}xyz^{-1}\right).$$

Recalling the definition (2.2), changing the order of summation, using that

$$\chi\left(z^{-1}\right) = \overline{\chi}(z),$$

if $\gcd(z,s)=1$, where $\overline{\chi}$ is the complex conjugated character, we derive

$$R_s(X,Y,Z;a) = \frac{1}{s-1} \sum_{\chi \in \Phi_s} \overline{\chi}(a)\, S_s(X;\chi) S_s(Y;\chi) S_s(Z;\overline{\chi}).$$

We now separate the contribution from the principal character $\chi = \chi_0$, getting

$$R_s(X,Y,Z;a) - \frac{XYZ}{s-1} = \frac{1}{s-1} \sum_{\chi \in \Phi_s *} \overline{\chi}(a)\, S_s(X;\chi) S_s(Y;\chi) S_s(Z;\overline{\chi}).$$

Using the orthogonality of characters, we easily derive

$$\begin{aligned}\sum_{a=1}^{s}\left|R_s(X,Y,Z;a)-\frac{XYZ}{s-1}\right|^2 &= \frac{1}{\varphi(s)}\sum_{\chi\in\Phi_s*}|S_s(X;\chi)|^2|S_s(Y;\chi)|^2|S_s(Z,\chi)|^2\\ &= \frac{1}{\varphi(s)}\sum_{\chi\in\Phi_s*}|S_s(\widetilde{X};\chi)|^2|S_s(\widetilde{Y};\chi)|^2|S_s(\widetilde{Z},\chi)|^2,\end{aligned}$$

for any permutation $(\widetilde{X},\widetilde{Y},\widetilde{Z})$ of (X,Y,Z). We now apply Lemma 2.1 to the last sum and then use Cauchy's inequality, arriving to

$$\begin{aligned}&\sum_{a=1}^{s}\left|R_s(X,Y,Z;a)-\frac{XYZ}{s-1}\right|^2 \leqslant\\ &\qquad\leqslant \frac{\widetilde{Z}^{2-2/\nu}s^{(\nu+1)/2\nu^2+o(1)}}{s-1}\sqrt{\sum_{\chi\in\Phi_s*}|S_s(\widetilde{X};\chi)|^4}\sqrt{\sum_{\chi\in\Phi_s*}|S_s(\widetilde{Y};\chi)|^4}.\end{aligned}$$

We now choose a permutation $(\widetilde{X},\widetilde{Y},\widetilde{Z})$ with $\widetilde{Z}=U=\min\{X,Y,Z\}$. Using Lemma 2.2, we obtain the desired result. □

3. Average values $\tau_{M,N}(k)$ over some families of progressions

3.1. One parameter family of progressions

Here we estimate the sums $\Delta_q(d;M,N)$ given by (1.2) and show how Lemma 2.3 implies a stronger and more general form of the estimate of Theorem 1.8 in [14], which asserts that if $M\ll N\ll M$ then

$$\Delta_q(d;M,N)\leqslant\frac{1}{q}N^{\max\{7/2,4-\delta\}+o(1)}, \tag{3.1}$$

uniformly over $q\leqslant N^{2-\delta}$ and $d\mid q$

Theorem 3.1. *For arbitrary positive integers q, M and N and a divisor $d\,|\,q$ we have*

$$\Delta_q(d;M,N)\leqslant MNq^{o(1)}\,.$$

Proof. Without loss of generality we can assume that $M\geqslant N$.

For each divisor $e\,|\,d$, we collect together the solutions to (2.4) with $\gcd(m,q)=e$, getting

$$T_q(M,N;a)=\sum_{e|d}T^*_{q/e}\big(\lfloor M/e\rfloor\,,N;a/e\big)\,,$$

where $T^*_s(X,Y;a)$ is defined in Section 2.3.

