Second Moment Of Dirichlet L -Functions, Character Sums Over Subgroups And Upper Bounds On Relative Class Numbers

Stéphane Louboutin, Marc Munsch

Second moment of Dirichlet L-functions, character sums over subgroups, and upper bounds on relative class numbers.

Stéphane R. LOUBOUTIN
Aix Marseille Université, CNRS, Centrale Marseille, I2M,
Marseille, FRANCE
stephane.louboutin@univ-amu.fr
Marc MUNSCH
5010 Institut für Analysis und Zahlentheorie
8010 Graz, Steyrergasse 30, Graz, AUSTRIA
munsch@math.tugraz.at

February 1, 2021

Abstract

We prove an asymptotic formula for the mean-square average of L- functions associated to subgroups of characters of sufficiently large size. Our proof relies on the study of certain character sums $\mathcal{A}(p,d)$ recently introduced by E. Elma, where $p \geq 3$ is prime and $d \geq 1$ is any odd divisor of $p-1$. We obtain an asymptotic formula for $\mathcal{A}(p,d)$ which holds true for any odd divisor d of $p-1$, thus removing E. Elma's restrictions on the size of d. This answers a question raised in Elma's paper. Our proof relies both on estimates on the frequency of large character sums and techniques from the theory of uniform distribution. As an application, in the range $1 \leq d \leq \frac{\log p}{3 \log\log p}$ we obtain the significant improvement $h_{p,d}^- \leq 2\left(\frac{(1+o(1))p}{24}\right)^{m/4}$ over the trivial bound $h_{p,d}^- \ll (\frac{dp}{24})^{m/4}$ on the relative class numbers of the imaginary number fields of conductor $p \equiv 1 \pmod{2d}$ and degree $m = (p-1)/d$, where $d \geq 1$ is odd.

1 Introduction

Throughout the paper $d \geq 1$ will be an odd integer and p will be an odd prime satisfying $p \equiv 1 \pmod{2d}$. We also write $\log_j$ for the j-th iterated logarithm. We let $\mathcal{X}_p$ denote the multiplicative cyclic group of order $p-1$ of the Dirichlet characters mod p and let $\mathcal{X}_p^*$ denote the set with $p-2$ elements of the non-trivial Dirichlet characters mod p. Whenever m divides $p-1$, we let $\chi_{p,m}$ denote any one of the $\phi(m)$ characters in $\mathcal{X}_p$ of order m. Notice that $\chi_{p,m}$ is odd, i.e. such that $\chi_{p,m}(-1) = -1$, if and only if $d = (p-1)/m$ is odd, which implies that m is even.

[0]2020 Mathematics Subject Classification. Primary. 11R42, 11L40. Secondary: 11A07, 11J71, 11M20, 11R18, 11R20. Key words and phrases: moments of Dirichlet L-functions, cyclotomic field, relative class number, character sums, multiplicative subgroups, exponential sums, Dedekind sums, discrepancy.

Let $h_{p,d}^-$ be the relative class number of the imaginary subfield $K_{p,d}$ of the cyclotomic field $\mathbb{Q}(\zeta_p)$ of even degree $(K_{p,d}:\mathbb{Q})=m$ and odd relative degree $(\mathbb{Q}(\zeta_p):K_{p,d})=d$ (e.g. see [Was, Chapter 4]). For $d=1$, we have $K_{p,1}=\mathbb{Q}(\zeta_p)$ and it has long been known that

$$h_{p,1}^- = h_{\mathbb{Q}(\zeta_p)}^- \le 2p\left(\frac{p}{24}\right)^{(p-1)/4} = 2p\left(\frac{p}{24}\right)^{m/4}, \tag{1}$$

see [Met] and [Wal]. See also [Lou93] where it is explained how to get explicit bounds better than (1) of the type $h_{p,1}^- \le 2p(1+o(1))(p/C)^{(p-1)/4}$ for any constant C greater than $4\pi^2$. Notice also that by [AC] we have $h_{p,1}^- = 2p^{1+o(1)}\left(\frac{p}{4\pi^2}\right)^{(p-1)/4}$ and see [Gra] for more subtle results according to which Kummer's conjecture on the asymptotic behavior $h_{p,1}^- \sim 2p\left(\frac{p}{4\pi^2}\right)^{(p-1)/4}$ is unlikely to be true.

Denote by $w_{p,d}$ the number of complex roots of unity contained in $K_{p,d}$; we have $w_{p,1}=2p$ and $w_{p,d}=2$ for $d>1$. The following bound holds (e.g. see [Was, Chapter 4, page 42] for the equality and then use the arithmetic-geometric mean inequality):

$$h_{p,d}^- = w_{p,d}\prod_{j=1}^{m/2}\frac{\sqrt{p}}{2\pi}L(1,\chi_{p,m}^{2j-1}) \le w_{p,d}\left(\frac{pM(p,m)}{4\pi^2}\right)^{m/4}, \tag{2}$$

where $M(p,m)$ denotes the following mean square of $L(1,\chi)$ as χ runs over the $m/2$ odd characters in the only subgroup of order m of $\mathcal{X}_p$:

$$M(p,m) := \frac{2}{m}\sum_{j=1}^{m/2}|L(1,\chi_{p,m}^{2j-1})|^2. \tag{3}$$

Therefore explicit formulas (or asymptotic formulas) for $M(p,m)$ allow to give precise upper bounds of type $h_{p,d}^- \le C_1\cdot C_2^{m/4}$. For $d=1$, H. Walum deduced (1) in [Wal] by proving that

$$M(p,p-1) = \frac{\pi^2}{6}\left(1-\frac{1}{p}\right)\left(1-\frac{2}{p}\right). \tag{4}$$

For $d=3,5$, some explicit formulas for $M(p,m)$ have been obtained in certain cases by the first author (see Section 2.2) allowing him to give upper bounds on $h_{p,3}^-$ and $h_{p,5}^-$. These results will be generalized in Proposition 7 below. In all these situations $M(p,(p-1)/d)$ is asymptotic to $\pi^2/6$. It is unrealistic to obtain an explicit formula for all values of d and the following simple argument gives a trivial bound on $M(p,m)$. Since in $M(p,m)$ we consider only $m/2$ of the $(p-1)/2$ odd Dirichlet characters that appear in $M(p,p-1)$, we have

$$M(p,m) \ \ \le \tfrac{2}{m}\tfrac{p-1}{2}M(p,p-1) = dM(p,p-1) = d\tfrac{\pi^2}{6}\left(1-\tfrac{1}{p}\right)\left(1-\tfrac{2}{p}\right). \tag{5}$$

By (2), this implies that

$$h_{p,d}^- \le 2\left(\frac{dp}{24}\right)^{\frac{p-1}{4d}} = 2\left(\frac{dp}{24}\right)^{m/4}. \tag{6}$$

For a given m it is hopeless to get an asymptotic on $M(p,m)$. Indeed, it is reasonable to conjecture that for a given even integer m there are infinitely many primes $p\equiv 1+m \pmod{2m}$ for which $M(p,m)\gg(\log\log p)^2$ and infinitely many primes $p\equiv 1+m \pmod{2m}$ for which $M(p,m)\ll(\log\log p)^{-2}$ (see [Lou16, bottom of page 166 and top of page 167]).

The aim of the paper is to give an asymptotic formula for $M(p,m)$ when m is of reasonable size with respect to p and an upper bound when m is small. As a consequence we obtain a significant improvement upon the trivial bound (6).

