SUMS OF EULER PRODUCTS AND STATISTICS OF ELLIPTIC CURVES

CHANTAL DAVID, DIMITRIS KOUKOULOPOULOS, AND ETHAN SMITH

Abstract. We present several results related to statistics for elliptic curves over a finite field $\mathbb{F}_p$ as corollaries of a general theorem about averages of Euler products that we demonstrate. In this general framework, we can reprove known results such as the average Lang-Trotter conjecture, the average Koblitz conjecture, and the vertical Sato-Tate conjecture, even for very short intervals, not accessible by previous methods. We also compute statistics for new questions, such as the problem of amicable pairs and aliquot cycles, first introduced by Silverman and Stange. Our technique is rather flexible and should be easily applicable to a wide range of similar problems. The starting point of our results is a theorem of Gekeler which gives a reinterpretation of Deuring's theorem in terms of an Euler product involving random matrices, thus making a direct connection between the (conjectural) horizontal distributions and the vertical distributions. Our main technical result then shows that, under certain conditions, a weighted average of Euler products is asymptotic to the Euler product of the average factors.

Contents

Date: September 26, 2016.
2010 *Mathematics Subject Classification.* 11G07, 11N45.

1. Introduction

Given a fixed elliptic curve E over $\mathbb{Q}$, let $a_p(E)$ denote its trace of Frobenius at the prime p. In [29], Lang and Trotter constructed a heuristic probability model to predict an asymptotic for

$$\#\{p \le x : a_p(E) = t\}, \tag{1.1}$$

where t is a fixed integer and $E/\mathbb{Q}$ is a fixed elliptic curve without complex multiplication. Considerations based on the Sato-Tate Conjecture and the Chebotarëv Density Theorem led them to postulate a model of the form

$$f_\infty(t,p) \cdot f(t,E) \tag{1.2}$$

for the probability that $a_p(E) = t$. To make their model compatible with the Sato-Tate Conjecture, Lang and Trotter chose[1]

$$f_\infty(t,p) = \begin{cases} \dfrac{1}{\pi\sqrt{p}}\sqrt{1-\left(\dfrac{t}{2\sqrt{p}}\right)^2} & \text{if } |t| < 2\sqrt{p}, \\ 0 & \text{otherwise.} \end{cases} \tag{1.3}$$

To make their model compatible with the Chebotarëv Density Theorem applied to every M-division field of E, they chose

$$f(t,E) = \varprojlim_{M} \frac{M \cdot |G_E(M)_t|}{|G_E(M)|},$$

where $G_E(M)$ denotes the image of the map

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_E} \prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}),$$

and $G_E(M)_t$ denotes the trace t elements of $G_E(M)$. Serre showed that the image of ρ_E is open in $\prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$, whence it follows that there exists a positive integer $M_E > 1$ such that

$$\begin{aligned} f(t,E) &= \frac{M_E \cdot |G_E(M_E)_t|}{|G_E(M_E)|} \cdot \prod_{\ell \nmid M_E} \left(\lim_{r\to\infty} \frac{\ell^r \cdot |\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})_t|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|} \right) \\ &= \frac{M_E \cdot |G_E(M_E)_t|}{|G_E(M_E)|} \cdot \prod_{\ell \nmid M_E} \frac{\ell \cdot |\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})_t|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}, \end{aligned}$$

since the ratios at each prime $\ell \nmid M_E$ are constant for all $r \ge 1$. We also remark that the infinite product over the primes $\ell \nmid M_E$ is absolutely convergent. Fixing t and letting $p \to \infty$, we have that $f_\infty(t,p) \sim \frac{1}{\pi\sqrt{p}}$, and summing the probabilities leads one to an "expected value" of

$$\sum_{p \le x} f_\infty(t,p) \cdot f(t,E) \sim C_{E,t} \sum_{p \le x} \frac{1}{2\sqrt{p}} \sim C_{E,t} \int_2^x \frac{\mathrm{d}u}{2\sqrt{u}\log u} \tag{1.4}$$

for (1.1), where $C_{E,t} = \frac{2}{\pi} f(t,E)$. This conjectural asymptotic for (1.1) is known as the "fixed trace" Lang-Trotter Conjecture.

[1] We have slightly changed the Lang-Trotter notation and absorbed the factor $c_p = 1/(2\sqrt{p})$ in $f_\infty(t,p)$ such that $f_\infty(t,p)$ now corresponds to the Sato-Tate measure $\frac{2}{\pi}\sqrt{1-u^2}$ with the change of variable $u = t/(2\sqrt{p})$, and then $\int_{\mathbb{R}} f_\infty(t,p)\,dt = 1$.

Alternatively, one may ask for a "vertical" analogue of the above problem, where one fixes the prime p and allows the elliptic curve E to vary over all isomorphism classes of elliptic curves over the finite field $\mathbb{F}_p$. Here it is natural to count the isomorphism class $E/\mathbb{F}_p$ with weight $1/|\operatorname{Aut}_p(E)|$, where $\operatorname{Aut}_p(E)$ denotes the $\mathbb{F}_p$-automorphism group of E as a curve over $\mathbb{F}_p$. If we let $\mathcal{C}_p$ be the set of isomorphism classes of elliptic curves over $\mathbb{F}_p$, then

$$\sum_{E\in\mathcal{C}_p} \frac{1}{|\operatorname{Aut}_p(E)|} = p,$$

as was observed in [30]. We may thus define a probability measure on $\mathcal{C}_p$ by setting

$$\mathbb{P}_{\mathcal{C}_p}(A) = \frac{1}{p}\sum_{E\in A} \frac{1}{|\operatorname{Aut}_p(E)|}$$

for all $A \subset \mathcal{C}_p$. Often, given a property Q depending only on the isomorphism class of elliptic curves over $\mathbb{F}_p$, we will write

$$\mathbb{P}_{\mathcal{C}_p}(E \text{ has property } Q) \quad \text{instead of} \quad \mathbb{P}_{\mathcal{C}_p}(\{E \in \mathcal{C}_p : E \text{ has property } Q\}).$$

The measure $\mathbb{P}_{\mathcal{C}_p}$ can be also interpreted as the probability measure on (isomorphism classes of) elliptic curves that is induced by the (uniform) counting measure on the set of nonsingular Weierstrass equations defined over $\mathbb{F}_p$. In particular, if one were to select elliptic curves defined over $\mathbb{F}_p$ by uniformly choosing nonsingular Weierstrass equations at random, then one would be $3 = 6/2$ times more likely to select a curve with automorphism group of size 2 than one would be to select a curve with automorphism group of size 6. We recall that the only possible sizes for the automorphism groups are 2, 4, and 6. Furthermore, all but a bounded number of elliptic curves over $\mathbb{F}_p$ have exactly 2 automorphisms. Thus, the difference between our induced measure on $\mathcal{C}_p$ and the uniform counting measure on $\mathcal{C}_p$ is only $O(1/p)$.

The distribution of the elements of $\mathcal{C}_p$ with a fixed trace was described by Deuring [15] in terms of class numbers of imaginary quadratic orders, who showed that

$$\mathbb{P}_{\mathcal{C}_p}(a_p(E) = t) = \begin{cases} \dfrac{H(D(t,p))}{p} & \text{if } |t| < 2\sqrt{p}, \\ 0 & \text{otherwise}, \end{cases} \tag{1.5}$$

where $D(t,p) := t^2 - 4p$ and $H(D)$ is the Kronecker class number of discriminant D, which we define as follows. Given a negative discriminant D, we define the associated Kronecker class number by

$$H(D) = \sum_{\substack{d^2|D \\ D/d^2\equiv 0,1 \ (\mathrm{mod}\ 4)}} \frac{h(D/d^2)}{w(D/d^2)},$$

where $h(\Delta)$ denotes the (ordinary) class number of the unique imaginary quadratic order of discriminant Δ, and $w(\Delta)$ denotes the cardinality of its unit group.

In [20], Gekeler gave a reinterpretation of the above "Deuring probability mass function" (1.5) in terms of random matrix theory, thus making even stronger the connection between the "vertical" fixed trace distribution and the "horizontal" fixed trace Lang-Trotter Conjecture. We state below Theorem 5.5 of [20] in a slightly modified form. We present in Section 3 a new proof of this result, relying on a more combinatorial approach. It also slightly strengthens Theorem 5.5 of [20]: as Gekeler showed, the limit defining $f_\ell(t,p)$ stabilizes for large enough r, and we improve on how large r needs to be in the case when ℓ does not divide the unique fundamental discriminant dividing $D(t,p)$. (See Theorem 3.2 for the precise statement concerning the stabilisation point.) Our new approach is not necessary for the claimed improvement, which would also follow from small modifications of Gekeler's proof, but we believe that it is interesting in its own right. The improvement itself will be important in the applications of Theorem 1.1. The connections with random matrix theory will be discussed later on.

Theorem 1.1 (Gekeler)**.** *Let p be a fixed prime number, and let t be any integer. We have that*

$$\mathbb{P}_{\mathcal{C}_p}(a_p(E)=t)=f_\infty(t,p)\cdot\prod_\ell f_\ell(t,p),$$

where $f_\infty(t,p)$ is defined by (1.3)*, and for each prime ℓ,*

$$f_\ell(t,p)=\lim_{r\to\infty}\frac{\ell^r\phi(\ell^r)\cdot\#\left\{\sigma\in M_2(\mathbb{Z}/\ell^r\mathbb{Z}):\begin{array}{c}\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell^r),\\ \det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^r)\end{array}\right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}.$$

Remark 1.1. As we mentioned above,

$$\int_{\mathbb{R}}f_\infty(t,p)\mathrm{d}t=1.$$

Moreover, as observed by [20, Remark 3.1], it is easy to see that

$$\int_{\mathbb{Z}_\ell}f_\ell(t,p)\mathrm{d}\mu_\ell(t)=1,$$

where μ_ℓ denotes the Haar measure on the ℓ-adic integers $\mathbb{Z}_\ell$, that is to say, the quantities $f_\ell(t,p)$ can be interpreted as probability density functions for t varying over $\mathbb{Z}_\ell$ or over $\mathbb{R}$.

Remark 1.2. As we will see later on, we have that

$$f_\ell(t,p)=1+\frac{\left(\frac{t^2-4p}{\ell}\right)}{\ell}+O\left(\frac{1}{\ell^2}\right)$$

for all $\ell\nmid t^2-4p$. In particular, the infinite product $\prod_\ell f_\ell(t,p)$ converges conditionally by the Prime Number Theorem for arithmetic progressions, but it does not converge absolutely. Similar remarks apply to Theorems 1.7, and 3.3 below. The fact that the convergence is so delicate will create some technical problems in the proof of Theorems 1.2–1.8 when we average the 'singular series' $f_\infty(t,p)\cdot\prod_\ell f_\ell(t,p)$. This is in contrast with the situation in [18, 19, 28]. There the authors study averages of singular series arising from the Hardy-Littlewood k-tuple conjectures, and such singular series are given by absolutely convergent Euler products.

The main purpose of this paper is to show how Gekeler's result can lead to new proofs of vertical distribution results in a way that is both more unified and more conceptual. Some of our results have already been in the literature with other techniques, some improve previous results in the literature and some are new. We indicate that clearly when stating our results in Section 1.1. Indeed, Deuring's formula (1.5) has been in the heart of the proof of many results about the statistics of elliptic curves, such as results about the average probability that an elliptic curve lies in a given isogeny class (average Lang-Trotter conjecture), about the probability that $a_p(E)$ lies in a given interval (vertical Sato-Tate conjecture), and about the average probability that $\#E(\mathbb{F}_p)$ is a prime number (average Koblitz's conjecture). The proof of these results typically involve some rather involved local computations. After these calculations have been performed, one finds that the quantities in question are asymptotic to $C \cdot M$, where M is some nice function varying smoothly in the various parameters involved and C is a certain infinite Euler product. Then more local calculations reveal that C has a natural probabilistic interpretation in terms of random matrices. In this paper, we will show how to use Gekeler's reinterpretation of Deuring's formula to arrive directly to a result of the form $C \cdot M$, where C is given already in terms of local probabilities. What is more, the local computations are now completely straightforward and intuitive. All the results we will state below are easy corollaries of a rather general result, Theorem 4.2.

1.1. **Statements of the results.** The first result involves averaging Gekeler's theorem. The study of this average originated in the work of Fouvry and Murty [16] and of David and Pappalardi [11] in their work on the average Lang-Trotter conjecture.

Theorem 1.2. *Let $t \in \mathbb{Z}$ and $A > 0$. For $x \geq 2$, we have that*

$$\sum_{p \leq x} \mathbb{P}_{\mathcal{C}_p}(a_p(E) = t) = C_{LT}(t) \cdot \int_2^x \frac{dt}{2\sqrt{t}\log t} + O_{t,A}\left(\frac{\sqrt{x}}{(\log x)^A}\right),$$

where

$$C_{LT}(t) := \frac{2}{\pi} \prod_{\ell} \frac{\ell \cdot \# \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})_t}{\# \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}.$$

This result gives evidence for the Lang-Trotter conjecture as stated in (1.4). In particular, note the similarity between the constants $C_{E,t}$ and $C_{\mathrm{LT}}(t)$. It was shown by Jones [24] that the factor M_E in $C_{E,t}$ can be controlled on average and that, for any fixed $t \in \mathbb{Z}$, the average of the constants $C_{E,t}$ of (1.4) over all elliptic curves over $\mathbb{Q}$ is indeed the constant $C_{\mathrm{LT}}(t)$; his results also apply to the average Koblitz constant C_{twin} of Theorem 1.4.

Remark 1.3. It is not immediately obvious that the Euler product defining the constant $C_{\mathrm{LT}}(t)$ converges. One could, of course, deduce this easily by calculating explicitly the factors for each prime ℓ. This is not necessary however, since the proof of Theorem 1.2 implies that the factor for the prime ℓ satisfies the estimate $1 + O(1/\ell^{3/2})$, unless ℓ is one of the finitely many prime divisors of some non-zero integer B. The size of B is controlled in terms of t, though the exact dependence is not needed here. Similar remarks apply to the constants appearing in all subsequent theorems of this section.

Next, we show a uniform version of the vertical Sato-Tate conjecture for the distribution of the normalized traces $a_p(E)/2\sqrt{p}$ in an interval $[\alpha, \beta] \subset [-1, 1]$. For fixed α and β, this theorem is due to Birch [6], and it has been proven for shorter intervals (and thin families of curves) by Banks and Shparlinski [5, Lemma 9] and by Baier and Zhao [3, Theorem 3]. Theorem 1.3 below represents an improvement over both these results, demonstrating that $a_p(E)$ is distributed according to the Sato-Tate measure in all intervals $I \subset [-1, 1]$ of length $\geq p^{-1/2+\epsilon}$.

Theorem 1.3. *Fix $\epsilon > 0$ and $A \geq 1$. For prime $p \geq 2$ and $-1 \leq \alpha \leq \beta \leq 1$ with $\beta - \alpha \geq p^{-1/2+\epsilon}$, we have that*

$$\mathbb{P}_{\mathcal{C}_p}\left(\alpha \leq \frac{a_p(E)}{2\sqrt{p}} \leq \beta\right) = \left(1 + O_{A,\epsilon}\left(\frac{1}{(\log p)^A}\right)\right)\frac{2}{\pi}\int_\alpha^\beta \sqrt{1-u^2}\,\mathrm{d}u.$$

Our next theorem has three parts. The first one concerns the probability that, given p, an elliptic curve over $\mathbb{F}_p$ has a prime number of points. This question was first studied by Galbraith and McKee [17], and Conjecture 1 of their paper amounts to saying that the error term of (1.9) can be controlled. This is true under standard conjectures on the distributions of the primes in short intervals, but not unconditionally. This is similar to the situation in [13, 14] for elliptic curves over $\mathbb{F}_p$ with a fixed number of points, or a fixed group. If we average over p, then it is possible to show that their conjecture holds. This is the result (1.10) below, and it is similar to the results in [9], again for elliptic curves over $\mathbb{F}_p$ with a fixed number of points, or a fixed group. See also the remarks before Theorem 1.5 and 1.8. The third statement of Theorem 1.4 is a new proof of a result that arose in the work of Balog, Cojocaru and David [4] on the average Koblitz conjecture. Here and in the statements of some other results, we shall use the notations

$$E(y,h;q) := \max_{(a,q)=1}\left|\sum_{\substack{y<p\leq y+h\\ p\equiv a\,(\mathrm{mod}\,q)}} \log p - \frac{h}{\phi(q)}\right| \tag{1.6}$$

and

$$R(x,h;m) := \frac{\phi(m)}{h\sqrt{x}}\sum_{q\leq \exp\{(\log\log 2x)^2\}}\int_{x^-}^{x^+} E(y,h;qm)\mathrm{d}y, \tag{1.7}$$

where

$$x^{\pm} := x \pm 2\sqrt{x} + 1. \tag{1.8}$$

Theorem 1.4. *Fix $\epsilon > 0$ and $A \geq 1$. For p prime and $h \in [p^\epsilon, \sqrt{p}/(\log p)^{2A+1}]$, we have that*

$$\mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| \textit{ is prime}) = \frac{C_{GM}(p)}{\log p}\left(1 + O\left(\frac{1}{(\log p)^A} + (\log\log p)^{O(1)}R(p,h;1)^{1/3}\right)\right), \tag{1.9}$$

where

$$C_{GM}(p) := \prod_{\ell\neq p}\left(1-\frac{1}{\ell}\right)^{-1}\cdot\frac{\#\left\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \begin{array}{c}\det(\sigma)+1-\mathrm{tr}(\sigma)\not\equiv 0\,(\mathrm{mod}\,\ell)\\ \det(\sigma)\equiv p\,(\mathrm{mod}\,\ell)\end{array}\right\}}{\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(\sigma)\equiv p\,(\mathrm{mod}\,\ell)\}},$$

and the implied constants depend at most on ϵ and A. Moreover,

$$\sum_{p\leq x}\left|\mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| \textit{ is prime}) - \frac{C_{GM}(p)}{\log p}\right| \ll_A \frac{x}{(\log x)^A} \tag{1.10}$$

and

$$\sum_{p\leq x}\mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| \textit{ is prime}) = C_{twin}\int_2^x \frac{\mathrm{d}u}{\log^2 u} + O_A\left(\frac{x}{(\log x)^A}\right), \tag{1.11}$$

where

$$C_{twin} := \prod_{\ell} \left(1 - \frac{1}{\ell}\right)^{-1} \cdot \frac{\#\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(\sigma) + 1 - \mathrm{tr}(\sigma) \not\equiv 0 \,(\mathrm{mod}\, \ell)\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}.$$

Next, we study the average probability that a curve $\mathbb{E}/\mathbb{F}_p$ has precisely N points. Note here we must have that $|N+1-p| < 2\sqrt{p}$ by Hasse's bound or, equivalently, that $N^- < p < N^+$, where N^-, N^+ are defined as in (1.8).The study of this question was initiated by the first and the third authors in [13, 12] and it was continued by the three authors of the paper and Chandee in [9]. The main term in Theorem 1.5 below is the expected one, but it is not possible to control the error term because we do not presently know how many primes are contained in an interval as short as (N^-, N^+). For the same reason, the results of [13, 12] are conditional on conjectures for primes in short intervals, and the unconditional results of [9] hold only for "most N". The same paper also contains an appendix written by Martin and the first and third authors, where some relevant computations involving random matrices are performed. The sum over primes p runs only over the primes $p \in (N^-, N^+)$ by the Hasse bound.

Theorem 1.5. *Fix $\epsilon > 0$ and $A \geq 1$. If $N \geq 2$ and $h \in [N^\epsilon, \sqrt{N}/(\log N)^{2A+1}]$, then*

$$\sum_p \mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| = N) = \frac{C(N)}{\log N}\left(1 + O\left(\frac{1}{(\log N)^A} + (\log\log N)^{O(1)} R(N,h;1)^{1/3}\right)\right),$$

where the implied constants depend at most on ϵ and A, and

$$C(N) := \prod_{\ell} \lim_{r\to\infty} \frac{\ell^r \cdot \#\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) :\ \mathrm{tr}(\sigma) \equiv \det(\sigma) + 1 - N \,(\mathrm{mod}\, \ell^r),\ \right\}}{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})}.$$

Furthermore,

$$\sum_{N \leq x} \left| \sum_p \mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| = N) - \frac{C(N)}{\log N} \right| \ll_A \frac{x}{(\log x)^A}.$$

Next, let $\boldsymbol{p} = (p_1, \ldots, p_d)$ be a d-tuple of distinct primes. The probability that choosing a 'random' elliptic curve $E/\mathbb{Q}$ such that the primes $p_1, \ldots, p_d$ form an *elliptic aliquot cycle of length d*, that is to say, $|E(\mathbb{F}_{p_j})| = p_{j+1}$, for $j \in \{1, \ldots, d\}$ (with the notational convention that $p_{d+1} = p_1$), is given by

$$\alpha_d(\boldsymbol{p}) := \prod_{j=1}^{d} \mathbb{P}_{\mathcal{C}_{p_j}}(|E_j(\mathbb{F}_{p_j})| = p_{j+1}).$$

This can also be interpreted as the probability of choosing randomly and independently d elliptic curves $E_1, \ldots, E_d$ over $\mathbb{F}_{p_1}, \ldots, \mathbb{F}_{p_d}$, respectively, with the property that $|E(\mathbb{F}_{p_j})| = p_{j+1}$, for $j \in \{1, \ldots, d\}$. Our next goal is to understand the average size of $\alpha_d(\boldsymbol{p})$, a question which arose in the work of Silverman and Stange [35] and has been also studied by Jones [25] and Parks [32, 33]. Of course, Hasse's bound implies that for $\alpha_d(\boldsymbol{p})$ to be non-zero, we must have that $|p_{j+1} - p_j - 1| < 2\sqrt{p_j}$ for all $j \in \{1, \ldots, d\}$. To this extent, we define the set

$$\mathcal{P}_d(x) = \{(p_1, \ldots, p_d) : p_1 \leq x,\ |p_{j+1} - p_j - 1| < 2\sqrt{p_j},\ 1 \leq j \leq d\}. \tag{1.12}$$

Then we have the following estimate, which sharpens and generalizes Theorem 1.6 in [32] and Theorem 1.4 in [33], and proves the vertical distribution for aliquot cycles of length d for all $d \geq 2$. For the case $d = 2$, the same result was proven independently by Parks in [32] with contributions from Giri using a different technique, and we discuss in the remark after Theorem 1.6 the relation between both results. A precise conjecture for the horizontal distribution was made by Jones in [25] following the probabilistic model of Lang-Trotter, and Theorem 1.6 confirms this asymptotic.

