The average number of subgroups of elliptic curves over finite fields

Corentin Perret-Gentil

Abstract. By adapting the technique of David, Koukoulopoulos and Smith for computing sums of Euler products, and using their interpretation of results of Schoof *à la* Gekeler, we determine the average number of subgroups (or cyclic subgroups) of an elliptic curve over a fixed finite field of prime size. This is in line with previous works computing the average number of (cyclic) subgroups of finite abelian groups of rank at most 2. A required input is a good estimate for the divisor function in both short interval and arithmetic progressions, that we obtain by combining ideas of Ivić–Zhai and Blomer. With the same tools, an asymptotic for the average of the number of divisors of the number of rational points could also be given.

Contents

1. Introduction 1
2. General strategy 5
3. Divisor function in arithmetic progressions and short intervals 13
4. Proofs of the results from Section 2 20
5. The number of subgroups ($h = s$) 28
6. The number of cyclic subgroups ($h = c$) 36
References 37

1. Introduction

1.1. **Counting subgroups.** Given a nontrivial finite group G, we let $s(G)$ and $c(G)$ be its number of subgroups, resp. cyclic subgroups.

We have the trivial bounds $2 \leqslant s(G) \leqslant 2^{|G|}$ and $1 \leqslant c(G) \leqslant |G|$, while Borovik–Pyber–Shalev [BPS96, Corollary 1.6] have shown the general upper bound

$$s(G) \leqslant \exp\left(\frac{(\log|G|)^2}{\log 2}\left(\frac{1}{4}+o(1)\right)\right). \tag{1}$$

For certain groups, such as finite abelian groups, explicit formulas for $s(G)$ and $c(G)$ are well-known (see e.g. [Ste92, Tă10] or (6) and Propositions 5.1, 6.1 below).

Date: September 2019.
2010 *Mathematics Subject Classification.* 11G07, 11N45, 11N37.

1.2. **Counting subgroups on average.** Given a finite family of finite groups $\mathcal{G}$, it may be interesting to understand the average

$$\frac{1}{|\mathcal{G}|}\sum_{G\in\mathcal{G}} h(G) \tag{2}$$

when $h \in \{s, c\}$, i.e. the average number of (cyclic) subgroups.

1.2.1. *Finite abelian groups of rank at most* 2. When $\mathcal{G}$ is the set of finite abelian groups of rank at most 2 and size at most x, Bhowmik and Menzer [BM97] determined that the average (2) for $h = s$ is given by

$$\frac{A_1 x(\log x)^2 + A_2 x(\log x) + A_3 x + O(x^{31/43+\varepsilon})}{\sum_{r\leqslant x}\tau(r)} = A_1 \log x + A_2 + o(1) \tag{3}$$

as $x \to +\infty$, where A_1, A_2, A_3 are effective constants and τ is the number of divisors function. The error term was later improved by other authors (see e.g. [Ivi97]).

1.3. **Elliptic curves.** Herein, we want to study the family $\mathcal{G} = \mathcal{E}ll(p)$ of (rational) isomorphism classes of elliptic curves defined over a finite field $\mathbb{F}_p$.

Since such curves are usually weighted by their number of automorphisms, we define a weighted version of (2) by

$$h(\mathcal{E}ll(p)) := \frac{1}{p}\sum_{E\in\mathcal{E}ll(p)} \frac{h\left(E(\mathbb{F}_p)\right)}{|\operatorname{Aut}(E)|}, \tag{4}$$

where $h \in \{s, c\}$. We recall that $\operatorname{Aut}(E) \in \{2, 4, 6\}$ if $p \geqslant 5$, and $\sum_{E\in\mathcal{E}ll(p)} |\operatorname{Aut}(E)|^{-1} = p$.

Our main result is the following:

Theorem 1.1. *For any $A > 0$, the weighted average number of subgroups of an elliptic curve over $\mathbb{F}_p$ is $<$*

$$\begin{aligned} s(\mathcal{E}ll(p)) \quad = \quad & \left(\prod_{\ell\mid p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\right)\sum_{u\mid d_1\mid p-1}\frac{\varphi(u)\tau(d_1/u)}{d_1^3} \\ & \sum_{k\mid d_1^2/u}\left(\log\left(\frac{p+1}{uk^2}\right)+2\gamma\right)\frac{\varphi(k)+\delta_{k=1}}{k} \\ & \prod_{\ell\mid k}\ell^{v_\ell(d_1)}\left(1+O\left(\frac{1}{\ell}\right)\right)\prod_{\ell\mid d_1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)^{-1} \\ & +O_A\left(\frac{1}{(\log p)^A}\right), \end{aligned}$$

with $\gamma = 0.5772\ldots$ the Euler–Mascheroni constant. The same result holds for $c(\mathcal{E}ll(p))$, after replacing $\varphi(u)$ by $(\varphi * \mu)(u)$, where μ is the Möbius function.

Remark 1.2. The second Euler product, over $\ell \mid k$, can be given explicitly, without the error terms (cf. Proposition 2.15 later on); the local factor at ℓ is a weighted sum of matrix densities in characteristic ℓ. We also note that

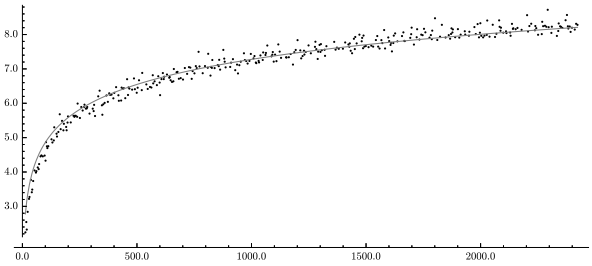

FIGURE 1. Graph of the average $y = \frac{1}{\pi(x)} \sum_{p \leqslant x} s(\mathcal{E}ll(p))$ for $x \leqslant 2423$ (black points) and of the least-squares fit $y = 1.053 \log x$ (gray line).

the first product $\prod_{\ell | p-1} (1 - (\ell(\ell^2 - 1))^{-1})$ is the asymptotic probability that $E(\mathbb{F}_p)$ is cyclic, by Vlăduţ [Vlă99] (see also [DKS17, Theorem 1.9])

Remark 1.3. The case of finite fields of higher degrees could be treated by extending the results of David–Koukoulopoulos–Smith (Proposition 2.2 below), as in the generalizations by Achter–Gordon [AG17] or Kaplan–Petrow [KP17] of the work of Gekeler [Gek03].

1.3.1. *Order of magnitude.* If $E \in \mathcal{E}ll(p)$, then $E(\mathbb{F}_p)$ is a finite abelian group of rank at most 2, i.e. there exist $d_1, d_2 \geqslant 1$ such that

$$E(\mathbb{F}_p) \cong \mathbb{Z}/d_1 \times \mathbb{Z}/d_1 d_2.$$

Moreover, by the Hasse–Weil bound, $p_- \leqslant d_1^2 d_2 \leqslant p_+$. Therefore, one may expect from (3) that $s(\mathcal{E}ll(p))$ is of order of magnitude $\log p$.

Indeed, averaging Theorem 1.1 over p, we find:

Proposition 1.4. *For $h \in \{s, c\}$, we have*

$$\frac{1}{\pi(x)} \sum_{p \leqslant x} h(\mathcal{E}ll(p)) \quad = \quad (C_h + o(1)) \log(x+1)$$

as $x \to \infty$, for some constant $C_h \geqslant 1$.

Pointwise, we find the following upper and lower bounds:

Proposition 1.5. *For $h \in \{s, c\}$ and $\varepsilon > 0$,*

$$\begin{aligned}
h(\mathcal{E}ll(p)) &\ll_\varepsilon (\log p)^{1+e^\gamma+\varepsilon} (\log_2 p) \sum_{d_1 | p-1} \frac{\tau(d_1^2)}{d_1} \\
&\ll (\log p)^{1+e^\gamma+\varepsilon} (\log_2 p) \min\left((\log p)^4, \tau((p-1)^2) \frac{\sigma(p-1)}{p-1} \right), \\
s(\mathcal{E}ll(p)) &\gg_\varepsilon \sum_{d_1 | p-1} \frac{\sigma(d_1)}{d_1^2} \geqslant \frac{\sigma(p-1)}{p-1}, \\
c(\mathcal{E}ll(p)) &\gg_\varepsilon \sum_{d_1 | p-1} \frac{(\sigma * \mathrm{id})(d_1)}{d_1^2} \gg \frac{\sigma(p-1)}{p-1}.
\end{aligned}$$

Remark 1.6. This is to be compared with the upper bound

$$s(\mathcal{E}ll(p)) \ll \exp\left(\frac{(\log p)^2}{\log 2}\left(\frac{1}{4}+o(1)\right)\right)$$

that follows from the Hasse–Weil bound and the general result (1) of Borovik–Pyber–Shalev, and to the bounds

$$\tau(d_1d_2)\sigma(d_1) \ll s(\mathbb{Z}/d_1\times\mathbb{Z}/d_1d_2) \ll \tau(d_1^2d_2)\sigma(d_1) \qquad (d_1,d_2\geqslant 1)$$

that are readily obtained from (6) below.

1.3.2. *Number of divisors of* $|E(\mathbb{F}_p)|$. Using the same tools and ideas, one could also give an explicit formula (as in Theorem 1.1) for

$$\frac{1}{p}\sum_{E\in\mathcal{E}ll(p)}\frac{\tau(|E(\mathbb{F}_p)|)}{|\operatorname{Aut}(E)|}, \tag{5}$$

i.e. the average number of divisors of the number of rational points, and an average of this quantity over primes $p\leqslant x$ (as in Proposition 1.4), of the order of $x\log x$ as $x\to\infty$. Since this is easier than Theorem 1.1 and that we plan to go back to averages of the type (5) in future work, we do not give further details here.

1.4. **Ideas and organization of the paper.** The idea of the proof of Theorem 1.1 is roughly the following:

(1) Condition the sum (4) on the $\mathbb{F}_p$-rational group structure, and use an explicit expression for the number of elliptic curves over $\mathbb{F}_p$ having a fix such structure, obtained by David–Koulouloupoulos–Smith [DKS17]. Their work translates a result of Schoof [Sch87] into a product of local densities over the primes, as in the very insightful work of Gekeler [Gek03];
(2) Adapt ideas from [DKS17] to compute the weighted sums of Euler products that arise, under the condition that h is well-distributed in some arithmetic progression in short intervals. Under additional assumptions, the main term can itself be given as a sum of Euler products with explicit local factors;
(3) Show that these conditions hold for $h=\{s,c\}$, using a known explicit expression for h as a convolution of arithmetic functions including Euler's totient, the divisor function, and the Möbius function. For example, we have (see Proposition 5.1 below):

$$s(\mathbb{Z}/d_1\times\mathbb{Z}/d_1d_2)=\sum_{u|d_1}\varphi(u)\tau(d_1/u)\tau(d_1^2d_2/u). \tag{6}$$

To control the asymptotic errors, we will prove the following result on the mean square error of the approximation of the divisor function in short intervals and arithmetic progression (see Section 3 for the notations):

Theorem 3.2. *Let $1 \leqslant A < B$, $1 \leqslant q \leqslant \sqrt{A}$, and $\varepsilon > 0$. We have*

$$\frac{1}{q}\sum_{a\in\mathbb{Z}/q}|\Delta(A,B,a,q)|^2 \tag{7}$$
$$\ll_\varepsilon (qB)^\varepsilon \begin{cases} \frac{(B-A)^{1/2}}{q}\left(\frac{B^3}{A}\right)^{1/4} & : B-A \leqslant \sqrt{B}, \\ \frac{(B-A)^{4/3}}{q^{4/3}}\left(\frac{B}{A}\right)^{1/3} & : \sqrt{B} \leqslant B-A \leqslant \sqrt{AB}. \end{cases}$$

This is obtained by combining ideas from Blomer [Blo07] (for the arithmetic progression aspect) and Ivić–Zhai [IZ14] (for the short interval aspect)

1.4.1. *Structure of the paper.* In Section 2, we give the general strategy to compute averages of the form (4), and obtain a result (Theorem 2.17) for a certain class of functions h. The proofs are then given in Section 4.

The remaining of the text focuses on the particular cases $h = s, c$. Section 3 is dedicated to proving the estimate (7). In Section 5, we deduce Theorem 1.1 for $h = s$ from Theorem 2.17, and the same is done for $h = c$ in Section 6.

1.4.2. *Notations.* Throughout, we will employ the usual convention that ε denotes a positive number as small as desired, whose exact size may change from one line to the next. Unless otherwise mentioned, the implied constants may depend on ε. For an integer n, we let $\mathrm{rad}(n)$ be the product of its prime factors without multiplicity, $P^+(n)$ its largest prime factor, $\omega(n)$ its number of distinct prime factors, and $\tau(n)$ (resp. $\sigma(n)$) the number (resp. sum) of its divisors. For $m \geqslant 1$, the notation $\log_m$ stands for the mth iterated natural logarithm.

Acknowledgements. The author thanks Dimitris Koukoulopoulos, as well as his other colleagues in Montréal, for helpful discussions during this project. We also thank an anonymous referee for providing comments that improved the exposition.

2. General strategy

In this section, we consider a real-valued function h on isomorphism classes of finite abelian groups of rank at most 2, and we aim to compute the weighted average $h(\mathcal{E}ll(q))$ defined in (4). We recall that the proofs of the following results will be given in Section 4.

For integers $d_1, d_2 \geqslant 1$, we use the abbreviation

$$h(d_1,d_2) := h(\mathbb{Z}/d_1 \times \mathbb{Z}/d_1d_2)$$

and for any group H, we define

$$\mathbb{P}\left(E(\mathbb{F}_p) \cong H\right) := \frac{1}{p}\sum_{E\in\mathcal{E}ll(p)}\frac{\delta_{E(\mathbb{F}_p)\cong H}}{|\operatorname{Aut}(E)|}. \tag{8}$$

2.1. **Conditioning on the group structure.** We start with an alternative expression for $h(\mathcal{E}ll(p))$.

Proposition 2.1. *We have*

$$h(\mathcal{E}ll(p)) = \sum_{\substack{d_2\geqslant 1\\ d_1\mid p-1\\ p_-\leqslant d_1^2d_2\leqslant p_+}} h(d_1,d_2)\mathbb{P}\left(E(\mathbb{F}_p)\cong \mathbb{Z}/d_1\times\mathbb{Z}/d_1d_2\right).$$

where $p_\pm := (\sqrt{p}\pm 1)^2$.

2.2. **Probability of having a given group of rational points.** Expressing a result of Schoof [Sch87, Lemma 4.8, Theorem 4.9] using ideas of Gekeler [Gek03], David, Koukoulopoulos and Smith gave the probability (8) as:

Proposition 2.2 ([DKS17, Theorem 1.7])**.** *For* $d_1,d_2\geqslant 1$*, we have*

$$\mathbb{P}\left(E(\mathbb{F}_p)\cong \mathbb{Z}/d_1\times\mathbb{Z}/d_1d_2\right) = f_\infty(p+1-d_1^2d_2,p)\prod_\ell f_\ell(d_1,d_2,p),$$

where ℓ *runs over primes and*

$$f_\ell(d_1,d_2,p) := \lim_{r\to+\infty}\frac{\left|\left\{g\in M_2(\mathbb{Z}/\ell^r): \begin{array}{c}\det(g)=p\\ \mathrm{tr}(g)=p+1-d_1^2d_2\\ g\equiv 1 \pmod{\ell^{v_\ell(d_1)}}\\ g\not\equiv 1 \pmod{\ell^{v_\ell(d_1)+1}}\end{array}\right\}\right|}{\ell^{2r}(1-1/\ell^2)}, \tag{9}$$

$$f_\infty(t,p) := \frac{1}{p\pi}\sqrt{4p-t^2}\,\delta_{|t|<2\sqrt{p}}. \tag{10}$$

We record the following important information about the asymptotic matrix densities f_ℓ:

Proposition 2.3 ([DKS17, Theorem 3.2])**.**

(1) The limit as $r\to\infty$ *defining* $f_\ell(d_1,d_2,p)$ *stabilizes when* $r > v_\ell(D_{d_1^2d_2,p})$*, where we let* $D_{a,p} := (p+1-a)^2-4p$ *for* $a\in\mathbb{Z}$. (11)

(2) If $\ell\nmid D_{d_1^2d_2,p}/d_1^2$*, then*

$$f_\ell(d_1,d_2,p) = \frac{1}{\ell^{v_\ell(d_1)}}\left(1-\frac{1}{\ell^2}\right)^{-1}\left(1+\frac{\chi_{d_1,d_2,p}(\ell)}{\ell}\right)$$

for the quadratic character $\chi_{d_1,d_2,p} = \left(\frac{D_{d_1^2d_2,p}/d_1^2}{\cdot}\right)$.