Theorem 1 *As p tends to infinity and $d \geq 1$ runs over the odd divisors of $p-1$ such that $1 \leq d \leq \frac{\log p}{3\log\log p}$, we have the asymptotic formula*

$$M(p,m) = M(p,(p-1)/d) = \frac{\pi^2}{6}\left(1 + O(d(\log p)^2 p^{-\frac{1}{d-1}})\right) = \frac{\pi^2}{6}\left(1+o(1)\right), \tag{7}$$

which implies the upper bound

$$h^-_{p,d} \leq 2\left(\frac{(1+o(1))p}{24}\right)^{m/4}. \tag{8}$$

If the previous bound does not apply but d is such that $\log d = o(\log p/\log_2 p)$, we have for some absolute constant $C>0$

$$M(p,m) = M(p,(p-1)/d) \leq C(\log_2 d)^2 \tag{9}$$

which implies, in this range of d, the upper bound

$$h^-_{p,d} \leq (Cp(\log_2 d)^2)^{m/4}. \tag{10}$$

Remarks 2 *The asymptotic formula* (7) *answers a question raised in [Lou16, Section 6, Question 2]. It should be emphasized that the error term in* (7) *is almost optimal, in view of Proposition 8. Furthermore* (8) *is in accordance with the known asymptotics (see [Lou96b, Theorem 4])* $\log h^-_{p,d} \sim \frac{m+o(1)}{4}\log p$. *For very large d, the bound $M(p,m) \ll \log^2 p$ remains the best known. This is not surprising if we look at the very extreme case $d=(p-1)/2$ and $p \equiv 3 \pmod 4$. In that situation, χ is the quadratic character given by the Legendre symbol $\chi(n) = \left(\frac{n}{p}\right)$ and $M(p,m) = |L(1,\chi)|^2$. Under GRH, Littlewood [Lit] proved that $L(1,\chi) \ll \log_2 p$ but improving upon the bound $L(1,\chi) \ll \log p$ remains out of reach unconditionally. On the other hand we cannot expect a uniform bound for $M(p,m)$ better than $(\log_2 p)^2$. Indeed, Chowla [Cho] proved unconditionally that there are infinitely many quadratic characters χ such that $L(1,\chi) \gg \log_2 p$. This supports the hypothesis that the bound* (9) *could be sharp.*

Finally, let d be an odd integer and $p \equiv 1 \pmod{2d}$ be a prime integer. Let χ be an odd Dirichlet character of (even) order $m=(p-1)/d$ dividing $p-1$ and prime conductor $p \geq 3$. Set

$$\mathcal{A}(p,d) = \frac{1}{p-1}\sum_{N=1}^{p-1}\left(\sum_{\substack{1\leq n_1,n_2\leq N\\ \chi(n_1)=\chi(n_2)}} 1\right) \tag{11}$$

(the results depend only on p and d, not on the choice of χ). Then the paper is organized as follows. To begin, in Section 2, we recall (and give a simple proof of) a formula discovered by Elma relating $M(p,m)$ to the character sums $\mathcal{A}(p,d)$ defined in (11). In Section 3, Proposition

8, we show that for a certain family of primes p and d we can compute exactly $M(p,m)$ using properties of Dedekind sums. Finally, in Section 4, we answer a question of Elma and prove the following asymptotic formula for $\mathcal{A}(p,d)$ which directly implies Theorem 1 (see Section 5):

Theorem 3 *As p tends to infinity and $d \geq 1$ runs over the odd divisors of $p-1$, we have*

$$\mathcal{A}(p,d) = \frac{(2d+1)p}{6} + o(dp).$$

A crucial point of the analysis comes from the fact that the average in (3) is made over a family of $m/2$ characters which could be of any size with respect to p. The same difficulty carries into the analysis of $\mathcal{A}(p,d)$ with a character sum averaged over a subgroup of $\mathbb{F}_p^*$ of size d. On the one hand when d is small (see Theorem 10) we write $\mathcal{A}(p,d)$ as an average of a function evaluated at equidistributed points modulo 1 and use techniques from discrepancy theory. On the other hand, when d is large (see Theorem 19) we rely on character sums techniques and incorporate recent estimates on the frequency of large character sums [BGGK].

2 Elma's character sums

2.1 Elma's character sums and the mean square value $M(p,m)$

E. Elma proved a nice connection between the mean square values $M(p,m)$'s and these character sums $\mathcal{A}(p,d)$. We give a simple and short proof of [Elm, Theorem 1.1]:

Theorem 4 *Let χ be a primitive Dirichlet character modulo $f > 2$, its conductor. Set $S(k,\chi) = \sum_{l=0}^{k} \chi(l)$ and let $L(s,\chi) = \sum_{n\geq 1} \chi(n) n^{-s}$ be its associated Dirichlet L-series. Then*

$$\sum_{k=1}^{f-1} |S(k,\chi)|^2 = \frac{f^2}{12} \prod_{p|f} \left(1 - \frac{1}{p^2}\right) + a_\chi \frac{f^2}{\pi^2} |L(1,\chi)|^2, \text{ where } a_\chi := \begin{cases} 0 & \text{if } \chi(-1) = +1, \\ 1 & \text{if } \chi(-1) = -1. \end{cases}$$

Proof. Our simple proof is based on an easy to remember idea: we apply Parseval's formula $\int_0^1 |F(x)|^2 \mathrm{d}x = \sum_{n=-\infty}^{\infty} |c_n(F)|^2$ to the function $x \in [0,1) \mapsto F(x) := \sum_{0\leq l\leq fx} \chi(l)$ extended to $x \in \mathbb{R}$ by 1-periodicity. The reader would be able to reconstruct the argument using this simple idea. Let us now give all the details. Since χ is primitive, the Gauss sums $\tau(n,\chi) = \sum_{k=1}^{f} \chi(k) \exp(2\pi i n k/f)$ and $\tau(\chi) = \tau(1,\chi)$ satisfy $\tau(n,\chi) = \overline{\chi(n)}\tau(\chi)$ and $|\tau(\chi)|^2 = f$, e.g. see [Was, Lemmas 4.7 and 4.8]. (These properties are easy to check when $f = p \geq 3$ is prime). Since $x \mapsto F(x) = S(k,\chi)$ is constant for $x \in [k/f, (k+1)/f)$, we have

$$\int_0^1 |F(x)|^2 \mathrm{d}x = \sum_{k=0}^{f-1} \int_{k/f}^{(k+1)/f} |F(x)|^2 \mathrm{d}x = \sum_{k=0}^{f-1} \int_{k/f}^{(k+1)/f} |S(k,\chi)|^2 \mathrm{d}x = \frac{1}{f} \sum_{k=0}^{f-1} |S(k,\chi)|^2,$$

and the n-th Fourier coefficient of F is given by

$$c_n(F) = \int_0^1 F(x) e^{-2\pi i n x} \mathrm{d}x = \sum_{k=0}^{f-1} \int_{k/f}^{(k+1)/f} F(x) e^{-2\pi i n x} \mathrm{d}x = \sum_{k=0}^{f-1} S(k,\chi) \int_{k/f}^{(k+1)/f} e^{-2\pi i n x} \mathrm{d}x.$$