Theorem 1.6. *For all $x \geq 2$ and any fixed $A > 0$, we have that*

$$\sum_{\boldsymbol{p} \in \mathcal{P}_d(x)} \alpha_d(\boldsymbol{p}) = C^{(d)}_{aliquot} \int_2^x \frac{du}{2\sqrt{u}(\log u)^d} + O_A\left(\frac{\sqrt{x}}{(\log x)^A}\right) \sim C^{(d)}_{aliquot} \frac{\sqrt{x}}{(\log x)^d},$$

where $C^{(d)}_{aliquot}$ is defined the be the product of the archimedian factor

$$\frac{2^d}{\pi^d} \underset{\substack{|t_j| \leq 1 \ (1 \leq j \leq d) \\ t_1 + \cdots + t_d = 0}}{\int \cdots \int} \prod_{j=1}^{d} \sqrt{1 - t_j^2} \, \mathrm{d}t_1 \cdots \mathrm{d}t_{d-1}$$

times the singular series

$$\prod_{\ell} \lim_{r \to \infty} \frac{\ell^{rd} \cdot \ \# \left\{ \boldsymbol{\sigma} \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})^d : \begin{array}{l} \det(\sigma_j) + 1 - \mathrm{tr}(\sigma_j) \equiv \det(\sigma_{j+1}) \pmod{\ell^r} \\ \textit{for } 1 \leq j \leq d, \textit{ where } \sigma_{d+1} = \sigma_1 \end{array} \right\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|^d}.$$

Remark 1.4. Unlike the situation in Theorems 1.2, 1.4, 1.5 and 1.8, the sequence

$$P^{(d)}_{\text{aliquot}}(\ell^r) := \frac{\ell^{rd} \cdot \ \# \left\{ \boldsymbol{\sigma} \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})^d : \begin{array}{l} \det(\sigma_j) + 1 - \mathrm{tr}(\sigma_j) \equiv \det(\sigma_{j+1}) \pmod{\ell^r} \\ \text{for } 1 \leq j \leq d, \text{ where } \sigma_{d+1} = \sigma_1 \end{array} \right\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|^d}$$

does not seem to become constant for large enough r. We do prove that the sequence $P^{(d)}_{\text{aliquot}}(\ell^r)$ converges as $r \to \infty$ and that its limit satisfies the asymptotic estimate

$$\lim_{r \to \infty} P^{(d)}_{\text{aliquot}}(\ell^r) = 1 + O_d\left(\frac{1}{\ell^{3/2}}\right),$$

but we do not have a closed expression for its value. For the case $d = 2$, Parks [33], with contributions from Giri, obtained Theorem 1.6 with a different technique, without using Gekeler's theorem, but following similar steps as in the original proofs of Theorems 1.2, 1.4, 1.5 and 1.8 [16, 11, 4, 13, 14]. Theorem 1.4 of [33] (or, rather, its proof) implies that

$$\lim_{r \to \infty} P^{(2)}_{\text{aliquot}}(\ell^r) = 1 - \frac{(2\ell^4 + 3\ell^3)(\ell - 2) - (\ell - 1)(\ell^4 - 2\ell^3 - 4\ell^2 + 1)}{(\ell - 1)(\ell^2 - 1)^3},$$

and it remains a challenge to obtain a proof of this formula by a direct calculation of $P^{(2)}_{\text{aliquot}}(\ell^r)$.

So far the questions we have introduced involved understanding the probability that $a_p(E)$ or $\#E(\mathbb{F}_p)$ has a certain property. Next, we will study questions about the group structure of $E(\mathbb{F}_p)$, where E is an elliptic curve over $\mathbb{F}_p$. It is well-known that

$$E(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$$

for some positive integers m and k satisfying the Hasse bound $|p+1-m^2k| < 2\sqrt{p}$, which can be rewritten as $N^- < p < N^+$, where $N = m^2k$. Moreover, the Weil pairing implies that such a prime p must lie in the class $1 \pmod{m}$. The following theorem is the analogous result to Theorem 1.1 for $\mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \cong G)$, where G is a group of the form $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$. As in Gekeler [20], our starting point is a formula similar to (1.5) proven by Schoof, which we reinterpret probabilistically.

Theorem 1.7. *Let p be a fixed prime number. Given positive integers m and k, let $t = t(m,k) = p+1-m^2k$ and $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$. We have that*

$$\mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \cong G) = f_\infty(t,p) \cdot \prod_\ell f_\ell(G,p),$$

where $f_\infty(t,p)$ is defined by (1.3), *for each prime ℓ,*

$$f_\ell(G,p) = \lim_{r\to\infty} \frac{\ell^r \phi(\ell^r) \cdot \# \left\{ \sigma \in M_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l} \operatorname{tr}(\sigma) \equiv t \pmod{\ell^r}, \\ \det(\sigma) \equiv p \pmod{\ell^r}, \\ \sigma \equiv I \pmod{\ell^{\nu_\ell(m)}}, \\ \sigma \not\equiv I \pmod{\ell^{\nu_\ell(m)+1}} \end{array} \right\}}{|\operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}.$$

Remark 1.5. Note that, in accordance with the Hasse bound, $f_\infty(t,p)$ vanishes unless $|t| < 2\sqrt{p}$. Furthermore, $f_\ell(G,p)$ vanishes if $p \not\equiv 1 \pmod{\ell^{\nu_\ell(m)}}$. This is all in accordance with the restriction imposed by the Weil pairing. Therefore, the probability of choosing an elliptic curve $E/\mathbb{F}_p$ with group G is equal to zero unless we have both $|t| < 2\sqrt{p}$ and $p \equiv 1 \pmod{m}$, in which case the probability is nonzero.

We shall use Theorem 1.7 to deduce two other results. The first one is a reproof of Theorem 2.5 in [9], where the constant $C(G)$ below is denoted by $K(G) \cdot |G|/|\operatorname{Aut}(G)|$ in [9]. Dealing with this constant using the original technique of averaging class numbers as in [9] involves lengthy unpleasant computations, whereas the new proof we present here gives directly the value of $C(G)$ as a product of matrix counts. From Theorem 1.8, one can recover the average results of [14] using some additional hypotheses on the distribution of primes in short arithmetic progression to control the error terms, and the unconditional results of [9] for “most” groups G.

Theorem 1.8. *Fix $\epsilon > 0$ and $A \geq 10$. Let $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ with $k \geq 2$ and $1 \leq m \leq k^A$. If $N = m^2k$ and $h \in [mk^\epsilon, \sqrt{N}/(\log k)^{2A+1}]$, then*

$$\sum_p \mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \cong G) = \frac{C(G)}{\log |G|} \left(1 + O\left(\frac{1}{(\log k)^A} + \frac{(\log\log k)^{O(1)} R(N,h;m)^{1/3}}{\log k} \right) \right),$$

where the implied constants depend at most on ϵ and A, and

$$C(G) := \prod_\ell \lim_{r\to\infty} \frac{\ell^r \cdot \# \left\{ \sigma \in \operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l} \operatorname{tr}(\sigma) \equiv \det(\sigma) + 1 - N \pmod{\ell^r}, \\ \sigma \equiv I \pmod{\ell^{\nu_\ell(m)}}, \\ \sigma \not\equiv I \pmod{\ell^{\nu_\ell(m)+1}} \end{array} \right\}}{\# \operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})}.$$

Our last result is a reproof of a weaker version of a result due to Vlăduţ [38], who built on work by Howe [22].

Theorem 1.9. *For p a prime and $A \geq 1$, we have that*

$$\sum_p \mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \text{ is cyclic}) = C_{cyclic}(p) + O_A\left(\frac{1}{(\log p)^A}\right),$$

where

$$C_{cyclic}(p) := \prod_{\ell \neq p} \frac{\#\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \setminus \{I\} : \det(\sigma) \equiv p \pmod{\ell}\right\}}{\#\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(\sigma) \equiv p \pmod{\ell}\right\}} = \prod_{\ell \mid (p-1)} \left(1 - \frac{1}{\ell(\ell^2-1)}\right).$$

1.2. **Outline of the paper.** Before we embark on the more technical aspects of the paper, we discuss in Section 2 the connection between Gekeler's theorem and Theorem 1.7 with the general equidistribution philosophy originating from the work of Deligne, saying that Frobenius elements of elliptic curves (and in general abelian varieties) are equidistributed in groups of matrices. This provides a natural explanation for the local factors $f_\ell(t,p)$ obtained by Gekeler, at least when the prime ℓ is small compared to p. A more complete analysis of Gekeler's theorem in terms of equidistribution can be found in [26].

In Section 3, we prove Theorems 1.1 and 1.7 that re-express the quantities $\mathbb{P}_{\mathcal{C}_p}(a_p(E) = t)$ and $\mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \cong G)$ as a product of local probabilities. Theorem 1.1 was proven by Gekeler in [20], but we present a new proof of his results relying on a more combinatorial approach. We also obtain a slight improvement over his results, showing that the limits defining the local probabilities stabilize earlier in some cases, and this will be important when we apply Theorem 1.1 to prove the results of Section 1.

Section 4 is devoted to stating and explaining our main technical result which deals with averages of certain Euler products. This general result provides a unified framework, under which the results of Section 1 become easy corollaries. The general result is quite technical, so we begin Section 4 by motivating, in a non-rigorous way, our particular choice of hypotheses. Section 4.1 then contains the general axiomatic framework in which we will work in and the statement of our first result about sums of Euler products, Theorem 4.1. Then, we state in Section 4.2 a second result about sums of Euler products, Theorem 4.2, that holds under a simplified set of axioms. This is actually the result that will be invoked in all applications. The advantage of the more general set of axioms is that it is easier to see what is required by the mechanism of the proof, something that could be useful in applications of our results beyond the scope of this paper.

In Section 5, we use Theorem 4.2 to prove the results claimed in Section 1. Most of them follow as easy corollaries. However, there are some subtleties when proving Theorem 1.3, especially when the interval $[\alpha, \beta]$ lies very close to 1 or -1. Moreover, Theorems 1.4 and 1.6 require a technical auxiliary result, which will be proven separately in Section 7. The main input for this auxiliary result is a theorem about primes in short arithmetic progressions proven by the second author [27]. Finally, Section 6 contains the proof of Theorems 4.1 and 4.2.

Acknowledgements. We would like to thank Henri Darmon, Dennis Eriksson, Gerard Freixas i Montplet, Jennifer Park, James Parks and Nicolas Templier for useful conversations. The research of the first author was partially supported by the National Science and Engineering Research Council of Canada (NSERC), and of the second author by NSERC and by the Fonds de recherche du Québec – Nature et technologies (FRQNT).

2. Links with equidistribution in groups of matrices

We can re-interpret the work of Gekeler about the probability that $a_p(E) = t$ over curves over $\mathbb{F}_p$ in terms of standard equidistribution results for the action of $\mathrm{Frob}_p(E)$, the pth power Frobenius, on the ℓ-torsion subgroups $E[\ell]$ as E varies over isomorphism classes of elliptic curves over $\mathbb{F}_p$. This is the framework of the random matrix theory philosophy, initialized by Deligne with its equidistribution theorem, and further developed by Katz and Sarnak, who refined Deligne's equidistribution theorem to predict the statistical behavior for families of curves over finite fields. In a nutshell, the conjugacy classes of the Frobenius at p acting on the ℓ-torsion subgroup $E[\ell]$ become equidistributed in $\mathrm{GL}_2(\mathbb{F}_\ell)$ as one varies over the family of elliptic curves over $\mathbb{F}_p$ and p becomes large enough compared to ℓ. In order to make the connection clear, we state a precise theorem for the equidistribution of $\mathrm{Frob}_p(E)$. This is based on [8], but other similar explicit results for this case can also be found in [1].

Let N be a positive integer, and we write $N = N'p^e$, where $(N', p) = 1$ and $e \geq 0$ is an integer. Let, also, E be an elliptic curve over $\mathbb{F}_p$. If $e \geq 1$, we further suppose that E is ordinary. Then

$$E[N] \cong E[N'] \times E[p^e] \cong \mathbb{Z}/N'\mathbb{Z} \times \mathbb{Z}/N'\mathbb{Z} \times \mathbb{Z}/p^e\mathbb{Z}.$$

Choosing a basis for $E[N']$ and a generator for $E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$, the action of the $\mathrm{Frob}_p(E)$ is given by a pair

$$(F, T) \in \mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z}) \times (\mathbb{Z}/p^e\mathbb{Z})^*$$

such that

$$\begin{aligned} \det(F) &\equiv p \pmod{N'} \\ \mathrm{tr}(F) &\equiv a_p(E) \pmod{N'} \\ T &\equiv a_p(E) \pmod{p^e}. \end{aligned}$$

Then $\mathrm{Frob}_p(E)$ corresponds to a pair $(\mathcal{F}_E, \mathcal{T}_E)$ where $\mathcal{F}_E$ is a conjugacy class in $\mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z})$ of determinant p and $\mathcal{T}_E \in (\mathbb{Z}/p^e\mathbb{Z})^*$. The following equidistribution theorem was proved by Castryck and Hubrechts in [8]. We state their result only when $N \leq p^{1/4}$. In particular, $e = 0$ here. This is without loss of generality, because the result of Castryck and Hubrechts is trivial when $N > p^{1/4}$; its error term becomes $\gg 1$ then, and they have to look at elliptic curves over $\mathbb{F}_q$ for q a large enough power of p to get the desired equidistribution of the Frobenius.

Theorem 2.1. [8, Theorem 2] *Let p be a prime and $N \in [1, p^{1/4}] \cap \mathbb{Z}$. For any conjugacy class $\mathcal{F}$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with determinant p, we have*

$$\left| \mathbb{P}_{\mathcal{C}_p}(\mathcal{F}_E \in \mathcal{F}) - \frac{\#\mathcal{F}}{\#\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \det(\sigma) \equiv p \pmod{N}\}} \right| \ll \frac{N^2 \log\log N}{\sqrt{p}}.$$

We remark that Theorem 2.1 is proven by an application to the function field Cebotarëv's Density Theorem applied to the modular covering $X(p^2; \zeta_{N'}) \to X(1; 1)$. The same result (under some mild restrictions on p and N) was proved by Achter [2] via a direct application of the Katz-Sarnak equidistribution theorem.

We prove a result which is related to Theorem 2.1. In fact, our result improves the range of validity of the asymptotic in Theorem 2.1 to $N \leq p^{1/2-\epsilon}$ when $(t^2 - 4p, N) = 1$, since in that case there is only one conjugacy class in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of trace t and determinant p.

Theorem 2.2. *Let $\epsilon > 0$, $A \geq 1$, p be a prime, $N \in [1, p^{1/2-\epsilon}] \cap \mathbb{Z}$ and $t \in \mathbb{Z}$. If*

$$\lambda = \frac{\#\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \begin{array}{c} \mathrm{tr}(\sigma) \equiv t \,(\mathrm{mod}\, N), \\ \det(\sigma) \equiv p \,(\mathrm{mod}\, N) \end{array}\right\}}{\#\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \det(\sigma) \equiv p \,(\mathrm{mod}\, N)\}},$$

then

$$\mathbb{P}_{\mathcal{C}_p}\left(a_p(E) \equiv t \,(\mathrm{mod}\, N)\right) = \lambda \cdot \left(1 + O_{\epsilon,A}\left(\frac{1}{(\log p)^A}\right)\right).$$

Theorem 2.2 will be proven in the end of Section 5.

3. Class Number Formulas and matrices with fixed invariants

In this section, we prove Theorems 1.1 and 1.7. We start by giving in Theorem 3.1 a formula for the Kronecker Class Number that is analogous to Dirchlet's Class Number Formula. After the completion of this paper, it was brought to our attention that the same formula appears in the work of Soundararajan and Young [36, Lemma 2.1], building on some previous work of Bykovskii [7], and in a different context in the work of Zagier [39]. We include our result for completeness, whose proof is different that [36, Lemma 2.1].

Here and for the rest of the section, given $d \in \mathbb{Z}$, we set

$$\begin{aligned} N_d(m) &= \#\{0 \leq x < 2m : x^2 \equiv d \,(\mathrm{mod}\, 4m)\} \\ &= \frac{\#\{x \,(\mathrm{mod}\, 4m) : x^2 \equiv d \,(\mathrm{mod}\, 4m)\}}{2}. \end{aligned} \tag{3.1}$$

If $d \equiv 2, 3 \,(\mathrm{mod}\, 4)$, then $N_d = 0$, whereas if $d \equiv 0, 1 \,(\mathrm{mod}\, 4)$, then N_d is a multiplicative function.

Theorem 3.1. *For $D < 0$, we have that*

$$H(D) = \frac{\sqrt{|D|}}{2\pi} \prod_{\ell} \left(1 + \frac{1}{\ell}\right)^{-1} \sum_{j=0}^{\infty} \frac{N_D(\ell^j)}{\ell^j}.$$

Proof. If D is not a discriminant, both sides of the claimed identity are 0 and thus trivially equal. Assume now that D is a negative discriminant. Given a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$, we set $d_f = \gcd(a, b, c)$. Recall that a form f is called primitive if $d_f = 1$. Let $\mathcal{F}_D$ be a set of representatives for the equivalence classes of binary quadratic forms of discriminant D under the usual action of $\mathrm{SL}_2(\mathbb{Z})$, and let $\mathcal{F}_D^*$ be a set of representatives for the equivalence classes of *primitive* binary quadratic forms of discriminant D. We write $u(f)$ for the cardinality of the set of matrices in $\mathrm{SL}_2(\mathbb{Z})$ that leave f invariant. Note that if f is a form of discriminant D, then $d_f^2 | D$ and f/d_f is a primitive form of discriminant D/d_f^2. By the classical correspondence between class numbers of binary quadratic forms and of quadratic orders, we have that $h(D) = \#\mathcal{F}_D^*$. Also, for a primitive form of discriminant D, $u(f) = w(D)$, where $w(D)$ is the number of units in the order of discriminant D as defined before. Thus $u(f) = w(D/d_f^2)$.

We will use the proof of the class number formula for the class number $h(D)$ to prove the theorem. We write $r_f(n)$ for the number of representations of n by values of the form f and set

$$R_D(n) = \sum_{f \in \mathcal{F}_D} \frac{r_f(n)}{u(f)} = \sum_{\substack{d^2 | D \\ d | n}} \sum_{\substack{f \in \mathcal{F}_D \\ d_f = d}} \frac{r_f(n)}{u(f)} = \sum_{\substack{d^2 | D \\ d | n}} \sum_{g \in \mathcal{F}^*_{D/d^2}} \frac{r_g(n/d)}{w(D/d^2)}.$$

Therefore

$$\begin{aligned}\frac{1}{x}\sum_{n\le x}R_D(n)&=\sum_{d^2|D}\sum_{g\in\mathcal{F}^*_{D/d^2}}\frac{1}{d\cdot w(D/d^2)}\cdot\frac{1}{x/d}\sum_{m\le x/d}r_g(m)\\&\sim\sum_{d^2|D}\frac{h(D/d^2)}{d\cdot w(D/d^2)}\cdot\frac{2\pi}{\sqrt{|D/d^2|}}=H(D)\cdot\frac{2\pi}{\sqrt{|D|}}\end{aligned}$$

as $x\to\infty$ (see, for example, [10, p. 48-49]).

On the other hand, [31, Theorem 3.27] implies that

$$R_D(n)=\sum_{f\in\mathcal{F}_D}\frac{r_f(n)}{u(f)}=\sum_{d^2|n}N_D(n/d^2).$$

In particular, R_D is a multiplicative function. We write it as $R_D=1*\left(\frac{D}{\cdot}\right)*\alpha_D$. If $\ell\nmid D$, then $N_D(\ell^j)=1+\left(\frac{D}{\ell}\right)$, so $R_D(\ell)=1+\left(\frac{D}{\ell}\right)$, $\alpha_D(\ell)=0$ and $|\alpha_D(\ell^j)|\le 2\tau_4(\ell^j)\ll j^3$ for $j\ge 2$. Finally, if $\ell|D$, then we use the bound $\alpha_D(\ell^j)\ll j^3\ell^{\lfloor j/2\rfloor}$, which follows from the elementary bound $N_D(\ell^j)\ll\ell^{\lfloor j/2\rfloor}$. It is then easy to conclude that

$$\begin{aligned}\sum_{n\le y}|\alpha_D(n)|\ll\sum_{\substack{d\le y\\ p|b\implies p|D}}|\alpha_D(b)|\sum_{\substack{m\le y/b\\(m,D)=1}}|\alpha_D(m)|&\ll_\epsilon\sum_{\substack{b\le y\\ p|b\implies p|D}}|\alpha_D(b)|\cdot\frac{y^{1/2+\epsilon}}{b^{1/2+\epsilon}}\\&=y^{1/2+\epsilon}\prod_{\ell|D}\left(1+\frac{|\alpha_D(\ell)|}{\ell^{1/2+\epsilon}}+\frac{|\alpha_D(\ell^2)|}{\ell^{2(1/2+\epsilon)}}+\cdots\right)\\&\ll_{\epsilon,D}y^{1/2+\epsilon},\end{aligned}$$

for all $y\ge 1$. Also, $\sum_{n\le y}\left(\frac{D}{n}\right)\ll_D 1$ since $D<0$ and thus D is not a perfect square. Consequently, Dirichlet's hyperbola method implies that

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\le x}R_D(n)=\prod_\ell\left(1-\frac{1}{\ell}\right)\sum_{j=0}^\infty\frac{R_D(\ell^j)}{\ell^j}.$$

Finally, note that

$$R_D(\ell^j)=\sum_{\substack{0\le i\le j\\ i\equiv j\,(\mathrm{mod}\,2)}}N_D(\ell^i),$$

so that

$$\sum_{j=0}^\infty\frac{R_D(\ell^j)}{\ell^j}=\left(1-\frac{1}{\ell^2}\right)^{-1}\sum_{j=0}^\infty\frac{N_D(\ell^j)}{\ell^j}.$$

Putting together the above formulas completes the proof of the theorem. □

Next, we turn our attention to calculating the cardinality of the sets

$$C(t,u,n;\ell^r):=\left\{\sigma\in\mathrm{M}_2(\mathbb{Z}/\ell^r\mathbb{Z}):\begin{array}{c}\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell^r),\\ \det(\sigma)\equiv u\,(\mathrm{mod}\,\ell^r),\\ \sigma\equiv I\,(\mathrm{mod}\,\ell^{\nu_\ell(n)})\end{array}\right\}$$

and the limits

$$f_\ell(t,u,n):=\lim_{r\to\infty}\frac{\ell^r\phi(\ell^r)\cdot|C(t,u,n;\ell^r)|}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|},\tag{3.2}$$

where u now is a general integer. Given any integers t and u, we set $D = D(t,u) = t^2 - 4u$. Note that, for the purposes of this discussion, we do not need to assume that $D < 0$.