(3) If $d_1\mid p-1$*,*

$$f_\ell(d_1,d_2,p) = \frac{1}{\ell^{v_\ell(d_1)}}\left(1+O\left(\frac{1}{\ell}\right)\right).$$

More precisely, $1\leqslant f_\ell(d_1,d_2,p)\ell^{v_\ell(d_1)}\leqslant 1+\frac{2}{\ell}\left(1+\frac{1}{\ell-1}\right)$. (12)

(4) For p *large enough, we have*

$$f_p(d_1,d_2,p) = 1+\frac{\delta_{p\mid d_1^2d_2-1}}{p-1}.$$

Remark 2.4. If $E(\mathbb{F}_p) \cong \mathbb{Z}/d_1 \times \mathbb{Z}/d_1 d_2$ and $p \mid d_1^2 d_2 - 1$, then E is supersingular. There are only $O(\sqrt{p}\log p)$ isomorphism classes of such curves over $\mathbb{F}_p$ (see e.g. [Cox89, Theorem 14.18]); in particular, those can be ignored in (4) up to introducing an error of size $O(p^{-1/2}\log p)$.

2.3. **Sum of Euler products.** By Propositions 2.1 and 2.2, we have

$$h(\mathcal{E}ll(p)) \quad = \sum_{\substack{d_1,d_2 \\ p_- \leqslant d_1^2 d_2 \leqslant p_+}} w_{h,p}(d_1,d_2) \prod_{\ell} f_\ell(d_1,d_2,p), \tag{13}$$

where $w_{h,p}(d_1,d_2) := h(d_1,d_2) f_\infty(p+1-d_1^2 d_2, p)$. (14)

2.3.1. *The work of David–Koukoulopoulos–Smith.* The computation of weighted sums of Euler products similar to (13) is another topic of [DKS17], more particularly when summing over primes. David, Koukoulopoulos and Smith give general results to evaluate sums of the form

$$\sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} \prod_{\ell} (1+\delta_\ell(\boldsymbol{a})),$$

where $d \geqslant 1$, $\mathcal{A} \subset \mathbb{Z}^d \cap [-X,X]^d$, asymptotically when $X \to \infty$, with $\delta_\ell(\boldsymbol{a}), w_{\boldsymbol{a}} \in \mathbb{C}$ satisfying certain properties, such as:

(1) For primes ℓ small enough (with respect to X) and integers $r \geqslant 1$, there exists $\Delta_{\ell^r} : \mathbb{Z}/\ell^r \to \mathbb{C}$ such that $\delta_\ell(\boldsymbol{a}) = \Delta_{\ell^r}(\boldsymbol{a} \pmod{\ell^r})$ for "most" $\boldsymbol{a} \in \mathcal{A}$;

(2) The parameter set $\mathcal{A}$ is well-distributed modulo small enough $q \geqslant 2$, with respect to the weights $w_{\boldsymbol{a}}$, i.e.

$$\sum_{\substack{\boldsymbol{a}\in\mathcal{A} \\ \boldsymbol{a}\equiv\boldsymbol{b} \pmod q}} w_{\boldsymbol{a}} \approx \frac{1}{q} \sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}}$$

for all $\boldsymbol{b} \in (\mathbb{Z}/q)^d$.

In [DKS17], the set $\mathcal{A}$ essentially parametrizes primes in some intervals, and statistics on elliptic curves over $\mathbb{F}_p$ are obtained on average over primes $p \leqslant X$. Condition (2) then amounts to studying the distribution of primes in (short) arithmetic progressions.

However, Theorems 4.1 and 4.2 of ibid. are not directly applicable to our situation, since the condition (1) above ((4) or (4') in ibid.) does not hold: the matrix density in the limit defining $f_\ell(d_1,d_2,p)$ is periodic with respect to d_2, but not with respect to d_1. Moreover, the distribution of h in arithmetic progressions is not as simple as in (2), as we will see.

Nonetheless, we can still use the ideas and some of the results of David–Koukoulopoulos–Smith towards our goal, as we describe in the remaining of this section.[1]

[1] An alternative approach allowing to use [DKS17, Theorem 4.2] directly would be to move the factors at primes $\ell \mid d_2$ into the weights $w_{h,p}$. However, essentially the same additional work is then needed to identify the main term as an Euler product and control the errors. Moreover, this would only apply to the $h = s, c$, while Theorem 2.17 applies to a more general class of functions.

2.3.2. *Approximate independence of local factors.* We can write (13) as

$$h(\mathcal{E}ll(p)) = W_{h,p} \cdot \mathbb{E}_{h,p}\left(\prod_{\ell} f_\ell(d_1, d_2, p)\right) \tag{15}$$

with respect to the probability measure on $\{(d_1, d_2) : d_1 \mid p-1,\ p_- \leqslant d_1^2 d_2 \leqslant p_+\}$ induced by the weights $w_{h,p}(d_1, d_2)$, where $W_{h,p} := \sum_{d_1,d_2} w_{h,p}(d_1, d_2)$ is the normalization factor.

If the local densities $f_\ell(d_1, d_2, p)$ behave independently at each prime ℓ, then the expectation in (15) becomes

$$\prod_{\ell} \mathbb{E}_{h,p}\left(f_\ell(d_1, d_2, p)\right) = \prod_{\ell} \mathbb{E}_{h,p}\left(1 + \delta_\ell(d_1, d_2, p)\right) \tag{16}$$

$$= \sum_{n \geqslant 1} \mu(n)^2 \mathbb{E}_{h,p}(\delta_n(d_1, d_2, p)), \tag{17}$$

where $\delta_n(d_1, d_2, p) := \prod_{\ell \mid n}(f_\ell(d_1, d_2, p) - 1)$. (18)

This independence can be approximated by truncating the Euler product (16), as in [DKS17, pp. 37–38], using a result of Elliott:

Proposition 2.5. *For any $\varepsilon > 0$, $\alpha \geqslant 1$ and $Z \geqslant \exp(\sqrt{\log(4p)})$,*

$$h(\mathcal{E}ll(p)) = W_{h,p} \sum_{\substack{n \geqslant 1 \\ P^+(n) \leqslant z}} \mu(n)^2 \mathbb{E}_{h,p}(\delta_n(d_1, d_2, p)) + O\left(Z^{\frac{2}{\alpha}+\varepsilon} E_{h,p}^{(B)} + \frac{E_{h,p}^{(G)}}{(\log Z)^{\alpha-\varepsilon}}\right), \tag{19}$$

where $z = (\log Z)^{8\alpha^2}$ and (20)

$$E_{h,p}^{(B)} := \frac{1}{\sqrt{p}} \max\left(\frac{|h(d_1, d_2)|}{d_1} : p_- \leqslant d_1^2 d_2 \leqslant p_+\right), \tag{21}$$

$$E_{h,p}^{(G)} := \frac{1}{p} \sum_{d_1 \mid p-1} \int_0^{2\sqrt{p}} \sum_{\frac{p+1-y}{d_1^2} < d_2 \leqslant \frac{p+1+y}{d_1^2}} |h(d_1, d_2)| d_p y. \tag{22}$$

The implied constants depend only on ε and α. If there are no Siegel zeros, we may assume that $E_{h,p}^{(B)} = 0$.

Remark 2.6. If $h(d_1, d_2) \ll d_1 (d_1 d_2)^\varepsilon$ (e.g. for $h = s, c$), then $E_{h,p}^{(B)} \ll p^{-1/2+\varepsilon}$. The second error term will be discussed in more details in Lemma 4.5.

2.3.3. *Computation of local factors.* The starting point to compute (17) or (19) is to note that each $f_\ell(d_1, d_2, p)$ is given, according to Proposition 2.3, by a limit as $r \to +\infty$ that stabilizes at $r = v_\ell(D_{d_1^2 d_2, p}) + 1$, and that depends only on $v_\ell(d_1)$ and $d_1^2 d_2$. Splitting the sums defining the expected values according to $v_\ell(D_{d_1^2 d_2, p})$ yields the following:

Proposition 2.7. *For $n \geqslant 1$,*

$$\mathbb{E}_{h,p}(\delta_n(d_1,d_2,p)) \quad = \quad \sum_{\substack{q\geqslant 1\\ \mathrm{rad}(q)=n}} \sum_{\substack{a\in\mathcal{H}(q)\\ d_1\mid p-1}} \Delta_q(a,d_1,p)\frac{\overline{w}_{h,p}(d_1,a,q)}{W_{h,p}},$$

where $\mathcal{H}(q) := \{a \in \mathbb{Z}/q : v_\ell(D_{a,p}) = v_\ell(q) - 1 \ \forall \ell \mid q\}$, *and* (23)

$$\overline{w}_{h,p}(d_1,a,q) \quad := \quad \sum_{\substack{\frac{p_-}{d_1^2}<d_2\leqslant\frac{p_+}{d_1^2}\\ d_1^2d_2\equiv a \pmod q}} w_{h,p}(d_1,d_2), \tag{24}$$

and $\Delta_q : \mathbb{Z}/q\times\mathbb{N}\times\mathbb{N} \to \mathbb{R}$ *is a function satisfying* $\delta_q(d_1,d_2,p) = \Delta_q(d_1^2d_2,d_1,p)$.

Remark 2.8. The map Δ_q exists (and is unique when evaluated at the parameters considered) since $\delta_q(d_1,d_2,p)$ depends only on $a = d_1^2d_2 \pmod q$ and $v_\ell(d_1)$.

2.3.4. *Distribution of $w_{h,p}$ in arithmetic progressions.* To understand $\overline{w}_{h,p}$, we start by applying Abel's summation formula to the smooth factor f_∞.

Lemma 2.9.

$$\overline{w}_{h,p}(d_1,a,q) \quad = \quad \frac{1}{\pi p}\int_0^{2\sqrt{p}} \sum_{\substack{\frac{p+1-y}{d_1^2}<d_2\leqslant\frac{p+1+y}{d_1^2}\\ d_1^2d_2\equiv a \pmod q}} h(d_1,d_2)d_py,$$

where $d_py := \frac{ydy}{\sqrt{4p-y^2}}$ *on* $[-2\sqrt{p},2\sqrt{p}]$. (25)

For all $q \geqslant 1$ and $a \in \mathbb{Z}/q$, we may expect that

$$\sum_{\substack{\frac{p+1-y}{d_1^2}<d_2\leqslant\frac{p+1+y}{d_1^2}\\ d_1^2d_2\equiv a \pmod q}} h(d_1,d_2) \quad = \quad \delta_{(d_1^2,q)\mid a}\frac{2y}{d_1^2}\frac{C_{h,p}(a,d_1,q)}{q} \tag{26}$$

$$+O\left(\delta_{(d_1^2,q)\mid a}|E_{h,p}(y,d_1,a,q)|\right)$$

for some $C_{h,p}(a,d_1,q), E_{h,p}(y,d_1,a,q) \in \mathbb{R}$ depending only on the variables in the arguments, assuming at least that the modulus is not too large ($q \leqslant 2y/d_1^2$) and that the interval is large enough ($y \geqslant d_1^2/2$).

Proposition 2.10. *If* (26) *holds, then the main term of* (19) *is*

$$\sum_{d_1\mid p-1}\frac{1}{d_1^2}\sum_{q\in Q(d_1,z)}\frac{1}{q}\sum_{a\in\mathcal{H}(q)}\delta_{(q,d_1^2)\mid a}C_{h,p}(a,d_1,q)\Delta_q(a,d_1,p) + O\left(E_{h,p}^{(P)}(z)\right), \tag{27}$$

where $Q(d_1,z) := \{q \geqslant 1 : \ell \leqslant z$ *and* $v_\ell(q) > v_\ell(d_1^2)$ *for all* $\ell \mid q\}$ *and* (28)

$$E_{h,p}^{(P)}(z) := \sum_{\substack{d_1\mid p-1\\ d_1\ll p^{1/2}}}\sum_{q\in Q(d_1,z)}\frac{O(1)^{\omega(q)}}{\mathrm{rad}(q)}\frac{1}{p}\int_0^{2\sqrt{p}}\sum_{\substack{a\in\mathcal{H}(q)\\ (q,d_1^2)\mid a}}|E_{h,p}(y,d_1,a,q)|d_py. \tag{29}$$

2.4. **The main term as an Euler product.** At this point, one may want to use the multiplicative properties of Δ_q with respect to q to recover an Euler product from (27). However, we need to deal with the additional factor $C_{h,p}(a,d_1,q)$ that may depend on a, and that may not be multiplicative in q. Note that in [DKS17], the analogue of this factor depends neither on the class a nor on the modulus q.

To overcome this, we now make the additional assumption that when $q \in Q(d_1,z)$, we have

$$\begin{aligned} C_{h,p}(a,d_1,q) &= \sum_{\boldsymbol{v}\in\mathbb{N}^m} C_{h,p}^{(1)}(\boldsymbol{v},d_1)C_{h,p}^{(2)}(a,\boldsymbol{v},d_1,q)\prod_{\ell\mid q} C_{h,p}^{(3)}(\boldsymbol{v},d_1,\ell) \\ |E_{h,p}(y,d_1,a,q)| &\ll \sum_{\boldsymbol{v}\in\mathbb{N}^m} |C_{h,p}^{(1)}(\boldsymbol{v},d_1)||E'_{h,p}(y,\boldsymbol{v},d_1,a,q)| \end{aligned} \tag{30}$$

for some $m \geqslant 1$, where $C_{h,p}^{(1)}(\boldsymbol{v},d_1)$, $C_{h,p}^{(3)}(\boldsymbol{v},d_1,\ell)$, $E'_{h,p}(y,\boldsymbol{v},d_1,a,q) \in \mathbb{R}$, the sums and the product have finite support, and $q \mapsto C_{h,p}^{(2)}(a,\boldsymbol{v},d_1,q) \in \mathbb{R}$ is multiplicative. The multiplicativity of $C_{h,p}^{(2)}$ and Δ_q then allows to express the main term of (19) as a weighted sum of (truncated) Euler products:

Proposition 2.11. *If (30) holds, then the main term of (19) is given by*

$$\sum_{\substack{d_1\mid p-1\\ \boldsymbol{v}\in\mathbb{N}^m}} \frac{C_{h,p}^{(1)}(\boldsymbol{v},d_1)}{d_1^2}\prod_{\ell} P_{h,p}(\ell,\boldsymbol{v},d_1),$$

with the local factors

$$\begin{aligned} P_{h,p}(\ell,\boldsymbol{v},d_1) &:= C_{h,p}^{(3)}(\boldsymbol{v},d_1,\ell) \\ &\quad +\delta_{\ell\leqslant z}\sum_{r>v_\ell(d_1^2)}\frac{1}{\ell^r}\sum_{\substack{a\in\mathcal{H}(\ell^r)\\ v_\ell(a)\geqslant v_\ell(d_1^2)}} C_{h,p}^{(2)}(a,\boldsymbol{v},d_1,\ell^r)\Delta_{\ell^r}(a,d_1,p). \end{aligned} \tag{31}$$

2.5. **Computation of the local factors.** Under further natural assumptions, the local factors $P_{h,p}$ can be rewritten as limits of weighted matrix densities:

Proposition 2.12. *For $d_1 \mid p-1$ and $\boldsymbol{v}\in\mathbb{N}^m$ fixed, let us assume that for some integer $r_{\ell,\boldsymbol{v},d_1} \geqslant v_\ell(d_1^2)$,*

$$r \mapsto C_{h,p}^{(2)}(a,\boldsymbol{v},d_1,\ell^r) \quad \begin{cases} \text{vanishes if} & v_\ell(d_1^2) \leqslant r \leqslant r_{\ell,\boldsymbol{v},d_1}, \\ \text{stabilizes as} & r > r_{\ell,\boldsymbol{v},d_1}, \end{cases} \tag{32}$$

$$C_{h,p}^{(2)}(a,\boldsymbol{v},d_1,\ell^r) \quad \begin{cases} \text{depends only on} & v_\ell(a), \\ \text{vanishes if} & v_\ell(a) < r_{\ell,\boldsymbol{v},d_1}. \end{cases} \tag{33}$$

Then, the local factor at ℓ is

$$P_{h,p}(\ell,\boldsymbol{v},d_1) = C_{h,p}^{(3)}(\boldsymbol{v},d_1,\ell) + \delta_{\ell\leqslant z}L_{h,p}(\boldsymbol{v},d_1,\ell,r_{\ell,\boldsymbol{v},d_1}),$$

where for any integers $r \geqslant 1$ and $v, w \geqslant 0$ (in (35)),

$$L_{h,p}(\boldsymbol{v}, d_1, \ell, r) := \delta_{v_\ell(p-1)\geqslant \frac{r}{2}} \lim_{R\to\infty} \sum_{w=r}^{R} C_{h,p}^{(2)}(\ell^w, \boldsymbol{v}, d_1, \ell^R) g_p(w, v_\ell(d_1), \ell^R), \tag{34}$$

$$g_p(w, v, \ell^R) := \frac{\left|\left\{ g \in M_2(\mathbb{Z}/\ell^R) : \begin{smallmatrix} \det(g)=p \\ v_\ell(p+1-\mathrm{tr}(g))=w \\ g\equiv 1 \pmod{\ell^v} \\ g\not\equiv 1 \pmod{\ell^{v+1}} \end{smallmatrix} \right\}\right|}{\ell^{3R}(1-1/\ell^2)} - \frac{1-1/\ell}{\ell^w}. \tag{35}$$

Remark 2.13. Concerning (33), note that it is natural that $C_{h,p}(a, d_1, \ell^r)$ in (26) depends only mildly on a.