Hence, by [Was, Theorem 4.2] we have

$$c_0(f) = \frac{1}{f}\sum_{k=0}^{f-1} S(k,\chi) = \frac{1}{f}\sum_{k=0}^{f-1}\sum_{l=0}^{k}\chi(l) = \frac{1}{f}\sum_{l=0}^{f-1}(f-l)\chi(l) = -\frac{1}{f}\sum_{l=0}^{f-1} l\chi(l) = L(0,\chi)$$

and for $n \neq 0$ we have

$$\begin{aligned} c_n(F) &= \sum_{k=0}^{f-1} S(k,\chi)\frac{\exp\left(-\frac{2\pi i n(k+1)}{f}\right) - \exp\left(-\frac{2\pi i n k}{f}\right)}{-2\pi i n} \\ &= \sum_{k=1}^{f-1}\frac{(S(k,\chi)-S(k-1,\chi))\exp\left(-\frac{2\pi i n k}{f}\right)}{2\pi i n} \qquad \text{(notice that } S(0,\chi)=S(f-1,\chi)=0) \\ &= \frac{\tau(-n,\chi)}{2\pi i n} = \frac{\tau(\chi)}{2\pi i}\times\frac{\overline{\chi(-n)}}{n} = -\chi(-1)c_{-n}(F). \end{aligned}$$

Now, $L(0,\chi)=0$ if $\chi(-1)=+1$ and $|L(0,\chi)|^2 = \frac{f}{\pi^2}|L(1,\chi)|^2$ if $\chi(-1)=-1$, e.g. see [Was, Chapter 4, page 30]. Therefore, Parseval's formula gives

$$\frac{1}{f}\sum_{k=0}^{f-1}|S(k,\chi)|^2 = a_\chi\frac{f}{\pi^2}|L(1,\chi)|^2 + 2\sum_{\substack{n\geq 1\\ \gcd(n,f)=1}}\frac{f}{4\pi^2}\times\frac{1}{n^2} = a_\chi\frac{f}{\pi^2}|L(1,\chi)|^2 + \frac{f}{12}\prod_{p|f}\left(1-\frac{1}{p^2}\right)$$

and the desired result follows. Notice that this proof is similar to the ones in [BC]. •

Corollary 5 *Let χ be an odd Dirichlet character of (even) order m dividing $p-1$ and prime conductor $p \geq 3$. Set $d=(p-1)/m$ (an odd integer) and let $\mathcal{A}(p,d)$ be as in (11). Then*

$$M(p,m) := \frac{2}{m}\sum_{\substack{j=0\\ j\ odd}}^{m-1}|L(1,\chi^j)|^2 = \frac{\pi^2}{6}\frac{p-1}{p^2}\left(12\mathcal{A}(p,d) - (4d+1)p - d - 1\right). \tag{12}$$

In particular,

$$\frac{(4d+1)p+d+1}{12} \leq \mathcal{A}(p,d) \leq \frac{(5d+1)p+d+1}{12}. \tag{13}$$

Moreover, by [Lou96a], we have

$$0 \leq M(p,m) \leq (\log p + 2 + \gamma - \log\pi)^2/4. \tag{14}$$

Proof. By Theorem 4, for j odd we have

$$|L(1,\chi^j)|^2 = -\frac{\pi^2}{12}\left(1-\frac{1}{p^2}\right) + \frac{\pi^2}{p^2}\sum_{k=1}^{p-1}|S(k,\chi^j)|^2$$

The χ^j's are primitive modulo p for $1 \leq j \leq m-1$, whereas χ^0 is the non-primitive trivial Dirichlet character modulo p. Therefore, on the one hand we have

$$\sum_{j=0}^{m-1}\sum_{k=1}^{p-1}|S(k,\chi^j)|^2 = \sum_{j=0}^{m-1}\sum_{k=1}^{p-1}\left|\sum_{l=1}^{k}\chi^j(l)\right|^2 = \sum_{j=0}^{m-1}\sum_{k=1}^{p-1}\sum_{1\leq l_1,l_2\leq k}\chi^j(l_1)\overline{\chi^j(l_2)} = m(p-1)\mathcal{A}(p,d),$$

by using the orthogonality relation

$$\sum_{j=0}^{m-1} \chi^j(n_1)\overline{\chi^j(n_2)} = \begin{cases} m & \text{if } \chi(n_1) = \chi(n_2) \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

On the other hand, Theorem 4 gives

$$\sum_{j=1}^{m-1}\sum_{k=1}^{p-1} |S(k,\chi^j)|^2 = \frac{(m-1)(p^2-1)}{12} + \frac{mp^2}{2\pi^2} M(p,m).$$

Since

$$\sum_{k=1}^{p-1} |S(k,\chi^0)|^2 = \sum_{k=1}^{p-1} \left|\sum_{l=1}^{k} 1\right|^2 = \sum_{k=1}^{p-1} k^2 = \frac{(p-1)p(2p-1)}{6},$$

it follows that

$$m(p-1)\mathcal{A}(p,d) = \frac{m(p^2-1)}{12} + \frac{(p-1)^2(4p+1)}{12} + \frac{mp^2}{2\pi^2} M(p,m).$$

The desired identity (12) follows.

Now, noticing that $M(p,m) \geq 0$, the lower bound on $\mathcal{A}(p,d)$ in (13) follows from (12). Finally, by (5) we have

$$M(p,m) \leq \frac{d\pi^2}{6}\left(1 - \frac{1}{p}\right).$$

Plugging this bound in (12) we obtain the upper bound on $\mathcal{A}(p,d)$ in (13). •

By (2) and (12), upper bounds on $\mathcal{A}(p,d)$ would yield upper bounds on $h^-_{p,d}$. More precisely, for $d > 1$, $M(p,m) \leq \pi^2/6$ which is equivalent to $\mathcal{A}(p,d) < \big((4d+2)p + d + 2\big)/12$ would yield $h^-_{p,d} \leq 2(p/24)^{m/4}$.

Remarks 6 *Corollary 5 gives* $\frac{13p+4}{12} \leq \mathcal{A}(p,3) \leq \frac{16p+4}{12}$, *whereas* $\mathcal{A}(p,3) = \frac{14p+4}{12}$, *by (18) below. Hence it should be possible to improve upon the upper bound in* (13).

2.2 Exact formulas for $M(p,m)$ and $\mathcal{A}(p,d)$ in specific cases

There are only four cases listed below where an explicit formula for $\mathcal{A}(p,d)$ is known.