When $n = 1$, the computation of $\#C(t,u,n;\ell^r)$ was already carried out by Gekeler in [20] for r sufficiently large. Also, in the case that $n = 1$, the count was carried out by Castryck and Hubrechts [8] for all $r \ge 1$. Theorem 3.2(a) below gives a formula for $\#C(t,u,1;\ell^r)$ that improves slightly Theorem 4.4 of [20], in the sense that the claimed formula holds for $r > \nu_\ell(D)$. However, note that, unlike in [20] and in [8], we do not give an explicit formula for $\#C(t,u,1;\ell^r)$; the stated combinatorial expression suffices for our purposes and makes the exposition cleaner.

Throughout, we will be assuming that $u \equiv 1 \,(\mathrm{mod}\, n)$ and $u + 1 - t \equiv 0 \,(\mathrm{mod}\, n^2)$. This can be justified by the observation that if either of these conditions fails, then the set $C(t,u,n;\ell^r)$ will be empty for some ℓ dividing n and r large enough. Indeed, writing

$$\sigma = \begin{pmatrix} 1+n\alpha & n\beta \\ n\gamma & 1+n\delta \end{pmatrix}, \tag{3.3}$$

we find that $\sigma \in C(t,u,n;\ell^r)$ if, and only if,

$$\begin{aligned} 2 + n(\alpha+\delta) &\equiv t \,(\mathrm{mod}\, \ell^r), \\ 1 + n(\alpha+\delta) + n^2(\alpha\delta - \beta\gamma) &\equiv u \,(\mathrm{mod}\, \ell^r). \end{aligned} \tag{3.4}$$

In particular, if $r \ge 2\nu_\ell(n)$, then we must have that $u \equiv 1 \,(\mathrm{mod}\, \ell^{\nu_\ell(n)})$ and $u \equiv t - 1 \,(\mathrm{mod}\, \ell^{2\nu_\ell(n)})$. So, from now on, we will always be working under the assumption that $u \equiv 1 \,(\mathrm{mod}\, n)$ and $u + 1 - t \equiv 0 \,(\mathrm{mod}\, n^2)$, which holds trivially when $n = 1$ too. Under this assumption,

$$D \equiv t^2 - 4(t-1) \equiv (t-2)^2 \,(\mathrm{mod}\, 4n^2)$$

and $n \mid (t-2)$. Hence, it follows that $n^2 \mid D$ and D/n^2 is a discriminant.

Theorem 3.2. *Let $t,u \in \mathbb{Z}$, $D = D(t,u) = t^2 - 4u$ and $n \in \mathbb{N}$ with $u \equiv 1 \,(\mathrm{mod}\, n)$ and $u + 1 \equiv t \,(\mathrm{mod}\, n^2)$.*

(a) *For $r \ge 1$ and $u' \equiv u \,(\mathrm{mod}\, \ell^{\nu_\ell(D)+1})$, we have that*

$$\#C(t,u',1;\ell^r) = \ell^{2r} + \ell^{2r} \sum_{j=1}^{\min\{r,\nu_\ell(D)+1\}} \frac{N_D(\ell^j) - N_D(\ell^{j-1})}{\ell^j}.$$

If, in addition, $r > \nu_\ell(D)$, then

$$\frac{\ell^r \phi(\ell^r) \cdot |C(t,u',1;\ell^r)|}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|} = \left(1 + \frac{1}{\ell}\right)^{-1} \sum_{j=0}^{\infty} \frac{N_D(\ell^j)}{\ell^j}.$$

In particular, the limit defining $f_\ell(t,u,1)$ exists and it equals the right hand side of the above identity.

(b) *The sequence over r defining $f_\ell(t,u,n)$ is constant for $r > \nu_\ell(D)$. In particular, $f_\ell(t,u,n)$ is well-defined. Moreover, we have the formulas*

$$f_\ell(t,u,n) = \frac{f_\ell(t_1,u_1,1)}{\ell^{\nu_\ell(n)}} \quad \text{and} \quad f_\ell(t,u,n) - f_\ell(t,u,\ell n) = \frac{f_\ell^*(t_1,u_1,1)}{\ell^{\nu_\ell(n)}},$$

where $t_1 = (t-2)/n$, $u_1 = (u+1-t)/n^2$ and $f_\ell^*(t_1,u_1,1)$ is defined as $f_\ell(t_1,u_1,1)$ with the difference that we replace $|C(t_1,u_1,1;\ell^r)|$ by $\#\{\sigma \in C(t_1,u_1,1;\ell^r) : \sigma \not\equiv$

$0 \pmod{\ell}\}$. *Finally, the sequence over r defining $f_\ell^*(t_1,u_1,1)$ is constant for $r > \nu_\ell(t_1^2-4u_1)$.*

(c) *If $\ell \nmid D/n^2$, then $f_\ell(t,u,\ell n)=0$ and*

$$f_\ell(t,u,n) = \frac{1}{\ell^{\nu_\ell(n)}}\left(1-\frac{1}{\ell^2}\right)^{-1}\left(1+\frac{\left(\frac{D/n^2}{\ell}\right)}{\ell}\right).$$

(d) *For every $r \geq 1$, we have that*

$$\#C(t,u,n;\ell^r) = \ell^{2r-\nu_\ell(n)} + O(\ell^{2r-\nu_\ell(n)-1}).$$

Proof. (a) For convenience, set $D' = D(t,u') = t^2-4u'$ and note that $\nu_\ell(D') = \nu_\ell(D)$, since $D' \equiv D \pmod{4\ell^{\nu_\ell(D)+1}}$. Now, note that $\#C(t,u',1;\ell^r)$ counts quadruples $(a,b,c,d) \in (\mathbb{Z}/\ell^r\mathbb{Z})^4$ with $a+d \equiv t \pmod{\ell^r}$ and $ad-bc \equiv u' \pmod{\ell^r}$. Equivalently, it counts triples $(a,b,c) \in (\mathbb{Z}/\ell^s\mathbb{Z})^3$ such that $bc \equiv a(t-a)-u' \pmod{\ell^r}$. We write $b = \ell^j b'$, where $0 \leq j \leq r$ and $b' \in (\mathbb{Z}/\ell^{r-j}\mathbb{Z})^*$. We must have that $a(t-a)-u' \equiv 0 \pmod{\ell^j}$, and for each such a and b, there are exactly ℓ^j possibilities for c. Therefore

$$\begin{aligned}\#C(t,u',1;\ell^r) &= \sum_{j=0}^{r} \phi(\ell^{r-j}) \cdot \#\{a \pmod{\ell^r} : a^2-ta+u' \equiv 0 \pmod{\ell^j}\} \cdot \ell^j \\ &= \ell^r \sum_{j=0}^{r} \phi(\ell^{r-j}) \cdot \#\{0 \leq a < \ell^j : a^2-ta+u' \equiv 0 \pmod{\ell^j}\}.\end{aligned}$$

We note that $a^2-ta+u' \equiv 0 \pmod{\ell^j}$ if, and only if, $(2a-t)^2 \equiv D' \pmod{4\ell^j}$. To this end, we make the change of variable $x = 2a-t$, which caries the restriction $x \equiv t \pmod 2$. However, this is automatic if $x^2 \equiv D' \pmod 4$, and we find that

$$\begin{aligned}\#\{0 \leq a < \ell^j : a^2-ta+u' \equiv 0 \pmod{\ell^j}\} &= \#\{-t \leq x < 2\ell^j - t : x^2 \equiv D' \pmod{4\ell^j}\} \\ &= N_{D'}(\ell^j),\end{aligned}$$

since the function x^2 is $2\ell^j$-periodic mod $4\ell^j$. So, using the identity $\phi(n) = n\sum_{d|n}\mu(d)/d$, we deduce that

$$\begin{aligned}\#C(t,u',1;\ell^r) = \ell^{2r}\sum_{j=0}^{r}\frac{N_{D'}(\ell^j)}{\ell^j}\sum_{i=0}^{r-j}\frac{\mu(\ell^i)}{\ell^i} &= \ell^{2r}\sum_{i=0}^{r}\frac{\mu(\ell^i)}{\ell^i}\sum_{j=0}^{r-i}\frac{N_{D'}(\ell^j)}{\ell^j} \\ &= \ell^{2r} + \ell^{2r}\sum_{i=1}^{r}\frac{N_{D'}(\ell^i)-N_{D'}(\ell^{i-1})}{\ell^i}.\end{aligned}$$

Using Hensel's lemma, it is relatively easy to see that the sequence $N_{D'}(\ell^i)$ is constant for $i \geq \nu_\ell(D')+1$, so

$$\#C(t,u',1;\ell^r) = \ell^{2r} + \ell^{2r}\sum_{j=1}^{\min\{r,\nu_\ell(D')+1\}}\frac{N_{D'}(\ell^j)-N_{D'}(\ell^{j-1})}{\ell^j}.$$

Recall that $\nu_\ell(D') = \nu_\ell(D)$ and that $D' \equiv D \pmod{4\ell^{\nu_\ell(D)+1}}$. So, if $j \leq \nu_\ell(D')+1$, then $N_{D'}(\ell^j) = N_D(\ell^j)$, which proves the first formula in the statement of part (a). Finally, using again the fact that $N_D(\ell^i)$ is constant for $i \geq \nu_\ell(D)+1$, we find that if $r > \nu_\ell(D)$, then

$$\frac{\#C(t,u',1;\ell^r)}{\ell^{2r}} = 1 + \sum_{j=1}^{\infty} \frac{N_D(\ell^j) - N_D(\ell^{j-1})}{\ell^j} = \left(1 - \frac{1}{\ell}\right) \sum_{j=0}^{\infty} \frac{N_D(\ell^j)}{\ell^j}.$$

Since

$$|\operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})| = \ell^{4(r-1)}(\ell^2-1)(\ell^2-\ell) = \ell^{4r}\left(1-\frac{1}{\ell}\right)^2\left(1+\frac{1}{\ell}\right),$$

the second formula of part (a) follows too.

(b) Set $a = \nu_\ell(n)$. Making the change of variables (3.3), we immediately see by (3.4) that

$$\begin{aligned} |C(t,u,n;\ell^r)| &= \#\left\{\sigma \in \operatorname{M}_2(\mathbb{Z}/\ell^{r-a}\mathbb{Z}) : \begin{array}{l} \operatorname{tr}(\sigma) \equiv t_1 \,(\operatorname{mod} \ell^{r-a}), \\ \det(\sigma) \equiv u_1 \,(\operatorname{mod} \ell^{r-2a}) \end{array}\right\} \\ &= \sum_{\substack{0 \leq u_2 < \ell^{r-a} \\ u_2 \equiv u_1 \,(\operatorname{mod} \ell^{r-2a})}} |C\left(t_1, u_2, 1; \ell^{r-a}\right)|. \end{aligned} \tag{3.5}$$

Set $D_1 = D(t_1,u_1) = D/n^2$ and note that if $u_2 \equiv u_1 \,(\operatorname{mod} \ell^{r-2a})$ and $r > \nu_\ell(D)$, then $u_2 \equiv u_1 \,(\operatorname{mod} \ell^{\nu_\ell(D_1)+1})$. Therefore, if $r > \nu_\ell(D)$, then part (a) implies that

$$|C(t,u,n;\ell^r)| = \ell^a |C(t_1,u_1,1;\ell^{r-a})|$$

and, consequently,

$$\frac{\ell^r\phi(\ell^r)\cdot|C(t,u,n;\ell^r)|}{|\operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|} = \frac{1}{\ell^a}\cdot\frac{\ell^{r-a}\phi(\ell^{r-a})\cdot|C(t_1,u_1,1;\ell^{r-a})|}{|\operatorname{GL}_2(\mathbb{Z}/\ell^{r-a}\mathbb{Z})|}.$$

Moreover, the right hand side is constant for $r - a > \nu_\ell(D_1) = \nu_\ell(D) - 2a$, by part (a). In particular, it is constant if $r > \nu_\ell(D)$. This proves that the sequence over r defining $f_\ell(t,u,n)$ is constant for $r > \nu_\ell(D)$ and that

$$f_\ell(t,u,n) = \frac{f_\ell(t_1,u_1,1)}{\ell^a}. \tag{3.6}$$

Next, note that

$$f_\ell(t,u,n) - f_\ell(t,u,\ell n) = \frac{f_\ell(t_1,u_1,1)}{\ell^a} - \frac{f_\ell(t_1/\ell,u_1/\ell^2,1)}{\ell^{a+1}} \tag{3.7}$$

by (3.6), where the second term vanishes unless $\ell | t_1$ and $\ell^2 | u_1$. Making the change of variables $\tau = \sigma + I$, we see that

$$\begin{aligned} &\#\{\sigma \in C(t_1,u_1,1;\ell^r) : \sigma \not\equiv 0 \,(\operatorname{mod} \ell)\} \\ &\quad = \#\{\tau \in C(t_1+2,u_1+t_1+1,1;\ell^r) : \tau \not\equiv I \,(\operatorname{mod} \ell)\} \\ &\quad = |C(t_1+2,u_1+t_1+1,1;\ell^r)| - |C(t_1+2,u_1+t_1+1,\ell;\ell^r)|. \end{aligned}$$

In particular, we see that

$$\begin{aligned} f_\ell^*(t_1,u_1,1) &= f_\ell(t_1+2,u_1+t_1+1,1) - f_\ell(t_1+2,u_1+t_1+1,\ell) \\ &= f_\ell(t_1,u_1,1) - \frac{f_\ell(t_1/\ell,u_1/\ell^2,1)}{\ell} \end{aligned}$$

by (3.6), where the second term vanishes unless $\ell | t_1$ and $\ell^2 | u_1$, which, together with (3.7), demonstrates the claimed formula for $f_\ell(t,u,n) - f_\ell(t,u,\ell n)$.

It remains to prove that the limit defining $f_\ell^*(t_1,u_1,1)$ stabilizes for $r > \nu_\ell(D_1)$. As above, making the change of variables $\tau = \sigma + I$, it suffices to prove the same statement for the limits defining $f_\ell(t_1+2, u_1+t_1, 1)$ and $f_\ell(t_1+2, u_1+t_1+1, \ell)$. We have already seen this that the sequence over r defining the former is constant for $r > \nu_\ell(D_1)$. We will show the same for the limit defining $f_\ell(t_1+2, u_1+t_1+1, \ell)$. If $\ell | t_1$ and $\ell^2 | u_1$, then this follows by the portion of part (b) already proven. Assume now that either $\ell \nmid t_1$ or $\ell^2 \nmid u_1$. Then it is easy to see that $C(t_1+1, u_1+t_1+1, \ell; \ell^r) = \emptyset$ for $r \geq 2$ (see, for example, the discussion preceding the statement of Theorem 3.2). Therefore, if $\nu_\ell(D_1) \geq 1$, then our claim has been proven. Finally, if $\nu_\ell(D_1) = 0$, then $C(t_1+2, u_1+t_1+1, \ell; \ell^r) = \emptyset$ for $r \geq 1$. Indeed, if $\sigma \equiv I \pmod{\ell}$, then $\mathrm{tr}(\sigma) \equiv 2 \pmod{\ell}$, and $\det(\sigma) \equiv 1 \pmod{\ell}$. So, if in addition, $\mathrm{tr}(\sigma) \equiv t_1 + 2 \pmod{\ell}$ and $\det(\sigma) \equiv u_1 + t_1 + 1 \pmod{\ell}$, then we must have that $\ell | t_1$ and $\ell | u_1$, whence $\ell | D_1$, a contradiction. This proves that $C(t_1+2, u_1+t_1+1, \ell; \ell^r) = \emptyset$ for $r \geq 1 = 1 + \nu_\ell(D_1)$ when $\nu_\ell(D_1) = 0$, thus completing the proof of part (b).

(c) Since $\ell \nmid D_1 = D/n^2$, we see immediately that $C(t,u,\ell n; \ell^r) = \emptyset$ for large enough r, by the discussion preceding the theorem, so $f_\ell(t,u,\ell n) = 0$. Finally, part (b) and the first formula in part (a) imply that

$$f_\ell(t,u,n) = \frac{f_\ell(t_1,u_1,1)}{\ell^{\nu_\ell(n)}} = \frac{1}{\ell^{\nu_\ell(n)}(1-1/\ell^2)}\left(1 + \frac{N_{D_1}(\ell) - 1}{\ell}\right).$$

Since $N_{D_1}(\ell) = 1 + \left(\frac{D_1}{\ell}\right)$ when $\ell \nmid D_1$, the claimed formula for $f_\ell(t,u,n)$ follows.

(d) This follows by (3.5) and the fact that

$$|C(t_1,u_2,1;\ell^s)| = \ell^{2s} + O(\ell^{2s-1}),$$

which is a simple consequence of part (a) together with the fact that $N_{D_1}(\ell^j) \ll \ell^{\lfloor j/2 \rfloor}$. (See, also Theorem 7 in [8].) □

It is now straightforward to deduce Theorems 1.1 and 1.7. As an intermediate step, we fix an integer n and ask for the proportion of elliptic curves $E/\mathbb{F}_p$ with $a_p(E) = t$ and $E(\mathbb{F}_p)[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then Lemma 4.8 and Theorem 4.9 of [34] essentially say that

$$\mathbb{P}_{\mathcal{C}_p}(a_p(E) = t,\, E(\mathbb{F}_p)[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \frac{H(D/n^2)}{p}$$

if $|t| < 2\sqrt{p}$, $n \mid p-1$ and $n^2 \mid p+1-t$; otherwise, this probability equals 0. As before, the conditions $n \mid p-1$ and $n^2 \mid p+1-t$ together imply that $n^2 \mid D$ and that D/n^2 is a negative discriminant. Thus, the Kronecker class number $H(D/n^2)$ is well-defined. As a direct corollary of Theorem 3.1 and parts (a) and (b) of Theorem 3.2, we have the following result.

Corollary 3.3. *Let p be a fixed prime number, and let t and n be any integers with $n \geq 1$. Then*

$$\mathbb{P}_{\mathcal{C}_p}(a_p(E) = t,\, E(\mathbb{F}_p)[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = f_\infty(t,p) \cdot \prod_\ell f_\ell(t,p,n),$$

where $f_\infty(t,p)$ is defined by (1.3) *and $f_\ell(t,p,n)$ is defined by* (3.2).

Taking $n = 1$ in Corollary 3.3 yields Theorem 1.1. Lastly, we show how to deduce Theorem 1.7.

Proof of Theorem 1.7. If

$$G = G_{m,k} := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z},$$

then the principle of inclusion-exclusion and Corollary 3.3 imply that the probability of choosing an elliptic curve with group $G = G_{m,k}$ is given by

$$\begin{aligned}\mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \cong G) &= \sum_{j^2|k} \mu(j)\mathbb{P}_{\mathcal{C}_p}(a_p(E) = t,\ E(\mathbb{F}_p)[jm] \cong G_{jm,1}) \\ &= f_\infty(t,p) \cdot \sum_{\substack{j^2|k \\ jm|p-1}} \mu(j) \prod_\ell f_\ell(t,p,jm),\end{aligned}$$

where $\mu(j)$ denotes the usual Möbius function. By the definition of $f_\ell(t,p,jm)$, we have that $f_\ell(t,p,jm) = f_\ell(t,p,\ell^{\nu_\ell(j)}m)$. Therefore, if $\mathcal{P}$ denotes the set of primes ℓ with $\ell^2|k$ and $\ell|(p-1)/m$ and $\mathcal{S}(\mathcal{P})$ the set of integers composed only of primes from $\mathcal{P}$, then

$$\begin{aligned}\mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \cong G) &= f_\infty(t,p) \sum_{j\in\mathcal{S}(\mathcal{P})} \mu(j) \prod_{\ell|j} f_\ell(t,p,\ell m) \prod_{\ell\nmid j} f_\ell(t,p,m) \\ &= f_\infty(t,p) \cdot \left(\prod_{\ell\notin\mathcal{P}} f_\ell(t,p,m)\right) \prod_{\ell|\mathcal{P}} (f_\ell(t,p,m) - f_\ell(t,p,\ell m))\end{aligned}$$

by inclusion-exclusion. Note that if $\ell \notin \mathcal{P}$, then $f_\ell(t,p,\ell m) = 0$ by the discussion preceding Theorem 3.2. So we deduce that

$$\mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \cong G) = f_\infty(t,p) \cdot \prod_\ell (f_\ell(t,p,m) - f_\ell(t,p,\ell m)) = f_\infty(t,p) \prod_\ell f_\ell(G,p),$$

which completes the proof of the theorem. □

4. Sums of Euler products

In this section, we provide a unified framework under which Theorems 1.2-1.8 fall. Before we state the general set-up in which we will work in, we use Theorem 1.2 as a working example to describe our main idea.