Example 2.14. In the case $h \in \{s, c\}$, we will have $m = 3$, $\boldsymbol{v} = (u, k, i) \in \mathbb{N}^3$ for $i \in \{0, 1\}$, $u \mid d_1$, $k \mid d_1^2/u$, and

$$C_{h,p}^{(2)}(a, \boldsymbol{v}, d_1, \ell^r) = \begin{cases} (d_1^2, \ell^r) & : i = 0 \\ (d_1^2, \ell^r) c_k(\ell^{v_\ell(a/d_1^2)}) \delta_{r\geqslant v_\ell(d_1^2 k)} & : i = 1 \end{cases} \tag{36}$$

for c_k the Ramanujan sum modulo k (see Sections 5–6). In Proposition 5.4, we will see that this implies that (32)–(33) hold with $r_{\ell,\boldsymbol{v},d_1} = v_\ell(d_1^2) + \delta_{i=1} \max(0, v_\ell(k) - 1)$.

2.5.1. *Computation of the local densities.* Using the computations of Gekeler [Gek03] and David–Koukoulopoulos–Smith [DKS17], explicit and asymptotic expressions for the densities $g_p(w, v, \ell^r)$ can be given. For the sake of brevity, we give only the latter; for the former, it suffices to combine the proof of the proposition below with [Gek03, Theorem 4.4].

Proposition 2.15. *For R large enough with respect to ℓ, v and w, we have, assuming $\ell^v \mid p-1$ and $w \geqslant 2v$,*

$$g_p(w, v, \ell^R) = \frac{1}{\ell^w}\left(1-\frac{1}{\ell}\right)\left(\frac{1}{\ell^v}\left(1+O\left(\frac{1}{\ell}\right)\right)-1\right).$$

Moreover, if $\ell \neq p$, $\lim_{R\to\infty} \sum_{w=0}^{R} g_p(w, 0, \ell^R) = -\frac{\delta_{\ell\mid p-1}}{\ell(\ell^2-1)}$.

2.6. **Conclusion.**

Definition 2.16. For $d_1 \mid p-1$, $\boldsymbol{v} \in \mathbb{N}^m$, $r \geqslant 1$ and ℓ prime, we let

$$L'_{h,p}(\boldsymbol{v}, d_1, \ell, r) := \delta_{v_\ell((p-1)^2)\geqslant r}\left(1-\frac{1}{\ell}\right) \lim_{R\to\infty} \sum_{w=r}^{R} \frac{C_{h,p}^{(2)}(\ell^w, \boldsymbol{v}, d_1, \ell^R)}{\ell^w},$$

$$E_{h,p}^{(T)}(z, \boldsymbol{v}, d_1) := \sum_{\ell > z} \left| \frac{L_{h,p}(\boldsymbol{v}, d_1, \ell, r_{\ell,\boldsymbol{v},d_1})}{C_{h,p}^{(3)}(\boldsymbol{v}, d_1, \ell)} \right|.$$

Combining the previous sections together, we obtain:

Theorem 2.17. *Let $\varepsilon > 0$, $\alpha \geqslant 1$, and $Z \geqslant \exp(\sqrt{\log(4p)})$. If (30), (32), (33) and*

$$E_{h,p}^{(T)}(z, \boldsymbol{v}, d_1) \leqslant 1 \qquad \text{whenever} \qquad C_{h,p}^{(1)}(\boldsymbol{v}, d_1) \neq 0 \tag{37}$$

hold, then

$$\begin{aligned} h(\mathcal{E}ll(p)) \quad = \quad & \sum_{\substack{d_1 \mid p-1 \\ \boldsymbol{v} \in \mathbb{N}^m}} \frac{C_{h,p}^{(1)}(\boldsymbol{v}, d_1)}{d_1^2} \prod_{\ell} \left[C_{h,p}^{(3)}(\boldsymbol{v}, d_1, \ell) + L_{h,p}(\boldsymbol{v}, d_1, \ell, r_{\ell,\boldsymbol{v},d_1}) \right] \\ & \left(1 + O\left(E_{h,p}^{(T)}(z, \boldsymbol{v}, d_1)\right)\right) \\ & + O\left(Z^{\frac{2}{\alpha}+\varepsilon} E_{h,p}^{(B)} + \frac{E_{h,p}^{(G)}}{(\log Z)^{\alpha-\varepsilon}} + E_{h,p}^{(P)}\left((\log Z)^{8\alpha^2}\right) \right) \end{aligned}$$

where $L_{h,p}$, as defined in (34), satisfies

$$L_{h,p}(\boldsymbol{v}, d_1, \ell, r_{\ell,\boldsymbol{v},d_1}) \quad = \quad L'_{h,p}(\boldsymbol{v}, d_1, \ell, r_{\ell,\boldsymbol{v},d_1}) \left(\frac{1}{\ell^{v_\ell(d_1)}} \left(1 + O\left(\frac{1}{\ell}\right)\right) - 1 \right).$$

The implied constants depend only on ε and α.

Remark 2.18. The error terms account for (B)ad conductors and (G)ood conductors (in Proposition 2.5), distribution of h in arithmetic (P)rogressions (in Proposition 2.10), and completion of the (T)runcated products (in Theorem 2.17).

Index of notations. For convenience, we provide a index of the most important quantities defined above.

Notation	Reference/page	Description
$h(d_1, d_2)$	p. 5	$h(\mathbb{Z}/d_1 \times \mathbb{Z}/d_1 d_2)$
$P(E(\mathbb{F}_p) \cong H)$	(8) p. 5	
$p_\pm$	p. 6	$p + 1 \pm 2\sqrt{p}$
f_ℓ and f_∞	(9) p. 6 and (10) p. 6	Local factors
$D_{a,p}$	(11) p. 6	Discriminant
$w_{h,p}(d_1, d_2)$	(14) p. 7	Weights
$\delta_n(d_1, d_2, p)$	(18) p. 8	Local factors
$z = (\log Z)^{8\alpha^2}$	(20) p. 8	Euler product truncation
$E_{h,p}^{(B)}$ and $E_{h,p}^{(G)}$	(22) p. 8 and (21) p. 8	Errors in truncating the Euler product
$\Delta_q(a, d_1, p)$	Proposition 2.7 p. 8	$\delta_q(d_1, d_2, p) = \Delta_q(d_1^2 d_2, d_1, p)$
$\mathcal{H}(q)$	(23) p. 9	Classes $a \in \mathbb{Z}/q$ verifying conditions on $D_{a,p}$
$\overline{w}_{h,p}(d_1, a, q)$	(24) p. 9	$w(d_1, \cdot)$ in short intervals and arithmetic progressions (SIAP)

Notation	Reference/page	Description
$d_p y$	(25) p. 9	$ydy/\sqrt{4p-y^2}$
$C_{h,p}(a,d_1,q)$	(26) p. 9	Main term for $h(d_1,\cdot)$ in SIAP
$E_{h,p}(y,d_1,a,q)$	(26) p. 9	Error for $h(d_1,\cdot)$ in SIAP
$Q(d_1,z)$	(28) p. 9	Admissible moduli
$E_{h,p}^{(P)}(z)$	(29) p. 9	Total error for h in SIAP
$C_{h,p}^{(1)}(\boldsymbol{v},d_1)$, $C_{h,p}^{(3)}(\boldsymbol{v},d_1,\ell)$	(30) p. 10	Decomposition of $C_{h,p}$
$C_{h,p}^{(2)}(a,\boldsymbol{v},d_1,q)$	(30) p. 10	Multiplicative part of $C_{h,p}$
$E'_{h,p}(y,\boldsymbol{v},d_1,a,q)$	(30) p. 10	Decomposition of $E_{h,p}$
$P_{h,p}(\ell,\boldsymbol{v},d_1)$	(31) p. 10	Local factors in the main term
$r_{\ell,\boldsymbol{v},d_1}$	Proposition 2.12 p. 10	Threshold
$L_{h,p}(\boldsymbol{v},d_1,\ell,r)$	(34) p. 11	Weighted sum of matrix densities
$g_p(w,v,\ell^R)$	(35) p. 11	Matrix density
$L'_{h,p}(\boldsymbol{v},d_1,\ell,r)$	Definition 2.16 p. 11	Factor of $L_{h,p}$
$E_{h,p}^{(T)}(z,\boldsymbol{v},d_1)$	Definition 2.16 p. 11	Truncation error

3. Divisor function in arithmetic progressions and short intervals

To apply Theorem 2.17 to $h \in \{s,c\}$, in order to show that (26) holds, we will need to understand

$$\sum_{\substack{A<n\leqslant B\\ n\equiv a \pmod q}} \tau(n), \tag{38}$$

where $1 \leqslant q \leqslant A$, $a \in \mathbb{Z}/q$ and $[A,B]$ is a short interval (i.e. of length $o(A)$).

The sum (38) should be asymptotically equal (under admissible ranges) to $D(B,a,q) - D(A,a,q)$, where

$$D(X,a,q) := \frac{1}{q}\sum_{k|q}\frac{c_k(a)}{k} X\left(\log\left(\frac{X}{k^2}\right) + 2\gamma - 1\right),$$

with $c_k(a)$ the Ramanujan sum modulo k given by

$$c_k(a) = \sum_{n\in(\mathbb{Z}/k)^\times} e(an/k) = \sum_{f|(k,a)} f\mu(k/f). \tag{39}$$

DEFINITION 3.1. For $1 \leqslant q \leqslant A < B$ and $a \in \mathbb{Z}/q$, we let

$$\begin{aligned}\Delta(B,a,q) &:= \sum_{\substack{n\leqslant B\\ n\equiv a \pmod q}} \tau(n) - D(B,a,q),\\ \Delta(B) &:= \Delta(B,0,1),\\ \Delta(A,B,a,q) &:= \Delta(B,a,q)-\Delta(A,a,q)\\ \Delta(A,B) &:= \Delta(A,B,0,1).\end{aligned}$$

For $C>0$, we will also use the abbreviation $\Delta(A\mp C,a,q)$ for $\Delta(A-C,A+C,a,q)$.

Combining ideas from [Blo07] (for the arithmetic progression aspect) and [IZ14] (for the short interval aspect), we will prove the following mean square result on the divisor function simultaneously in arithmetic progressions and short intervals:

Theorem 3.2. *Let $1\leqslant A<B$, $1\leqslant q\leqslant \sqrt{A}$, and $\varepsilon>0$. We have*

$$\begin{aligned}&\frac{1}{q}\sum_{a\in\mathbb{Z}/q}|\Delta(A,B,a,q)|^2\\ &\qquad\ll (qB)^{\varepsilon}\begin{cases}\frac{(B-A)^{1/2}}{q}\left(\frac{B^3}{A}\right)^{1/4} & : B-A\leqslant\sqrt{B},\\ \frac{(B-A)^{4/3}}{q^{4/3}}\left(\frac{B}{A}\right)^{1/3} & : \sqrt{B}\leqslant B-A\leqslant\sqrt{AB}.\end{cases}\end{aligned}$$

Remark 3.3. The range we will need is $B\ll A\ll B$, $B-A\leqslant\sqrt{B}$ and $q\leqslant A^{1/2}$. The first part of theorem then gives that $|\Delta(A,B,a,q)|^2$ is at most $(qB)^{\varepsilon}\sqrt{A(B-A)}/q$ on average over a.

3.1. **Some existing results.** Up to smoothing the sum, the Voronoi summation formula (see [IK04, Section 4]) gives an explicit expression for $\Delta(B,a,q)$, from which one readily gets that if $(a,q)=1$, then for any $\varepsilon>0$

$$\Delta(B,a,q)\ll (qB)^{\varepsilon}(q^{1/2}+B^{1/3}), \tag{40}$$

and Pongsriiam–Vaughan [PV15] showed that this also holds when $(a,q)>1$. We also mention their result [PV18] on average over q and a, improving on Motohashi (here in a weakened form):

$$\sum_{q\leqslant Q}\sum_{a\in(\mathbb{Z}/q)^\times}|\Delta(B,a,q)|^2\ll B^{\varepsilon}\left(QB+B^{5/3}+Q^{1+\theta}B^{1-\theta}\right)$$

for $1\leqslant Q<B$ and $\theta\in(0,1)$.

Improving significantly on previous results of Banks–Heath-Brown–Shparlinski [BHBS05], Blomer [Blo07] showed that for any $\varepsilon>0$

$$\sum_{a\in\mathbb{Z}/q}|\Delta(B,a,q)|^2\ll B^{1+\varepsilon}, \tag{41}$$

which gives a better result on average than (40) if $B\ll_{\varepsilon} q^{2-\varepsilon}$.

3.1.1. *Short intervals.* Let us assume that $q = 1$ and let $\varepsilon > 0$. Using (40), we get $|\Delta(A, B)| \ll B^{1/3+\varepsilon}$, which can be nontrivial only when $B - A \gg B^{1/3}$. The exponent can be reduced to $131/416 + \varepsilon$ using the latest result of Huxley on $\Delta(B)$, and conjecturally to $1/4 + \varepsilon$, for any $\varepsilon > 0$.

Exploiting the short interval aspect, Ivić and Zhai [IZ14, Section 3] recently obtained that

$$|\Delta(A, B)| \ll A^{\nu_1}(B - A)^{\nu_2} \text{ if } 1 \ll B - A \ll A^{\nu_3} \tag{42}$$

when $(\nu_1, \nu_2, \nu_3) = (1/4 + \varepsilon, 1/4, 3/5)$ or $(2/9 + \varepsilon, 1/3, 2/3)$, for any $\varepsilon > 0$.

A conjecture of Jutila (see [Jut84], [IZ14, Conjecture 3]) asserts that (42) holds with $(\nu_1, \nu_2, \nu_3) = (\delta, 1/2, 1/2 - \delta)$ if $\delta \in (0, 1/4)$ and $B - A \geqslant A^{\delta}$. This is supported by average results over A for certain ranges: for example

$$\int_T^{T+H} |\Delta(A, A + U)|^2 dA \ll T^{\varepsilon}(HU + T) \tag{43}$$

if $1 \leqslant U \leqslant \sqrt{T}/2 \ll H \leqslant T$ (see [Jut84], [Jut89, Theorem 2]).

Remark 3.4. With an additional average over A when $[A, B] = [A, A + U]$ with U fixed, Theorem 3.2 could probably be improved as in Jutila's results (see (43) below). We also mention a recent preprint of Kerr and Shparlinski [KS18] combining Blomer's technique with bounds on bilinear sums of Kloosterman sums.

3.2. **Proof of Theorem 3.2.** We start by a truncated Voronoi formula in arithmetic progressions:

Lemma 3.5. *For any $\varepsilon > 0$, $X \geqslant 1$, $q \geqslant 1$, $a \in \mathbb{Z}/q$ and $N \geqslant 1$ such that $1/X \leqslant N/q^2 \leqslant X$, we have*

$$\Delta(X, a, q) = \frac{1}{q} \sum_{k|q} \sum_{W=Y,K} F_W(X, a, k, N) + O\left((Xq)^{\varepsilon}\left(\left(\frac{X}{N}\right)^{1/2} + 1\right)\right),$$

and

$$\sum_{a \in \mathbb{Z}/q} \left| \Delta(X, a, q) - \frac{1}{q} \sum_{k|q} \sum_{W=Y,K} F_W(X, a, k, N) \right|^2 \ll (Xq)^{\varepsilon} \frac{qX}{N},$$

where

$$\begin{aligned} F_W(X, a, k, N) &:= \frac{C_W}{k} \sum_{n \leqslant N} \tau(n) \operatorname{Kl}_k(\delta_W a, n) \int_0^X W_0\left(\frac{4\pi}{k}\sqrt{nx}\right) dx \\ &\ll (Xq)^{\varepsilon}\left(\frac{X}{N}\right)^{1/2}, \\ (C_W, \delta_W) &= \begin{cases} (-2\pi, 1) & W = Y \\ (4, -1) & W = K, \text{ and} \end{cases} \\ \operatorname{Kl}_k(c, d) &= \sum_{x \in (\mathbb{Z}/k)^{\times}} e\left(\frac{cx + d\overline{x}}{k}\right) \qquad (c, d \in \mathbb{Z}/k), \end{aligned}$$

for $W \in \{Y, K\}$, with Y (resp. K) the Bessel (resp. modified Bessel) functions of the second kind.