1. By (4) and (12), for $d = 1$ we have

$$\mathcal{A}(p,1) = \frac{p}{2} = \frac{(2d+1)p}{6}. \tag{15}$$

2. For $d = 3$ we proved in [Lou16, Theorem 1] that

$$M(p,(p-1)/3) = \frac{\pi^2}{6}\left(1 - \frac{1}{p}\right) \qquad (\text{for } p \equiv 1 \pmod 6) \tag{16}$$

and the corresponding bound on the relative class number

$$h^-_{p,3} \leq 2\left(\frac{p}{24}\right)^{(p-1)/12} = 2\left(\frac{p}{24}\right)^{m/4}. \tag{17}$$

By (12), this gives for $d = 3$ and $p \equiv 1 \pmod 6$,

$$\mathcal{A}(p,3) = \frac{7p+2}{6} = \frac{(2d+1)p}{6} + o(p). \tag{18}$$

3. For $d = 5$ we proved in [Lou16, Theorem 5] that

$$M(p,(p-1)/5) = \frac{\pi^2}{6}\left(1 + \frac{2a(a+1)^2-1}{p}\right) \qquad (\text{for } p > 5 \text{ of the form } p = \tfrac{a^5-1}{a-1}). \tag{19}$$

and the corresponding bound on the relative class number

$$h^-_{p,5} \le 2\left(\frac{p}{24}\right)^{(p-1)/20} = 2\left(\frac{p}{24}\right)^{m/4}. \tag{20}$$

By (19) and (12), this implies

$$\mathcal{A}(p,5) = \frac{11p+3}{6} + \frac{a(a+1)^2 p}{6(p-1)} = \frac{(2d+1)p}{6} + o(p). \tag{21}$$

4. For $d = (p-1)/2$ and $3 < p \equiv 3 \pmod 4$. In that situation, χ is the quadratic character given by the Legendre symbol $\chi(n) = \left(\frac{n}{p}\right)$, $L(1,\chi) = \pi h_{\mathbb{Q}(\sqrt{-p})}/\sqrt{p}$ and (12) gives

$$\begin{aligned}\mathcal{A}(p,(p-1)/2) &= \frac{4p^2-p+1}{24} + \frac{p^2}{2\pi^2(p-1)}|L(1,\chi)|^2 \\ &= \frac{4p^2-p+1}{24} + \frac{p h^2_{\mathbb{Q}(\sqrt{-p})}}{2(p-1)} = \frac{dp}{3} + O(p\log^2 p),\end{aligned}$$

where we used the bound $|L(1,\chi)| \ll \log p$.

Remarks 7 *In fact, $d = 1$ is the only case for which we could come up with a direct proof of the formula for $\mathcal{A}(p,d)$. Indeed, we have $\chi_{p,p-1}(n_1) = \chi_{p,p-1}(n_2)$ if and only if $n_1 \equiv n_2 \pmod p$. Hence,*

$$\mathcal{A}(p,1) = \frac{1}{p-1}\sum_{N=1}^{p-1} N = \frac{p}{2}.$$

It would be nice to have similar independent and direct proofs of (18) and (21).

3 Evaluation of $M(p,m)$ for primes $p = (a^d-1)/(a-1) \equiv 1 \pmod{2d}$

We gave an explicit formula for $\mathcal{A}(p,3)$, see (18), and one for $\mathcal{A}(p,5)$, but only for the primes p of the form $p = (a^5-1)/(a-1)$, see (21). After some numerical computation for primes of the form $(a^5-2^5)/(a-2)$ or $(a^5-3^5)/(a-3)$ we could not guess any formula for $M(p,(p-1)/5)$ or $\mathcal{A}(p,5)$. However, we now prove a general result which recover (16) and (19) (let us say that we forgot to deal with the case $a < 0$ in the proof of [Lou16, Theorem 5]). We want to point out that here again we do not directly compute $\mathcal{A}(p,d)$. Instead we give an exact formula for $M(p,m)$ and then use (12) to deduce an expression for $\mathcal{A}(p,d)$.

Proposition 8 *Set $Q_l(X) = (X^l - 1 - l(X-1))/(X-1)^2 \in \mathbb{Z}[X]$, $l \geq 1$. Hence, $Q_1(X) = 0$, $Q_2(X) = 1$ and $Q_l(X) = X^{l-2} + 2X^{l-3} + \cdots + (l-2)X + (l-1)$ for $l \geq 2$. Let $d \geq 3$ be a prime integer. For a prime integer of the form $p = (a^d - 1)/(a-1)$ for some $a \neq -1, 0, 1$, we have*

$$M(p, (p-1)/d) = \frac{\pi^2}{6}\left(1 + \frac{2a(a+1)^2 Q_{\frac{d-1}{2}}(a^2) - 1}{p}\right), \tag{22}$$

$$\mathcal{A}(p,d) = \frac{(2d+1)p + \frac{d+1}{2}}{6} + \frac{p}{p-1}\cdot\frac{a(a+1)^2 Q_{\frac{d-1}{2}}(a^2)}{6} = \frac{2d+1}{6}p + O\left(p^{1-\frac{1}{d-1}}\right), \tag{23}$$

and

$$h^-_{p,d} \leq 2\,(p/24)^{m/4} \text{ for } p = (a^d-1)/(a-1) \text{ with } a \leq -2.$$

Proof. We keep the notation of [Lou16], use the properties of Dedekind sums

$$s(c,d) = \frac{1}{4d}\sum_{n=1}^{|d|-1} \cot\left(\frac{\pi n}{d}\right)\cot\left(\frac{\pi n c}{d}\right) \qquad (c \in \mathbb{Z},\ d \in \mathbb{Z}\setminus\{-1,0,1\})$$

recalled in [Lou16] and set $l = (d-1)/2$. To deal in one stroke with the two cases $a \leq -2$ and $a \geq 2$ we have extended the definition of Dedekind sums, allowing d to be negative. The reciprocity and complementary laws for these generalized Dedekind sums are

$$s(c,d) + s(d,c) = \frac{c^2 + d^2 - 3|cd| + 1}{12cd} \text{ and } s(1,d) = \frac{d^2 - 3|d| + 2}{12d}.$$

Set $p_k = (a^k - 1)/(a-1)$. By [Lou16, Corollary 3] we have

$$M(p,(p-1)/d) = \frac{\pi^2}{6}\left(1 + \frac{N}{p}\right), \text{ where } N = 24\left(\sum_{k=1}^{l} s(a^k, p)\right) - 3 + \frac{2}{p}.$$

Now, $p \equiv p_k \pmod{a^k}$ and $a^k \equiv 1 \pmod{p_k}$ for $1 \leq k \leq d$. Hence

$$s(a^k,p) = \frac{a^{2k} + p^2 - 3|a|^k p + 1}{12a^k p} - s(p,a^k) = \frac{a^{2k} + p^2 - 3|a|^k p + 1}{12a^k p} - s(p_k, a^k)$$

and

$$s(p_k,a^k) = \frac{p_k^2 + a^{2k} - 3|p_k a^k| + 1}{12 p_k a^k} - s(a^k, p_k) = \frac{p_k^2 + a^{2k} - 3|p_k a^k| + 1}{12 p_k a^k} - s(1,p_k),$$

by the reciprocity law for Dedekind sums. Since

$$s(1,p_k) = \frac{p_k^2 - 3|p_k| + 2}{12 p_k},$$

by the complementary law for Dedekind sums, we obtain

$$s(a^k,p) = \frac{a^{2k} + p^2 - 3|a|^k p + 1}{12a^k p} - \left(\frac{p_k^2 + a^{2k} - 3|p_k a^k| + 1}{12 p_k a^k} - \frac{p_k^2 - 3|p_k| + 2}{12 p_k}\right).$$