In view of Theorem 1.1, Theorem 1.2 (or, rather, a soft version of this theorem) is reduced to showing that

$$\sum_{p\le x} f_\infty(t,p) \prod_\ell f_\ell(t,p) \sim C_{\mathrm{LT}}(t) \frac{\sqrt{x}}{\log x} \quad (x \to \infty),$$

where $C_{\mathrm{LT}}(t)$ is as in the statement of this theorem. We set

$$\delta_\ell(a) = \mathbf{1}_{\ell\nmid a} \cdot (f_\ell(t,a) - 1).$$

Since

$$f_\infty(t,p) f_p(t,p) \sim \frac{1}{\pi\sqrt{p}}$$

for large primes p, we find that

$$\sum_{p\le x} f_\infty(t,p) \prod_\ell f_\ell(t,p) \sim \sum_{p\le x} \frac{1}{\pi\sqrt{p}} \prod_\ell (1 + \delta_\ell(p)),$$

which reduces Theorem 1.2 to showing that

$$\sum_{p\le x}\frac{1}{\sqrt{p}}\prod_{\ell}(1+\delta_\ell(p))\sim\frac{\pi\cdot C_{\mathrm{LT}}(t)}{2}\sum_{p\le x}\frac{1}{\sqrt{p}}\sim\pi\cdot C_{\mathrm{LT}}(t)\cdot\frac{\sqrt{x}}{\log x},$$

where the last estimate is a consequence of the Prime Number Theorem. If we define a probability measure on the primes $p\le x$ via the relation

$$\mathbb{E}_{p\le x}[f(p)]=\frac{\sum_{p\le x}f(p)/\sqrt{p}}{\sum_{p\le x}1/\sqrt{p}},$$

then we need to show that

$$\mathbb{E}_{p\le x}\left[\prod_{\ell}(1+\delta_\ell(p))\right]\sim\frac{\pi}{2}\cdot C_{\mathrm{LT}}(t)=\prod_{\ell}\frac{\ell\cdot\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}):\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell)\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}.$$

Now, $\delta_\ell(p)$ depends only on the congruence class of $p\,(\mathrm{mod}\,\ell^r)$ for some appropriate r, and the residue classes in which p lies modulo powers of different primes ℓ^r should behave independent from each. Therefore, it is reasonable to expect that

$$\mathbb{E}_{p\le x}\left[\prod_{\ell}(1+\delta_\ell(p))\right]\sim\prod_{\ell}\Big(1+\mathbb{E}_{p\le x}\left[\delta_\ell(p)\right]\Big).$$

Note that if $\ell\nmid p$, then $\delta_\ell(p)=\lim_{r\to\infty}\Delta_{\ell^r}(p)$, where

$$\Delta_{\ell^r}(p)=-1+\frac{\phi(\ell^r)\ell^r\cdot\#\left\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}):\begin{array}{c}\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell^r)\\ \det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^r)\end{array}\right\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}.$$

Clearly, the function Δ_{ℓ^r} is ℓ^r-periodic and its mean value over $(\mathbb{Z}/\ell^r\mathbb{Z})^*$ is

$$\begin{aligned}\frac{1}{\phi(\ell^r)}\sum_{a\in(\mathbb{Z}/\ell^r\mathbb{Z})^*}\Delta_{\ell^r}(a)&=-1+\frac{\ell^r\cdot\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}):\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell^r)\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}\\&=-1+\frac{\ell\cdot\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}):\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell)\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}.\end{aligned}$$

Since the primes p are well distributed in reduced arithmetic progressions mod ℓ^r, we should then have that

$$\mathbb{E}_{p\le x}[\delta_\ell(p)]\sim\Delta_\ell:=-1+\frac{\ell\cdot\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}):\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell)\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|},$$

which yields Theorem 1.2 heuristically.

Of course, there are several stumbling blocks in the road map laid above. First of all, the assumption that different primes behave independently from each other is only true asymptotically, and for small primes. Therefore, the first thing we need to do is to truncate the product $\prod_\ell(1+\delta_\ell(p))$. This can be indeed accomplished because of Theorem 3.2(c), which implies that

$$\delta_\ell(p)=\frac{\left(\frac{t^2-4p}{\ell}\right)}{\ell}+O\left(\frac{1}{\ell^2}\right), \tag{4.1}$$

unless ℓ is one of the finitely many prime divisors of t^2-4p. Estimating sums of the form

$$\sum_{\ell>z} \frac{\left(\frac{t^2-4p}{\ell}\right)}{\ell} \tag{4.2}$$

is related to our knowledge about the zeroes of the Dirichlet L-function associated to the character $(t^2-4p\,|\,\cdot\,)$. The Generalized Riemann Hypothesis would imply that the sum in (4.2) is small as soon as $z>(\log d)^{2+\epsilon}$, where d is the conductor of the character $(t^2-4p\,|\,\cdot\,)$. However, unconditionally, we only know that the sum in (4.2) is small for $z>\exp\{d^\epsilon\}$, which is a much stronger restriction. This problem can be rectified by appealing to zero-density estimates which guarantee that, for most p, the sum in (4.2) is small as soon as $z>(\log d)^A$, with A a large enough constant. This is good enough for our purposes and allows us for most primes $p\le x$ to replace the product $\prod_\ell(1+\delta_\ell(p))$ by $\prod_{\ell\le(\log x)^A}(1+\delta_\ell(p))$ with a very small total error. Then, we expand this short product to find that

$$\sum_{p\le x}\frac{1}{\sqrt{p}}\prod_{\ell\le(\log x)^A}(1+\delta_\ell(p)) = \sum_{\ell|n\,\Rightarrow\,\ell\le(\log x)^A}\mu^2(n)\sum_{p\le x}\frac{\delta_n(p)}{\sqrt{p}},$$

where, for convenience, we have set $\delta_n(p)=\prod_{\ell|n}\delta_\ell(p)$. The next crucial step is that, for all p with $\ell^r\nmid t^2-4p$, Theorem 3.2(c) implies that $\delta_\ell(p)=\Delta_{\ell^r}(p)$, and the function Δ_{ℓ^r} is ℓ^r-periodic. Setting

$$\Delta_q(a)=\prod_{\ell^r\|q}\Delta_{\ell^r}(a),$$

we find that

$$\sum_{p\le x}\frac{\delta_n(p)}{\sqrt{p}} = \sum_{q\in\mathbb{N},\ \mathrm{rad}(q)=n}\ \sum_{\substack{p\le x\\ \nu_\ell(t^2-4p)=\nu_\ell(q)-1\\ \forall\ell|n}}\frac{\Delta_q(p)}{\sqrt{p}} = \sum_{\substack{q\in\mathbb{N}\\ \mathrm{rad}(q)=n}}\ \sum_{a\in\mathcal{H}(q)}\Delta_q(a)\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,q)}}\frac{1}{\sqrt{p}},$$

where

$$\mathcal{H}(q)=\{a\in(\mathbb{Z}/q\mathbb{Z})^*:\ell^r\nmid t^2-4a,\ \ell^{r-1}\mid t^2-4a\quad\text{whenever } \ell^r\|q\}.$$

We then use the Bombieri-Vinogradov theorem in order to control the number of primes in arithmetic progressions on average. We also have to use some more trivial arguments when the modulus q is too large, exploiting the fact that this is a $(\log x)^A$-smooth number and there are very few such numbers. We are then left with the task of showing that

$$\sum_{r=1}^{\infty}\frac{1}{\phi(\ell^r)}\sum_{a\in\mathcal{H}(\ell^r)}\Delta_{\ell^r}(a)=\Delta_\ell.$$

Indeed, we have that

$$\sum_{r=1}^{R}\frac{1}{\phi(\ell^r)}\sum_{a\in\mathcal{H}(\ell^r)}\Delta_{\ell^r}(a)=\frac{1}{\phi(\ell^R)}\sum_{\substack{a\in(\mathbb{Z}/\ell^R\mathbb{Z})^*\\ \ell^R\nmid t^2-4a}}\Delta_{\ell^R}(a)=\Delta_\ell-\frac{1}{\phi(\ell^R)}\sum_{\substack{a\in(\mathbb{Z}/\ell^R\mathbb{Z})^*\\ \ell^R|t^2-4a}}\Delta_{\ell^R}(a),$$

which is easily seen to tend to Δ_ℓ as $R\to\infty$, since the congruence $t^2-4a\not\equiv 0\,(\mathrm{mod}\,\ell^R)$ has at most 8 solutions $a\,(\mathrm{mod}\,\ell^R)$.

4.1. **General axiomatic framework.** We describe here in rather abstract terms the general set-up in which we work to show Theorems 1.2-1.8. We fix a natural number d and a set

$$\mathcal{A} \subset ([-X,X]\cap\mathbb{Z})^d,$$

where X is some parameter that we consider given from now on. In general, we denote d-dimensional vectors with bold letters, e.g. $\boldsymbol{x}$ or $\boldsymbol{a}$, and we index their coordinates as $\boldsymbol{x}=(x_1,\dots,x_d)$, $\boldsymbol{a}=(a_1,\dots,a_d)$, etc. Moreover, given $\boldsymbol{a},\boldsymbol{b}\in\mathbb{Z}^d$ and $q\in\mathbb{N}$, we write $\boldsymbol{a}\equiv\boldsymbol{b}\,(\operatorname{mod} q)$ if $a_j\equiv b_j\,(\operatorname{mod} q)$, for all $j\in\{1,\dots,d\}$. Similarly, we write $\boldsymbol{a}\,(\operatorname{mod} q)$ to denote the vector $(a_1\,(\operatorname{mod} q),\dots,a_d\,(\operatorname{mod} q))$.

In addition, we fix a set of complex weights $(w_{\boldsymbol{a}})_{\boldsymbol{a}\in\mathcal{A}}$ and we set

$$W=\sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}}.$$

In practice, we cannot handle weights for which W is significantly smaller than $\sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}}$. We simply allow $w_{\boldsymbol{a}}$ to be complex numbers to gain some extra flexibility. Next, for each prime ℓ, we consider a set $\mathcal{G}(\ell)\subset(\mathbb{Z}/\ell\mathbb{Z})^d$, and for $q\in\mathbb{N}$ we set

$$\mathcal{G}(q)=\left\{\boldsymbol{g}\in(\mathbb{Z}/q\mathbb{Z})^d : \boldsymbol{g}\,(\operatorname{mod}\ell)\in\mathcal{G}(\ell)\text{ for all primes }\ell|q\right\}. \tag{4.3}$$

We think of $\mathcal{A}$ as being well-distributed among the elements of $\mathcal{G}(q)$. To this end, we set

$$E(\mathcal{A};q)=\max_{\boldsymbol{g}\in\mathcal{G}(q)}\left|\sum_{\substack{\boldsymbol{a}\in\mathcal{A}\\ \boldsymbol{a}\equiv\boldsymbol{g}\,(\operatorname{mod} q)}} w_{\boldsymbol{a}}-\frac{W}{|\mathcal{G}(q)|}\right|$$

for all $q\in\mathbb{N}$. In order to avoid working with very sparse sets $\mathcal{A}$, we also assume that

$$|\mathcal{G}(\ell)|\gg\ell^d\quad(\ell\text{ prime}). \tag{4.4}$$

Finally, we set

$$Q=\exp\{(\log\log X)^2\} \tag{4.5}$$

and we assume that $\mathcal{A}$ does not contain many more elements than it should in each residue class $\boldsymbol{g}\in\mathcal{G}(q)$ for $q\le Q$. To handle the case when we don't have good estimates for W (see, for example, the proof of Theorem 1.4), we assume the existence of a quantity $\widetilde{W}$, which we heuristically think of comparable size with W, such that:

$$\sum_{\substack{\boldsymbol{a}\in\mathcal{A}\\ \boldsymbol{a}\equiv\boldsymbol{g}\,(\operatorname{mod} q)}}|w_{\boldsymbol{a}}|\ll\frac{\widetilde{W}}{|\mathcal{G}(q)|}\quad(q\le Q,\ \boldsymbol{g}\in\mathcal{G}(q)). \tag{4.6}$$

In many of the applications, $d=1$ and $\mathcal{A}$ is taken to be the set of primes in an interval or the set of integers in an interval and, respectively, $\mathcal{G}(q)=(\mathbb{Z}/q\mathbb{Z})^*$ or $\mathcal{G}(q)=\mathbb{Z}/q\mathbb{Z}$, so the reader can work with these two simple examples in mind.

We are going to average certain Euler products over our set $\mathcal{A}$. We consider a sequence of complex numbers $\{\delta_\ell(\boldsymbol{a}):\boldsymbol{a}\in\mathcal{A},\ \ell\text{ prime}\}$ and set

$$P_{\boldsymbol{a}}=\prod_{\ell\text{ prime}}(1+\delta_\ell(\boldsymbol{a})).$$

Our goal is to estimate the sum

$$\sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}}.$$

Of course, we do not even know whether the infinite product $P_{\boldsymbol{a}}$ converges, so we certainly need to impose some conditions on the numbers $\delta_\ell(\boldsymbol{a})$. Indeed, we assume that there is an absolute constant $\eta > 0$ and an integer $k \ge 0$ such that the following conditions hold:

(1) $\delta_\ell(\boldsymbol{a}) = 0$ if $\boldsymbol{a} \pmod{\ell} \notin \mathcal{G}(\ell)$.
(2) $\delta_\ell(\boldsymbol{a}) \ll 1/\ell$ if $\boldsymbol{a} \pmod{\ell} \in \mathcal{G}(\ell)$.
(3) For each $j \in \{1, \dots, k\}$ and each $\boldsymbol{a} \in \mathcal{A}$, there are non-principal Dirichlet characters $\chi_{j,\boldsymbol{a}}$ mod $M_{j,\boldsymbol{a}}$, an integer $L_{\boldsymbol{a}} \ge 1$, and complex coefficients $\lambda_{j,\boldsymbol{a}}$ such that for all primes $\ell \nmid L_{\boldsymbol{a}}$, we have that $\boldsymbol{a} \pmod{\ell} \in \mathcal{G}(\ell)$ and

$$\delta_\ell(\boldsymbol{a}) = \frac{\lambda_{1,\boldsymbol{a}}\chi_{1,\boldsymbol{a}}(\ell) + \cdots + \lambda_{k,\boldsymbol{a}}\chi_{k,\boldsymbol{a}}(\ell)}{\ell} + O\left(\frac{1}{\ell^{1+\eta}}\right).$$

(4) For every prime $\ell \le Q$ and every exponent $r \ge 1$, there is a set $\mathcal{E}(\ell^r) \subset (\mathbb{Z}/\ell^r\mathbb{Z})^d$ and a function $\Delta_{\ell^r} : \mathbb{Z}^d \to \mathbb{C}$ such that:
   (a) Δ_{ℓ^r} is ℓ^r-periodic;
   (b) $\delta_\ell(\boldsymbol{a}) = \Delta_{\ell^r}(\boldsymbol{a})$ if $\boldsymbol{a} \pmod{\ell^r} \in \mathcal{G}(\ell^r) \setminus \mathcal{E}(\ell^r)$, where the sequence of sets $\{\boldsymbol{a} \in \mathbb{Z}^d : \boldsymbol{a} \pmod{\ell^r} \in \mathcal{E}(\ell^r)\}_{r\ge1}$ is decreasing and its intersection is contained in $\mathbb{Z}^d \setminus \mathcal{A}$;
   (c) Δ_{ℓ^r} vanishes on average over the set $\mathcal{G}(\ell^r)$ as $r \to \infty$, that is to say[2]

$$\lim_{r\to\infty} \frac{1}{|\mathcal{G}(\ell^r)|} \sum_{\boldsymbol{a}\in\mathcal{G}(\ell^r)} \Delta_{\ell^r}(\boldsymbol{a}) = 0;$$

   (d) $\|\Delta_{\ell^r}\|_\infty \ll_\ell 1$, for all $r \ge 1$.
(5) For all $j \in \{1, \dots, k\}$ and all $\boldsymbol{a} \in \mathcal{A}$, we have $M_{j,\boldsymbol{a}} \le X^{O(1)}$, $\omega(L_{\boldsymbol{a}}) \le (\log X)^{O(1)}$ and $\lambda_{j,\boldsymbol{a}} \ll 1$.

Under these assumptions and notations, we have the following result.

Theorem 4.1. *Assume the above set-up and fix $\epsilon > 0$, $\lambda > 1$ and $C \ge 1$. Then*

$$\sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}} = W + O\left(\frac{e^{O(S)}\widetilde{W}}{(\log X)^C} + MX^\epsilon + (\log\log X)^{O(1)} e^{O(S)} \widetilde{W}^{1/\lambda} E^{1-1/\lambda}\right),$$

where

$$M = \max_{\substack{1\le j\le k \\ c\ge2}} \sum_{\substack{a\in\mathcal{A} \\ \mathrm{cond}(\chi_{j,\boldsymbol{a}})=c}} |w_{\boldsymbol{a}}|, \qquad E = \sum_{q\le Q} q^{d-1} E(\mathcal{A}; q),$$

and

$$S = \sum_{\ell\le Q} \sum_{r=1}^\infty \frac{(|\mathcal{E}(\ell^r)|/\ell^{r(d-1)})^\lambda}{\ell^{r+1}},$$

with Q is defined by (4.5) *and* $\mathrm{cond}(\chi)$ *denoting the conductor of the Dirichlet character χ. All implied constants depend at most on $d, k, \lambda, \eta, \epsilon, C$ and the implicit constants in conditions* (1) - (5) *above and in relations* (4.4) *and* (4.6).

[2] Our assumption that Δ_{ℓ^r} is 0 on average does not harm generality significantly. The case when its average is some number Δ_ℓ follows from the case $\Delta_\ell = 0$ by considering sequence $\delta'_\ell(\boldsymbol{a})$ instead, also supported on those $\boldsymbol{a} \in \mathcal{G}(\ell)$, where $1 + \delta_\ell(\boldsymbol{a}) = (1 + \Delta_\ell)(1 + \delta'_\ell(\boldsymbol{a}))$ when $\boldsymbol{a} \pmod{\ell} \in \mathcal{G}(\ell)$. We would also need to assume then that the series $\sum_\ell |\Delta_\ell|$ converges fast enough. This argument will be used later on.

Remark 4.1. When $k = 0$, then Property (3) states that $\delta_\ell(\boldsymbol{a}) = 1 + O(1/\ell^{1+\eta})$ whenever $\ell \nmid L_{\boldsymbol{a}}$. This is much stronger than the bound (6.2) which is used in the proof of Theorem 4.1 in Section 6, and in this case, the error term $e^{O(S)}\widetilde{W}/(\log X)^C$ can be replaced by $e^{O(S)}\widetilde{W}/X^\alpha$ for some $\alpha > 0$, provided that (4.6) holds with $Q = X^\beta$ for some $\beta > 0$ (and then α depends on β). The key observation is that, if $\delta_n(\boldsymbol{a}) = \prod_{\ell | n} \delta_\ell(\boldsymbol{a})$, we then have that

$$\sum_{n=1}^{\infty} \mu^2(n) n^\epsilon |\delta_n(\boldsymbol{a})| \le \prod_{\ell | L_{\boldsymbol{a}}} \left(1 + \frac{O(1)}{\ell^{1-\epsilon}}\right) \prod_{\ell \nmid L_{\boldsymbol{a}}} \left(1 + \frac{O(1)}{\ell^{1+\eta-\epsilon}}\right) \ll \prod_{\ell | L_{\boldsymbol{a}}} \left(1 + \frac{1}{\ell^{1-\epsilon}}\right)^{O(1)},$$

for any fixed $\epsilon < \eta$. Since $\omega(L_{\boldsymbol{a}}) \le (\log X)^K$ for some $K \ge 1$ by property (5) above, we deduce that

$$\prod_{\ell | L_{\boldsymbol{a}}} \left(1 + \frac{1}{\ell^{1-\epsilon}}\right) \ll \prod_{\ell \le (\log X)^{K/(1-\epsilon)}} \left(1 + \frac{1}{\ell^{1-\epsilon}}\right) \ll_{\epsilon, K} e^{(\log X)^{\epsilon K/(1-\epsilon)}} = X^{o(1)},$$

provided that $\epsilon < 1/(K+1)$. This allows us to handle the tails of various summations in the proof via Rankin's trick. For example, we have the bound

$$\sum_{n > N} \mu^2(n) |\delta_n(\boldsymbol{a})| \le \frac{1}{N^\epsilon} \sum_{n=1}^{\infty} \mu^2(n) n^\epsilon |\delta_n(\boldsymbol{a})| = \frac{X^{o(1)}}{N^\epsilon},$$

which is good enough for our purposed by choosing $\epsilon < \min\{\eta, 1/(K+1)\}$ and N to be an appropriate power of X. We do not pursue this strengthening of the error term when $k = 0$ since it is not necessary for our purposes.

4.2. **A simplified set of axioms.** For the applications we have in mind, we can simplify further the conditions of Theorem 4.2. Instead of (4.4), we suppose that $|\mathcal{G}(\ell)|$ is usually very close to ℓ^d:

$$\#\mathcal{G}(\ell) = \ell^d + O(\ell^{d-\eta}), \tag{4.7}$$

where $\eta > 0$ is some fixed absolute constant. We notice once and for all that $\mathcal{G}(\ell) = (\mathbb{Z}/\ell\mathbb{Z})^d$ and $\mathcal{G}(\ell) = ((\mathbb{Z}/\ell\mathbb{Z})^*)^d$ satisfy this condition.

We continue assuming conditions (1) and (2), but conditions (3)-(5) are simplified as we describe below. Here and for the rest of this paper, given a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, we write $\mathscr{C}(f)$ for its content, that is to say, the greatest common divisor of its coefficients, and $H(f)$ for its height, that is to say the maximum absolute modulus of its coefficients. With this notation, we postulate the existence of some polynomials $D_j(x_1, \dots, x_d)$, $1 \le j \le k$, and $F(x_1, \dots, x_k)$ over $\mathbb{Z}$, an integer $L \ge 1$ and some complex coefficients λ_j, $1 \le j \le k$ satisfying the following hypotheses:

(3') For each $j \in \{1, \dots, k\}$ and each $\boldsymbol{a} \in \mathcal{A}$, $D_j(\boldsymbol{a})$ is a discriminant (i.e. $D_j(\boldsymbol{a})$ is not a perfect square and $D_j(\boldsymbol{a}) \equiv 0, 1 \pmod 4$) and if $\ell \nmid L \cdot D_1(\boldsymbol{a}) \cdots D_k(\boldsymbol{a})$, then $\boldsymbol{a} \pmod{\ell} \in \mathcal{G}(\ell)$ and

$$\delta_\ell(\boldsymbol{a}) = \frac{\lambda_1 \left(\frac{D_1(\boldsymbol{a})}{\ell}\right) + \cdots + \lambda_k \left(\frac{D_k(\boldsymbol{a})}{\ell}\right)}{\ell} + O\left(\frac{1}{\ell^{1+\eta}}\right).$$

(4') For every prime ℓ and every exponent $r \ge 1$, there is a function $\Delta_{\ell^r} : \mathbb{Z}^d \to \mathbb{C}$ such that:

(a) Δ_{ℓ^r} is ℓ^r-periodic;

(b) $\delta_\ell(\boldsymbol{a}) = \Delta_{\ell^r}(\boldsymbol{a})$ if $\boldsymbol{a} \,(\mathrm{mod}\, \ell^r) \in \{\boldsymbol{g} \in \mathcal{G}(\ell^r) : F(\boldsymbol{g}) \not\equiv 0 \,(\mathrm{mod}\, \ell^r)\}$;

(c) Δ_{ℓ^r} has a mean value as $r \to \infty$ over $\mathcal{G}(\ell^r)$, that is to say there is a $\Delta_\ell \in \mathbb{C}$ such that

$$\lim_{r\to\infty} \frac{1}{|\mathcal{G}(\ell^r)|} \sum_{\boldsymbol{a}\in\mathcal{G}(\ell^r)} \Delta_{\ell^r}(\boldsymbol{a}) = \Delta_\ell.$$

Moreover, $|1+\Delta_\ell| \gg 1$.