Recalling (2.3) and (1.3), we obtain

$$\begin{aligned}\Delta_q(d;M,N) &= \sum_{\substack{a=1\\ \gcd(a,q)=d}}^{q} \left|T_q(M,N;a) - \frac{MN}{q^2}\Phi(q,d)\right|^2\\ &= \sum_{\substack{a=1\\ \gcd(a,q)=d}}^{q} \left(\sum_{e\mid d}\left|T^*_{q/e}(\lfloor M/e\rfloor, N; a/e) - \frac{MNe}{q^2}\varphi(q/e)\right|\right)^2.\end{aligned}$$

Thus, using Cauchy's inequality, we obtain

$$\Delta_q(d;M,N) \leqslant q^{o(1)}\sum_{e\mid d}\sum_{\substack{a=1\\ \gcd(a,q)=d}}^{q} \left|T^*_{q/e}(\lfloor M/e\rfloor, N; a/e) - \frac{MNe}{q^2}\varphi(q/e)\right|^2. \tag{3.2}$$

We now note that

$$\begin{aligned}\frac{MNe}{q^2}\varphi(q/e) &= \frac{(M/e)N}{(q/e)^2}\varphi(q/e)\\ &= \frac{\lfloor M/e\rfloor N}{(q/e)^2}\varphi(q/e) + O(Ne/q) = \frac{\lfloor M/e\rfloor N}{(q/e)^2}\varphi(q/e) + O(Nd/q).\end{aligned}$$

We now see from (3.2) that

$$\begin{aligned}\Delta_q(d;M,N) \leqslant q^{o(1)}&\sum_{e\mid d}\sum_{\substack{a=1\\ \gcd(a,q)=d}}^{q} \left|T^*_{q/e}(\lfloor M/e\rfloor, N; a/e) - \frac{\lfloor M/e\rfloor N}{(q/e)^2}\varphi(q/e)\right|^2\\ &+ N^2d^2q^{-2+o(1)}\sum_{e\mid d}\sum_{\substack{a=1\\ \gcd(a,q)=d}}^{q} 1\\ \leqslant q^{o(1)}&\sum_{e\mid d}\sum_{\substack{a=1\\ \gcd(a,q)=d}}^{q} \left|T^*_{q/e}(\lfloor M/e\rfloor, N; a/e) - \frac{\lfloor M/e\rfloor N}{(q/e)^2}\varphi(q/e)\right|^2\\ &+ N^2dq^{-1+o(1)}.\end{aligned}$$

Writing $a = ce$, we derive

$$\begin{aligned}&\Delta_q(d;M,N) \leqslant\\ &\quad\leqslant q^{o(1)}\sum_{e\mid d}\sum_{c=1}^{q/e}\left|T^*_{q/e}(\lfloor M/e\rfloor, N; c) - \frac{\lfloor M/e\rfloor N}{(q/e)^2}\varphi(q/e)\right|^2 + N^2dq^{-1+o(1)}.\end{aligned}$$

Now recalling Lemma 2.3, we obtain

$$\Delta_q(d;M,N) \leqslant MNq^{o(1)} + N^2dq^{-1+o(1)} \leqslant (M+N)Nq^{o(1)}.$$

Since $M \geqslant N$, this concludes the proof. □

Note that the bound of Theorem 3.1 is more general than (3.1) as it works for M and N of essentially different sizes. Furthermore, if $M \ll N \ll M$, then this bound takes form $N^2 q^{o(1)}$, which improves (3.1) for $\delta > 1/2$, that is, for $N \geqslant q^{2/3+\varepsilon}$ for any fixed $\varepsilon > 0$.

3.2. Two parameter family of progressions

Note that in [14] the bound (3.1) has been used to prove several other results. Theorem 3.1 can be used to get corresponding generalisations and improvements of these bounds. For example, bounds of $\Delta_q(d; M, N)$ are used in Theorem 1.9 of [14] to derive the estimate on the sums $\Gamma_q(M, N, R)$ given by (1.4). In particular, by Theorem 1.9 in [14] we have

$$\Gamma_q(M, N, R) \leqslant N^4 R^2 \big(R^{-2} + N^{\max\{-1/2, -\delta\}}\big) q^{-1+o(1)}, \tag{3.3}$$

provided $M \ll N \ll M$, $R \leqslant q \leqslant N^{2-\delta}$ (note that the condition of Theorem 1.9 in [14] that $R \geqslant N^{\eta}$ for some positive $\eta > 0$ does not seem to be needed for the bound, but the bound is nontrivial only if it is satisfied). The estimate (3.3) shows that the conjectured asymptotic formula (1.1) holds on average under appropriate averaging conditions, see Corollary 1.10 in [14].

As in the case of $\Delta_q(d; M, N)$, using Theorem 3.1 one now obtains a similar generalisation and improvement for $\Gamma_q(M, N, R)$. One can probably use similar arguments to sharpen Theorem 4.5 of [14] as well.