Proof. By Voronoi's summation formula [IK04, (4.49)], if $g \in C_c^\infty(\mathbb{R}_+)$ and $(b,q)=1$, we have

$$\begin{aligned}&\sum_{n\geqslant 1}\tau(n)e(bn/q)g(n) \qquad (44)\\ &=\frac{1}{q}\int_0^\infty\left(\log\left(\frac{x}{q^2}\right)+2\gamma\right)g(x)dx\\ &+\frac{1}{q}\sum_{W=Y,K}C_W\sum_{n\geqslant 1}\tau(n)e(-\delta_W\bar{b}n/k)\int_0^\infty W_0\left(\frac{4\pi}{q}\sqrt{nx}\right)g(x)dx.\end{aligned}$$

By the orthogonality relations for $\mathbb{Z}/q$,

$$\begin{aligned}\sum_{\substack{n\geqslant 1\\ n\equiv a \pmod q}}\tau(n)g(n) &= \frac{1}{q}\sum_{b\in\mathbb{Z}/q}e(-ab/q)\sum_{n\geqslant 1}\tau(n)e(bn/q)g(n)\\ &= \frac{1}{q}\sum_{k|q}\sum_{b\in(\mathbb{Z}/k)^\times}e(-ab/k)\sum_{n\geqslant 1}\tau(n)e(bn/k)g(n).\end{aligned}$$

Using (44), this is equal to

$$\begin{aligned}&\frac{1}{q}\sum_{k|q}\frac{c_k(a)}{q}\int_0^\infty\left(\log\left(\frac{x}{q^2}\right)+2\gamma\right)g(x)dx\\ &+\frac{1}{q}\sum_{k|q}\sum_{W=Y,K}\frac{C_W}{k}\sum_{n\geqslant 1}\mathrm{Kl}_k(\delta_W a,n)\tau(n)\int_0^\infty W_0\left(\frac{4\pi}{k}\sqrt{nx}\right)g(x)dx.\end{aligned}$$

For $0\leqslant X_1\ll X$, let $g=g_{X,X_1}$ be supported on $[0,X+X_1]$, identically equal to 1 on $[0,X]$, and such that $||g^{(i)}||_\infty\ll 1/X_1^i$ for all $i\geqslant 0$, where $g^{(i)}$ is the ith derivative. Then

$$\Delta(X,a,q) = \frac{1}{q}\sum_{k|q}\sum_{W=Y,K}\tilde{F}_W(g,a,k)+O\Big((Xq)^\varepsilon\rho(X,X_1,a,q)\Big),$$

where $\rho(X,X_1,a,q)=|\{n\in[X,X+X_1]\cap\mathbb{N}: n\equiv a \pmod q\}|$, and for $W\in\{Y,K\}$,

$$\tilde{F}_W(g,a,k) := \frac{C_W}{k}\sum_{n\geqslant 1}\tau(n)\,\mathrm{Kl}_k(\delta_W a,n)\int_0^\infty W_0(4\pi\sqrt{nx}/k)g(x)dx.$$

For any $j\geqslant 1$, we have from the decay of g and W_0 that (see [Blo07, (9-10)])

$$\begin{aligned}\left|\int_0^\infty W_0\left(4\pi\sqrt{nx}/k\right)g(x)dx\right| &\ll \frac{1}{(\sqrt{n}/k)^{j+1/2}}\int_0^\infty x^{j/2-1/4}|g^{(j)}(x)|dx\\ &\ll \frac{k^{j+1/2}}{n^{j/2+1/4}X_1^{j-1}}X^{j/2-1/4}.\end{aligned}$$

Thus, for any integer $j \geqslant 2$ and $\varepsilon > 0$, using the bound $|\operatorname{Kl}_k(\delta_W a, n, k)| \leqslant \tau(k)(a, n, k)^{1/2} k^{1/2}$, we have

$$\begin{aligned}\tilde{F}_W(g, a, k) &= \frac{C_W}{k} \sum_{n \leqslant N} \tau(n) \operatorname{Kl}_k(\delta_W a, n) \int_0^X W_0\left(4\pi\sqrt{nx}/k\right) dx \\ &\quad + O\left(\frac{k^{j+1/2+\varepsilon} X^{j/2-1/4}}{X_1^{j-1} N^{j/2-3/4-\varepsilon}}\right).\end{aligned}$$

Therefore,

$$\begin{aligned}\Delta(X, a, q) &= \frac{1}{q} \sum_{k \mid q} \sum_{W = Y, K} F_W(X, a, k, N) \\ &\quad + O\left((Xq)^{\varepsilon} \rho(X, X_1, a, q) + \frac{q^{j+1/2+\varepsilon} X^{j/2-1/4}}{X_1^{j-1} N^{j/2-3/4-\varepsilon}}\right).\end{aligned}$$

The results follows from taking j large enough and choosing

$$X_1 = \left\lfloor q \left(\frac{X}{N}\right)^{1/2} \left(\frac{qN^{1/2}}{X^{1/2}}\right)^{\frac{3}{2j}} \right\rfloor,$$

which is admissible under the conditions on N. □

It follows from Lemma 3.5 and the Cauchy–Schwarz inequality that for

$$1 + q^2/A \leqslant N \leqslant q^2 B, \tag{45}$$

we have

$$\sum_{a \in \mathbb{Z}/q} |\Delta(A, B, a, q)|^2 \ll \frac{1}{q^2} \sum_{k \mid q} \sum_{W = Y, K} \sum_{a \in \mathbb{Z}/q} \left|[F_W(X, a, k, N)]_A^B\right|^2 + \frac{(qB)^{1+\varepsilon}}{N}. \tag{46}$$

Then, we open the square and exploit cancellation among Kloosterman sums:

Lemma 3.6. *For $W \in \{Y, K\}$, $k \mid q$, any $Z \in C([A, B], \mathbb{R}_{>0})$ and $N \geqslant 1$, we have*

$$\begin{aligned}\sum_{a \in \mathbb{Z}/q} \left|[F_W(X, a, k, N)]_A^B\right|^2 &\ll \frac{q}{k^2} \int_A^B Z(v)^2 dv \\ &\quad \sum_{f \mid k} f \sum_{\substack{n, n' \leqslant N \\ n \equiv n' \pmod f}} \tau(n)\tau(n') |S_{W,Z}(n, n', k)|,\end{aligned}$$

where $$S_{W,Z}(n, n', k) := \int_A^B \frac{1}{Z(v)^2} W_0\left(\frac{4\pi}{k}\sqrt{nv}\right) W_0\left(\frac{4\pi}{k}\sqrt{n'v}\right) dv.$$

Proof. By Cauchy–Schwarz, the square $\left|[F_W(X, a, k, N)]_A^B\right|^2$ is

$$\ll \frac{1}{k^2} \left(\int_A^B Z(v)^2 dv\right) \int_A^B \left| \sum_{n \leqslant N} \frac{\tau(n) \operatorname{Kl}_k(\delta_W a, n)}{Z(v)} W_0\left(\frac{4\pi}{k}\sqrt{nv}\right) \right|^2 dv.$$

The second integral is

$$\sum_{n,n'\leqslant N} \tau(n)\tau(n')\,\mathrm{Kl}_k(\delta_W a,n)\,\mathrm{Kl}_k(\delta_W a,n') \int_A^B \frac{1}{Z(v)^2} W_0\left(\frac{4\pi}{k}\sqrt{nv}\right) W_0\left(\frac{4\pi}{k}\sqrt{n'v}\right) dv.$$

By orthogonality and the alternative expression (39) for the Ramanujan sum,

$$\begin{aligned} &\sum_{a\in\mathbb{Z}/q} \mathrm{Kl}_k(\delta_W a,n)\,\mathrm{Kl}_k(\delta_W a,n') \\ =\ & \sum_{x_1,x_2\in(\mathbb{Z}/k)^\times} e\left((n\overline{x}_1+n'\overline{x}_2)/k\right) \sum_{a\in\mathbb{Z}/q} e\left(a\delta_W(x_1+x_2)/k\right) \\ =\ & q\sum_{x\in(\mathbb{Z}/k)^\times} e\left(x(n-n')/k\right) = qc_k(n-n') = q\sum_{f\mid k} f\delta_{f\mid n-n'}\mu(k/f). \end{aligned}$$

□

Finally, we compute the right-hand side of the expression in Lemma 3.6 by approximating the Bessel functions.

Lemma 3.7. *If $q\ll\sqrt{A}$ and $B-A\ll\sqrt{AB}$, then, for $W\in\{Y,K\}$, $k\mid q$, and $N\geqslant 1$,*

$$\sum_{a\in\mathbb{Z}/q}\left|[F_W(X,a,k,N)]_A^B\right|^2 \ll (kN)^\varepsilon \frac{q(B-A)}{\sqrt{A}}\left[(B-A)\sqrt{N}+N\sqrt{B}\right].$$

Proof. We have the well-known asymptotic expansions

$$\begin{aligned} Y_0(x) &= \left(\frac{2}{\pi x}\right)^{1/2}\sin(x-\pi/4)\left(1+O\left(\frac{1}{x}\right)\right), \\ K_0(x) &= \left(\frac{\pi}{2x}\right)^{1/2}\frac{1}{e^x}\left(1+O\left(\frac{1}{x}\right)\right), \end{aligned}$$

so that $S_{Y,Z}(n,n',k)$ is equal to

$$\frac{k}{2(nn')^{1/4}}\int_A^B\left(\cos(4\pi\sqrt{v}(\sqrt{n}-\sqrt{n'})/k)-\sin(4\pi\sqrt{v}(\sqrt{n}+\sqrt{n'})/k)\right)dv + O\left(\frac{(B-A)k^2}{\sqrt{A}(nn')^{1/4}}\left(\frac{1}{\min(n,n')^{1/2}}+\frac{k}{(nn')^{1/2}\sqrt{A}}\right)\right),$$

taking $Z(v)=v^{-1/4}$. Using that $\int\cos(\lambda\sqrt{x})dx = \frac{2\sqrt{x}\sin(\lambda\sqrt{x})}{\lambda}+\frac{2\cos(\lambda\sqrt{x})}{\lambda^2}$ (and similarly for sin), we get

$$S_{Y,Z}(n,n',k)\ll\begin{cases}\frac{k(B-A)}{\sqrt{n}}\left(1+\frac{k}{\sqrt{A}}\left(\frac{1}{\sqrt{n}}+\frac{k}{n\sqrt{A}}\right)\right), & :n=n'\\ \frac{k^2}{(nn')^{1/4}}\left(\frac{\sqrt{B}}{\sqrt{n'}-\sqrt{n}}+\frac{B-A}{\sqrt{A}}\left(\frac{1}{\sqrt{n}}+\frac{k}{(nn')^{1/2}\sqrt{A}}\right)\right) & :n<n'.\end{cases}$$

If $q\ll\sqrt{A}$, this is

$$\ll\begin{cases}\frac{k(B-A)}{\sqrt{n}}, & :n=n'\\ \frac{k^2}{(nn')^{1/4}}\left(\frac{\sqrt{B}}{\sqrt{n'}-\sqrt{n}}+\frac{B-A}{\sqrt{nA}}\right) & :n<n',\end{cases}$$

and

$$\sum_{a\in\mathbb{Z}/q}\left|[F_Y(X,a,k,N)]_A^B\right|^2 \ll \frac{q}{k}\frac{B-A}{\sqrt{A}}\sum_{f|k} f\left[(B-A)\sum_{n\leqslant N}\frac{\tau(n)^2}{n^{1/2}}\right.$$
$$\left. + \sum_{\substack{n,n'\leqslant N\\ n\equiv n' \pmod f\\ n\neq n'}}\frac{\tau(n)\tau(n')k}{(nn')^{1/4}}\left(\frac{\sqrt{B}}{\sqrt{n'}-\sqrt{n}}+\frac{B-A}{\sqrt{A}\min(n,n')^{1/2}}\right)\right]$$
$$\ll (kN)^{\varepsilon}\frac{q(B-A)}{\sqrt{A}}\left[(B-A)\sqrt{N}+N\left(\sqrt{B}+\frac{B-A}{\sqrt{A}}\right)\right].$$

If moreover $B-A\ll\sqrt{AB}$, this is

$$\ll (kN)^{\varepsilon}\frac{q(B-A)}{\sqrt{A}}\left[(B-A)\sqrt{N}+N\sqrt{B}\right].$$

Similarly, $S_{K,Z}(n,n',k)$ is equal to, taking $Z(v)=v^{-1/4}$ as well,

$$\frac{k}{4(nn')^{1/4}}\int_A^B e^{-4\pi(\sqrt{n}+\sqrt{n'})\sqrt{v}/k}\left(1+O\left(\frac{k}{\sqrt{v}\min(n,n')^{1/2}}+\frac{k^2}{v\sqrt{nn'}}\right)\right)dv$$
$$\ll \frac{k}{(nn')^{1/4}}\int_A^B e^{-4\pi(\sqrt{n}+\sqrt{n'})\sqrt{v}/k}dv + \frac{k^2\sqrt{B}}{(nn')^{1/4}\min(n,n')^{1/2}\sqrt{A}}+\frac{k^3(B-A)}{A(nn')^{3/4}}.$$

If $q\leqslant\sqrt{A}$, then the first summand is

$$\ll \frac{k^3(B-A)}{(nn')^{1/4}(n+n')A}.$$

In this case, by Lemma 3.6,

$$\sum_{a\in\mathbb{Z}/q}\left|[F_K(X,a,k,N)]_A^B\right|^2 \ll (kN)^{\varepsilon}\frac{q(B-A)}{\sqrt{A}}\left((B-A)\frac{\sqrt{N}k}{\sqrt{A}}+N\sqrt{B}\right).$$

□

Proof of Theorem 3.2. By (46) and Lemma 3.7, if $q\leqslant\sqrt{A}$ and $B-A\ll\sqrt{AB}$, then for any $N\geqslant 1$ satisfying (45),

$$\sum_{a\in\mathbb{Z}/q}|\Delta(A,B,a,q)|^2 \ll (qB)^{\varepsilon}\left(\frac{B-A}{q\sqrt{A}}\left[(B-A)\sqrt{N}+N\sqrt{B}\right]+\frac{qB}{N}\right).$$

If $B-A\leqslant\sqrt{B}$, then this is

$$\ll (qB)^{\varepsilon}\left(\frac{B-A}{q}\left(\frac{B}{A}\right)^{1/2}N+\frac{qB}{N}\right),$$

and we choose $N = \left\lfloor q\left(\frac{(BA)^{1/2}}{B-A}\right)^{1/2}\right\rfloor$, which satisfies (45). Similarly, if $B - A \geqslant \sqrt{B}$, we choose $N = \left\lfloor \left(\frac{q^4B^2A}{(B-A)^4}\right)^{1/3}\right\rfloor$. □

4. Proofs of the results from Section 2

Proof of Proposition 2.1. This follows immediately from the properties recalled in Section 1.3.1 along with the fact that $d_1 \mid p-1$ by the Weil pairing (see [Sil09, III.8]). □

Proof of Proposition 2.3. The Proposition is fully contained in [DKS17, Theorem 3.2], except (4) that we now check. If $p \nmid d_1^2d_2 - 1$, then the limit stabilizes at $r = 1$, and

$$\begin{aligned} f_p(d_1, d_2, p) &= \frac{|\{g \in M_2(\mathbb{F}_p) : \mathrm{tr}(g) = 1 - d_1^2d_2,\ \det(g) = 0\}|}{p^2-1} \\ &= \frac{2(1\cdot p + (p-1)\cdot 1) + (p-2)(p-1)}{p^2-1} \end{aligned}$$

If $p \mid d_1^2d_2 - 1$, then $d_1^2d_2 = p+1$, E is supersingular, the limit stabilizes at $r = 2$, and

$$\begin{aligned} f_p(d_1, d_2, p) &= \frac{|\{g \in M_2(\mathbb{Z}/p^2) : \mathrm{tr}(g) = \det(g) = 0\}|}{p^4-p^2} \\ &= \frac{\varphi(p^2)^2 + p(\varphi(p^2) + \varphi(p)p)}{p^4-p^2} = 1. \end{aligned}$$

□

4.1. Truncating the Euler product and proof of Proposition 2.5.

Proposition 4.1. *If $\alpha \geqslant 1$, $\varepsilon, \delta > 0$, and $\log Z \geqslant \sqrt{\log(4p)}$, then*

$$\begin{aligned} h(\mathcal{E}ll(p)) = W_{h,p} &\sum_{\substack{n\geqslant 1 \\ P^+(n)\leqslant (\log Z)^{8\alpha^2}}} \mu(n)^2 \mathbb{E}_{h,p}(\delta_n(d_1,d_2,p)) \\ &+ O\left(Z^{O(1)\delta + \frac{2}{\alpha}} \max_{c\geqslant 2} \sum_{\substack{d_1,d_2 \\ \mathrm{cond}(\chi_{d_1,d_2,p})=c}} \frac{|w_{h,p}(d_1,d_2)|}{d_1} \right) \\ &+ O\left(\frac{1}{(\log Z)^{\alpha-\varepsilon}} \sum_{d_1,d_2} |w_{h,p}(d_1,d_2)| \right). \end{aligned}$$

The implied constants depend only on α, δ and ε.

Proof. This is similar to [DKS17, pp. 37–38], but we spell out the argument because we need different expressions for the errors.