(d) $\|\Delta_{\ell^r}\|_\infty \ll 1/\ell$, for all $r \geq 1$.

(5') We have[3] $\omega(L) \leq (\log X)^{O(1)}$, $\mathscr{C}(F) \ll 1$, and $\lambda_j \ll 1$ for $1 \leq j \leq k$. Moreover, $F(\boldsymbol{a}) \neq 0$ for all $\boldsymbol{a} \in \mathcal{A}$. Finally, for each $j \in \{1, \dots, k\}$, we have that $H(D_j) \leq X^{O(1)}$ and the polynomials $\pm D_j/\mathscr{C}(D_j)$ are not perfect squares in the ring $\mathbb{Z}[x_1, \dots, x_d]$.

Theorem 4.2. *Assume that the above simplified set-up holds and fix $\epsilon > 0$ and $C \geq 1$. Moreover, suppose that $\mathcal{A} \subset \{\boldsymbol{a} \in \mathbb{Z}^d : \boldsymbol{a} \,(\mathrm{mod}\, \ell) \in \mathcal{G}(\ell)\}$ for each prime $\ell \leq Q$. Then the infinite product*

$$P := \prod_\ell (1+\Delta_\ell)$$

converges absolutely and we have that

$$\sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}} = P \cdot \left(W + O\left(\frac{\widetilde{W}}{(\log X)^C} + MX^\epsilon + (\log\log X)^{O(1)} \widetilde{W}^{m/(m+1)} E^{1/(m+1)} \right)\right),$$

where $m = \deg(F)$,

$$M = \max_{\substack{1\leq j\leq k \\ n\neq 0}} \sum_{\substack{\boldsymbol{a}\in\mathcal{A} \\ D_j(\boldsymbol{a})/n \text{ is a square}}} |w_{\boldsymbol{a}}|, \qquad E = \sum_{q\leq Q} q^{d-1} E(\mathcal{A}; q),$$

and Q is defined by (4.5). *All implied constants depend at most on $d, k, \eta, \epsilon, C, m$ and the implicit constants in conditions* (1), (2), (3'), (4') and (5')*, and in relations* (4.6) *and* (4.7).

5. Applications of Theorem 4.2

This section is devoted to the proof of Theorems 1.2-1.8.

5.1. **The average Lang-Trotter conjecture.**

We prove here Theorem 1.2. By a dyadic decomposition argument, it is enough to show that

$$\sum_{x<p\leq 2x} \mathbb{P}_{\mathcal{C}_p}(a_p(E)=t) = C_{\mathrm{LT}}(t) \int_x^{2x} \frac{\mathrm{d}u}{2\sqrt{u}\log u} + O_t\left(\frac{\sqrt{x}}{(\log x)^A}\right),$$

We set

$$w_p = f_p(t,p) f_\infty(t,p) = \frac{1}{\pi\sqrt{p}} + O_t\left(\frac{1}{x}\right).$$

Furthermore, we set

$$\delta_\ell(p) = \begin{cases} f_\ell(t,p) - 1 & \text{if } \ell \neq p, \\ 0 & \text{otherwise.} \end{cases} \tag{5.1}$$

[3] The polynomials $F, D_1, \dots, D_k$ and the parameters L and λ_j might depend on X or on some other parameters whose size is controlled by X, and we are majoring here this dependence.

With this notation, we see that

$$\mathbb{P}_{\mathcal{C}_p}(a_p(E)=t) = w_p \prod_{\ell}(1+\delta_\ell(p)). \tag{5.2}$$

We shall apply Theorem 4.2 with $d=k=1$, $\mathcal{A}=\{x<p\le 2x\}$, $\mathcal{G}(\ell)=(\mathbb{Z}/\ell\mathbb{Z})^*$, $F(a)=t^2-4a$, $D_1(a)=a^2(t^2-4a)$ (the factor a^2 is added to guarantee that if $\ell\nmid D_1(a)$, then $a\,(\mathrm{mod}\,\ell)\notin\mathcal{G}(\ell)$), $L=1$ and $X=2x$. We need to check that the necessary conditions are satisfied. Condition (1) holds by definition and conditions (2) and (3') follow from parts (d) and (c) of Theorem 3.2, respectively. Condition (4') holds with

$$\Delta_{\ell^r}(a) = -1 + \frac{\ell^r\phi(\ell^r)\cdot\#\left\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}):\begin{array}{l}\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell^r),\\ \det(\sigma)\equiv a\,(\mathrm{mod}\,\ell^r)\end{array}\right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|},$$

which satisfies conditions (4'a)-(4'd) with average value

$$\begin{aligned}\Delta_\ell &:= -1 + \lim_{r\to\infty}\frac{\ell^r\cdot\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}):\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell^r)\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}\\ &= -1+\frac{\ell\cdot\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}):\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell)\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}.\end{aligned}$$

(Here we use parts (b) and (d) of Theorem 3.2 to see conditions (4'b) and (4'd), respectively.) Finally, it is easy to verify condition (5'), and relation (4.6) follows easily by the Brun-Titchmarsh inequality with $\widetilde{W}=\sqrt{x}/\log x$.

In conclusion, we may apply Theorem 4.2. This will complete the proof of Theorem 1.2, as long as we can control the quantities W, E and M that appear there. We use the Prime Number Theorem to see that

$$\begin{aligned}W=\sum_{x<p\le 2x}w_p &= \frac{2}{\pi}\sum_{x<p\le 2x}\left(\frac{1}{2\sqrt{p}}+O_t\left(\frac{1}{x}\right)\right)\\ &= \frac{2}{\pi}\int_x^{2x}\frac{\mathrm{d}u}{2\sqrt{u}\log u}+O_t\left(\frac{\sqrt{x}}{(\log x)^A}\right).\end{aligned}$$

We use the Bombieri-Vinogradov theorem to see that $E\ll\sqrt{x}/(\log x)^B$ for any fixed B, and finally, we have that

$$M=\max_{n\le -4}\sum_{\substack{x<p\le 2x\\ (t^2-4p)/n\text{ is a square}}}|w_p|\ll\max_{n\le -4}\frac{\#\{m\in\mathbb{Z}:4x<|n|m^2+t^2\le 8x\}}{\sqrt{x}}\ll 1,$$

an estimate that is good enough for our purposes. This completes the proof of Theorem 1.2.

5.2. **The vertical Sato-Tate conjecture.** In this section, we prove Theorem 1.3. Clearly, it suffices to consider the case when $p^{\epsilon-1/2}\le\beta-\alpha\le 2p^{\epsilon-1/2}$; the general case will follow by dividing the interval $[\alpha,\beta]$ into shorter intervals. We start by noting that

$$\mathbb{P}_{\mathcal{C}_p}\left(\alpha\le\frac{a_p(E)}{2\sqrt{p}}\le\beta\right)=\sum_{2\alpha\sqrt{p}\le t\le 2\beta\sqrt{p}}\mathbb{P}_{\mathcal{C}_p}(a_p(E)=t).$$

So here p is fixed and the averaging is performed over $t \in I := [2\alpha\sqrt{p}, 2\beta\sqrt{p}]$. To this end, we let $\mathcal{A} = I \cap \mathbb{Z}$, $\mathcal{G}(\ell) = \mathbb{Z}/\ell\mathbb{Z}$, $w_t = f_\infty(t,p) f_p(t,p)$ and $\delta_\ell(t) = \mathbf{1}_{\ell \neq p} \cdot (f_\ell(t,p) - 1)$, so that

$$\mathbb{P}_{\mathcal{C}_p}\left(\alpha \le \frac{a_p(E)}{2\sqrt{p}} \le \beta\right) = \sum_{t \in \mathcal{A}} w_t \prod_\ell (1 + \delta_\ell(t)).$$

We are going to apply Theorem 4.2 with $k = d = 1$, $D_1(t) = F(t) = t^2 - 4p$, $L = p$ and $X = 2\sqrt{p}$. We need to check that the necessary conditions are satisfied. Condition (1) holds by definition and conditions (2) and (3') follow from parts (d) and (c) of Theorem 3.2, respectively. Condition (4') holds with

$$\Delta_{\ell^r}(t) = -1 + \frac{\ell^r \cdot \# \left\{ \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{c} \mathrm{tr}(\sigma) \equiv t \,(\mathrm{mod}\, \ell^r), \\ \det(\sigma) \equiv p \,(\mathrm{mod}\, \ell^r) \end{array} \right\}}{\# \left\{ \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \det(\sigma) \equiv p \,(\mathrm{mod}\, \ell^r) \right\}}$$

when $\ell \neq p$ and $\Delta_{p^r}(t) = 0$, which satisfies conditions (4'a)-(4'd) with $\Delta_\ell = 0$ (here we use parts (a) and (d) of Theorem 3.2 to see conditions (4'b) and (4'd), respectively). Moreover, it is easy to verify condition (5').

In conclusion, we may indeed apply Theorem 4.2, provided that we verify that (4.6) is satisfied, which is not as obvious as before. We do this below (we shall take $\widetilde{W} = W$), and we also estimate the quantities W, E and M appearing in Theorem 4.2. This is a bit more delicate than in the proof of Theorem 1.2. Without loss of generality, we assume that $\alpha \ge 0$; the case $\alpha < 0$ is treated in an analogous way.

Let $\eta = 1 - \alpha \ge \beta - \alpha \ge p^{-1/2+\epsilon}$. Since $\alpha \ge 0$, we immediately have that

$$\sqrt{1-u^2} \le \sqrt{1-\alpha^2} \asymp \sqrt{\eta} \quad (\alpha \le u \le \beta). \tag{5.3}$$

Moreover, we claim that

$$\frac{2}{\pi}\int_\alpha^\beta \sqrt{1-u^2}\mathrm{d}u \asymp \sqrt{\eta}(\beta - \alpha) \asymp \frac{\sqrt{\eta}}{p^{1/2-\epsilon}}. \tag{5.4}$$

The implicit upper bound follows immediately by (5.3). For the lower bound, we separate two cases. Firstly, if $\beta \le 1 - \eta/2$, then we immediately see that $\sqrt{1-u^2} \asymp \sqrt{\eta}$ for all $u \in [\alpha, \beta]$. Finally, if $\beta \ge 1 - \eta/2 = \alpha + \eta/2$, then $\eta \ge \beta - \alpha \ge \eta/2$. Therefore,

$$\frac{2}{\pi}\int_\alpha^\beta \sqrt{1-u^2}\mathrm{d}u \ge \frac{2}{\pi}\int_\alpha^{\alpha+\eta/2} \sqrt{1-u^2}\,\mathrm{d}u \gg \eta \cdot \sqrt{1-(\alpha+\eta/2)} \asymp \eta \cdot \sqrt{\eta} \asymp \sqrt{\eta}(\beta - \alpha),$$

which completes the proof of (5.4).

Next, for any $q \le p^{\epsilon/2}$ and $a \in \mathbb{Z}$, partial summation implies that

$$\begin{aligned}\sum_{\substack{t\in I\\ t\equiv a \,(\mathrm{mod}\, q)}} f_\infty(t,p) &= \frac{1}{\pi\sqrt{p}}\int_{2\alpha\sqrt{p}}^{2\beta\sqrt{p}} \sqrt{1-\left(\frac{t}{2\sqrt{p}}\right)^2}\,\mathrm{d}\left(\frac{t}{q}+O(1)\right)\\ &= \frac{2}{\pi q}\int_\alpha^\beta \sqrt{1-u^2}\,\mathrm{d}u + O\left(\sqrt{\frac{\eta}{p}}+\frac{1}{\sqrt{p}}\int_{2\alpha\sqrt{p}}^{2\beta\sqrt{p}}\left|\frac{\mathrm{d}}{\mathrm{d}t}\sqrt{1-\left(\frac{t}{2\sqrt{p}}\right)^2}\right|\mathrm{d}t\right)\\ &= \frac{2}{\pi q}\int_\alpha^\beta \sqrt{1-u^2}\,\mathrm{d}u + O\left(\sqrt{\frac{\eta}{p}}\right)\\ &= \left(1+O\left(\frac{q}{p^\epsilon}\right)\right)\frac{2}{\pi q}\int_\alpha^\beta \sqrt{1-u^2}\,\mathrm{d}u.\end{aligned}$$

where we used (5.4) to get the last line. Since $f_p(t,p) = 1 + O(1/p)$, we deduce that

$$\sum_{\substack{t\in I\\ t\equiv a \,(\mathrm{mod}\, q)}} w_t = \left(1+O\left(\frac{q}{p^\epsilon}\right)\right)\frac{2}{\pi q}\int_\alpha^\beta \sqrt{1-u^2}\,\mathrm{d}u.$$

In particular, (4.6) holds for all $q \le p^{\epsilon/2}$ with $\widetilde{W} = W$. Moreover, for the quantity E appearing in the statement of Theorem 4.2, we have that

$$E \ll \frac{e^{(\log\log 2p)^2}}{p^\epsilon}\cdot\int_\alpha^\beta \sqrt{1-u^2}\mathrm{d}u.$$

Finally, for the quantity M, we have the estimate

$$\begin{aligned}M = \max_{n\le -4}\sum_{\substack{t\in\mathcal{A}\\ D(t)/n \text{ is a square}}} w_t &\ll \sqrt{\frac{\eta}{p}}\max_{n\le -4}\#\{(t,m)\in\mathbb{Z} : t^2 - nm^2 = 4p\}\\ &\ll \sqrt{\frac{\eta}{p}} \asymp \frac{1}{p^\epsilon}\cdot\int_\alpha^\beta \sqrt{1-u^2}\,\mathrm{d}u,\end{aligned}$$

which is good enough for our purposes. This completes the proof of Theorem 1.3.

5.3. **Elliptic curves with a prime number of points.** We show here how to prove Theorem 1.4. First, we deal with the proof of (1.9). We have that

$$\begin{aligned}\mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| \text{ prime}) &= \sum_{\substack{q \text{ prime}\\ p^-<q<p^+}} \mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| = q)\\ &= \sum_{\substack{q \text{ prime}\\ p^-<q<p^+}} f_\infty(p+1-q,p)\prod_\ell f_\ell(p+1-q,p)\end{aligned}\tag{5.5}$$

using Theorem 1.1(a). We set $\mathcal{G}(\ell) = (\mathbb{Z}/\ell\mathbb{Z})^*$,

$$\delta_\ell(a) = \begin{cases} f_\ell(p+1-a,p)-1 & \text{if } \ell\nmid pa,\\ 0 & \text{otherwise,}\end{cases}$$

$$\mathcal{A} = \{q \text{ prime} : p^- < q < p^+\}$$

and

$$\begin{aligned} w_q &= f_\infty(p+1-q,p)f_p(p+1-q,p)f_q(p+1-q,p) \\ &= \frac{1}{\pi\sqrt{p}}\sqrt{1-\left(\frac{p+1-q}{2\sqrt{p}}\right)^2}\left(1+O\left(\frac{1}{p}\right)\right). \end{aligned}$$

With this notation, we find that

$$\mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| \text{ prime}) = \sum_{q\in\mathcal{A}} w_q \prod_\ell (1+\delta_\ell(q)).$$

We are going to apply Theorem 4.2 with $d=k=1$, $F(a)=(p+1-a)^2-4p$, $D_1(a)=a^2F(a)$, $L=p$ and $X=2p$. We need to check that the necessary conditions are satisfied. As in the previous applications, condition (1) holds by definition, and conditions (2) and (3') follow immediately by Theorem 3.2. The same result implies that condition (4') holds with

$$\Delta_{\ell^r}(a) = -1 + \frac{\ell^r\cdot\#\left\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l}\mathrm{tr}(\sigma)\equiv p+1-a \pmod{\ell^r},\\ \det(\sigma)\equiv p \pmod{\ell^r}\end{array}\right\}}{\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \det(\sigma)\equiv p \pmod{\ell^r}\}}$$

if $\ell\neq p$ and with $\Delta_{p^r}(a)=0$, which satisfies condition (4'c) with

$$\begin{aligned} \Delta_\ell &= -1 + \lim_{r\to\infty}\frac{\ell^r\cdot\#\left\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l}(\det(\sigma)+1-\mathrm{tr}(\sigma),\ell^r)=1,\\ \det(\sigma)\equiv p \pmod{\ell^r}\end{array}\right\}}{\phi(\ell^r)\cdot\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \det(\sigma)\equiv p \pmod{\ell^r}\}} \\ &= -1 + \frac{\ell}{\ell-1}\cdot\frac{\#\left\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \begin{array}{l}(\det(\sigma)+1-\mathrm{tr}(\sigma),\ell)=1,\\ \det(\sigma)\equiv p \pmod{\ell}\end{array}\right\}}{\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(\sigma)\equiv p \pmod{\ell}\}} \end{aligned}$$

when $\ell\neq p$ and with $\Delta_p=0$. Finally, it is easy to see that condition (5') holds too, and relation (4.6) follows easily by the Brun-Titchmarsh inequality with $\widetilde{W}=1/\log p$.

In conclusion, we have shown that Theorem 4.2 is indeed applicable. This will complete the proof of (1.9), as long as we can control the quantities W, M and E there. For M, we have that

$$\begin{aligned} M &= \max_{n\le -4}\sum_{\substack{p^-<q<p^+\\ D_1(q)/n \text{ is a square}}} w_q \\ &\ll \max_{n\le-4}\frac{\#\{(q,m):(p+1-q)^2-nm^2=4p\}}{\sqrt{p}} \ll \frac{1}{\sqrt{p}}, \end{aligned} \tag{5.6}$$

an estimate that is good enough for our purposes. Finally, for W and for E, we use the following result with $N=p$.

Lemma 5.1. *For $1\le b\le h\le\sqrt{N}$ and $(a,b)=1$, we have that*

$$\sum_{\substack{N^-<q<N^+\\ q \text{ prime}\\ q\equiv a \pmod b}}\sqrt{1-\left(\frac{N+1-q}{2\sqrt{N}}\right)^2} = \frac{\pi\sqrt{N}}{\phi(b)\log N} + O\left(\frac{h}{b}+\frac{1}{h\log N}\int_{N^-}^{N^+}E(y,h;b)\mathrm{d}y\right),$$

where $E(y,h;b)$ is defined in (1.6).

Proof. This result follows by Lemma 7.1 in [9], since if $N = m^2 k$ and $q \in (N^-, N^+)$, then the quantity $d(q)$ there equals

$$d(q) = \frac{(N+1-q)^2 - 4N}{m^2} = 4k \cdot \left(\left(\frac{N+1-p}{2\sqrt{N}} \right)^2 - 1 \right).$$

□

Lemma 5.1 then implies that, for any $h \in [p^\epsilon, \sqrt{p}/(\log p)^{2A+1}]$, we have

$$W = \frac{1}{\log p} + O\left(\frac{1}{(\log p)^{2A+1}} + \frac{1}{\sqrt{p}\log p} \int_{p^-}^{p^+} \frac{E(y,h;1)}{h} \mathrm{d}y \right)$$

and

$$\begin{aligned} E &\ll \sum_{b \le e^{(\log\log 2p)^2}} \left(\frac{1}{(\log p)^{2A+1} b} + \frac{1}{\sqrt{p}\log p} \int_{p^-}^{p^+} \frac{E(y,h;b)}{h} \mathrm{d}y \right) \\ &\ll \frac{1}{(\log p)^{2A}} + \sum_{b \le e^{(\log\log 2p)^2}} \frac{1}{\sqrt{p}\log p} \int_{p^-}^{p^+} \frac{E(y,h;b)}{h} \mathrm{d}y. \end{aligned}$$

So, relation (1.9) follows.

Next, we pass to the proof of relations (1.10) and (1.11). In both of these estimates, we note that, by a dyadic decomposition argument, we may restrict the range of p to the interval $(x/2, x]$. Relation (1.10) is then an easy consequence of Lemma 7.1 below and of (1.9) with $h = x^{1/3}$, say. Finally, we prove (1.11), which has been reduced to proving that

$$\sum_{x/2 < p \le x} \mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| \text{ is prime}) = C_{\text{twin}} \int_{x/2}^{x} \frac{\mathrm{d}u}{\log^2 u} + O_A\left(\frac{x}{(\log x)^A} \right).$$

We could use (1.10) or we could work directly with a sum over two primes, p and q. We choose the second approach. As before, our starting point is (5.5). We then set $\mathcal{G}(\ell) = (\mathbb{Z}/\ell\mathbb{Z})^* \times (\mathbb{Z}/\ell\mathbb{Z})^*$ and

$$\delta_{a,b}(\ell) = \begin{cases} f_\ell(a+1-b, a) - 1 & \text{if } \ell \nmid ab, \\ 0 & \text{otherwise,} \end{cases}$$

$$\mathcal{A} = \{(p,q) : x/2 < p \le x, \ |q-p-1| < 2\sqrt{p}\},$$

and

$$\begin{aligned} w_{p,q} &= f_\infty(p+1-q, p) f_p(p+1-q, p) f_q(p+1-q, p) \\ &= \frac{1}{\pi\sqrt{p}} \sqrt{1 - \left(\frac{p+1-q}{2\sqrt{p}} \right)^2} \left(1 + O\left(\frac{1}{x} \right) \right). \end{aligned}$$

With this notation, we find that

$$\sum_{x/2 < p \le x} \mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| \text{ prime}) = \sum_{(p,q) \in \mathcal{A}} w_{p,q} \prod_{\ell} (1 + \delta_\ell(p,q)).$$

We are going to apply Theorem 4.2 with $d = 2$, $k = 1$, $F(a,b) = (a+1-b)^2 - 4a$, $D_1(a,b) = a^2 b^2 F(a,b)$, $L = 1$ and $X = 2x$. We need to check that the necessary conditions are satisfied. As in the previous applications, condition (1) holds by definition, and conditions (2), (3') and (4') follow by Theorem 3.2 with

$$\Delta_{\ell^r}(a,b) = -1 + \frac{\phi(\ell^r)\ell^r \cdot \#\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{c}\det(\sigma) \equiv a \pmod{\ell^r}, \\ \det(\sigma)+1-\mathrm{tr}(\sigma) \equiv b \pmod{\ell^r}\end{array}\right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|},$$

which satisfies condition (4'c) with

$$\begin{aligned}\Delta_\ell &= -1 + \lim_{r\to\infty} \frac{\ell^r \cdot \#\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : (\det(\sigma)+1-\mathrm{tr}(\sigma), \ell^r) = 1\}}{\phi(\ell^r)\cdot|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|} \\ &= -1 + \frac{\ell}{\ell-1}\frac{\#\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(\sigma)+1-\mathrm{tr}(\sigma) \not\equiv 0 \pmod{\ell}\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}.\end{aligned}$$

Finally, condition (5') is easy to verify too, and relation (4.6) follows easily by the Brun-Titchmarsh inequality with $\widetilde{W} = x/(\log x)^2$.