The contribution of the three terms with absolute values is equal to $-\frac{\epsilon^k}{4}+\frac{\epsilon^{2k+1}}{4}-\frac{\epsilon^{k+1}}{4}$, where $\epsilon=a/|a|$ is the sign of a and therefore ϵ^{k+1} is the sign of p_k. Hence, this contribution is equal to $-\frac{1}{4}$ whatever the value of $\epsilon\in\{-1,1\}$. Since this contribution does not depend on ϵ, we may get rid of the absolute values and we obtain

$$\begin{aligned} s(a^k,p) &= \frac{a^{2k}+p^2-3a^kp+1}{12a^kp}-\left(\frac{p_k^2+a^{2k}-3p_ka^k+1}{12p_ka^k}-\frac{p_k^2-3p_k+2}{12p_k}\right)\\ &= \frac{a^{2k}+p^2-3a^kp+1}{12a^kp}-\left(\frac{p_k-3a^k}{12a^k}-\frac{p_k-3}{12}+\frac{a^{2k}+1}{12a^kp_k}-\frac{2}{12p_k}\right)\\ &= \frac{a^{2k}+p^2-3a^kp+1}{12a^kp}-\left(\frac{p_k(1-a^k)}{12a^k}+\frac{(a^k-1)^2}{12a^kp_k}\right)\\ &= \frac{a^{2k}+p^2-3a^kp+1}{12a^kp}-\left(\frac{(1-a)p_k^2}{12a^k}+\frac{(a-1)(a^k-1)}{12a^k}\right) \end{aligned}$$

and

$$s(a^k,p)=\frac{a^{2k}+p^2-3a^kp+1}{12a^kp}+(a-1)\frac{p_k^2+1-a^k}{12a^k}.$$

Notice that the more natural congruence $p\equiv p_{k-1} \pmod{a^k}$ and $a^k\equiv a \pmod{p_{k-1}}$ would lead to slightly more complicated computations.
An easy but boring computation using $\sum_{k=1}^{l} b^k = b(b^l-1)/(b-1)$ then finally yields $N = 2a(a+1)^2Q_l(a^2)-1$, as desired. •

Remarks 9 *It is a long standing conjecture that there are infinitely many primes of the form $p=(a^d-1)/(a-1)$, as first investigated in the special case of Mersenne primes 2^p-1 ($a=2$). More precise results about the number of such primes less than x are expected. This is sometimes called the Lenstra-Pomerance-Wagstaff conjecture (see the survey [Pom] for more information and references on this topic).*

4 Asymptotic behavior of Elma's sums and proof of Theorem 3

Let us remark that

$$\frac{\mathcal{A}(p,d)}{dp/3}=\frac{pM(p,m)}{2\pi^2d(p-1)}+1+\frac{1}{4d}+\frac{1}{4p}+\frac{1}{4dp},$$

by (12). Hence, as $d/\log^2 p$ tends to infinity (or equivalently $m=o(p/\log^2 p)$), we have by (14)

$$\mathcal{A}(p,d)\sim\frac{dp}{3}, \tag{24}$$

as noticed in [Elm]. However, according to the results of Section 2.2, for a given d we cannot expect this asymptotic but rather the refined asymptotic

$$A(p,d)\sim\frac{(2d+1)p}{6}. \tag{25}$$

Our goal in this section is to prove Theorem 3, i.e. that (25) indeed holds true without any restriction on the size of the parameter d.

We will split the discussion into two cases depending on whether d goes or not to infinity. Theorem 3 follows from Theorems 10 (d small) and 19 (d large) proved below. In the former case, we obtain the more precise asymptotic expansion $A(p,d) \sim \frac{(2d+1)p}{6}$. By (12), this allows us to deduce an asymptotic formula for $M(p,m)$. In the latter case, Theorem 3 is not sufficient to infer an asymptotic formula for $M(p,m)$ and only implies an upper bound.

4.1 Asymptotic for small d's

Our goal in this section is to prove the following theorem which gives Theorem 3 for small d's:

Theorem 10 *Let d range over the odd integers. Set $\gamma(d) = \max_{k|d} \phi(k) \leq d-1$. Let p range over the prime integers such that $p \equiv 1 \pmod{2d}$. Then we have the following asymptotic formula*

$$\mathcal{A}(p,d) = \frac{2d+1}{6}p + O\left(d(\log p)^2 p^{1-1/\gamma(d)}\right) = \frac{2d+1}{6}p + O\left(dp(\log p)^2 p^{-1/(d-1)}\right)$$

where the implicit constant in the error term is absolute.
In particular, in the range $1 \leq d \leq \frac{\log p}{3\log\log p}$, we have

$$\mathcal{A}(p,d) \sim \frac{2d+1}{6}p.$$

Remarks 11 *Observe that $\gamma(d) = d-1$ whenever d is an odd prime. Hence by (23) the power of p in the error term of Theorem 10 is optimal.*

4.1.1 Results from uniform distribution theory

For any fixed integer s, we consider the s-dimensional cube $I_s = [0,1]^s$ equipped with its s-dimensional Lebesgue measure λ_s. We denote by $\mathcal{B}$ the set of rectangular boxes of the form

$$\prod_{i=1}^{s}[\alpha_i, \beta_i) = \{x \in I_s, \alpha_i \leq x_i < \beta_i\}$$

where $0 \leq \alpha_i < \beta_i \leq 1$.

If S is a finite subset of I^s, we define the discrepancy $D(S)$ by

$$D(S) = \sup_{B\in\mathcal{B}} \left| \frac{\#(B \cap S)}{\#S} - \lambda_s(B) \right|.$$

The discrepancy measures in a quantitative way the deviation of a pointset S from equidistribution. In particular a sequence of sets S_n is uniformly distributed if and only if $D(S_n) \xrightarrow[n\to\infty]{} 0$. In order to state a quantitative version of this phenomenon known as the **Koksma-Hlawka inequality**, the concept of functions of bounded Hardy-Krause variation is used. In words, the Hardy-Krause variation is the sum of the Vitali variations [1] of all the restrictions of f to the faces of I_s.

[1] To have a rough idea in two dimensions, look at the variation of f over the rectangle $R := [x_1, x_2] \times [y_1, y_2]$, namely $v_R(f) := f(x_2,y_2) - f(x_1,y_2) - f(x_2,y_1) + f(x_1,y_1)$. The Vitali variation can then be obtained by summing $v_R(f)$ over a partition of I_2 and taking the supremum over all possible partitions.

Theorem 12 *[DT, Theorem* 1.14*] Let $f(\mathbf{x})$ a function of bounded variation on I_s in the sense of Hardy and Krause and $\mathbf{x_1}, \dots, \mathbf{x_N}$ a finite sequence of points in I_s. Then*

$$\left| \frac{1}{N} \sum_{i=1}^{N} f(\mathbf{x_i}) - \int_{I_s} f(u) d\lambda_s(u) \right| \leq V(f) D(S)$$

where $V(f)$ is the Hardy-Krause variation of f (see also [KN, Chapter 2*]).*

In order to estimate the discrepancy, we recall the inequality of **Erdős-Turán-Koksma**:

Theorem 13 *[DT, Theorem* 1.21*]. Let $S = \{\mathbf{x_1}, \dots, \mathbf{x_N}\}$ be a set of points in I_s and H a positive integer. Then we have*

$$D(S) \leq \left(\frac{3}{2}\right)^s \left(\frac{2}{H+1} \sum_{0 < \|\mathbf{h}\|_\infty \leq H} \frac{1}{r(\mathbf{h})} \left| \frac{1}{N} \sum_{n=1}^{N} e(\langle \mathbf{h}, \mathbf{x_N} \rangle) \right| \right), \tag{26}$$

where $e(z) = \exp(2\pi i z)$, $r(\mathbf{h}) = \prod_{i=1}^{s} \max\{1, |h_i|\}$ for $\mathbf{h} = (h_1, \dots, h_s) \in \mathbb{Z}^s$ and $\langle , \rangle$ denotes the standard inner product in $\mathbb{R}^s$.