Let $z = (\log Z)^{8\alpha^2}$. Using Proposition 2.3, we have

$$\begin{aligned}\log \prod_{\ell>z}(1+\delta_\ell(d_1,d_2,p)) &= \sum_{\ell>z}\delta_\ell(d_1,d_2,p) + O\left(\frac{1}{z\log z}\right)\\ &= \sum_{\substack{\ell>z\\ \ell\nmid D_{d_1^2d_2,p}/d_1^2}}\frac{\chi_{d_1,d_2,p}(\ell)}{\ell} + \sum_{\substack{\ell>z\\ \ell\mid D_{d_1^2d_2,p}/d_1^2}}\delta_\ell(d_1,d_2,p) + O\left(\frac{1}{z\log z}\right)\\ &= \sum_{\ell>z}\frac{\chi_{d_1,d_2,p}(\ell)}{\ell} + O\left(\frac{1}{z\log z} + \frac{\omega(D_{d_1^2d_2,p}/d_1^2)}{z}\right).\end{aligned}$$

By [DKS17, Lemma 6.1] (a result going back to Elliott), there exists a set $\mathcal{E}_\alpha(Z) \subset [1,Z]\cap\mathbb{Z}$ of "bad conductors" of size $|\mathcal{E}_\alpha(Z)| \leqslant Z^{2/\alpha}$ such that if χ is a Dirichlet character modulo $d \leqslant \exp((\log Z)^2)$ with $\mathrm{cond}(\chi)\notin\mathcal{E}_\alpha(Z)$, then

$$\prod_{\ell>z}\left(1-\frac{\chi(\ell)}{\ell}\right)^{-1} = 1+O\left(\frac{1}{z^{\frac{1}{8\alpha}}}\right), \text{ so that } \sum_{\ell>z}\frac{\chi(\ell)}{\ell} \ll \frac{1}{z\log z}+\frac{1}{z^{\frac{1}{8\alpha}}}.$$

By hypothesis, $|D_{d_1^2d_2,p}/d_1^2| \leqslant 4p/d_1^2 \leqslant \exp((\log Z)^2)$. Thus, if $\mathrm{cond}(\chi_{d_1,d_2,p})\notin\mathcal{E}_\alpha(Z)$, then

$$\begin{aligned}\prod_{\ell}(1+\delta_\ell(d_1,d_2,p)) &= \prod_{\ell\leqslant z}(1+\delta_\ell(d_1,d_2,p))\\ &\quad + O\left(\frac{(\log z)^{O(1)}}{\prod_{\ell\leqslant z}\ell^{v_\ell(d_1)}}\left(\frac{1}{z^{\frac{1}{8\alpha}}}+\frac{\log p}{z\log_2 p}\right)\right)\end{aligned}$$

since, by Proposition 2.3,

$$\prod_{\ell\leqslant z}(1+\delta_\ell(d_1,d_2,p)) = \prod_{\ell\leqslant z}\frac{1}{\ell^{v_\ell(d_1)}}\prod_{\ell\leqslant z}\left(1+O\left(\frac{1}{\ell}\right)\right) \ll \frac{(\log z)^{O(1)}}{\prod_{\ell\leqslant z}\ell^{v_\ell(d_1)}}.$$

On the other hand, if $\mathrm{cond}(\chi_{d_1,d_2,p})\in\mathcal{E}_\alpha(Z)$, let us write

$$\prod_{\ell}(1+\delta_\ell(d_1,d_2,p)) = \prod_{\ell\leqslant z_1}(1+\delta_\ell(d_1,d_2,p))\prod_{\ell>z_1}(1+\delta_\ell(d_1,d_2,p)).$$

for $z_1 \geqslant \exp(Z^\delta) \geqslant \exp(\mathrm{cond}(\chi_{d_1,d_2,p})^\delta)$. As above, we get that this is

$$\prod_{\ell}(1+\delta_\ell(d_1,d_2,p)) \ll \frac{(\log z_1)^{O(1)}}{\prod_{\ell\leqslant z_1}\ell^{v_\ell(d_1)}}\exp\left(O(1)+\frac{\log p}{z_1\log_2 p}\right),$$

using that $\sum_{\ell>z_1}\frac{\chi_{d_1,d_2,p}(\ell)}{\ell} \ll_\delta 1$, with the implied constant depending only on δ.

If p is large enough, then $z_1 \geqslant p$ and we get by (13) that

$$\begin{aligned} h(\mathcal{E}ll(p)) &= \sum_{d_1,d_2} w_{h,p}(d_1,d_2) \prod_{\ell \leqslant z} (1+\delta_\ell(d_1,d_2,p)) \\ &\quad + O\left(Z^{O(1)\delta} \sum_{\substack{d_1,d_2 \\ \mathrm{cond}(\chi_{d_1,d_2,p}) \in \mathcal{E}_\alpha(Z)}} \frac{|w_{h,p}(d_1,d_2)|}{d_1} \right) \\ &\quad + O\left(\left(\frac{1}{z^{\frac{1}{8\alpha}-\varepsilon}} + \frac{\log p}{z^{1-\varepsilon}\log_2 p} \right) \sum_{d_1,d_2} |w_{h,p}(d_1,d_2)| \right), \end{aligned}$$

giving the desired expression. □

4.1.1. *Error terms in the truncation.*

Lemma 4.2. *The error terms in Proposition 4.1 are respectively bounded by* $Z^{\frac{2}{\alpha}+\varepsilon} E_{h,p}^{(B)}$ *and* $E_{h,p}^{(G)}/(\log Z)^{\alpha-\varepsilon}$, *where* $E_{h,p}^{(B)}$ *and* $E_{h,p}^{(G)}$ *are as defined in Proposition 2.5.*

Proof. The bound for characters of good conductors follows from Abel's summation formula (see Lemma 2.9).

For characters of bad conductors, we start by noting that if $\mathrm{cond}(\chi_{d_1,d_2,p}) = c$, then $|D_{d_1^2 d_2,p}| = d_1^2 c y^2$ for some $u \geqslant 1$, i.e.

$$\begin{aligned} (p+1-d_1^2 d_2)^2 + (d_1 u)^2 c &= 4p, \\ \text{i.e. } y^2 + (d_1 u)^2 c &= 4p \quad (y = p+1-d_1^2 d_2), \\ \text{i.e. } y^2 + x^2 c &= 4p \quad (d_1 \mid x). \end{aligned}$$

The number of solutions $x, y \in \mathbb{Z}$ to this last diophantine equation is $\ll 1$ (with no dependency on p). Indeed, the number of representations of $4p$ by nonequivalent primitive positive-definite binary quadratic forms, up to the $\leqslant 6$ automorphisms, is $\sum_{m \mid 4p} \left(\frac{-4c_p}{m}\right) \leqslant \tau(4p) \leqslant 6$. Hence, the number of possible values for u, d_1, d_2 is $\ll 1$, and

$$\begin{aligned} \sum_{\substack{d_1,d_2 \\ \mathrm{cond}(\chi_{d_1,d_2,p})=c}} \frac{|w_{h,p}(d_1,d_2)|}{d_1} &\ll \frac{1}{p} \sum_{u \geqslant 1} \sum_{d_1 \mid p-1} \sum_{\substack{\frac{p_-}{d_1^2} < d_2 \leqslant \frac{p_+}{d_1^2} \\ |D_{d_1^2 d_2,p}| = d_1^2 c u^2}} \sqrt{|D_{d_1^2 d_2,p}|} \frac{|h(d_1,d_2)|}{d_1} \\ &\ll \frac{1}{\sqrt{p}} \max_{p_- \leqslant d_1^2 d_2 \leqslant p_+} \frac{|h(d_1,d_2)|}{d_1}. \end{aligned}$$

□

4.1.2. *Proof of Proposition 2.5.* The latter now follows from Proposition 4.1 and Lemma 4.2. □

4.2. **Computation of the main term in (19) and proofs of Propositions 2.7 and 2.10.**

4.2.1. *Preliminary lemmas.*

Lemma 4.3. *For $\alpha > 0$, we have*

$$\frac{1}{p}\int_0^{2\sqrt{p}} y^\alpha d_p y \quad = \quad \frac{\sqrt{\pi}\Gamma(\alpha/2+2)2^\alpha}{2(\alpha+2)\Gamma((\alpha+3)/2)} p^{\frac{\alpha-1}{2}} \ll_\alpha p^{\frac{\alpha-1}{2}}.$$

Lemma 4.4. *For $q \geqslant 2$, we have $|\mathcal{H}(q)| \leqslant \sqrt{q\,\mathrm{rad}(q)}$. Moreover, if $\mathcal{H}(q)$ is not empty, then $\mathrm{rad}(q), q/\mathrm{rad}(q) \ll p$.*

Proof. We have $|\mathcal{H}(\ell^r)| \leqslant \ell \cdot |\{a \in \mathbb{Z}/\ell^{r-1} : a^2 \equiv 4p\}| \leqslant \ell \cdot \ell^{\lfloor \frac{r-1}{2} \rfloor}$ (see e.g. [KP17, Lemma 10] for the second inequality), so $|\mathcal{H}(q)| \leqslant \mathrm{rad}(q)\sqrt{q/\mathrm{rad}(q)}$. The last statement follows from the fact that $|D_{a,p}| \leqslant 4p$. □

4.2.2. *Proof of Proposition 2.7.* The expected value is given by

$$\sum_{\substack{q\geqslant 1\\ \mathrm{rad}(q)=n}} \sum_{d_1,d_2} \frac{w_{h,p}(d_1,d_2)}{W_{h,p}} \delta_q(d_1,d_2,p) \prod_{\ell\mid q} \delta_{v_\ell(D_{d_1^2 d_2,p})=v_\ell(q)-1}.$$

The limit over r defining $\delta_\ell(d_1,d_2,p)$ then stabilizes at $r = v_\ell(q)$ and the above is

$$= \sum_{\substack{q\geqslant 1\\ \mathrm{rad}(q)=n}} \sum_{d_1,d_2} \frac{w_{h,p}(d_1,d_2)}{W_{h,p}} \Delta_q(d_1^2 d_2, d_1, p) \prod_{\ell\mid q} \delta_{v_\ell(D_{d_1^2 d_2,p})=v_\ell(q)-1}$$

$$= \sum_{\substack{q\geqslant 1\\ \mathrm{rad}(q)=n}} \sum_{d_1\mid p-1} \sum_{a\in\mathcal{H}(q)} \Delta_q(a,d_1,p) \sum_{d_2} \frac{w_{h,p}(d_1,d_2)}{W_{h,p}} \delta_{d_1^2 d_2 \equiv a \pmod q}.$$

□

4.2.3. *Proof of Proposition 2.10.* First, we note that if there exists $a \in \mathcal{H}(q)$ with $(d_1^2, q) \mid a$, then $v_\ell(q) > v_\ell(d_1^2)$ for all $\ell \mid q$. Indeed, assume that $r = v_\ell(q) \leqslant v_\ell(d_1^2)$ and that a is as described. Since $D_{a,p} = (p-1)^2 + a(2(p+1)-a)$ and $v_\ell(a) \geqslant r$, we have $v_\ell(d_1^2) \leqslant v_\ell((p-1)^2) = r-1 < r \leqslant v_\ell(d_1^2)$, a contradiction. Thus, we can assume that $q \in Q(d_1, z)$.

By Lemma 2.9 and (26), $\overline{w}_{h,p}(d_1,a,q)$ is given by

$$\delta_{(d_1^2,q)\mid a}\left[\frac{1}{d_1^2}\frac{C_{h,p}(a,d_1,q)}{q} + O\left(\frac{1}{p}\int_0^{2\sqrt{p}} |E_{h,p}(y,d_1,a,q)| d_p y\right)\right].$$

To estimate the total error, we note that, by Proposition 2.3,

$$|\Delta_q(a,d_1,p)| \quad = \quad \prod_{\substack{\ell\mid q\\ \ell\nmid d_1}} O\left(\frac{1}{\ell}\right) \prod_{\ell\mid (q,d_1)} \left(1 + O\left(\frac{1}{\ell}\right)\right)$$

$$\ll \quad \frac{O(1)^{\omega(q)}}{\mathrm{rad}(q/(q,d_1))} = \frac{O(1)^{\omega(q)}}{\mathrm{rad}(q)},$$

since $v_\ell(q) > v_\ell(d_1^2)$.

Hence, by Proposition 2.7, the main term of (19) is as claimed. □

4.3. The main term as an Euler product and proofs of Propositions 2.11, 2.12 and 2.15.

4.3.1. *Proof of Proposition 2.11.* This is clear. □

4.3.2. *Proof of Proposition 2.12.* If (32) holds, then

$$\begin{aligned}
&\sum_{r>v_\ell(d_1^2)} \frac{1}{\ell^r} \sum_{\substack{a\in\mathcal{H}(\ell^r)\\ v_\ell(a)\geqslant v_\ell(d_1^2)}} C^{(2)}_{h,p}(a,\boldsymbol{v},d_1,\ell^r)\Delta_{\ell^r}(a,d_1,p)\\
&= \lim_{R\to\infty} \sum_{r_{\ell,\boldsymbol{v},d_1}<r\leqslant R} \frac{1}{\ell^r} \sum_{\substack{a\in\mathbb{Z}/\ell^r\\ v_\ell(D_{a,p})=r-1\\ v_\ell(a)\geqslant v_\ell(d_1^2)}} C^{(2)}_{h,p}(a,\boldsymbol{v},d_1,\ell^R)\Delta_{\ell^R}(a,d_1,p)\\
&= \lim_{R\to\infty} \frac{1}{\ell^R} \sum_{\substack{a\in\mathbb{Z}/\ell^R\\ r_{\ell,\boldsymbol{v},d_1}\leqslant v_\ell(D_{a,p})<R\\ v_\ell(a)\geqslant v_\ell(d_1^2)}} C^{(2)}_{h,p}(a,\boldsymbol{v},d_1,\ell^R)\Delta_{\ell^R}(a,d_1,p)\\
&= \lim_{R\to\infty} \frac{1}{\ell^R} \sum_{\substack{a\in\mathbb{Z}/\ell^R\\ v_\ell(D_{a,p})\geqslant r_{\ell,\boldsymbol{v},d_1}\\ v_\ell(a)\geqslant v_\ell(d_1^2)}} C^{(2)}_{h,p}(a,\boldsymbol{v},d_1,\ell^R)\Delta_{\ell^R}(a,d_1,p),
\end{aligned}$$

where the last equality follows from the fact that the number of solutions to $(p+1-a)^2\equiv 4p \pmod{\ell^R}$ in a is $\ll \ell^{R/2}$ (see also the proof of Lemma 4.4) and $\max_{a\in\mathbb{Z}/\ell^R}|C^{(2)}_{h,p}(a,\boldsymbol{v},d_1,\ell^R)\Delta_{\ell^R}(a,d_1,p)|$ is bounded independently from R.

If (33) holds, then this is

$$\delta_{v_\ell((p-1)^2)\geqslant r_{\ell,\boldsymbol{v},d_1}} \lim_{R\to\infty}\frac{1}{\ell^R} \sum_{\substack{a\in\mathbb{Z}/\ell^R\\ v_\ell(a)\geqslant r_{\ell,\boldsymbol{v},d_1}}} C^{(2)}_{h,p}(a,\boldsymbol{v},d_1,\ell^R)\Delta_{\ell^R}(a,d_1,p),$$

using that $D_{a,p}=(p-1)^2+a(2(p-1)-a)$. The limit is

$$\begin{aligned}
&\lim_{R\to\infty}\frac{1}{\ell^R}\sum_{w=r_{\ell,\boldsymbol{v},d_1}}^{R} C^{(2)}_{h,p}(\ell^w,\boldsymbol{v},d_1,\ell^R) \sum_{b\in(\mathbb{Z}/\ell^{R-w})^\times}\Delta_{\ell^R}(\ell^w b,d_1,p)\\
&= \lim_{R\to\infty}\frac{1}{\ell^{3R}}\sum_{w=r_{\ell,\boldsymbol{v},d_1}}^{R} C^{(2)}_{h,p}(\ell^w,\boldsymbol{v},d_1,\ell^R)\frac{\left|\left\{g\in M_2(\mathbb{Z}/\ell^R) : \begin{smallmatrix}\det(g)=p\\ v_\ell(p+1-\mathrm{tr}(g))=w\\ g\equiv 1 \pmod{\ell^v}\\ g\not\equiv 1 \pmod{\ell^{v+1}}\end{smallmatrix}\right\}\right|}{1-1/\ell^2}\\
&\qquad -\left(1-\frac{1}{\ell}\right)\lim_{R\to\infty}\sum_{w=r_{\ell,\boldsymbol{v},d_1}}^{R}\frac{C^{(2)}_{h,p}(\ell^w,\boldsymbol{v},d_1,\ell^R)}{\ell^w}.
\end{aligned}$$

□

4.3.3. *Proof of Proposition 2.15.*

(1) According to [DKS17, Lemma 3.2(d)], with $C(\cdots)$ defined in [DKS17, (3.2)] and $v = v_\ell(d_1)$, the matrix density $g_p(w, v, \ell^R)$ is given by

$$\begin{aligned} & \sum_{i=0}^{1} \sum_{a \in (\mathbb{Z}/\ell^{R-w})^\times} (-1)^i \frac{|C(p+1-a\ell^w, p, \ell^{v+i}, \ell^R)|}{\ell^{3R}(1-1/\ell^2)} - \frac{1-1/\ell}{\ell^w} \\ = \; & \frac{1}{\ell^w}\left(\frac{1}{\ell^{v_\ell(d_1)}}\left(1+O\left(\frac{1}{\ell}\right)\right) - 1 + \frac{1}{\ell}\right). \end{aligned}$$

(2) If $\ell \neq p$, then $\sum_{w=0}^{R} g_p(w, 0, \ell^R)$ is given by

$$\begin{aligned} & 1 - \frac{1}{\ell^{3R}(1-1/\ell^2)} \left| \left\{ g \in M_2(\mathbb{Z}/\ell^R) : \substack{\det(g)=p \\ g \equiv 1 \pmod{\ell}} \right\} \right| - \left(1 - \frac{1}{\ell^{R+1}}\right) \\ = \; & -\frac{\delta_{\ell \mid p-1}}{\ell(\ell^2-1)} + \frac{1}{\ell^{R+1}} \end{aligned}$$

by [LW07, Lemma 2] and Hensel's Lemma.

□

4.4. **Bounding the errors.** Finally, we give some general bounds on the errors appearing in Theorem 2.17 that will be useful later on.