In conclusion, we have shown that Theorem 4.2 is indeed applicable. This will complete the proof of Theorem 1.4, as long as we can control the quantities W, M and E there. The estimation of W and of E will be carried out in Lemma 7.2 below. Finally, we have that $M \ll \sqrt{x}$, as in (5.6). So relation (1.11) follows.

5.4. **Elliptic curves with a given number of points.** We demonstrate here Theorem 1.8. In view of Theorem 1.1, we have that

$$\sum_p \mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| = N) = \sum_{N^- < p < N^+} f_\infty(p+1-N,p)\prod_\ell f_\ell(N,p).$$

We let $\mathcal{G}(\ell) = (\mathbb{Z}/\ell\mathbb{Z})^*$, $\mathcal{A} = \{p \text{ prime} : |p-1-N| < 2\sqrt{N}\}$ and

(5.7)
$$\begin{aligned}w_p = f_\infty(p+1-N,p)f_p(p+1-N,p) &= \frac{\sqrt{4p-(p+1-N)^2}}{2\pi p}\left(1+O\left(\frac{1}{N}\right)\right) \\ &= \frac{\sqrt{4N-(N+1-p)^2}}{2\pi p}\left(1+O\left(\frac{1}{N}\right)\right) \\ &= \frac{1}{\pi\sqrt{N}}\sqrt{1-\left(\frac{N+1-p}{2\sqrt{N}}\right)^2}\left(1+O\left(\frac{1}{\sqrt{N}}\right)\right)\end{aligned}$$

for $p \in (N^-, N^+)$. Moreover, we set

$$\delta_\ell(a) = \begin{cases} f_\ell(a+1-N,a)-1 & \text{if } \ell \nmid a, \\ 0 & \text{otherwise,}\end{cases}$$

so that

$$\sum_p \mathbb{P}_{\mathcal{C}_p}(|E(\mathbb{F}_p)| = N) = \sum_{p\in\mathcal{A}} w_p \prod_\ell (1+\delta_\ell(p)).$$

We are going to apply Theorem 4.2 with $d = k = 1$ and $F(x) = (x+1-N)^2 - 4x = (x-1-N)^2 - 4N$, $D_1(x) = x^2F(x)$, $L = 1$ and $X = 2N$. We need to check that the necessary conditions are satisfied. Condition (1) holds by definition, and conditions (2), (3') and (4') follow by Theorem 3.2, as before, with

$$\Delta_{\ell^r}(a) = -1 + \frac{\ell^r \phi(\ell^r) \cdot \# \left\{ \sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l} \det(\sigma) \equiv a \pmod{\ell^r}, \\ \mathrm{tr}(\sigma) \equiv \det(\sigma) + 1 - N \pmod{\ell^r} \end{array} \right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}$$

and

$$\Delta_\ell = -1 + \lim_{r\to\infty} \frac{\ell^r \cdot \#\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \mathrm{tr}(\sigma) \equiv \det(\sigma) + 1 - N \pmod{\ell^r}\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}.$$

Finally, it is easy to verify condition (5') too, and relation (4.6) follows easily by the Brun-Titchmarsh inequality with $\widetilde{W} = 1/\log N$.

In conclusion, we have shown that Theorem 4.2 is indeed applicable. This will complete the proof of Theorem 1.5, as long as we can control the quantities W, M and E in Theorem 4.2. For M, we have that

$$\begin{aligned} M &= \max_{n\le -4} \sum_{\substack{p\in\mathcal{A} \\ D(p)/n \text{ is a square}}} w_p \\ &\ll \max_{n\le -4} \frac{\#\{(p,m)\in\mathbb{N}^2 : (p-1-N)^2 - nm^2 = 4N\}}{\sqrt{N}} \ll_\epsilon N^{-1/2+\epsilon}, \end{aligned}$$

an estimate that is good enough for our purposes. Finally, we need to estimate W and E. This is accomplished using Lemma 5.1, as in the proof of relation (1.9) in Section 5.3 above.

5.5. **Elliptic aliquot cycles.** In this subsection, we prove Theorem 1.6. By a dyadic decomposition argument, it suffices to show that

$$\sum_{\boldsymbol{p}\in\mathcal{P}'_d(x)} \alpha_d(\boldsymbol{p}) = C_{\text{aliquot}}^{(d)} \int_x^{2x} \frac{\mathrm{d}u}{2\sqrt{u}(\log u)^d} + O_A\left(\frac{\sqrt{x}}{(\log x)^A}\right),$$

where

$$\mathcal{P}'_d(x) := \{(p_1,\dots,p_d) : x < p_1 \le 2x,\ |p_{j+1} - p_j - 1| < 2\sqrt{p_j}\ (1\le j\le d) \text{ with } p_{d+1} = p_1\}.$$

Theorem 1.1(a) implies that

$$\alpha_d(\boldsymbol{p}) = \prod_{j=1}^d \left(f_\infty(p_j + 1 - p_{j+1}, p_j) \prod_\ell f_\ell(p_j + 1 - p_{j+1}, p_j) \right) = w_{\boldsymbol{p}} \prod_\ell (1 + \delta_\ell(\boldsymbol{p})),$$

where

$$\begin{aligned} w_{\boldsymbol{p}} &:= \prod_{j=1}^d \prod_{\ell\in\{p_1,\dots,p_d,\infty\}} f_\ell(p_j + 1 - p_{j+1}, p_j) \\ &= \prod_{j=1}^d \frac{1}{\pi\sqrt{p_j}} \sqrt{1 - \left(\frac{p_j + 1 - p_{j+1}}{2\sqrt{p_j}}\right)^2} \left(1 + O\left(\frac{1}{x}\right)\right) \end{aligned}$$

and $\delta_\ell(\boldsymbol{p})$ is defined as

$$\delta_\ell(\boldsymbol{p}) := \begin{cases} -1 + \prod_{j=1}^d f_\ell(p_j + 1 - p_{j+1}, p_j) & \text{if } \ell \nmid p_1\cdots p_d, \\ 0 & \text{otherwise.} \end{cases}$$

We are going to apply Theorem 4.2 with d, the length of the aliquot cycle here, playing the role of the dimension d there. We also take $k = d$,

$$D_j(x_1, \dots, x_d) = x_j^2((x_j + 1 - x_{j+1})^2 - 4x_j) \quad (1 \le j \le d,\ x_{d+1} = x_1),$$

$F(\boldsymbol{x}) = \prod_{j=1}^{k}((x_j+1-x_{j+1})^2-4x_j)$, $L = 1$ and $X = 3x$. We need to check that the necessary conditions are satisfied. As in the previous examples, condition (1) holds by definition, and conditions (2) and (3') follow immediately by Theorem 3.2. Next, we check condition (4'). If $\boldsymbol{a} = (a_1, \dots, a_d) \in \mathbb{Z}^d$, then we set

$$\Delta_{\ell^r}(\boldsymbol{a}) = -1 + \frac{\phi(\ell^{2r})^d \cdot \# \left\{ \boldsymbol{\sigma} \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})^d : \begin{array}{l} \det(\sigma_j) \equiv a_j \pmod{\ell^r} \quad \text{and} \\ \det(\sigma_j) + 1 - \mathrm{tr}(\sigma_j) \equiv \det(\sigma_{j+1}) \pmod{\ell^r} \\ \text{for } 1 \le j \le d, \text{ where } \sigma_{d+1} = \sigma_1 \end{array} \right\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|^d}.$$

Theorem 3.2 implies that conditions (4'a), (4'b) and (4'd) are satisfied. We also need to prove that (4'c) holds, that is to to say that the limit

$$\Delta_\ell := -1 + \lim_{r \to \infty} \frac{\ell^{rd} \cdot \# \left\{ \boldsymbol{\sigma} \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})^d : \begin{array}{l} \det(\sigma_j) + 1 - \mathrm{tr}(\sigma_j) \equiv \det(\sigma_{j+1}) \pmod{\ell^r} \\ \text{for } 1 \le j \le d, \text{ where } \sigma_{d+1} = \sigma_1 \end{array} \right\}}{|\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|^d}.$$

exists. As noticed in the remark after the statement of Theorem 1.6, this step was not necessary in the proof of the other theorems as the limits were stabilizing for small values of r (often $r = 1$), which does not seem the case for aliquot cycles.

In view of Theorem 3.2(a), proving that the sequence

$$T_r := \frac{1}{\ell^{rd}} \sum_{\boldsymbol{a} \in (\mathbb{Z}/\ell^r\mathbb{Z})^d} \prod_{m=1}^{d} \left(1 + \sum_{j=1}^{\min\{r, \nu_\ell(G_m(\boldsymbol{a}))+1\}} \frac{N_{G_m(\boldsymbol{a})}(\ell^j) - N_{G_m(\boldsymbol{a})}(\ell^{j-1})}{\ell^j} \right)$$

where $G_m(\boldsymbol{a}) := (a_m + 1 - a_{m+1})^2 - 4a_m$, is convergent suffices to conclude that Δ_ℓ is well-defined. We will show that $(T_r)_{r \ge 1}$ is a Cauchy sequence. To this end, we consider two large integers $r > s$ and relate T_r to T_s. We note that

$$(5.8)\quad T_r = \frac{1}{\ell^{rd}} \sum_{\boldsymbol{a} \in (\mathbb{Z}/\ell^r\mathbb{Z})^d} \prod_{m=1}^{d} \left(1 + \sum_{j=1}^{\min\{s, \nu_\ell(G_m(\boldsymbol{a}))+1\}} \frac{N_{G_m(\boldsymbol{a})}(\ell^j) - N_{G_m(\boldsymbol{a})}(\ell^{j-1})}{\ell^j} \right) + o_{s \to \infty}(1).$$

Indeed, either $\nu_\ell(G_m(\boldsymbol{a})) \le s-1 \le r$ for all m, in which case there is nothing to prove for that summand, or $\min\{v_\ell(G_m(\boldsymbol{a})) + 1, r\} \ge s$ for some m, in which case we use the elementary bound $N_D(\ell^j) \ll \ell^{j/2}$ to control the size of the tails of sum over j in the definition of T_r. Now, note that the main term in (5.8) only depends on $G_m(\boldsymbol{a}) \pmod{\ell^s}$, that is to say on $\boldsymbol{a} \pmod{\ell^s}$. Therefore

$$\begin{aligned} T_r &= \frac{1}{\ell^{sd}} \sum_{\boldsymbol{a} \in (\mathbb{Z}/\ell^s\mathbb{Z})^d} \prod_{m=1}^{d} \left(1 + \sum_{j=1}^{\min\{s, \nu_\ell(D_m(\boldsymbol{a}))+1\}} \frac{N_{D_m(\boldsymbol{a})}(\ell^j) - N_{D_m(\boldsymbol{a})}(\ell^{j-1})}{\ell^j} \right) + o_{s \to \infty}(1) \\ &= T_s + o_{s \to \infty}(1), \end{aligned}$$

which means that $(T_r)_{r \ge 1}$ is a Cauchy sequence, so a convergent sequence. So condition (4') does hold.

Finally, it is easy to verify condition (5') too, and relation (4.6) follows easily by the Brun-Titchmarsh inequality with $\widetilde{W} = \sqrt{x}/(\log x)^d$. In conclusion, Theorem 4.2 is indeed applicable. This completes the proof of Theorem 1.6, as long as we can control the quantities W, M and E there. The estimation of W and of E will be carried out in Lemma 7.2 below. Finally, we note that $M \le M_1 + \cdots + M_d$, where

$$M_j = \max_{n \le -4} \sum_{\substack{\boldsymbol{p} \in \mathcal{P}_d'(x) \\ ((p_j+1-p_{j+1})^2 - 4x_j)/n \text{ is a square}}} w_{\boldsymbol{p}},$$

and we bound each of the M_j's individually. We shall demonstrate the argument for M_1, the details for the estimation of $M_2, \ldots, M_d$ being very similar. We make the change of variables $h_i = p_i - p_{i-1}$ for $i \in \{2, \ldots, d\}$. Then $(p_1 + 1 - p_2)^2 - 4p_1 = (h_2 - 1)^2 - 4p_1$, so that

$$M_1 \ll \max_{n \le -4} \frac{\# \left\{ (p_1, h_2, \ldots, h_d) \in \mathbb{Z}^d : \begin{array}{c} 1 \le p_1 \le x, \ |h_i| \ll \sqrt{x} \ (2 \le i \le d) \\ ((h_2-1)^2 - 4p_1)/n \text{ is a square} \end{array} \right\}}{x^{d/2}} \ll 1,$$

which we obtain by noting that, for fixed $h_2, \ldots, h_d$, there are always $\ll \sqrt{x}$ choices for p_1. Similarly, we may show that $M_j \ll 1$, $2 \le j \le d$. We conclude that $M \ll 1$, an estimate that is good enough for our purposes. This completes the proof of Theorem 1.6.

5.6. **Elliptic curves with a given group structure.** We demonstrate here Theorem 1.8. We recall that $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$. In view of Theorem 1.7, we have that

$$\sum_p \mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \cong G) = \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} f_\infty(G, p) \prod_\ell f_\ell(G, p).$$

We let

$$\mathcal{A} = \left\{ \frac{p-1}{m} : p \text{ prime}, \ p \equiv 1 \,(\mathrm{mod}\, m), \ N^- < p < N^+ \right\}$$

and

$$\mathcal{G}(\ell) = \{ a \in \mathbb{Z}/\ell\mathbb{Z} : 1 + am \not\equiv 0 \,(\mathrm{mod}\, \ell) \}.$$

Moreover, if $a \in \mathcal{A}$ and $p = 1 + am$ is the associated prime, then we define

$$w_a = f_\infty(G, p) f_p(G, p) = \frac{1}{\pi\sqrt{N}} \sqrt{1 - \left(\frac{N+1-p}{2\sqrt{N}} \right)^2} \left(1 + O\left(\frac{1}{\sqrt{N}} \right) \right)$$

for $p \in (N^-, N^+)$, as in (5.7). Finally, we set $\nu_\ell = \nu_\ell(m)$ and

$$\delta_\ell(a) = \begin{cases} -1 + \ell^{\nu_\ell} \cdot f_\ell(G, 1+am) & \text{if } \ell \nmid 1 + am \\ 0 & \text{otherwise,} \end{cases}$$

so that

$$\sum_p \mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \cong G) = \frac{1}{m} \sum_{a \in \mathcal{A}} w_{\boldsymbol{a}} \prod_\ell (1 + \delta_\ell(a)). \tag{5.9}$$

If $\ell \nmid 1+am$, then applying Theorem 3.2(b) with $t = p+1-N = am - m^2k + 2$, $u = 1+am$ and $n = m$, so that $t_1 = a - mk$ and $u_1 = k$, implies that

$$1 + \delta_\ell(a) = \lim_{r\to\infty} \frac{\ell^r \phi(\ell^r) \cdot \# \left\{ \sigma \in M_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l} \operatorname{tr}(\sigma) \equiv a - mk \,(\operatorname{mod} \ell^r), \\ \det(\sigma) \equiv k \,(\operatorname{mod} \ell^r) \\ \sigma \not\equiv 0 \,(\operatorname{mod} \ell) \end{array} \right\}}{|\operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}. \tag{5.10}$$

Moreover, the same result implies that the above limit stabilizes for $r > \nu_\ell((a+mk)^2 - 4k)$.

We are going to apply Theorem 4.2 with the parameters d and k there both equal to 1, $F(a) = (a-mk)^2 - 4k$, $D_1(a) = (1+am)^2F(a)$, $L = 1$ and $X = 2\sqrt{k}$. (We allow ourself a slight double notation for one line here, as the k in the definition of D_1, F and X is the k from the statement of Theorem 1.8, not the parameter in Theorem 4.2.) We need to check that the necessary conditions are satisfied. As before, condition (1) holds by definition, and conditions (2) and (3') follow immediately by Theorem 3.2. Next, in view of relation (5.10), we take

$$\Delta_{\ell^r}(a) = -1 + \frac{\phi(\ell^r)\ell^r \cdot \# \left\{ \sigma \in M_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l} \operatorname{tr}(\sigma) \equiv a - mk \,(\operatorname{mod} \ell^r), \\ \det(\sigma) \equiv k \,(\operatorname{mod} \ell^r) \\ \sigma \not\equiv 0 \,(\operatorname{mod} \ell) \end{array} \right\}}{|\operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}.$$

Note that $\det(I + m\sigma) \equiv 1 + m\operatorname{tr}(\sigma) + m^2\det(\sigma) \equiv 1 + am \,(\operatorname{mod} \ell)$, so we naturally take

$$\begin{aligned} \Delta_\ell &= -1 + \lim_{r\to\infty} \frac{\phi(\ell^r)\ell^r \cdot \# \left\{ \begin{array}{l} \sigma \in M_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \ell \nmid \det(I+m\sigma) \end{array} : \begin{array}{l} \det(\sigma) \equiv k \,(\operatorname{mod} \ell^r) \\ \sigma \not\equiv 0 \,(\operatorname{mod} \ell) \end{array} \right\}}{|\mathcal{G}(\ell^r)| \cdot |\operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|} \\ &= -1 + \frac{\phi(\ell^{\nu_\ell})}{\ell^{\nu_\ell}} \lim_{r\to\infty} \frac{\ell^r \cdot \# \left\{ \begin{array}{l} \sigma \in M_2(\mathbb{Z}/\ell^r\mathbb{Z}) \\ \ell \nmid \det(I+m\sigma) \end{array} : \begin{array}{l} \det(\sigma) \equiv k \,(\operatorname{mod} \ell^r) \\ \sigma \not\equiv 0 \,(\operatorname{mod} \ell) \end{array} \right\}}{|\operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|} \\ &= -1 + \frac{\phi(\ell^{\nu_\ell})}{\ell^{5\nu_\ell}} \lim_{r\to\infty} \frac{\ell^r \cdot \# \left\{ \begin{array}{l} \sigma \in M_2(\mathbb{Z}/\ell^{r+\nu_\ell}\mathbb{Z}) \\ \ell \nmid \det(I+m\sigma) \end{array} : \begin{array}{l} \det(\sigma) \equiv k \,(\operatorname{mod} \ell^r) \\ \sigma \not\equiv 0 \,(\operatorname{mod} \ell) \end{array} \right\}}{|\operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}, \end{aligned}$$

where we used the formula $|\mathcal{G}(\ell^r)| = \phi(\ell^r)\ell^{\nu_\ell}/\phi(\ell^{\nu_\ell})$ to get from the first line to the second line. Making the change of variable $g = I + m\sigma$, which determines g mod $\ell^{r+2\nu_\ell}$, we find that

$$\begin{aligned} \Delta_\ell &= -1 + \frac{\phi(\ell^{\nu_\ell})}{\ell^{5\nu_\ell}} \lim_{r\to\infty} \frac{\ell^r \cdot \# \left\{ g \in \operatorname{GL}_2(\mathbb{Z}/\ell^{r+2\nu_\ell}\mathbb{Z}) : \begin{array}{l} \det(g) + 1 - \operatorname{tr}(g) \equiv N \,(\operatorname{mod} \ell^{r+2\nu_\ell}) \\ g \equiv I \,(\operatorname{mod} \ell^{\nu_\ell}) \\ g \not\equiv I \,(\operatorname{mod} \ell^{\nu_\ell+1}) \end{array} \right\}}{|\operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|} \\ &= -1 + \phi(\ell^{2\nu_\ell}) \lim_{r\to\infty} \frac{\ell^r \cdot \# \left\{ g \in \operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l} \det(g) + 1 - \operatorname{tr}(g) \equiv N \,(\operatorname{mod} \ell^r) \\ g \equiv I \,(\operatorname{mod} \ell^{\nu_\ell}) \\ g \not\equiv I \,(\operatorname{mod} \ell^{\nu_\ell+1}) \end{array} \right\}}{|\operatorname{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}. \end{aligned}$$

Finally, it is easy to verify condition (5') too, and relation (4.6) follows easily by the Brun-Titchmarsh inequality with $\widetilde{W} = 1/(\phi(m)\log k)$.