Furthermore, we now present a different approach, based on Lemma 2.4, which allows to obtain estimates on $\Gamma_q(M, N, R)$ that are sometimes stronger that those of Theorem 1.9 in [14] or following from Theorem 3.1. We demonstrate this approach only in the case of prime modulus q. In the general case, one can use it as well, but involves rather cluttered expressions arising from the inclusion-exclusion principle.

Theorem 3.2. *For a prime q and positive integers $M, N, R < q$, the bound*

$$\Gamma_q(M, N, R) \leqslant MNRL^{1-2/\nu} q^{(\nu+1)/2\nu^2 + o(1)}$$

holds, where $L = \min\{M, N, R\}$ and $\nu \geqslant 1$ is an arbitrary fixed positive integer.

Proof. As in the proof of Theorem 3.1, we see that

$$\Gamma_q(M, N, R) = \sum_{a=1}^{q-1} \left| R_q(M, N, R; a) - \frac{MNR}{q} \right|^2,$$

and using Lemma 2.4, we conclude the proof. □

For example, if q is prime then for $M, N = q^{2/3+o(1)}$ and $R = q^{1/2+o(1)}$, applying Theorem 3.2 with $\nu = 2$ we obtain

$$\Gamma_q(M, N, R) \leqslant q^{53/24+o(1)}$$

while (3.3) gives only

$$\Gamma_q(M, N, R) \leqslant q^{7/3+o(1)}$$

for the above choice of parameters. One can certainly easily produce many other examples of the parameters (M, N, R) for which Theorem 3.2 is stronger than (3.3).

As we have said, the argument used in the proof of Lemma 2.4 an thus of Theorem 3.2 can also be applied in the case of composite q. However we recall that the Burgess bound for character sums modulo a composite q has some limitations on the possible choices of ν, see Theorem 12.6 in [11] for details.

References

[1] Ayyad, A., Cochrane, T. and Zheng, Z.: The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$ and the mean value of character sums. *J. Number Theory* **59** (1996), no. 2, 398–413.

[2] Banks, W. D., Heath-Brown, D. R. and Shparlinski, I. E.: On the average value of divisor sums in arithmetic progressions. *Int. Math. Res. Not.* **2005**, 1–25.

[3] Blomer, V.: The average value of divisor sums in arithmetic progressions. *Q. J. Math.* **59** (2008), no. 3, 275–286.

[4] Cochrane, T. and Shi, S.: The congruence $x_1x_2 \equiv x_3x_4 \pmod p$ and mean values of character sums. *J. Number Theory* **130** (2010), no. 3, 767–785.

[5] Fouvry, É: Sur le probléme des diviseurs de Titchmarsh. *J. Reine Angew Math.* **357** (1985), 51–76.

[6] Friedlander, J. B. and Iwaniec, H.: Incomplete Kloosterman sums and a divisor problem. *Ann. of Math. (2)* **121** (1985), no. 2, 319–350.

[7] Friedlander, J. B. and Iwaniec, H.: The divisor problem for arithmetic progressions. *Acta Arith.* **45** (1985), no. 3, 273–277.

[8] Garaev, M. Z. and Garcia, V.: The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications. *J. Number Theory* **128** (2008), no. 9, 2520–2537.

[9] Hardy, G. H. and Wright, E. M.: *An introduction to the theory of numbers.* The Clarendon Press, Oxford University Press, New York, 1979.

[10] Heath-Brown, D. R.: Pair correlation for fractional parts of αn^2. *Math. Proc. Cambridge Philos. Soc.* **148** (2010), no. 3, 385–407.

[11] Iwaniec, H. and Kowalski, E.: *Analytic number theory.* American Mathematical Society Colloquium Publocations 53, American Math. Soc., Providence, RI, 2004.

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

[13] Shparlinski, I. E.: Distribution of modular inverses and multiples of small integers and the Sato–Tate conjecture on average. *Michigan Math. J.* **56** (2008), no. 1, 99–111.

[14] Truelsen, J. L.: Divisor problems and the pair correlation for the fractional parts of $n^2\alpha$. *Int. Math. Res. Not.* **2010**, no. 16, 3144–3183.

Received April 13, 2010; revised June 9, 2010.

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

The author is grateful to Jimi Truelsen and to the referee for very useful comments. During the preparation of this paper, the author was supported in part by ARC grant DP1092835.