4.4.1. *Bound on $E_{h,p}^{(G)}$.* Applying (30) with $q = 1$, the following is clear:

Lemma 4.5. *If (30) holds, then $E_{h,p}^{(G)}$ is*

$$\ll \sum_{\substack{d_1 \mid p-1 \\ \boldsymbol{v} \in \mathbb{N}^m}} |C_{h,p}^{(1)}(\boldsymbol{v}, d_1)| \left[\frac{\prod_\ell |C_{h,p}^{(3)}(\boldsymbol{v}, d_1, \ell)|}{d_1^2} + \frac{\int_0^{2\sqrt{p}} |E'_{h,p}(y, \boldsymbol{v}, d_1, 0, 1)| d_p y}{p} \right].$$

4.4.2. *Bound on $E_{h,p}^{(P)}$.*

Definition 4.6. For $\boldsymbol{\mu} \in [0,1]^3$, $\boldsymbol{\nu} \in [0,1]^5$, we let

$$\begin{aligned} G_{h,p}(\boldsymbol{\mu}) &:= \frac{1}{p^{\mu_1}} \sum_{\substack{d_1 \mid p-1 \\ d_1 \ll p^{\mu_2}}} \frac{1}{d_1^{\mu_3}} \max_{\frac{p_-}{d_1^2} < d_2 \leqslant \frac{p_+}{d_1^2}} |h(d_1, d_2)|, \\ F_{h,p}(z, \boldsymbol{\nu}) &:= \frac{1}{p^{\nu_1}} \sum_{\substack{d_1 \mid p-1 \\ d_1 \ll p^{\nu_2}}} \frac{1}{d_1^{\nu_3}} \sum_{\substack{n \geqslant 1 \\ P^+(n) \leqslant z}} \frac{\mu(n)^2 O(1)^{\omega(n)}}{n^{\nu_4}} \\ & \qquad \sum_{\substack{q \geqslant 1 \\ \mathrm{rad}(q) \mid n}} \frac{\max_{a \in \mathbb{Z}/qn} |C_{h,p}(a, d_1, qn)|}{q^{\nu_5} (qn, d_1^2)^{1/2}}, \end{aligned}$$

and for $\delta \in (0,1]$, $\boldsymbol{\beta} \in [0, 1/2] \times [0,1]^3$, we let

$$E_{h,p}^{(S)}(z, \delta) := \sum_{\substack{d_1 \mid p-1 \\ d_1 \ll p^{1/4}}} \frac{1}{p} \int_{d_1^2/2}^{2\sqrt{p}} \sum_{\substack{q \leqslant (2y/d_1^2)^\delta \\ q \in Q(d_1, z)}} \frac{O(1)^{\omega(q)}}{\mathrm{rad}(q)} \sum_{\substack{a \in \mathcal{H}(q) \\ (d_1^2, q) \mid a}} |E_{h,p}(y, d_1, a, q)| d_p y,$$

$$\begin{aligned} E_{h,p}^{(L1)}(\beta_4) &:= G_{h,p}\left(\frac{1}{2},\frac{1}{4},0\right)+G_{h,p}\left(\frac{1-\beta_4}{2},\frac{1}{2},2\beta_4\right), \\ E_{h,p}^{(L2)}(z,\boldsymbol{\beta},\delta) &:= \sum_{i=1}^{2} F_{h,p}\left(z,\frac{\beta_i\delta}{4},\frac{1}{4},2-\beta_i\delta,1-\delta_{i=2}\beta_2,\frac{1}{2}-\delta_{i=1}\beta_1\right) \\ &\quad +F_{h,p}\left(z,\frac{1-\beta_3}{2},\frac{1}{2},2\beta_3,1,\frac{1}{2}\right). \end{aligned}$$

Proposition 4.7. *For any $\varepsilon>0$, $\delta\in(0,1]$ and $\boldsymbol{\beta}\in[0,1/2]\times[0,1]^3$, we have*

$$E_{h,p}^{(P)}(z) \ll p^{\varepsilon}\left((\log z)^{O(1)}E_{h,p}^{(L1)}(\beta_4)+E_{h,p}^{(L2)}(z,\boldsymbol{\beta},\delta)\right)+E_{h,p}^{(S)}(z,\delta).$$

Remark 4.8. If $h(d_1,d_2)\ll d_1(d_1d_2)^{\varepsilon}$, then $E_{h,p}^{(L1)}(1/2)\ll 1/p^{1/4-\varepsilon}$. The most delicate contribution to understand will be $E_{h,p}^{(S)}$, which is a sum of the error terms for $h(d_1,\cdot)$ in short intervals and arithmetic progressions (both of admissible sizes).

Proof of Proposition 4.7. We split $E_{h,p}^{(P)}$ into three parts, according to the ranges of y,q and d_1:

(1) Small enough moduli and large enough intervals: $q\leqslant(2y/d_1^2)^{\delta}$;
(2) Large moduli and large enough intervals: $q>(2y/d_1^2)^{\delta}$ and $2y/d_1^2>1$;
(3) Small intervals: $y\leqslant d_1^2/2$.

The contribution of the range (1) gives $E_{h,p}^{(S)}$, since $d_1\ll y^{1/2}\ll p^{1/4}$. The contribution of the range (2) is

$$\ll \sum_{\substack{d_1\mid p-1\\ d_1\ll p^{1/4}}}\frac{1}{p}\int_{d_1^2/2}^{2\sqrt{p}}\sum_{\substack{q\geqslant(2y/d_1^2)^{\delta}\\ P^+(q)\leqslant z\\ \mathrm{rad}(q),\frac{q}{\mathrm{rad}(q)}\ll p}}\frac{c^{\omega(q)}}{\mathrm{rad}(q)}$$
$$\left[\max_{\frac{p+1-y}{d_1^2}<d_2\leqslant\frac{p+1+y}{d_1^2}}|h(d_1,d_2)|+\frac{y}{d_1^2q}\sum_{\substack{a\in\mathcal{H}(q)\\ (d_1^2,q)\mid a}}|C_{h,p}(a,d_1,q)|\right]d_py$$

for some constant $c\geqslant 1$, using Lemma 4.4. Since

$$\sum_{\substack{q\ll p^2\\ P^+(q)\leqslant z}}\frac{c^{\omega(q)}}{\mathrm{rad}(q)}\ll\sum_{\substack{n\geqslant 1\\ P^+(n)\leqslant z}}\frac{\mu(n)^2}{n}\sum_{\substack{q\ll p^2\\ \mathrm{rad}(q)=n}}1\ll(\log z)^{O(1)}\exp(\sqrt{\log p})^{O(1)},$$

the first summand yields the first part of $E_{h,p}^{(L1)}$. Then, we start noting that, by Lemma 4.4,

$$|\{a\in\mathcal{H}(q):(d_1^2,q)\mid a\}|\ll\left(\frac{q}{(d_1^2,q)}\,\mathrm{rad}(q)\right)^{1/2}.$$

Thus, the second summand gives a contribution of

$$\ll \sum_{\substack{d_1 \mid p-1 \\ d_1 \ll p^{1/4}}} \frac{1}{p} \int_{d_1^2/2}^{2\sqrt{p}} \frac{y}{d_1^2} \sum_{\substack{q \geqslant (2y/d_1^2)^{\delta} \\ P^+(q) \leqslant z \\ \mathrm{rad}(q), \frac{q}{\mathrm{rad}(q)} \ll p}} \frac{c^{\omega(q)} \max_{a \in \mathbb{Z}/q} |C_{h,p}(a, d_1, q)|}{(q \,\mathrm{rad}(q))^{1/2} (q, d_1^2)^{1/2}} d_p y$$

$$\ll \sum_{\substack{d_1 \mid p-1 \\ d_1 \ll p^{1/4}}} \frac{1}{d_1^2} \frac{1}{p} \int_{d_1^2/2}^{2\sqrt{p}} y \sum_{\substack{n \geqslant 1 \\ P^+(n) \leqslant z}} \frac{\mu(n)^2 c^{\omega(n)}}{n} \sum_{\substack{q' n \gg (y/d_1^2)^{\delta} \\ \mathrm{rad}(q') \mid n}} \frac{\max_{a \in \mathbb{Z}/q'n} |C_{h,p}(a, d_1, q'n)|}{(q')^{1/2} (qn', d_1^2)^{1/2}} d_p y,$$

where we let $q' = q/\mathrm{rad}(q)$. Since either $q' \gg (y/d_1^2)^{\delta/2}$ or $n \gg (y/d_1^2)^{\delta/2}$, this is

$$\ll \sum_{i=1}^{2} F_{h,p}\left(z, \frac{\beta_i \delta}{4}, \frac{1}{4}, 2 - \beta_i \delta, 1 - \delta_{i=2}\beta_2, \frac{1}{2} - \delta_{i=1}\beta_1\right),$$

using Lemma 4.3, giving the first part of $E_{h,p}^{(L2)}$.

The contribution of the range (3) above is

$$\sum_{\substack{d_1 \mid p-1 \\ d_1 \ll p^{1/2}}} \sum_{\substack{q \geqslant 1 \\ P^+(q) \leqslant z}} \frac{c^{\omega(q)}}{\mathrm{rad}(q)} \frac{1}{p} \int_0^{\min(d_1^2/2, 2\sqrt{p})} \frac{y}{d_1^2} \max_{\frac{p_-}{d_1^2} < d_2 \leqslant \frac{p_+}{d_1^2}} |h(d_1, d_2)| d_p y$$

$$+ \sum_{\substack{d_1 \mid p-1 \\ d_1 \ll p^{1/2}}} \sum_{\substack{q \geqslant 1 \\ P^+(q) \leqslant z}} \frac{c^{\omega(q)} \max_{a \in \mathbb{Z}/q} |C_{h,p}(a, d_1, q)|}{(q \,\mathrm{rad}(q))^{1/2} (q, d_1^2)^{1/2}} \frac{1}{p} \int_0^{\min(d_1^2/2, 2\sqrt{p})} \frac{y}{d_1^2} d_p y.$$

By Lemma 4.3, the first summand is

$$\ll \frac{(\log z)^{O(1)}}{p^{\frac{1-\beta_4-\varepsilon}{2}}} \sum_{\substack{d_1 \mid p-1 \\ d_1 \ll p^{1/2}}} \frac{1}{d_1^{2\beta_4}} \max_{\frac{p_-}{d_1^2} < d_2 \leqslant \frac{p_+}{d_1^2}} |h(d_1, d_2)|,$$

which gives the remaining of $E_{h,p}^{(L1)}$. Similarly, the second summand is

$$\ll \frac{p^{\varepsilon}}{p^{\frac{1-\beta_3}{2}}} \sum_{\substack{d_1 \mid p-1 \\ d_1 \ll p^{1/2}}} \frac{1}{d_1^{2\beta_3}} \sum_{\substack{n \geqslant 1 \\ P^+(n) \leqslant z}} \frac{\mu(n)^2 c^{\omega(n)}}{n} \sum_{\substack{q' \geqslant 1 \\ \mathrm{rad}(q') \mid n}} \frac{\max_{a \in \mathbb{Z}/q'n} |C_{h,p}(a, d_1, q'n)|}{(q')^{1/2} (q'n, d_1^2)^{1/2}}$$

$$\ll p^{\varepsilon} F_{h,p}\left(z, \frac{1-\beta_3}{2}, \frac{1}{2}, 2\beta_3, 1, \frac{1}{2}\right),$$

which gives the second part of $E_{h,p}^{(L2)}$. □

To estimate $F_{h,p}$, we see directly from the decomposition (30) of $C_{h,p}$ that:

Lemma 4.9. *If* (30) *holds, then*

$$F_{h,p}(z,\boldsymbol{\nu}) \ll \frac{1}{p^{\nu_1}} \sum_{\substack{d_1 \mid p-1 \\ \boldsymbol{v}\in\mathbb{N}^m \\ d_1 \ll p^{\nu_2}}} \frac{|C^{(1)}_{h,p}(\boldsymbol{v},d_1)|}{d_1^{\nu_3}} \sum_{\substack{n\geqslant 1 \\ P^+(n)\leqslant z}} \frac{\mu(n)^2 O(1)^{\omega(n)}}{n^{\nu_4}}$$
$$\sum_{\substack{q\geqslant 1 \\ \mathrm{rad}(q)\mid n}} \frac{\max_{a\in\mathbb{Z}/qn} |C^{(2)}_{h,p}(\boldsymbol{v},d_1,qn)|}{q^{\nu_5}(qn,d_1^2)^{1/2}} \prod_{\ell\nmid q} |C^{(3)}(\boldsymbol{v},d_1,\ell)|.$$

5. The number of subgroups ($h = s$)

In this section, we finally prove the first part of Theorem 1.1. It remains to check that the hypotheses of Theorem 2.17 hold and to bound the errors. Again, all implied constants may depend on a parameter $\varepsilon > 0$.

5.1. Number of subgroups of an abelian group of rank at most 2.

The starting point is the following expression for $h = s$, that we already mentioned in (6):

Proposition 5.1. *For all integers $d_1, d_2 \geqslant 1$,*

$$s(\mathbb{Z}/d_1 \times \mathbb{Z}/d_1d_2) = \sum_{u\mid d_1} \varphi(u)\tau(d_1/u)\tau(d_1^2d_2/u).$$

Proof. By [Cal87], the number of subgroups of $\mathbb{Z}/m \times \mathbb{Z}/n$ is

$$\begin{aligned}\sum_{\substack{a\mid m\\ b\mid n}} \left(a, \frac{(m+1)^n-1}{(m+1)^b-1}\right) &= \sum_{\substack{a\mid m\\ b\mid n}} \left(a, 1+(m+1)+\cdots+(m+1)^{b-1}\right) \\ &= \sum_{a\mid m,\, b\mid n} (a,b) = \sum_{a\mid m,\, b\mid n} \sum_{u\mid (a,b)} \varphi(u) \\ &= \sum_{u\mid (m,n)} \varphi(u)\tau(m/n)\tau(n/u).\end{aligned}$$

Alternatively, see [HHTW14, Theorem 4]. □

5.2. The densities $w_{s,p}$ in arithmetic progressions.

To apply Theorem 2.17, we start by proving that (30) holds.

Proposition 5.2. *In the case $h = s$, Equation* (30) *holds with $m = 3$, $\boldsymbol{v} = (u,k,i) \in \mathbb{N}^3$,*

$$C^{(1)}_{s,p}(\boldsymbol{v},d_1) = \delta_{u\mid d_1}\varphi(u)\tau(d_1/u)\left(\log\left(\frac{p+1}{uk^2}\right)+2\gamma\right)\frac{\delta_{i=0}\delta_{k\mid d_1^2/u}\varphi(k)+\delta_{i=1}}{k},$$

$$C^{(2)}_{s,p}(a,\boldsymbol{v},d_1,q) = (d_1^2,q)\left(\delta_{i=0}+\delta_{i=1}c_{(k,q)}\left(\frac{a}{(d_1^2,q)}\right)\prod_{\ell\mid q}\delta_{v_\ell(q)\geqslant v_\ell(d_1^2k)}\right),$$

$$C^{(3)}_{s,p}(\boldsymbol{v},d_1,\ell) = \delta_{i=0}+\delta_{i=1}\delta_{\ell\mid k}.$$

Moreover, if $1 \leqslant q \leqslant 2y/d_1^2$, *then, under the notations of Section 3,*

$$|E'_{s,p}(y, \boldsymbol{v}, d_1, a, q)| \ll \left|\Delta\left(\frac{p+1\mp y}{u}, A_{a,u,q}, \frac{qd_1^2}{u(d_1^2,q)}\right)\right| + p^{\varepsilon}\frac{y^2(d_1^2,q)}{pqd_1^2},$$

where $A_{a,u,q} \equiv 0 \pmod{d_1^2/u}$ *and* $uA_{a,u,q} \equiv a \pmod{q}$.

Remark 5.3. The variable $u \mid d_1$ in $\boldsymbol{v}$ comes from the sum in the explicit expression for s (Proposition 5.1), $k \mid d_1^2/u$ comes from the sum in the main term for τ in arithmetic progressions, and $i \in \{0,1\}$ comes from two different cases in the evaluation of the Ramanujan sums.