4.1.2 Notions from pseudo random generators theory

In the rest of the paper the results of the previous section will only be used for $s = 2$.
We introduce some tools from the theory of pseudo-random generators and optimal coefficients in a very basic situation. We refer for more information to the survey of Korobov [Kor], the work of Niederreiter [Nied77, Nied78] or the book of Konyagin and Shparlinski [KS, Chapter 12] and keep their notations. For any prime p and integer $1 \leq \lambda \leq p-1$ we define

$$\sigma(\lambda, p) := \sum_{0 < \|\mathbf{h}\|_\infty \leq p-1} \frac{\delta_p(h_1 + h_2 \lambda)}{r(\mathbf{h})}$$

where $\delta_p(a) = 1$ if $a = 0 \bmod p$ and $\delta_p(a) = 0$ otherwise.

For any λ, we define

$$\rho(\lambda, p) = \min_{\mathbf{h} \neq 0} r(\mathbf{h})$$

where the min is taken over all non trivial solutions $\mathbf{h} = (h_1, h_2)$ of the congruence

$$h_1 + h_2 \lambda = 0 \bmod p.$$

The next lemma shows that $\frac{1}{\rho(\lambda,p)}$ and $\sigma(\lambda, p)$ are relatively close to each other:

Lemma 14 *[Nied77, Theorem* 3.8*]. There exists $C > 0$ such that, for any prime $p \geq 3$, and $\lambda \in \{1, \dots, p-1\}$ we have*

$$\frac{1}{\rho(\lambda, p)} \leq \sigma(\lambda, p) \leq C \frac{(\log p)^2}{\rho(\lambda, p)}. \tag{27}$$

In some cases which are of interest for our problem, we can control from below $\rho(\lambda, p)$:

Lemma 15 *Let λ be an element order $k \geq 3$ in the multiplicative group $\mathbb{F}_p^*$. Then*

$$\rho(\lambda, p) \geq p^{1/\phi(k)}/\sqrt{8},$$

where ϕ denotes as usual the Euler's totient function.

Proof. Let

$$\Phi_k(X) = \sum_{0 \leq l \leq \phi(k)} a_l X^l = \prod_{\substack{1 \leq l \leq k \\ \gcd(k,l)=1}} (X - \zeta_k^l)$$

denote the k-th cyclotomic polynomial. Set

$$\|\Phi_k(X)\|_2 = \left(\sum_{0 \leq l \leq \phi(k)} |a_l|^2 \right)^{1/2} = \left(\frac{1}{2\pi} \int_0^{2\pi} |\Phi_k(e^{it})|^2 dt \right)^{1/2} \leq 2^{\phi(k)}.$$

We clearly have $\Phi_k(\lambda) = 0 \bmod p$. For $\mathbf{h} = (h_1, h_2) \neq 0$ we define $P(X) = h_1 + h_2 X$. Assume that $P(\lambda) = 0 \bmod p$, then p divides the resultant $R = \mathrm{Res}(P, \Phi_k)$. The polynomial Φ_k being irreducible of degree ≥ 2, we deduce that $R \neq 0$. It follows that $|R| \geq p$. Since R is the determinant of the Sylvester matrix of $P(X)$ and $\Phi_k(X)$, by Hadamard's inequality we have

$$|R| \leq \|P(X)\|_2^{\deg \Phi_k(X)} \|\Phi_k(X)\|_2^{\deg P(X)} \leq \left(h_1^2 + h_2^2\right)^{\phi(k)/2} 2^{\phi(k)} \leq \left(\max(|h_1|, |h_2|)\right)^{\phi(k)} 8^{\phi(k)/2}.$$

Hence we have

$$r(\mathbf{h}) \geq \max(|h_1|, |h_2|) \geq |R|^{1/\phi(k)}/\sqrt{8} \geq p^{1/\phi(k)}/\sqrt{8}.$$

All together we obtain the lower bound $\rho(\lambda, p) \gg p^{1/\phi(k)}/\sqrt{8}$. •

4.1.3 Reduction to a problem of equidistribution

Set $\mathrm{H} = \ker(\chi)$, the subgroup of $\mathbb{F}_p^*$ of order d. We interpret the condition $\chi(n_1) = \chi(n_2)$ as $n_1 n_2^{-1} \in \mathrm{H}$. We write H as a disjoint union

$$\mathrm{H} = \bigcup_{k|d} \mathrm{H}_k, \text{ where } \mathrm{H}_k := \{\theta \in \mathrm{H}, ord(\theta) = k\}.$$

Proposition 16 *For any pair (x, y) of I_2 we define*

$$f_d(x, y) = \frac{x}{d-1} + \min(x, y).$$

We have the following relation

$$\mathcal{A}(p, d) = \frac{1}{p-1} \sum_{\substack{1 \leq n_1, n_2 \leq p-1 \\ \chi(n_1) = \chi(n_2)}} \min(n_1, n_2) = \frac{p}{(p-1)} \sum_{\substack{k|d \\ k \neq 1}} \sum_{\theta \in H_k} \sum_{x \bmod p} f_d\left(\frac{x}{p}, \frac{x\theta}{p}\right).$$

Proof. Changing the order of summation in (11) and making the change of variables $(n_1, n_2) \mapsto (p - n_1, p - n_2)$, we do have

$$(p-1)\mathcal{A}(p,d) = \sum_{\substack{1\le n_1,n_2\le p-1\\ \chi(n_1)=\chi(n_2)}} (p - \max(n_1,n_2)) = \sum_{\substack{1\le n_1,n_2\le p-1\\ \chi(n_1)=\chi(n_2)}} \min(n_1,n_2).$$

Now we have

$$\sum_{\substack{1\le n_1,n_2\le p-1\\ \chi(n_1)=\chi(n_2)}} \min(n_1,n_2) = \sum_{x \bmod p} \left(x + \sum_{\substack{\theta\in \mathrm{H}\\ \theta\neq 1}} \min(x,\theta x) \right).$$

We remark that if $\theta \neq 1$, we have

$$\min(x,\theta x) = p f_d\left(\frac{x}{p}, \frac{x\theta}{p}\right) - \frac{x}{d-1}.$$

Using the decomposition $\mathrm{H} = \bigcup_{k|d} \mathrm{H}_k$ and summing over H, the proposition follows. •

Remarks 17 *The reader might wonder why we did not express directly the sum $\mathcal{A}(p,d)$ using the more natural function on I_d given by $g(x_1,\dots,x_d) = \sum_{i=1}^d \min(x_1,x_i)$ evaluated at the points $\left(\frac{x}{p}, \frac{x\lambda}{p}, \dots, \frac{x\lambda^{d-1}}{p}\right)$, where λ generates H. This comes from the fact that these points are not equidistributed in I_d because they lie in the hyperplane of equation $x_1 + \cdots + x_d = 0$.*

4.1.4 Proof of Theorem 10

We introduce the set of points in I_2:

$$S_\theta = \left\{ \left(\frac{x}{p}, \frac{x\theta}{p}\right), x \bmod p \right\}$$

for any $\theta \in \mathrm{H}\backslash\{1\}$. By Theorem 12 we have for any θ

$$\left| \frac{1}{p} \sum_{x \bmod p} f_d\left(\frac{x}{p}, \frac{x\theta}{p}\right) - \int_{I_2} f_d(u,v)dudv \right| \le V(f_d) D(S_\theta).$$