In conclusion, we have show that Theorem 4.2 is indeed applicable. Theorem 1.8 then follows as long as we can control the quantities W, M and E in the statement of Theorem 4.2. For M, we have that

$$\begin{aligned} M &\le \max_{n\le -4} \sum_{\substack{a\in\mathcal{A} \\ D_1(a)/n \text{ is a square}}} w_a \\ &\ll \max_{n\le -4} \frac{\#\{(a,b)\in\mathbb{N}^2 : (a-mk)^2-nb^2=4k\}}{\sqrt{N}} \ll_\epsilon \frac{k^\epsilon}{\sqrt{N}}, \end{aligned}$$

an estimate that is good enough for our purposes. an estimate that is good enough for our purposes. Finally, the quantities W and E are estimated using Lemma 5.1, as in the proof of relation (1.9) in Section 5.3 above. For $h\in[mk^\epsilon,\sqrt{N}/(\log k)^{2A+1}]$, we have

$$\begin{aligned} W = \sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} &= \sum_{\substack{N^-<p<N^+ \\ p\equiv 1\,(\mathrm{mod}\,m)}} \frac{1}{\pi\sqrt{N}}\sqrt{1-\left(\frac{N+1-p}{2\sqrt{N}}\right)^2}\left(1+O\left(\frac{1}{\sqrt{N}}\right)\right) \\ &= \frac{1}{\phi(m)\log N} + O\left(\frac{1}{m(\log N)^{2A+1}} + \frac{1}{\sqrt{N}\log N}\int_{N^-}^{N^+}\frac{E(y,h;m)}{h}\mathrm{d}y\right). \end{aligned}$$

Similarly, if $(1+bm,q)=1$, then

$$\begin{aligned} \sum_{\substack{\boldsymbol{a}\in\mathcal{A} \\ \boldsymbol{a}\equiv b\,(\mathrm{mod}\,q)}} w_{\boldsymbol{a}} &= \sum_{\substack{N^-<p<N^+ \\ p\equiv 1+bm\,(\mathrm{mod}\,qm)}} \frac{1}{\pi\sqrt{N}}\sqrt{1-\left(\frac{N+1-p}{2\sqrt{N}}\right)^2}\left(1+O\left(\frac{1}{\sqrt{N}}\right)\right) \\ &= \frac{1}{\phi(qm)\log N} + O\left(\frac{1}{qm(\log N)^{2A+1}}\right) \\ &\quad + O\left(\frac{1}{h\sqrt{N}\log N}\int_{N^-}^{N^+} E(y,h;qm)\mathrm{d}y\right). \end{aligned}$$

Since $\phi(qm)=|\mathcal{G}(q)|\phi(m)$, we deduce that

$$E \ll \frac{1}{m(\log k)^{2A}} + \frac{R(N,h;m)}{\phi(m)\log N}$$

This completes the proof of Theorem 1.8.

5.7. **Elliptic curves with a cyclic group of points.** We demonstrate here Theorem 1.9. In view of Theorem 1.7, we have that

$$\begin{aligned} \mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \text{ is cyclic}) &= \sum_{p^-<k<p^+} \mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p)\cong\mathbb{Z}/k\mathbb{Z}) \\ &= \sum_{p^-<k<p^+} f_\infty(p+1-k,p)\prod_\ell f_\ell(\mathbb{Z}/k\mathbb{Z},p). \end{aligned}$$

We let $\mathcal{G}(\ell)=\mathbb{Z}/\ell\mathbb{Z}$, $\mathcal{A}=(p^-,p^+)\cap\mathbb{Z}$, $w_k=f_\infty(p+1-k,p)f_p(p+1-k,p)$ and $\delta_\ell(k)=\mathbf{1}_{\ell\ne p}\cdot(f_\ell(p+1-\mathbb{Z}/k\mathbb{Z},p)-1)$, so that

$$\mathbb{P}_{\mathcal{C}_p}(E(\mathbb{F}_p) \text{ is cyclic}) = \sum_{k\in\mathcal{A}} w_k\prod_\ell(1+\delta_\ell(k)).$$

We are going to apply Theorem 4.2 with the parameters d and k both equal to 1, and with $D_1(x) = F(x) = (p+1-x)^2 - 4p$, $L = p$ and $X = 2p$. We need to check that the necessary conditions are satisfied. Condition (1) holds by definition, and conditions (2), (3') and (4') follow by Theorem 3.2 with

$$\Delta_{\ell^r}(a) = -1 + \frac{\phi(\ell^r)\ell^r \cdot \#\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l} \mathrm{tr}(\sigma) \equiv p+1-k \,(\mathrm{mod}\,\ell^r), \\ \det(\sigma) \equiv p \,(\mathrm{mod}\,\ell^r), \\ \sigma \not\equiv I \,(\mathrm{mod}\,\ell) \end{array}\right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}$$

when $\ell \nmid p$ and with $\Delta_{p^r}(a) = 0$, which satisfies condition (4'c) with

$$\begin{aligned}\Delta_\ell &= -1 + \lim_{r\to\infty} \frac{\phi(\ell^r) \cdot \#\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l} \det(\sigma) \equiv p \,(\mathrm{mod}\,\ell^r), \\ \sigma \not\equiv I \,(\mathrm{mod}\,\ell) \end{array}\right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|} \\ &= -\lim_{r\to\infty} \frac{\phi(\ell^r) \cdot \#\left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z}) : \begin{array}{l} \det(\sigma) \equiv p \,(\mathrm{mod}\,\ell^r), \\ \sigma \equiv I \,(\mathrm{mod}\,\ell) \end{array}\right\}}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})|}\end{aligned}$$

when $\ell \neq p$ and with $\Delta_p = 0$. Finally, condition (5') is easy to verify too, and relation (4.6) holds with $\widetilde{W} = 1$.

Before we proceed further, note that

$$\Delta_\ell = -\frac{\mathbf{1}_{\ell|(p-1)}}{\ell(\ell^2-1)}.$$

It's easy to see that this is true when $\ell \nmid p-1$ (the condition $\sigma \equiv I \,(\mathrm{mod}\,\ell)$ would imply $\det(\sigma) \equiv 1 \,(\mathrm{mod}\,\ell)$). Finally, if $\ell | p-1$, then note that $\#\{\tau \in M_2(\mathbb{Z}/\ell^{r-1}\mathbb{Z}) : \det(I + \ell\tau) \equiv p \,(\mathrm{mod}\,\ell^r)\} = \ell^{3(r-1)}$. Therefore

$$\Delta_\ell = -\phi(\ell^r)\frac{\ell^{3(r-1)}}{\ell^{4(r-1)}(\ell^2-\ell)(\ell^2-1)} = -\frac{\ell-1}{(\ell^2-\ell)(\ell^2-1)} = -\frac{1}{\ell(\ell^2-1)},$$

as claimed.

In conclusion, we have shown that Theorem 4.2 is indeed applicable. This will complete the proof of Theorem 1.9, as long as we can control the quantities W, M and E in Theorem 4.2. For M, we have that

$$\begin{aligned} M &= \max_{n \le -4} \sum_{\substack{p^- < k < p^+ \\ D(k)/n \text{ is a square}}} w_k \\ &\ll \max_{n\le -4} \frac{\#\{(k,m) \in \mathbb{N}^2 : (p+1-k)^2 - nm^2 = 4p\}}{\sqrt{p}} \ll p^{-1/2}, \end{aligned}$$

an estimate that is good enough for our purposes. Finally, we need to estimate W and E. By partial summation, we have that

$$\sum_{\substack{p^- < k < p \\ k \equiv a \,(\mathrm{mod}\, q)}} w_k = \frac{1}{\pi\sqrt{p}} \int_{p^-}^{p^+} \sqrt{1 - \left(\frac{p+1-t}{2\sqrt{p}}\right)^2}\, \mathrm{d}\left(\frac{t}{q} + O(1)\right) = \frac{1}{q} + O\left(\frac{1}{\sqrt{p}}\right).$$

So Theorem 1.9 follows.

5.8. **Restricting the trace to an arithmetic progression.** We demonstrate here Theorem 2.2. Again, Theorem 1.1 implies that

$$\begin{aligned}\mathbb{P}_{\mathcal{C}_p}(a_p(E)\equiv t\,(\mathrm{mod}\,N)) &= \sum_{\substack{p^-<s<p^+\\ s\equiv t\,(\mathrm{mod}\,N)}} \mathbb{P}_{\mathcal{C}_p}(a_p(E)=s)\\ &= \sum_{\substack{p^-<s<p^+\\ s\equiv t\,(\mathrm{mod}\,N)}} f_\infty(s,p)\prod_{\ell} f_\ell(s,p).\end{aligned}$$

We let $\mathcal{G}(\ell)=\mathbb{Z}/\ell\mathbb{Z}$, $\mathcal{A}=\{a\in\mathbb{Z}: p^-<t+aN<p^+\}$, $w_a=f_\infty(t+Na,p)f_p(t+Na,p)$ and $\delta_\ell(a)=\mathbf{1}_{\ell\neq p}\cdot(f_\ell(t+Na,p)-1)$, so that

$$\mathbb{P}_{\mathcal{C}_p}(a_p(E)\equiv t\,(\mathrm{mod}\,N))=\sum_{a\in\mathcal{A}} w_a\prod_{\ell}(1+\delta_\ell(a)).$$

We let $g=(t^2-4p,N)$. We are going to apply Theorem 4.2 with $d=k=1$, $D_1(x)=(t+Na)^2-4p$, $F(x)=D_1(x)/g$, $L=p$ and $X=2p$. We need to check that the necessary conditions are satisfied. Condition (1) holds by definition, and conditions (2), (3') and (4') follow by Theorem 3.2 with

$$\Delta_{\ell^r}(a)=-1+\frac{\ell^{r+\nu_\ell(g)}\cdot\#\left\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^{r+\nu_\ell(g)}\mathbb{Z}):\begin{array}{l}\mathrm{tr}(\sigma)\equiv t+Na\,(\mathrm{mod}\,\ell^{r+\nu_\ell(g)}),\\ \det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^{r+\nu_\ell(g)})\end{array}\right\}}{\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^{r+\nu_\ell(g)}\mathbb{Z}):\det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^{r+\nu_\ell(g)})\}}$$

when $\ell\neq p$ and with $\Delta_{p^r}(a)=0$, which satisfies condition (4'c) with

$$\Delta_\ell=-1+\lim_{r\to\infty}\frac{\ell^{\nu_\ell(N)}\cdot\#\left\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^{r+\nu_\ell(g)}\mathbb{Z}):\begin{array}{l}\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell^{\nu_\ell(N)}),\\ \det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^{r+\nu_\ell(g)})\end{array}\right\}}{\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^{r+\nu_\ell(g)}\mathbb{Z}):\det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^{r+\nu_\ell(g)})\}}$$

when $\ell\neq p$ and with $\Delta_p=0$. Finally, for condition (5'), we note that $\mathscr{C}(F)\ll 1$ since $N<p$, and in relation (4.6) we take $\widetilde{W}=1/N$.

Before we proceed further, we simplify Δ_ℓ. If $\ell\nmid N$, then it is easy to see that $\Delta_\ell=0$. Assume, now, that $\ell|N$. In particular, $\ell\neq p$. Making the change of variable $r+\nu_\ell(g)=s+\nu_\ell(N)$, we find that

$$\Delta_\ell=-1+\lim_{s\to\infty}\frac{\ell^{\nu_\ell(N))}\cdot\#\left\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^{s+\nu_\ell(N)}\mathbb{Z}):\begin{array}{l}\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell^{\nu_\ell(N)}),\\ \det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^{s+\nu_\ell(N)})\end{array}\right\}}{\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^{s+\nu_\ell(N)}\mathbb{Z}):\det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^{s+\nu_\ell(N)})\}}.$$

For each $\sigma_0\in\mathrm{GL}_2(\mathbb{Z}/\ell^{\nu_\ell(N)}\mathbb{Z})$ with $\mathrm{tr}(\sigma_0)\equiv t\,(\mathrm{mod}\,\ell^{\nu_\ell(N)})$ and $\det(\sigma_0)\equiv p\,(\mathrm{mod}\,\ell^{\nu_\ell(N)})$, it is easy to see that there are precisely ℓ^{3s} matrices $\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^{s+\nu_\ell(N)}\mathbb{Z})$ with $\sigma\equiv\sigma_0\,(\mathrm{mod}\,\ell^{\nu_\ell(N)})$ and $\det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^{s+\nu_\ell(N)})$. Therefore,

$$\Delta_\ell=-1+\frac{\ell^{\nu_\ell(N))}\cdot\#\left\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^{\nu_\ell(N)}\mathbb{Z}):\begin{array}{l}\mathrm{tr}(\sigma)\equiv t\,(\mathrm{mod}\,\ell^{\nu_\ell(N)}),\\ \det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^{\nu_\ell(N)})\end{array}\right\}}{\#\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^{\nu_\ell(N)}\mathbb{Z}):\det(\sigma)\equiv p\,(\mathrm{mod}\,\ell^{\nu_\ell(N)})\}},$$

and hence the Chinese Remainder Theorem implies that

$$\prod_\ell (1+\Delta_\ell) = \frac{N\cdot \#\left\{\sigma\in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \begin{array}{l} \mathrm{tr}(\sigma)\equiv t \pmod N, \\ \det(\sigma)\equiv p \pmod N \end{array}\right\}}{\#\{\sigma\in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \det(\sigma)\equiv p \pmod N\}}.$$

The above discussion will complete the proof of Theorem 2.2 as long as we can control the quantities W, M and E in Theorem 4.2. For M, we have that

$$\begin{aligned} M &= \max_{n\le -4} \sum_{\substack{a\in\mathcal{A} \\ D_1(a)/n \text{ is a square}}} w_a \\ &\ll \max_{n\le -4} \frac{\#\{(a,m)\in\mathbb{N}^2 : (t+Na)^2 - ngm^2 = 4p\}}{\sqrt{p}} \ll \frac{1}{\sqrt{p}}, \end{aligned}$$

an estimate that is good enough for our purposes. Finally, we need to estimate W and E. As in the proof of Theorem 1.9, partial summation implies that

$$\sum_{\substack{p^- < t+aN < p \\ a\equiv b \pmod q}} w_a = \frac{1}{Nq} + O\left(\frac{1}{\sqrt{p}}\right).$$

So Theorem 2.2 follows by taking the parameter ϵ in the statement of Theorem 4.2 to be small enough.

6. Proof of Theorems 4.1 and 4.2

In this section, we prove Theorems 4.1 and 4.2. We start with the former. Before embarking on its proof, we state an auxiliary result, which is an application of zero-density estimates of L-functions, first observed by Elliott (see, also, [21, Proposition 2.2]). For a proof of it in the stated form, see [9, Lemma 2.3].

Lemma 6.1. *Let $\alpha\ge 1$ and $y\ge 3$. There is a set $\mathcal{E}_\alpha(y)\subset[1,y]\cap\mathbb{Z}$ of at most $y^{2/\alpha}$ integers such that if χ is a Dirichlet character modulo $d\le \exp\{(\log y)^2\}$ whose conductor does not belong to $\mathcal{E}_\alpha(y)$, then*

$$L(1,\chi) = \prod_{\ell\le(\log y)^{8\alpha^2}} \left(1-\frac{\chi(\ell)}{\ell}\right)^{-1}\left(1+O_\alpha\left(\frac{1}{(\log y)^\alpha}\right)\right).$$

Proof of Theorem 4.1. All implied constants might depend on the various parameters mentioned in the end of the statement of Theorem 4.1. We may assume that X is large enough. Firstly, we use Lemma 6.1 to truncate $P_{\boldsymbol{a}}$ and replace it by

$$P_{\boldsymbol{a}}^{(z)} := \prod_{\ell\le z}(1+\delta_\ell(\boldsymbol{a})).$$

We apply this result with $\alpha = A^2$ and $y = X^A$, where A is a constant to be chosen later. We assume that A is large enough, so that $y\ge M_{j,\boldsymbol{a}}$ for all $\boldsymbol{a}\in\mathcal{A}$ and all $j\in\{1,\dots,d\}$. Let $z = (\log y)^{8\alpha^2} = (A\log X)^{8A^4} \le e^{(\log\log X)^2} = Q$ for X large enough. If the conductor of

$\chi_{j,\boldsymbol{a}}$ does not belong to the exceptional set $\mathcal{E}_{A^2}(X^A)$ for all $j \in \{1, \dots, d\}$, then conditions (2) and (3) imply that

$$\sum_{\ell > z} \delta_\ell(\boldsymbol{a}) = \sum_{j=1}^{k} \lambda_{j,\boldsymbol{a}} \sum_{\ell > z} \frac{\chi_{j,\boldsymbol{a}}(\ell)}{\ell} + O\left(\sum_{\ell > z} \frac{1}{\ell^{1+\eta}} + \sum_{\substack{\ell | L_{\boldsymbol{a}} \\ \ell > z}} \frac{1}{\ell} \right) \ll \frac{1}{(\log X)^{C+1}},$$

provided that A is large enough, since $\omega(L_{\boldsymbol{a}}) \le (\log X)^{O(1)}$ by condition (5). Moreover, condition (2) implies that $P_{\boldsymbol{a}}^{(z)} \ll (\log z)^{O(1)} \ll (\log\log X)^{O(1)}$. Therefore

$$P_{\boldsymbol{a}} = P_{\boldsymbol{a}}^{(z)} + O\left(\frac{1}{(\log X)^C} \right)$$

for $\boldsymbol{a} \in \mathcal{A}$ with $\mathrm{cond}(\chi_{j,\boldsymbol{a}}) \notin \mathcal{E}_{A^2}(X^A)$ for all $j \in \{1, \dots, k\}$. Finally, when this last condition fails for some $j \in \{1, \dots, k\}$, then we recall that $\delta_\ell(\boldsymbol{a}) \ll 1/\ell$. So, if δ is small enough in terms of ϵ, then

$$P_{\boldsymbol{a}} \ll X^{\epsilon/2} \prod_{\ell > \exp\{X^\delta\}} |1 + \delta_\ell(\boldsymbol{a})|$$

by condition (2). So, using conditions (3) and (5), and and the Prime Number Theorem for arithmetic progressions, which implies that $\sum_{\ell > \exp\{q^\alpha\}} \chi(\ell)/\ell \ll_\alpha 1$ for fixed $\alpha > 0$ and a non-principal character mod q, we find that

$$\begin{aligned} P_{\boldsymbol{a}} &\ll X^{\epsilon/2} \exp\left\{ \mathrm{Re}\left(\sum_{j=1}^{k} \lambda_{j,\boldsymbol{a}} \sum_{\ell > \exp\{X^\delta\}} \frac{\chi_{j,\boldsymbol{a}}(\ell)}{\ell} \right) + O\left(\sum_{\ell > \exp\{X^\delta\}} \frac{1}{\ell^{1+\eta}} + \sum_{\substack{\ell | L_{\boldsymbol{a}} \\ \ell > \exp\{X^\delta\}}} \frac{1}{\ell} \right) \right\} \\ &\ll X^{\epsilon/2}. \end{aligned}$$

Hence,

$$\sum_{a \in \mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}} = \sum_{a \in \mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}}^{(z)} + O\left(\frac{W}{(\log X)^B} + X^{\epsilon/2} \sum_{j=1}^{k} \sum_{\substack{\boldsymbol{a} \in \mathcal{A} \\ \mathrm{cond}(\chi_{j,\boldsymbol{a}}) \in \mathcal{E}_{A^2}(X^A)}} |w_{\boldsymbol{a}}| \right).$$

Since

$$\sum_{\substack{\boldsymbol{a} \in \mathcal{A} \\ \mathrm{cond}(\chi_{j,\boldsymbol{a}}) \in \mathcal{E}_{A^2}(X^A)}} |w_{\boldsymbol{a}}| \le M \cdot |\mathcal{E}_{A^2}(X^A)| \le M X^{2/A},$$

where M is defined in the statement of Theorem 4.1, we find that

$$\sum_{\boldsymbol{a} \in \mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}} = \sum_{\boldsymbol{a} \in \mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}}^{(z)} + O\left(\frac{W}{(\log X)^C} + M X^\epsilon \right) \tag{6.1}$$

by taking $A \ge 4/\epsilon$.

Next, we turn to the estimation of the main term. We define multiplicatively, for $q \in \mathbb{N}$, $\boldsymbol{a} \in \mathcal{A}$ and $\boldsymbol{h} \pmod q$,

$$\delta_q(\boldsymbol{a}) = \prod_{\ell | q} \delta_\ell(\boldsymbol{a}) \quad \text{and} \quad \Delta_q(\boldsymbol{h}) = \prod_{\ell^r \| q} \Delta_{\ell^r}(\boldsymbol{h}).$$

It then follows from conditions (2) and (4b) that

$$|\delta_q(\boldsymbol{a})| \le \frac{c_1^{\omega(q)}}{\mathrm{rad}(q)} \quad \text{and} \tag{6.2}$$

$$|\Delta_q(\boldsymbol{h})| \le \frac{c_1^{\omega(q)}}{\mathrm{rad}(q)} \quad \text{if } \boldsymbol{h} \in \mathcal{G}(\ell^r) \setminus \mathcal{E}(\ell^r) \text{ whenever } \ell^r \| q, \tag{6.3}$$

where c_1 is some absolute constant. With this notation, we have that

$$P_{\boldsymbol{a}}^{(z)} = \sum_{P^+(n) \le z} \mu^2(n) \delta_n(\boldsymbol{a}).$$

Moreover, for each $\boldsymbol{a} \in \mathcal{A}$, we set

$$\nu_{\ell,\boldsymbol{a}} = \min\{r \ge 1 : \boldsymbol{a} \,(\mathrm{mod}\, \ell^r) \notin \mathcal{E}(\ell^r)\} \quad \text{and} \quad q_{n,\boldsymbol{a}} = \prod_{\ell | n} \ell^{\nu_{\ell,\boldsymbol{a}}},$$

which are well-defined in view of condition (4b). Additionally, we define

$$\mathcal{H}(\ell^r) = \{\boldsymbol{h} \in \mathcal{G}(\ell^r) : \boldsymbol{h} \notin \mathcal{E}(\ell^r), \boldsymbol{h} \,(\mathrm{mod}\, \ell^{r-1}) \in \mathcal{E}(\ell^{r-1})\}.$$

Then, for each $\boldsymbol{a} \in \mathcal{A}$ with $\boldsymbol{a} \,(\mathrm{mod}\, \ell) \in \mathcal{G}(\ell)$, we have that

$$\nu_{\ell,\boldsymbol{a}} = r \iff \boldsymbol{a} \,(\mathrm{mod}\, \ell^r) \in \mathcal{H}(\ell^r).$$

What is more, if $r = \nu_{\ell,\boldsymbol{a}}$, then $\delta_\ell(\boldsymbol{a}) = \Delta_{\ell^r}(\boldsymbol{h})$ for all $\boldsymbol{h} \equiv \boldsymbol{a} \,(\mathrm{mod}\, \ell^r)$. For the convenience of notation, given $q \in \mathbb{N}$, we define

$$\mathcal{H}(q) = \{\boldsymbol{h} \in (\mathbb{Z}/q\mathbb{Z})^d : \boldsymbol{h} \,(\mathrm{mod}\, \ell^r) \in \mathcal{H}(\ell^r) \text{ whenever } \ell^r \| q\}$$

and

$$\mathcal{E}(q) = \{\boldsymbol{h} \in (\mathbb{Z}/q\mathbb{Z})^d : \boldsymbol{h} \,(\mathrm{mod}\, \ell^r) \in \mathcal{E}(\ell^r) \text{ whenever } \ell^r \| q\}.$$

If $n = \mathrm{rad}(q)$ and $\boldsymbol{a} \,(\mathrm{mod}\, q) \in \mathcal{G}(q)$, then

$$\begin{aligned} \boldsymbol{a} \,(\mathrm{mod}\, q) \in \mathcal{H}(q) &\iff \ell^{\nu_{\ell,\boldsymbol{a}}} \| q \quad \text{for all primes } \ell | n \\ &\iff q_{n,\boldsymbol{a}} = \prod_{\ell | n} \ell^{\nu_{\ell,\boldsymbol{a}}} = q, \end{aligned}$$

and $\delta_n(\boldsymbol{a}) = \Delta_q(\boldsymbol{h})$ in that case, where $\boldsymbol{a} \,(\mathrm{mod}\, q) = \boldsymbol{h}$. If $P^+(n)$ denotes the large prime divisor of n with the convention that $P^+(1) = 1$, then

$$\sum_{a \in \mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}}^{(z)} = \sum_{P^+(n) \le z} \mu^2(n) \sum_{a \in \mathcal{A}} w_{\boldsymbol{a}} \delta_n(\boldsymbol{a}) = \sum_{P^+(n) \le z} \mu^2(n) \sum_{\substack{q \in \mathbb{N} \\ \mathrm{rad}(q) = n}} \sum_{\substack{a \in \mathcal{A} \\ q_{n,\boldsymbol{a}} = q}} w_{\boldsymbol{a}} \delta_n(\boldsymbol{a}) = S_1 + S_2$$

say, where S_1 is the part of the sum with $q \le Q$ and S_2 is the rest of the sum.