Proof. We need to compute the left-hand side of (26), which is, by Proposition 5.2,

$$\sum_{\substack{\frac{p+1-y}{d_1^2} < d_2 \leqslant \frac{p+1+y}{d_1^2} \\ d_1^2 d_2 \equiv a \pmod q}} s(d_1,d_2) = \sum_{u \mid d_1} \varphi(u)\tau(d_1/u) \sum_{\substack{\frac{p+1-y}{d_1^2} < d_2 \leqslant \frac{p+1+y}{d_1^2} \\ d_1^2 d_2 \equiv a \pmod q}} \tau(d_2 \cdot d_1^2/u).$$

The inner sum can be rewritten as

$$\sum_{\substack{\frac{p+1-y}{u} < d_2' \leqslant \frac{p+1+y}{u} \\ ud_2' \equiv a \pmod q \\ d_2' \equiv 0 \pmod{d_1^2/u}}} \tau(d_2') = \delta_{(d_1^2,q)\mid a} \sum_{\substack{\frac{p+1-y}{u} < d_2' \leqslant \frac{p+1+y}{u} \\ \frac{u}{(u,q)} d_2' \equiv \frac{a}{(u,q)} \pmod{\frac{q}{(u,q)}} \\ d_2' \equiv 0 \pmod{d_1^2/u}}} \tau(d_2').$$

Note that $[q/(u,q), d_1^2/u] = \frac{qd_1^2}{(d_1^2,q)u}$ and if $1 \leqslant A < B$ are such that $\frac{B-A}{2A} < 1$, then

$$[x\log x]_A^B = (B-A)\left(\log\left(\frac{A+B}{2}\right) + 1 + O\left(\frac{B-A}{A}\right)\right).$$

If $(d_1^2, q) \mid a$, then the left-hand side of (26) is given by

$$\frac{2y}{qd_1^2}\sum_{u\mid d_1}\varphi(u)\tau(d_1/u)(d_1^2,q) \sum_{k\mid[q/(u,q),d_1^2/u]} \frac{c_k(A_{a,u,q})}{k}\left(\log\left(\frac{p+1}{uk^2}\right) + 2\gamma + O\left(\frac{y}{p}\right)\right)$$
$$+O\left(\sum_{u\mid d_1}\varphi(u)\tau(d_1/u)\left|\Delta\left(\frac{p+1\mp y}{u}, A_{a,u,q}, \frac{qd_1^2}{u(d_1^2,q)}\right)\right|\right).$$

The main term is

$$\frac{2y}{qd_1^2}\sum_{u\mid d_1}\varphi(u)\tau(d_1/u)(d_1^2,q) \sum_{k\mid[q/(u,q),d_1^2/u]} \frac{c_k(A_{a,u,q})}{k}\left(\log\left(\frac{p+1}{uk^2}\right) + 2\gamma\right)$$
$$+O\left(\frac{y^2}{pqd_1^2}\sum_{u\mid d_1}\varphi(u)\tau(d_1/u)(d_1^2,q)\tau(qd_1^2)\right).$$

We write the sum over k as

$$\left[\sum_{k|d_1^2/u}\varphi(k)+\sum_{k|q/(d_1^2,q)}c_k(a/(d_1^2,q))\right]\frac{1}{k}\left(\log\left(\frac{p+1}{uk^2}\right)+2\gamma\right)(d_1^2,q).$$

and the two summands correspond respectively to the cases $i=0$ and $i=1$ in the statement. Finally, note that for a fixed integer a, $q\mapsto c_q(a)$ is multiplicative. □

5.3. **Main term.**

Proposition 5.4. *Hypotheses (32)–(33) hold with*

$$r_{\ell,\boldsymbol{v},d_1}=v_\ell(d_1^2)+\delta_{i=1}\max(0,v_\ell(k)-1).$$

Proof. The claim is clear for $i=0$. For $i=1$, it follows from von Sterneck's formula [IK04, (3.3)] that the Ramanujan sum is given by

$$c_{\ell^r}(a)=\ell^r\begin{cases}0 & :v_\ell(a)<r-1\\ (-1)/\ell & :v_\ell(a)=r-1\\ 1-1/\ell & :v_\ell(a)\geqslant r\end{cases}\qquad(r\geqslant 1).\tag{47}$$

□

Lemma 5.5. *For $C_{s,p}^{(2)}$ and $C_{s,p}^{(3)}$ as in Proposition 5.2, the Euler product in Theorem 2.17 is*

$$\begin{aligned}&\prod_\ell\left[C_{s,p}^{(3)}(\boldsymbol{v},d_1,\ell)+L_{s,p}(\boldsymbol{v},d_1,\ell,r_{\ell,\boldsymbol{v},d_1})\right]\\ =\ &\prod_{\substack{\ell\nmid d_1\\ \ell|p-1}}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\begin{cases}\prod_{\substack{\ell|d_1\\ \ell\nmid k}}\ell^{-v_\ell(d_1)}\left(1+O\left(1/\ell\right)\right) & :i=0\\ \delta_{k=1}\prod_{\ell|d_1}\ell^{-v_\ell(d_1)}\left(1+O\left(1/\ell\right)\right) & :i=1.\end{cases}\end{aligned}$$

Proof. When $i=0$,

$$\begin{aligned}L'_{s,p}(\boldsymbol{v},d_1,\ell,r_{\ell,\boldsymbol{v},d_1}) &= \left(1-\frac{1}{\ell}\right)\sum_{w\geqslant v_\ell(d_1^2)}\frac{\ell^{v_\ell(d_1^2)}}{\ell^w}=1,\ \text{so}\\ L_{s,p}(\boldsymbol{v},d_1,\ell,r_{\ell,\boldsymbol{v},d_1}) &= \frac{1}{\ell^{v_\ell(d_1)}}\left(1+O\left(\frac{1}{\ell}\right)\right)-1\end{aligned}$$

(see Definition 2.16), while when $i=1$, (47) gives

$$\begin{aligned}L'_{s,p}(\boldsymbol{v},d_1,\ell,r_{\ell,\boldsymbol{v},d_1}) &= \ell^{v_\ell(d_1^2k)}\left(-\frac{\delta_{v_\ell(k)\geqslant 1}}{\ell^{v_\ell(d_1^2k)}}+\frac{1}{\ell^{v_\ell(d_1^2k)}}\right)=\delta_{\ell\nmid k},\\ L_{s,p}(\boldsymbol{v},d_1,\ell,r_{\ell,\boldsymbol{v},d_1}) &= \delta_{\ell\nmid k}\left(\frac{1}{\ell^{v_\ell(d_1)}}\left(1+O\left(\frac{1}{\ell}\right)\right)-1\right).\end{aligned}$$

If $\ell \nmid d_1 kp$, the last part of Proposition 2.15 gives

$$\begin{aligned} L_{s,p}(\boldsymbol{v}, d_1, \ell, r_{\ell,\boldsymbol{v},d_1}) &= \lim_{R\to\infty} \sum_{w=0}^{R} C^{(2)}(\ell^w, \boldsymbol{v}, d_1, \ell^R) g_p(w, v_\ell(d_1), \ell^R) \\ &= \lim_{R\to\infty} \sum_{w=0}^{R} g_p(w, v_\ell(d_1), \ell^R) = \frac{-\delta_{\ell|p-1}}{\ell(\ell^2-1)}. \end{aligned}$$

□

5.4. **Estimation of the error $E_{s,p}^{(P)}$.** We use Proposition 4.7 to estimate the former from $E_{s,p}^{(L1)}$, $E_{s,p}^{(L2)}$ and $E_{s,p}^{(S)}$. Accordingly, let $\varepsilon > 0$, $\delta \in (0,1]$ and $\boldsymbol{\beta} \in [0,1/2] \times [0,1]^3$.

We make the following definition, so that $\prod_{\ell \leqslant z} (1+\ell^{-\nu}) \ll f(z,\nu)^{O(1)}$:

Definition 5.6. For $z \geqslant 1$ and $\nu \in [0,1]$, we let

$$f(z,\nu) = \begin{cases} \log z & : \nu = 1 \\ \exp\left(\frac{z^{1-\nu}}{\log z}\right) & : \nu < 1. \end{cases}$$

We will show:

Proposition 5.7. *If $\beta_2 \leqslant 1/(2+\delta)$ and $\delta < 1/2$, then*

$$E_{s,p}^{(P)}(z) \ll p^{\varepsilon} \left(\frac{f(z, 1-\beta_2)^{O(1)}}{p^{\beta_2\delta/4}} + \frac{(\log z)^{O(1)}}{p^{(1-2\delta)/8}} \right).$$

Remark 5.8. At the end, we will choose $z = (\log p)^A$ with $A \geqslant 1$ large. If we want $f(z,\nu) = O(p^{\varepsilon})$ and $\nu < 1$, we must pick $\nu \geqslant 1 - 1/A$.

5.4.1. *Estimation of $E_{s,p}^{(S)}$.*

Lemma 5.9. $E_{s,p}^{(S)}(z,\delta) \ll \frac{(\log z)^{O(1)}}{p^{(1-2\delta)/8-\varepsilon}}$.

Proof. By definition,

$$E_{s,p}^{(S)}(z,\delta) \ll \sum_{\substack{u|d_1|p-1 \\ d_1 \ll p^{1/4}}} u d_1^{\varepsilon} \frac{1}{p} \int_{d_1^2/2}^{2\sqrt{p}} \sum_{\substack{q \leqslant (2y/d_1^2)^{\delta} \\ q \in Q(d_1,z)}} \frac{c^{\omega(q)}}{\mathrm{rad}(q)} \sum_{\substack{a \in \mathcal{H}(q) \\ (d_1^2,q)|a}} |E_{s,p}(y, d_1, a, q)| d_p y$$

for some $c \geqslant 1$. Let $Q = \frac{qd_1^2}{u(d_1^2,q)} \leqslant \frac{2y}{u(d_1^2,q)}$. By Proposition 5.2 and Theorem 3.2, the sum over a is

$$\begin{aligned}
&\ll \sum_{a \in \mathbb{Z}/\frac{q}{(d_1^2,q)}} \left|\Delta\left(\frac{p+1\mp y}{u}, A_{a,u,q}, Q\right)\right| + p^{\varepsilon}\frac{q}{(d_1^2,q)}\frac{y^2(d_1^2,q)}{pqd_1^2}\\
&\ll \frac{u}{d_1^2}\sum_{a\in\mathbb{Z}/Q}\left|\Delta\left(\frac{p+1\mp y}{u}, a, Q\right)\right| + p^{\varepsilon}\frac{y^2}{pd_1^2}\\
&\ll \frac{uQ^{1/2}}{d_1^2}\left(\sum_{a\in\mathbb{Z}/Q}\left|\Delta\left(\frac{p+1\mp y}{u}, a, Q\right)\right|^2\right)^{1/2} + p^{\varepsilon}\frac{y^2}{pd_1^2}\\
&\ll \frac{q^{1/2}}{d_1(d_1^2,q)^{1/2}}(py)^{1/4} + p^{\varepsilon}\frac{y^2}{pd_1^2},
\end{aligned}$$

where $A_{a,u,q} \equiv 0 \pmod{d_1^2/u}$, $uA_{a,u,q} \equiv a \pmod{q}$, $\frac{u}{(u,q)}A_{a,u,q} \equiv \frac{a}{(u,q)} \pmod{\frac{q}{(u,q)}}$. Hence $E_{s,p}^{(S)}(z,\delta)$ is

$$\begin{aligned}
&\ll p^{1/4+\varepsilon}\sum_{\substack{u|d_1|p-1\\ d_1\ll p^{1/4}}}\frac{u}{d_1}\frac{1}{p}\int_{d_1^2/2}^{2\sqrt{p}} y^{1/4}\sum_{\substack{q\leqslant(2y/d_1^2)^{\delta}\\ q\in Q(d_1,z)}}\frac{c^{\omega(q)}}{\mathrm{rad}(q)}q^{1/2}d_p y\\
&\quad + \frac{1}{p^{1-\varepsilon}}\sum_{u|d_1|p-1}\frac{u}{d_1^2}\frac{1}{p}\int_0^{2\sqrt{p}} y^2\sum_{\substack{q\leqslant(2y/d_1^2)^{\delta}\\ q\in Q(d_1,z)}}\frac{c^{\omega(q)}}{\mathrm{rad}(q)}d_p y\\
&\ll (\log z)^{O(1)}\left(p^{1/4+\varepsilon}\sum_{\substack{d_1|p-1\\ d_1\ll p^{1/4}}} d_1^{-\delta}\frac{1}{p}\int_{d_1^2/2}^{2\sqrt{p}} y^{1/4+\delta/2}d_p y + \frac{1}{p^{1/2-\varepsilon}}\right) \ll \frac{(\log z)^{O(1)}}{p^{\frac{1-2\delta}{8}-\varepsilon}}.
\end{aligned}$$

□

Remark 5.10. At this point, one can check that applying only (40) instead of Theorem 3.2 at best yields the non-admissible bound $(\log z)^{O(1)}p^{\varepsilon}$, if $\delta < 1/3$.

5.4.2. *Bound on $E_{s,p}^{(L1)}$.* By Remark 4.8, we have $E_{s,p}^{(L1)}(1/2) \ll 1/p^{1/4-\varepsilon}$, since $s(d_1,d_2) \ll d_1(d_1d_2)^{\varepsilon}$ for any $\varepsilon > 0$.

5.4.3. *Bound on $E_{s,p}^{(L2)}$.*

Lemma 5.11. *If $\beta_2 < 1/(2+\delta)$, then*

$$E_{s,p}^{(L2)}(z,(\beta_2,\beta_2,1/2),\delta) \ll f(z,1-\beta_2)^{O(1)}p^{-\beta_2\delta/4+\varepsilon}.$$

We start with a preliminary lemma bounding $F_{s,p}$ (cf. Definition 4.6):

Lemma 5.12. *With $C_{s,p}^{(1)}, C_{s,p}^{(2)}$ as in Proposition 5.2, for any $\boldsymbol{\nu} \in [0,1]^4 \times (0,1/2)$, we have*

$$F_{s,p}(z,\boldsymbol{\nu}) \ll \frac{f(z,\nu_4)^{O(1)}}{p^{\nu_1-\varepsilon}} \sum_{\substack{d_1 \mid p-1 \\ d_1 \ll p^{\nu_2}}} d_1^{3-\nu_3-\nu_4-2\nu_5}.$$

Proof. By Lemma 4.9, $F_{s,p}(z,\boldsymbol{\nu})$ is

$$\begin{aligned} &\ll \frac{1}{p^{\nu_1-\varepsilon}} \sum_{\substack{u \mid d_1 \mid p-1 \\ d_1 \ll p^{\nu_2}}} \frac{u}{d_1^{\nu_3}} \sum_{\substack{n \geqslant 1 \\ P^+(n) \leqslant z}} \frac{\mu(n)^2 c^{\omega(n)}}{n^{\nu_4}} \sum_{\substack{q \geqslant 1 \\ \mathrm{rad}(q) \mid n}} \frac{(qn, d_1^2)}{q^{\nu_5} (qn, d_1^2)^{1/2}} \\ &\ll \frac{1}{p^{\nu_1-\varepsilon}} \sum_{\substack{u \mid d_1 \mid p-1 \\ d_1 \ll p^{\nu_2}}} \frac{u}{d_1^{\nu_3}} \sum_{\substack{n \geqslant 1 \\ P^+(n) \leqslant z}} \frac{\mu(n)^2 c^{\omega(n)} (n, d_1^2)^{1/2}}{n^{\nu_4}} \sum_{\substack{q \geqslant 1 \\ \mathrm{rad}(q) \mid n}} \frac{(q, d_1^2)^{1/2}}{q^{\nu_5}}. \end{aligned}$$

□

Proof of Lemma 5.11. By Lemma 5.12, $E_{s,p}^{(L2)}(z,\boldsymbol{\beta},\delta)$ is

$$\begin{aligned} \ll p^{\varepsilon} \Bigg[&\begin{cases} p^{-\beta_1\delta/4} & \beta_1 \in [0, \frac{1}{2+\delta}] \\ p^{-(1-2\beta_1)/4} & \beta_1 \in [\frac{1}{2+\delta}, \frac{1}{2}] \end{cases} + \begin{cases} p^{-(1-\beta_3)/4} & \beta_3 \in [0, 1/2] \\ p^{-(3-5\beta)/4} & \beta_3 \in [1/2, 3/5] \end{cases} \\ &+ f(z, 1-\beta_2)^{O(1)} \begin{cases} p^{-\beta_2\delta/4} & \beta_2 \in [0, \frac{1}{1+\delta}] \\ p^{-(1-\beta_2)/4} & \beta_2 \in [\frac{1}{1+\delta}, 1] \end{cases} \Bigg]. \end{aligned}$$

□

5.4.4. *Conclusion.* By Proposition 4.7 and the above, if $\beta_2 \leqslant 1/(2+\delta)$ and $\boldsymbol{\beta} = (\beta_2, \beta_2, 1/2, 1/2)$, then

$$\begin{aligned} E_{s,p}^{(P)}(z) &\ll (\log z)^{O(1)} p^{\varepsilon} E_{s,p}^{(L1)}(\beta_4) + p^{\varepsilon} E_{s,p}^{(L2)}(z,\boldsymbol{\beta},\delta) + E_{s,p}^{(S)}(z,\delta) \\ &\ll p^{\varepsilon} \left(\frac{(\log z)^{O(1)}}{p^{1/4}} + \frac{f(z,1-\beta_2)^{O(1)}}{p^{\beta_2\delta/4}} + \frac{(\log z)^{O(1)}}{p^{(1-2\delta)/8}} \right) \\ &\ll p^{\varepsilon} \left(\frac{f(z,1-\beta_2)^{O(1)}}{p^{\beta_2\delta/4}} + \frac{(\log z)^{O(1)}}{p^{(1-2\delta)/8}} \right). \end{aligned}$$

This proves Proposition 5.7. □

5.5. **Estimation of the remaining error terms.**

5.5.1. *Bound on $E_{s,p}^{(G)}$.*

Lemma 5.13. $E_{s,p}^{(G)} \ll (\log p)^5 \log_2 p$.