It is easy to compute the integral and obtain

$$\int_{I_2} f_d(u,v)dudv = \frac{1}{2(d-1)} + \frac{1}{3}.$$

Applying Proposition 16 and simplifying, we obtain the equation

$$\mathcal{A}(p,d) = \frac{2d+1}{6} p + O\left(ET\right) \tag{28}$$

where the error term is

$$ET := pV(f_d) \left(\sum_{\substack{k|d\\ k\neq 1}} \sum_{\theta\in \mathrm{H}_k} D(S_\theta) \right). \tag{29}$$

The readers can easily convince themselves that $V(f_d) \ll 1$ independently of d. Indeed we have $V(f_d) \leq \frac{1}{d-1} V((x,y) \to x) + V(\min(x,y)) \ll 1$ using basic properties of the Hardy-Krause variation (see for instance [AD, Equation (22)]) and the fact that the function $(x,y) \to \min(x,y)$ is of bounded Hardy-Krause variation. [2]

Hence to finish the proof, we need to bound the sum of discrepancies. Applying Theorem 26 with $H = p-1$ we obtain

$$D(S_\theta) \leq \left(\frac{3}{2}\right)^2 \left(\frac{2}{p} + \sum_{0<\|\mathbf{h}\|_\infty \leq p-1} \frac{1}{r(\mathbf{h})} \left| \frac{1}{p} \sum_{x=1}^{p} e\left(\frac{h_1 x + h_2 x\theta}{p}\right) \right| \right).$$

Using the orthogonality relations

$$\sum_{b \bmod p} e(bn/p) = \begin{cases} p, & \text{if } n \equiv 0 \pmod p, \\ 0, & \text{if } n \not\equiv 0 \pmod p, \end{cases}$$

we can bound the sum over $\mathbf{h}$ by

$$\sigma(\theta, p) := \sum_{0<\|\mathbf{h}\|_\infty \leq p-1} \frac{\delta_p(h_1 + h_2\theta)}{r(\mathbf{h})}$$

using the notations of subsection 4.1.2. For $\theta \in \mathrm{H}_k$, we apply consecutively Lemma 14 and Lemma 15 to obtain

$$\sigma(\theta, p) \leq C(\log p)^2 / p^{1/\phi(k)}$$

for an absolute constant C. Hence recalling that $\gamma(d) = \max_{k|d} \phi(k)$ and summing over k, we arrive at

$$ET = pV(f_d) \left(\sum_{\substack{k|d \\ k \neq 1}} \sum_{\theta \in \mathrm{H}_k} D(S_\theta) \right) \ll d(\log p)^2 p^{1-1/\gamma(d)}.$$

This concludes the proof of Theorem 10, in view of Equation (28).

4.2 Asymptotic for large d's

For a given non-principal Dirichlet character $\chi \mod p$, where p is a prime, let

$$M(\chi) := \max_{1 \leq x \leq p} \left| \sum_{n \leq x} \chi(n) \right|$$

and its renormalization

$$m(\chi) = \frac{M(\chi)}{e^\gamma \sqrt{p}/\pi}.$$

The Pólya–Vinogradov Theorem states that

$$m(\chi) \ll \log p \tag{30}$$

[2] Indeed the Hardy-Krause variation is obtained as a sum of the Vitali variations of $\min(x,y)$, $\min(x,1)$ and $\min(1,y)$.

for all non-principal characters $\chi \mod p$. Apart from some improvements on the implicit constant, this remains the state-of-the-art for the general non-principal character. However, for most of the characters $M(\chi)$ is much smaller and we can study how often $M(\chi)$ is large. The best result in this direction was obtained in [BGGK]:

Theorem 18 *Let $\eta = e^{-\gamma}\log 2$. If $1 \le \tau \le \log_2 p - M$ for some $M \ge 4$, then*

$$\Phi_p(\tau) := \frac{1}{p-1}\#\{\chi \mod p : m(\chi) > \tau\} \le \exp\left\{-\frac{e^{\tau-2-\eta}}{\tau}(1+O((\log\tau)/\tau))\right\}.$$

We are now in a position to prove Theorem 3 for large d's.

Theorem 19 *We have*

$$\mathcal{A}(p,d) = dp/3 + O(p\log^2 p),$$

where the implicit constant in this error term is absolute and effective. Moreover, if d and p go to infinity with $\log d = o(\log p/\log_2 p)$, then we have the better asymptotic

$$\mathcal{A}(p,d) = dp/3 + O(p(\log_2 d)^2),$$

where the implicit constant in this error term is absolute and effective. Consequently, if d goes to infinity, then

$$\mathcal{A}(p,d) = dp/3 + o(dp).$$

Remarks 20 *The condition $\log d = o(\log p/\log_2 p)$ could be made more explicit by specifying the constants in the proof below. Notice also that whereas Theorem 3 follows from Theorems 10 and 19, it does not follow from Theorem 10 and* (24).

Proof. The first part of the Theorem follows directly from (12) and the inequality $|L(1,\chi) \ll \log p$. This could also be proved following our argument below and using only the Pólya–Vinogradov inequality. Let us now focus on the case $\log d = o(\log p/\log_2 p)$. The condition $\chi(n_1) = \chi(n_2)$ is equivalent to $n_1 n_2^{-1}$ lying in the kernel of χ, which is a subgroup of order d of the multiplicative cyclic group $\mathbb{F}_p^*$. We apply the orthogonality of characters in the subgroup $<\chi>$ of order m generated by $\chi \in \mathcal{X}_p$ and rewrite the sum $\mathcal{A}(p,d)$ defined in (11) as

$$\mathcal{A}(p,d) = \frac{1}{(p-1)}\sum_{N=1}^{p-1}\frac{1}{m}\sum_{\substack{\Psi\in\mathcal{X}_p\\ \Psi^m=\chi_0}}\sum_{1\le n_1,n_2\le N}\Psi(n_1n_2^{-1}).$$

Separating the contribution of the trivial character from the others, this leads us to the equation

$$\mathcal{A}(p,d) = \frac{d}{(p-1)^2}\sum_{N=1}^{p-1}N^2 + \frac{1}{(p-1)}\sum_{N=1}^{p-1}\frac{1}{m}\sum_{\substack{\Psi\in\mathcal{X}_p^*\\ \Psi^m=\chi_0}}\left|\sum_{1\le n\le N}\Psi(n)\right|^2.$$

We have trivially

$$\frac{d}{(p-1)^2}\sum_{N=1}^{p-1}N^2 = \frac{dp}{3} + \frac{dp}{6(p-1)} = dp/3 + O(d).$$

Therefore we are left to bound the contribution of non-trivial characters and

$$\mathcal{A}(p,d) = dp/3 + O\left(d\frac{R}{(p-1)^2}\right) \tag{31}$$

where

$$R := \sum_{N=1}^{p-1} \sum_{\substack{\Psi \in \mathcal{X}_p^* \\ \Psi^m = \chi_0}} \left| \sum_{1 \le n \le N} \Psi(n) \right|^2 .$$

Let us set the parameter $\tau = \min\{C(\log_2 d), \log_2 p - M\}$, where M is the constant appearing in Theorem 18 and C is some large constant which will be specified later. We introduce the following set of characters

$$\mathcal{X}_{p,0}^{\tau} = \left\{ \Psi \in \mathcal{X}_p^* : m(\Psi) \le \tau \right\}$$

and further define for every integer $1 \le j \le J$

$$\mathcal{X}_{p,j}^{\tau} := \left\{ \Psi \in \mathcal{X}_p^* : 2^{j-1}\tau < m(\Psi) \le 2^j \tau \right\},$$

where J is chosen in order to allow an application of Theorem 18. Precisely, we choose J such that

$$\tau 2^J \le \log_2 p - M < \tau 2^{J+1}.$$

We now split the characters appearing in the summation in R as follows

$$\mathcal{X}_p^* = \left(\bigcup_{j=0}^{J} \mathcal{X}_{p,j}^{\tau} \right) \bigcup \left\{ \Psi \in \mathcal{X}_p^* : m(\Psi) > 2^J \tau \right\}.$$

Notice that if $\tau = \log_2 p - M$ then $J = 0$ and we only split the summation depending on whether $m(\Psi) \le \log_2 p - M$ or not. Remark that there are at most m characters $\Psi \in \mathcal{X}_{p,0}^{\tau}$ appearing in the sum. Hence, it follows from Theorem 18 and the inequality (30) that

$$\begin{aligned} R &\ll \sum_{N=1}^{p-1} \left(mp\tau^2 + p^2 \sum_{j=1}^{J} \tau^2 2^{2j} \Phi_p(\tau 2^{j-1}) + p^2 (\log p)^2 \Phi_p(\tau 2^J) \right) \\ &\ll \sum_{N=1}^{p-1} \left(mp\tau^2 + p^2 \sum_{j=1}^{J} \tau^2 2^{2j} \exp\left\{ -\frac{e^{\tau 2^{j-1}}}{100\tau 2^j} \right\} + p^2 (\log p)^2 \exp\left\{ -\frac{e^{\tau 2^J}}{100\tau 2^J} \right\} \right). \end{aligned} \tag{32}$$

The summation over j in the right hand side of (32) is clearly dominated by its first term. Thus we obtain after summing over N and recalling our choice of J:

$$R \ll \frac{p^3}{d}\tau^2 + p^3\tau^2 \exp\left\{ -c_1 \frac{e^{\tau}}{\tau} \right\} + p^3 (\log p)^2 e^{-c_2 \log p / \log\log p} \tag{33}$$

for some absolute constants $c_1, c_2 > 0$. We insert (33) in (31) and choose C large enough in the definition of τ to ensure that the second and third term in the right hand side of (33) have negligible contribution. This is indeed possible due to the restriction on the size of d and concludes the proof. •

5 Proof of Theorem 1

The first part of Theorem 1 follows from Theorem 10 and (12). The second part follows from Theorem 19 and (12).

6 Concluding remarks

We solved Elma's question about the asymptotic behavior of the character sums $\mathcal{A}(p,d)$ regardless of the size of d. As already noticed above, for d large, this is not precise enough to deduce an asymptotic formula for the mean-square value $M(p,m)$. To conclude, let us say that the upper bound (9) could be obtained by working directly with $L(1,\chi)$ following our method of proof of Theorem 19. This requires results about the distribution of $L(1,\chi)$ as the ones obtained by Granville and Soundararajan [GS1, GS2] instead of Theorem 18.

Funding

This work was supported (for M. M) by the Austrian Science Fund (FWF) [P-33043].

Acknowledgements

The second author would like to thank Igor Shparlinski for sketching a refinement of our argument in the proof of Theorem 19 leading to a better result.

References

[AC] N. C. Ankeny and S. Chowla. The class number of the cyclotomic field. . *Proc. Nat. Acad. Sci. U.S.A.* **35** (1949), 529–532.

[AD] C. Aistleitner and J. Dick. Functions of bounded variation, signed measures, and a general Koksma-Hlawka inequality. *Acta Arith.* **167(2)** (2015), 143–171.

[BC] P. T. Bateman and S. Chowla. Averages of character sums. *Proc. Amer. Math. Soc.* **1** (1950), 781–787.

[BGGK] J. Bober, L. Goldmakher, A. Granville, and D. Koukoulopoulos. The frequency and the structure of large character sums. *J. Eur. Math. Soc. (JEMS)*, 20(7): 1759–1818, 2018.

[Cho] S. Chowla. Improvement of a theorem of Linnik and Walfisz. *Proc. London Math. Soc* **50** (1949), 423–429.

[DT] M. Drmota and R. F. Tichy. *Sequences, discrepancies and applications*, volume 1651 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.

[Elm] E. Elma. On a problem related to discrete mean values of Dirichlet L-functions. *J. Number Theory* **217** (2020), 36–43.

[Gra] A. Granville. On the size of the first factor of the class number of a cyclotomic field. *Invent. Math.* **100** (1990), 321–338.

[GS1] A. Granville and K. Soundararajan. The distribution of values of $L(1,\chi_d)$. *Geometric and Funct. Anal.* **13** (2003), 992–1028.

[GS2] A. Granville and K. Soundararajan. Extreme values of $\zeta(1+it)$. *The Riemann zeta function and related themes: papers in honor of Professor K. Ramachandra, Ramanujan Math. Soc.* Lect. Notes Ser. 2 (2006), 65–80.

[KN] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences.* Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1974. Pure and Applied Mathematics.

[Kor] N. M. Korobov. Some problems in the theory of Diophantine approximation, *Russian Mathematical Surveys*, 22(3): 80–118, 1967.

[KS] S. V. Konyagin and I. E. Shparlinski. *Character sums with exponential functions and their applications*, volume 136 of *Cambridge Tracts in Mathematics.* Cambridge University Press, Cambridge, 1999.

[Lit] J.E. Littlewood. On the class number of the corpus $P(\sqrt{-k})$. *Proc. London Math. Soc* **27** (1928), 358–372.

[Lou93] S. Louboutin. Quelques formules exactes pour des moyennes de fonctions L de Dirichlet. *Canad. Math. Bull.* **36** (1993), 190–196. Addendum. *Canad. Math. Bull.* **37** (1994), p. 89.

[Lou96a] S. Louboutin. Majorations explicites de $|L(1,\chi)|$ (Suite). *C. R. Acad. Sci. Paris Sér. I Math.* **323** (1996), 443–446.

[Lou96b] S. Louboutin. A finitness theorem for imaginary abelian number fields. *Manuscripta Math.* **91** (1996), 343–352.

[Lou16] S. Louboutin. Dedekind sums, mean square value of L-functions at $s=1$ and upper bounds on relative class numbers. *Bull. Pol. Acad. Sci. Math.* **64** (2016), 165–174.

[Met] T. Metsänkylä. Class numbers and *mu*-invariants of cyclotomic fields. *Proc. Amer. Math. Soc.* **43** (1974), 299–300.

[Nied77] H. Niederreiter. Pseudo-random numbers and optimal coefficients. *Advances in Math.*, 26(2):99–181, 1977.

[Nied78] H. Niederreiter. Quasi-Monte Carlo methods and pseudo-random numbers. *Bull. Amer. Math. Soc.*, 84(6):957–1041, 1978.

[Pom] C. Pomerance. Recent developments in primality testing. *Math. Intelligencer.*, **3**, (1980/81), 97–105.

[Wal] H. Walum. An exact formula for an average of L-series. *Illinois J. of Math.* **26** (1982), 1–3.

[Was] L. C. Washington. *Introduction to Cyclotomic Fields.* Second Edition. Graduate Texts in Mathematics **83**. Springer-Verlag, New York, 1997.