Proof. By Lemma 4.5 and Proposition 5.2, we have

$$\begin{aligned} E_{s,p}^{(G)} \ll \log p \sum_{u \mid d_1 \mid p-1} \frac{\varphi(u)\tau(d_1/u)\tau(d_1^2/u)}{d_1^2} \\ + \sum_{u \mid d_1 \mid p-1} \frac{u}{p^{1-\varepsilon}} \int_0^{2\sqrt{p}} \left(\left| \Delta\left(\frac{p+1\mp y}{u}, 0, \frac{d_1^2}{u} \right) \right| + \frac{yu}{pd_1^2} \right) d_p y. \end{aligned}$$

The first summand is

$$\ll \log p \sum_{d_1 \mid p-1} \frac{1}{d_1^2} \sum_{u \mid d_1} \varphi(u)\tau(d_1/u)\tau(d_1^2/u)$$

$$\ll \log p \sum_{d_1 \mid p-1} \frac{\tau(d_1^2)}{d_1^2}\sigma(d_1) \ll \log p \log_2 p \sum_{d_1 \leqslant p-1} \frac{\tau(d_1)^2}{d_1} \ll (\log p)^5 \log_2 p,$$

since $\sum_{d \leqslant n} \tau(d)^2 = \Theta(n(\log n)^3)$.

The second summand is

$$\ll \sum_{u \mid d_1 \mid p-1} \frac{u}{p^{1-\varepsilon}} \int_0^{2\sqrt{p}} \left(\left| \Delta\left(\frac{p+1 \mp y}{u}, 0, \frac{d_1^2}{u} \right) \right| \right) d_p y + \frac{1}{p^{1-\varepsilon}}.$$

Let $\theta \in (0,1)$. By Theorem 3.2, the contribution of $y \geqslant (d_1^2/u)^{1/\theta}$ and that of $y \leqslant (d_1^2/u)^{1/\theta} \leqslant 2\sqrt{p}$ is

$$\ll p^{\varepsilon} \sum_{\substack{u \mid d_1 \mid p-1 \\ d_1 \ll p^{\theta/4}}} u \frac{1}{p} \int_0^{2\sqrt{p}} \frac{p^{1/4} y^{1/4}}{u^{1/2}} d_p y \ll p^{-(1-\theta)/8+\varepsilon}.$$

The remaining error is

$$\ll \frac{1}{p^{1-\varepsilon}} + \sum_{\substack{u \mid d_1 \mid p-1 \\ d_1^2/u \gg p^{\theta/2}}} \frac{u}{p^{1-\varepsilon}} \int_0^{2\sqrt{p}} \left(\frac{y}{u}\frac{u}{d_1^2} + 1 \right) d_p y \ll p^{-1/2+\theta/4+\varepsilon}.$$

□

5.5.2. *Bound on $E_{s,p}^{(B)}$.* By Remark 2.6, we have $E_{s,p}^{(B)} \ll 1/p^{1/2-\varepsilon}$.

5.5.3. *Bound on $E_{s,p}^{(T)}$.* By Section 5.3, we have

$$E_{s,p}^{(T)}(z, \boldsymbol{v}, d_1) \ll \sum_{\substack{\ell > z \\ \ell \mid d_1}} \frac{1}{\ell^{v_\ell(d_1)}} + \sum_{\substack{\ell > z \\ \ell \nmid d_1 \\ \ell \mid p-1}} \frac{1}{\ell^3} \ll \frac{\omega(d_1)}{z} \ll \frac{\log p}{z \log_2 p}.$$

5.6. **Conclusion.** By Theorem 2.17, Lemma 5.5, Proposition 5.2, and the estimations above, we get that $s(\mathcal{E}ll(p))$ is equal to

$$\sum_{u \mid d_1 \mid p-1} \frac{\varphi(u)\tau(d_1/u)}{d_1^3} \sum_{k \mid d_1^2/u} \left(\log\left(\frac{p+1}{uk^2} \right) + 2\gamma \right)$$

$$\frac{\varphi(k) + \delta_{k=1}}{k} \prod_{\ell \mid k} \ell^{v_\ell(d_1)} \left(1 + O\left(\frac{1}{\ell} \right) \right) \prod_{\substack{\ell \nmid d_1 \\ \ell \mid p-1}} \left(1 - \frac{1}{\ell(\ell^2-1)} \right)$$

$$+ O\left(\frac{Z^{\frac{2}{\alpha}+\varepsilon}}{p^{1/2-\varepsilon}} + \frac{(\log p)^{5+\varepsilon}}{(\log Z)^{\alpha-\varepsilon}} + \frac{f(z, 1-\beta_2)^{O(1)}}{p^{\beta_2\delta/4-\varepsilon}} + \frac{(\log z)^{O(1)}}{p^{(1-2\delta)/8-\varepsilon}} + \frac{(\log p)^6}{z} \right),$$

for any $\alpha \geqslant 1$, $\delta \in (0, 1/2)$, $\beta_2 \in [0, 1/(2+\delta)]$, $Z \geqslant \exp(\sqrt{\log(4p)})$, and $z = (\log Z)^{8\alpha^2}$.

We choose $Z = p$ and $\beta_2 \leqslant 1/(8\alpha^2)$, so that $f(z, 1-\beta_2) = O(p^{\varepsilon})$ according to Remark 5.8. By taking α large enough, the error can be made $\ll_A 1/(\log p)^A$ for any $A > 0$. This proves the first part of Theorem 1.1. □

Remark 5.14. If there are no Siegel zeros, according to Proposition 2.5, the first summand of the error above can be removed, and the limiting factor becomes the third summand.

5.7. **Order of magnitude.**

5.7.1. *Average over primes.*

Proof of Proposition 1.4. Let ρ be the totally multiplicative function defined by $\rho(\ell) = -(\ell^3 - \ell - 1)$ for every prime ℓ. By Abel's summation formula, we have

$$\begin{aligned}\frac{1}{\pi(x)}\sum_{p\leqslant x} s(\mathcal{E}ll(p)) = \sum_{m\leqslant x}\frac{1}{\rho(m)}\sum_{\substack{d_1\leqslant x\\ u\mid d_1}}\frac{\varphi(u)\tau(d_1/u)}{d_1^3}\sum_{k\mid d_1^2/u}\frac{\varphi(k)+\delta_{k=1}}{k}\\ \prod_{\ell\mid k}\ell^{v_\ell(d_1)}\left(1+O\left(\frac{1}{\ell}\right)\right)\prod_{\ell\mid d_1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)^{-1}\\ \left[\frac{\pi(x,1,[d_1,m])}{\pi(x)}\left(\log\left(\frac{x+1}{uk^2}\right)+2\gamma\right)\right.\\ \left.+O\left(\frac{1}{\pi(x)}\int_2^x\frac{\pi(t,1,[d_1,m])}{t}dt\right)\right]+O(1),\end{aligned}$$

where $\pi(x,a,q) = |\{p\leqslant x : p\equiv a \pmod q\}|$ as usual.

By the Siegel–Walfisz theorem [IK04, Corollary 5.29], the expression between square brackets is

$$\begin{aligned}&\left(\frac{1}{\varphi([d_1,m])}+O_A\left(\frac{1}{(\log x)^{A-1}}\right)\right)\left(\log\left(\frac{x+1}{uk^2}\right)+2\gamma\right)+O(1)\\ =\ &\frac{\log(x+1)}{\varphi([d_1,m])}+O_A(1),\end{aligned}$$

for any constant $A>1$. So the average above is

$$\begin{aligned}&\log(x+1)\sum_{m\leqslant x}\frac{1}{\rho(m)}\sum_{\substack{d_1\leqslant x\\ u\mid d_1}}\frac{\varphi(u)\tau(d_1/u)}{d_1^3\varphi([d_1,m])}\sum_{k\mid d_1^2/u}\frac{\varphi(k)+\delta_{k=1}}{k}\\ &\prod_{\ell\mid k}\ell^{v_\ell(d_1)}\left(1+O\left(\frac{1}{\ell}\right)\right)\prod_{\ell\mid d_1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)^{-1}+O(1)\\ =\ &(C_s+o(1))\log(x+1),\end{aligned}$$

for some constant $C_s\geqslant 1$. □

5.7.2. *Upper and lower bounds.*

Proof of Proposition 1.5. For the upper bound, we have

$$s(\mathcal{E}ll(p)) \ll \log p\sum_{u\mid d_1\mid p-1}\frac{\varphi(u)\tau(d_1/u)}{d_1^2}\sum_{k\mid d_1^2/u}\frac{\varphi(k)}{k}\prod_{\ell\mid k}\left(1+O\left(\frac{1}{\ell}\right)\right).$$

Going through Section 4 with (12), we see that the product can actually be replaced by

$$\prod_{\ell|k}\left(1+\frac{1}{\ell}\left(1+\frac{2}{\ell-1}\right)\right).$$

This gives

$$\begin{aligned} s(\mathcal{E}ll(p)) &\ll \log p \sum_{d_1|p-1}\frac{1}{d_1^2}\sum_{u|d_1}\varphi(u)\tau(d_1/u)\sum_{k|d_1^2/u}\exp\left(\frac{\sigma(k)}{k}\right) \\ &\ll (\log p)^{1+e^\gamma+\varepsilon}\sum_{d_1|p-1}\frac{\tau(d_1^2)}{d_1^2}\sigma(d_1) \ll (\log p)^{1+e^\gamma+\varepsilon}\log_2 p\sum_{d_1|p-1}\frac{\tau(d_1^2)}{d_1} \\ &\ll (\log p)^{1+e^\gamma+\varepsilon}\log_2 p\min\left((\log p)^4,\tau((p-1)^2)\frac{\sigma(p-1)}{p-1}\right) \end{aligned}$$

(see also Lemma 5.13).

For the lower bound, note that if $k \mid d_1^2/u$, then

$$\frac{p+1}{uk^2} \geqslant \frac{(p+1)u}{d_1^4} \geqslant (1+o(1))u$$

as $p\to\infty$, since $d_1^2 \leqslant d_1^2 d_2 \leqslant p+1+2\sqrt{p}$ by the Hasse–Weil bound. Hence

$$\begin{aligned} s(\mathcal{E}ll(p)) &\gg \sum_{u|d_1|p-1}\frac{\varphi(u)\tau(d_1/u)}{d_1^3}\sum_{k|d_1^2/u}\left(\log\left((1+o(1))u\right)+2\gamma\right)\varphi(k) \\ &\gg \sum_{u|d_1|p-1}\frac{\varphi(u)\tau(d_1/u)}{d_1 u}. \end{aligned}$$

□

6. The number of cyclic subgroups ($h=c$)

6.1. **Number of cyclic subgroups of an abelian group of rank at most 2.** Similarly to Proposition 5.1, we have:

Proposition 6.1. *For all integers $d_1, d_2 \geqslant 1$,*

$$c(\mathbb{Z}/d_1\times\mathbb{Z}/d_1d_2) = \sum_{u|d_1}(\varphi*\mu)(u)\tau(d_1/u)\tau(d_1^2d_2/u).$$

Proof. By [Tó12, Corollary 1], the number of cyclic subgroups of $\mathbb{Z}/m\times\mathbb{Z}/n$ is

$$\begin{aligned} \sum_{\substack{a|m\\ b|n}}\varphi((a,b)) &= \sum_{\substack{a|m\\ b|n}}\sum_{d|(a,b)}\mu(d)\frac{(a,b)}{d} = \sum_{\substack{a|m\\ b|n}}\sum_{e,d|(a,b)}\frac{\mu(d)}{d}\varphi(e) \\ &= \sum_{u|(a,b)}(\varphi*\mu)(u)\tau(m/u)\tau(n/u). \end{aligned}$$

Alternatively, see [HHTW14, Theorem 5]. □

6.2. **The densities $w_{s,p}$ in arithmetic progressions.** We note that the convolution $\varphi * \mu$ is multiplicative and

$$(\varphi * \mu)(\ell^e) = \begin{cases} \ell - 2 & : e = 1 \\ \ell^{e-2}(\ell-1)^2 & : e \geqslant 2. \end{cases}$$

Similarly to the case $h = s$, we find that:

Proposition 6.2. *Proposition 5.2 holds with $h = s$ replaced by c, up to changing $\varphi(u)$ to $(\varphi * \mu)(u)$ in $C^{(1)}_{h,p}$.*

Since $0 \leqslant (\varphi * \mu)(u) \leqslant u$, the bounds obtained in Section 5 still apply, up to Lemma 5.13. For that one, it suffices to note that

$$\begin{aligned} &\sum_{d_1 \mid p-1} \frac{1}{d_1^2} \sum_{u \mid d_1} (\varphi * \mu)(u) \tau(d_1/u) \tau(d_1^2/u) \\ \ll &\sum_{d_1 \mid p-1} \frac{\tau(d_1^2)}{d_1^2} (\sigma * \mathrm{id})(d_1) \ll \log_2 p \sum_{d_1 \mid p-1} \frac{\tau(d_1^2)}{d_1}. \end{aligned}$$

All in all, this gives the second part of Theorem 1.1.

6.3. **Order of magnitude.** The proof of the second parts of Propositions 1.4 and 1.5 is similar to the case $h = s$ (see Section 5.7).

References

[AG17] Jeffrey D. Achter and Julia Gordon. Elliptic curves, random matrices and orbital integrals. *Pacific J. Math.*, 286(1):1–24, 2017. With an appendix by S. Ali Altuğ.

[BHBS05] William D. Banks, Roger Heath-Brown, and Igor E. Shparlinski. On the average value of divisor sums in arithmetic progressions. *International Mathematics Research Notices*, (1):1–25, 2005.

[Blo07] Valentin Blomer. The average value of divisor sums in arithmetic progressions. *The Quarterly Journal of Mathematics*, 59(3):275–286, 2007.

[BM97] Gautami Bhowmik and Hartmut Menzer. On the number of subgroups of finite Abelian groups. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 67, pages 117–121. Springer, 1997.

[BPS96] Alexandre V. Borovik, Laszlo Pyber, and Aner Shalev. Maximal subgroups in finite and profinite groups. *Transactions of the American Mathematical Society*, 348(9):3745–3761, 1996.

[Cal87] William C. Calhoun. Counting the subgroups of some finite groups. *The American Mathematical Monthly*, 94(1):54–59, 1987.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, Inc., New York, 1989.

[DKS17] Chantal David, Dimitris Koukoulopoulos, and Ethan Smith. Sums of Euler products and statistics of elliptic curves. *Mathematische Annalen*, 368(1):685–752, 2017.

[Gek03] Ernst-Ulrich Gekeler. Frobenius distributions of elliptic curves over finite prime fields. *International Mathematics Research Notices*, 37:1999–2018, 2003.

[HHTW14] Mario Hampejs, Nicki Holighaus, László Tóth, and Christoph Wiesmeyr. Representing and counting the subgroups of the group $\mathbb{Z}/m \times \mathbb{Z}/n$. *Journal of Numbers*, 2014:1–6, 2014.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*. Colloquium Publications. American Mathematical Society, 2004.

[Ivi97] Aleksandar Ivić. On the number of subgroups of finite abelian groups. *Journal de Théorie des Nombres de Bordeaux*, 9(2):371–381, 1997.

[IZ14] Aleksandar Ivić and Wenguang Zhai. On the Dirichlet divisor problem in short intervals. *The Ramanujan Journal*, 33(3):447–465, 2014.

[Jut84] Matti Jutila. On the divisor problem for short intervals. *Annales Universitatis Turkuensis. Series A. I.*, 186:23–30, 1984.

[Jut89] Matti Jutila. Mean value estimates for exponential sums. In Hans Peter Schlickewei and Eduard Wirsing, editors, *Number Theory*, volume 1380, pages 120–136. Springer, 1989.

[KP17] Nathan Kaplan and Ian Petrow. Elliptic curves over a finite field and the trace formula. *Proceedings of the London Mathematical Society. Third Series*, 115(6):1317–1372, 2017.

[KS18] Bryce Kerr and Igor Shparlinski. Bilinear sums of Kloosterman sums, multiplicative congruences and average values of the divisor function over families of arithmetic progressions. 2018. Preprint, arXiv:1811.09329.

[LW07] Jody M. Lockhart and William P. Wardlaw. Determinants of matrices over the integers modulo m. *Mathematics Magazine*, 80(3):207–214, 2007.

[PV15] Prapanpong Pongsriiam and Robert C. Vaughan. The divisor function on residue classes I. *Acta Arithmetica*, 168(4):369–381, 2015.

[PV18] Prapanpong Pongsriiam and Robert C. Vaughan. The divisor function on residue classes II. *Acta Arithmetica*, 182(2):133–181, 2018.

[Sch87] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Number 106 in Graduate Texts in Mathematics. Springer, 2nd edition, 2009.

[Ste92] Thomas Stehling. On computing the number of subgroups of a finite Abelian group. *Combinatorica*, 12(4):475–479, 1992.

[Tó12] László Tóth. On the number of cyclic subgroups of a finite Abelian group. *Bulletin mathématique de la Société des Sciences Mathématiques de Roumanie*, 55 (103)(4):423–428, 2012.

[Tă10] Marius Tărnăuceanu. An arithmetic method of counting the subgroups of a finite abelian group. *Bulletin mathématique de la Société des Sciences Mathématiques de Roumanie*, pages 373–386, 2010.

[Vlă99] Serge G. Vlăduţ. Cyclicity statistics for elliptic curves over finite fields. *Finite Fields and Their Applications*, 5(1):13 – 25, 1999.

Centre de Recherches Mathématiques, Université de Montréal, Canada
Email address: corentin.perretgentil@gmail.com