Before estimating S_1 and S_2, we set

$$f(b) = |\mathcal{E}(b)|/b^{d-1},$$

which is a multiplicative function, and note that, for any fixed $\kappa > 0$ and $c > 0$, we have

$$\sum_{\substack{P^+(bn) \le z \\ \mathrm{rad}(b) | n}} \frac{\mu^2(n) c^{\omega(n)} f(b)^\lambda}{n^{1-\kappa/\log z} b} \ll (\log\log X)^{O(1)} e^{O(S)}, \tag{6.4}$$

where the implied constants depend on κ and c, and S is defined as in the statement of Theorem 4.1. Indeed, we note that if n is square-free and z-smooth, then $n^{1/\log z} \le e^{\omega(n)}$. Therefore, writing $n = \mathrm{rad}(b)a$, we deduce that

$$\sum_{\substack{P^+(bn)\le z \\ \mathrm{rad}(b)|n}} \frac{\mu^2(n)c^{\omega(n)}f(b)^\lambda}{n^{1-\kappa/\log z}b} \le \sum_{P^+(b)\le z} \frac{(ce^\kappa)^{\omega(b)}f(b)^\lambda}{\mathrm{rad}(b)b} \sum_{P^+(a)\le z} \frac{\mu^2(a)(ce^\kappa)^{\omega(a)}}{a}$$
$$\ll (\log\log X)^{O(1)} \exp\left\{ce^\kappa \sum_{\ell\le z}\sum_{r=1}^\infty \frac{f(\ell^r)^\lambda}{\ell^{1+r}}\right\} = (\log\log X)^{O(1)} e^{O(S)},$$

which proves (6.4).

Let us see now how to estimate S_1 and S_2. We start with the latter. We need to use (4.6), but the modulus q might be too large. Using (6.2) and condition (1), we find that

$$S_2 = \sum_{P^+(n)\le z} \mu^2(n) \sum_{\substack{\boldsymbol{a}\in\mathcal{A} \\ q_{n,\boldsymbol{a}}>Q}} w_{\boldsymbol{a}}\delta_n(\boldsymbol{a}) \ll \sum_{P^+(n)\le z} \frac{\mu^2(n)c_1^{\omega(n)}}{n} \sum_{\substack{\boldsymbol{a}\in\mathcal{A} \\ \boldsymbol{a}\,(\mathrm{mod}\,n)\in\mathcal{G}(n) \\ q_{n,\boldsymbol{a}}>Q}} |w_{\boldsymbol{a}}|.$$

Write $q_{n,\boldsymbol{a}} = nq'$, $q'\in\mathbb{N}$, and note that if $\ell^r\|q'$, then $\boldsymbol{a}\,(\mathrm{mod}\,\ell^r)\in\mathcal{E}(\ell^r)$. So, for each $s\in\{0,1,\dots,r\}$, we have that $\boldsymbol{a}\,(\mathrm{mod}\,\ell^s)\in\mathcal{E}(\ell^s)$, with the convention that $\mathcal{E}(1)=\{1\}$. (Here, we used condition (4b).) Clearly, if $q_{n,\boldsymbol{a}}>Q$, then either $n>Q^{1/2}$ or $q'>Q^{1/2}$. In the latter case, the z-smoothness of q' implies that q' has a divisor $b\in(Q^{1/2},Q^{1/2}z]\subset(Q^{1/2},Q]$. Moreover, we have that $\mathrm{rad}(b)|n$ and $\boldsymbol{a}\,(\mathrm{mod}\,b)\in\mathcal{G}(b)\cap\mathcal{E}(b)$. Therefore

$$S_2 \ll \sum_{\substack{P^+(n)\le z \\ n>Q^{1/2}}} \frac{\mu^2(n)c_1^{\omega(n)}}{n}\cdot\widetilde{W} + \sum_{\substack{P^+(b)\le z \\ Q^{1/2}<b\le Q}} \sum_{\substack{P^+(n)\le z \\ \mathrm{rad}(b)|n}} \frac{\mu^2(n)c_1^{\omega(n)}}{n} \sum_{\substack{\boldsymbol{a}\in\mathcal{A} \\ \boldsymbol{a}\,(\mathrm{mod}\,b)\in\mathcal{G}(b)\cap\mathcal{E}(b)}} |w_{\boldsymbol{a}}|$$
$$\ll \widetilde{W} \sum_{\substack{P^+(n)\le z \\ n>Q^{1/2}}} \frac{\mu^2(n)c_1^{\omega(n)}}{n} + (\log\log X)^{c_1} \sum_{\substack{P^+(b)\le z \\ Q^{1/2}<b\le Q}} \frac{c_1^{\omega(b)}}{\mathrm{rad}(b)} \sum_{\boldsymbol{h}\in\mathcal{G}(b)\cap\mathcal{E}(b)} \sum_{\substack{\boldsymbol{a}\in\mathcal{A} \\ \boldsymbol{a}\equiv\boldsymbol{h}\,(\mathrm{mod}\,b)}} |w_{\boldsymbol{a}}|.$$

We may now apply (4.6) to deduce that

$$S_2 \ll \widetilde{W} \sum_{\substack{P^+(n)\le z \\ n>Q^{1/2}}} \frac{\mu^2(n)c_1^{\omega(n)}}{n} + \widetilde{W}(\log\log X)^{c_1} \sum_{\substack{P^+(b)\le z \\ b>Q^{1/2}}} \frac{|\mathcal{E}(b)|}{\mathrm{rad}(b)|\mathcal{G}(b)|}. \tag{6.5}$$

Note that $|\mathcal{G}(b)| \geq c_2^{-\omega(b)} b^d$ for some absolute constant $c_2 \geq 1$, a consequence of relation (4.4). Therefore Hölder's inequality and (6.4) imply that

$$\sum_{\substack{P^+(b)\le z\\ b>Q^{1/2}}} \frac{|\mathcal{E}(b)|}{\mathrm{rad}(b)|\mathcal{G}(b)|} \le \sum_{\substack{P^+(b)\le z\\ b>Q^{1/2}}} \frac{c_2^{\omega(b)} f(b)}{b\,\mathrm{rad}(b)} \le \left(\sum_{\substack{P^+(b)\le z\\ b>Q^{1/2}}} \frac{c_2^{\frac{\lambda}{\lambda-1}\omega(b)}}{b}\right)^{1-\frac{1}{\lambda}} \left(\sum_{P^+(b)\le z} \frac{f(b)^\lambda}{\mathrm{rad}(b)^\lambda b}\right)^{\frac{1}{\lambda}}$$

$$\ll (\log\log X)^{O(1)} e^{O(S)} \cdot \left(\sum_{\substack{P^+(b)\le z\\ b>Q^{1/2}}} \frac{c_2^{\frac{\lambda}{\lambda-1}\omega(b)}}{b}\right)^{1-\frac{1}{\lambda}} .$$

For any $c \geq 1$ and any $\kappa > 0$, we have that

$$\sum_{\substack{P^+(b)\le z\\ b>Q^{1/2}}} \frac{c^{\omega(b)}}{b} \le \frac{1}{Q^{\kappa/(2\log z)}} \sum_{P^+(b)\le z} \frac{c^{\omega(b)}}{b^{1-\kappa/\log z}} \asymp \frac{1}{(\log X)^{\kappa/(16A^4)}} \prod_{p\le z}\left(1 - \frac{c}{p^{1-1/\log z}}\right)^{-1}.$$

Since $p^{1/\log z} = 1 + O(\log p/\log z)$ for $p \leq z$, we deduce that

$$\sum_{\substack{P^+(b)\le z\\ b>Q^{1/2}}} \frac{c^{\omega(b)}}{b} \ll \frac{(\log\log X)^c}{(\log X)^{\kappa/(16A^4)}}.$$

Putting together the above estimates with κ large enough implies that

$$S_2 \ll \frac{e^{O(S)}\widetilde{W}}{(\log X)^C}, \tag{6.6}$$

which of admissible size.

Next, we estimate S_1. We start by noticing that

$$S_1 = \sum_{P^+(n)\le z} \mu^2(n) \sum_{\substack{q\le Q\\ \mathrm{rad}(q)=n}} \sum_{\substack{a\in\mathcal{A}\\ q_{n,\boldsymbol{a}}=q}} w_{\boldsymbol{a}}\delta_n(\boldsymbol{a}) = \sum_{\substack{P^+(q)\le z\\ q\le Q}} \sum_{\boldsymbol{h}\in\mathcal{H}(q)} \Delta_q(\boldsymbol{h}) \sum_{\substack{\boldsymbol{a}\in\mathcal{A}\\ \boldsymbol{a}\equiv\boldsymbol{h}\,(\mathrm{mod}\,q)}} w_{\boldsymbol{a}}.$$

For the inner sum, we use the approximation

$$\frac{W}{|\mathcal{G}(q)|} + O(E(\mathcal{A};q)),$$

which implies that

$$S_1 = W \sum_{\substack{P^+(q)\le z\\ q\le Q}} \sum_{\boldsymbol{h}\in\mathcal{H}(q)} \frac{\Delta_q(\boldsymbol{h})}{|\mathcal{G}(q)|} + O\left(\sum_{\substack{q\le Q\\ P^+(q)\le z}} \sum_{\boldsymbol{h}\in\mathcal{H}(q)} |\Delta_q(\boldsymbol{h})| E(\mathcal{A};q)\right).$$

In the main term, we extend the summation of q to infinity. Using the bound (6.3), we then find that

$$S_1 = W \sum_{P^+(q)\le z} \sum_{\boldsymbol{h}\in\mathcal{H}(q)} \frac{\Delta_q(\boldsymbol{h})}{|\mathcal{G}(q)|} + O\left(\widetilde{W} \sum_{\substack{P^+(q)\le z\\ q>Q}} \frac{c_1^{\omega(q)}|\mathcal{H}(q)|}{\mathrm{rad}(q)|\mathcal{G}(q)|} + \sum_{\substack{q\le Q\\ P^+(q)\le z}} \frac{c_1^{\omega(q)}|\mathcal{H}(q)|}{\mathrm{rad}(q)} E(\mathcal{A};q) \right).$$

By Hölder's inequality and relation (4.6), we find that

$$\begin{aligned}\sum_{\substack{q\le Q\\ P^+(q)\le z}} \frac{c_1^{\omega(q)}|\mathcal{H}(q)|}{\mathrm{rad}(q)} E(\mathcal{A};q) &\le E^{1-1/\lambda}\cdot \left(\sum_{\substack{q\le Q\\ P^+(q)\le z}} \left(\frac{c_1^{\omega(q)}|\mathcal{H}(q)|}{q^{d-1}\,\mathrm{rad}(q)}\right)^{\lambda} q^{d-1}E(\mathcal{A};q)\right)^{1/\lambda} \\ &\ll E^{1-1/\lambda}\cdot \left(\sum_{\substack{q\le Q\\ P^+(q)\le z}} \left(\frac{c_1^{\omega(q)}|\mathcal{H}(q)|}{q^{d-1}\,\mathrm{rad}(q)}\right)^{\lambda} \frac{q^{d-1}\widetilde{W}}{|\mathcal{G}(q)|}\right)^{1/\lambda}.\end{aligned}$$

We set $n = \mathrm{rad}(q)$ and $q = bn$, so that $\mathrm{rad}(b)|n$ and $|\mathcal{H}(q)| \le n^d|\mathcal{E}(b)|$. Since $|\mathcal{G}(q)| \ge c_2^{-\omega(q)}q^d$, we deduce that

$$S_1 = W \sum_{P^+(q)\le z} \sum_{\boldsymbol{h}\in\mathcal{H}(q)} \frac{\Delta_q(\boldsymbol{h})}{|\mathcal{G}(q)|} + O(R),$$

where

$$\begin{aligned} R &= \widetilde{W} \sum_{\substack{P^+(bn)\le z\\ bn>Q\\ \mathrm{rad}(b)|n}} \frac{\mu^2(n)c_3^{\omega(n)}f(b)}{bn} + \widetilde{W}^{1/\lambda}E^{1-1/\lambda}\left(\sum_{\substack{P^+(bn)\le z\\ \mathrm{rad}(b)|n}} \frac{\mu^2(n)c_3^{\omega(n)}f(b)^{\lambda}}{bn}\right)^{1/\lambda} \\ &\le \frac{\widetilde{W}}{Q^{\kappa/\log z}} \sum_{\substack{P^+(bn)\le z\\ \mathrm{rad}(b)|n}} \frac{\mu^2(n)c_3^{\omega(n)}f(b)}{(bn)^{1-\kappa/\log z}} + \widetilde{W}^{1/\lambda}E^{1-1/\lambda}(\log\log X)^{O(1)}e^{O(S)}\end{aligned}$$

for some appropriate constant c_3, where we used (6.4). Applying Hölder's inequality and (6.4), we deduce that

$$\begin{aligned}\sum_{\substack{P^+(bn)\le z\\ \mathrm{rad}(b)|n}} \frac{c_3^{\omega(n)}f(b)}{(bn)^{1-\kappa/\log z}} &\le \left(\sum_{\substack{P^+(bn)\le z\\ \mathrm{rad}(b)|n}} \frac{\mu^2(n)}{(bn)^{1-\frac{\kappa\lambda}{\lambda-1}\frac{1}{\log z}}}\right)^{1-\frac{1}{\lambda}} \left(\sum_{\substack{P^+(bn)\le z\\ \mathrm{rad}(b)|n}} \frac{\mu^2(n)c_3^{\lambda\omega(n)}f(b)^{\lambda}}{bn}\right)^{\frac{1}{\lambda}} \\ &\ll (\log\log X)^{O(1)}e^{O(S)}.\end{aligned}$$

Putting together the above estimate and (6.6), we deduce that

$$\sum_{a\in\mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}}^{(z)} = W \sum_{P^+(q)\le z} \sum_{\boldsymbol{h}\in\mathcal{H}(q)} \frac{\Delta_q(\boldsymbol{h})}{|\mathcal{G}(q)|} + O\left(\frac{e^{O(S)}\widetilde{W}}{(\log X)^C} + \widetilde{W}^{1/\lambda}E^{1-1/\lambda}(\log\log X)^{O(1)}e^{O(S)}\right).$$

The above estimate and relation (6.1) imply Theorem 4.1, provided that we can show that

$$\sum_{P^+(q)\le z}\sum_{\boldsymbol{h}\in\mathcal{H}(q)}\frac{\Delta_q(\boldsymbol{h})}{|\mathcal{G}(q)|}=1. \tag{6.7}$$

We may assume that $S<\infty$; otherwise, the conclusion of Theorem 4.1 is trivial. In particular, the series $\sum_{r\ge1} f(\ell^r)^\lambda/\ell^{r+1}$ converges for each $\ell\le z$, which implies that

$$\lim_{r\to\infty}\frac{f(\ell^r)}{\ell^{r/\lambda}}=0 \quad\Longrightarrow\quad \lim_{r\to\infty}\frac{|\mathcal{E}(\ell^r)|}{\ell^{r(d-1+1/\lambda)}}=0. \tag{6.8}$$

Now, using multiplicativity, we see immediately that

$$\begin{aligned}\sum_{P^+(q)\le z}\sum_{\boldsymbol{h}\in\mathcal{H}(q)}\frac{\Delta_q(\boldsymbol{h})}{|\mathcal{G}(q)|}&=\prod_{\ell\le z}\left(1+\sum_{r\ge1}\sum_{\boldsymbol{h}\in\mathcal{H}(\ell^r)}\frac{\Delta_{\ell^r}(\boldsymbol{h})}{|\mathcal{G}(\ell^r)|}\right)\\&=\prod_{\ell\le z}\left(1+\lim_{R\to\infty}\sum_{r=1}^{R}\sum_{\boldsymbol{h}\in\mathcal{H}(\ell^r)}\frac{\Delta_{\ell^r}(\boldsymbol{h})}{|\mathcal{G}(\ell^r)|}\right)\\&=\prod_{\ell\le z}\left(1+\lim_{R\to\infty}\sum_{\boldsymbol{h}\in\mathcal{G}(\ell^R)\setminus\mathcal{E}(\ell^R)}\frac{\Delta_{\ell^R}(\boldsymbol{h})}{|\mathcal{G}(\ell^R)|}\right).\end{aligned}$$

Applying conditions (4c) and (4d), and recalling that $|\mathcal{G}(\ell)|\gg\ell^d$, we find that

$$\begin{aligned}\lim_{R\to\infty}\sum_{\boldsymbol{h}\in\mathcal{G}(\ell^R)\setminus\mathcal{E}(\ell^R)}\frac{\Delta_{\ell^R}(\boldsymbol{h})}{|\mathcal{G}(\ell^R)|}&=\lim_{R\to\infty}\sum_{\boldsymbol{h}\in\mathcal{G}(\ell^R)}\frac{\Delta_{\ell^R}(\boldsymbol{h})}{|\mathcal{G}(\ell^R)|}-\lim_{R\to\infty}\sum_{\boldsymbol{h}\in\mathcal{G}(\ell^R)\cap\mathcal{E}(\ell^R)}\frac{\Delta_{\ell^R}(\boldsymbol{h})}{|\mathcal{G}(\ell^R)|}\\&\ll\limsup_{R\to\infty}\frac{\|\Delta_{\ell^R}\|_\infty\cdot|\mathcal{E}(\ell^R)|}{|\mathcal{G}(\ell^R)|}\ll_\ell\limsup_{R\to\infty}\frac{|\mathcal{E}(\ell^R)|}{\ell^{dR}}=0\end{aligned}$$

by (6.8). So we deduce that relation (6.7) does hold, thus completing the proof of Theorem 4.1. □

Next, we show Theorem 4.2 in the special case when $\Delta_\ell=0$ for all primes ℓ, which is easy to deduce from Theorem 4.1. We need a preliminary result. Given a polynomial $f(x_1,\dots,x_d)\in\mathbb{Z}[x_1,\dots,x_d]$, we introduce the notation

$$\rho_f(n):=\#\{\boldsymbol{x}\in(\mathbb{Z}/n\mathbb{Z})^d: f(\boldsymbol{x})\equiv0\,(\mathrm{mod}\,n)\}.$$

Then we have the following result, part (b) of which is an easy corollary of a result due to Stewart [37].

Lemma 6.2. *Let ℓ be a prime and $f(x_1,\dots,x_d)\in\mathbb{Z}[x_1,\dots,x_d]$ a polynomial of degree m.*

(a) *If f is non-zero modulo ℓ, then*

$$\rho_f(\ell)\le dm\ell^{d-1}.$$

(b) *If $r\in\mathbb{N}$ and $v=\min\{r,\nu_\ell(\mathscr{C}(f))\}$, then*

$$\rho_f(\ell^r)\le m^d(r+1)^{d-1}\ell^{v/m+r(d-1/m)}.$$

Proof. (a) We use induction on d. When $d = 1$, the result is straightforward. Assume that it is true for polynomials of $d-1$ variables. We write f as a polynomial of x_d, whose coefficients are polynomials in $x_1, \dots, x_{d-1}$. At least one of these coefficients must be non-zero modulo ℓ. Call this coefficient $g(x_1, \dots, x_{d-1})$. For each given choice of $x_1, \dots, x_{d-1}$, either f is non-zero as a polynomial of x_d modulo ℓ, in which case we have $\le m$ choices for x_d with $f(x_1, \dots, x_d) \equiv 0 \pmod{\ell}$, or f is zero as a polynomial of x_d modulo ℓ, in which case we have ℓ choices for x_d but also $g(x_1, \dots, x_{d-1}) \equiv 0 \pmod{\ell}$. Therefore

$$\rho_f(\ell) \le m \cdot \ell^{d-1} + \ell \cdot \rho_g(\ell) \le m\ell^{d-1} + \ell \cdot (d-1)m\ell^{d-2} = dm\ell^{d-1}.$$

This completes the inductive step and hence the proof of part (a).

(b) First, we deal with the case $d = 1$, in which case we have to show that

$$\rho_f(\ell^r) \le m\ell^{v/m + r(1-1/m)}. \tag{6.9}$$

Let $f_k(x) = f(x) + k\ell^r$ and note that $\rho_{f_k}(\ell^r) = \rho_f(\ell^r)$ and $\min\{r, \nu_\ell(\mathscr{C}(f_k))\} = v$. On the other hand, if $k \to \infty$, then the roots of f_k over $\mathbb{C}$ tend to infinity too, so they cannot be roots of f_k' at the same time for k large enough. So, by taking k large enough, we may assume that the discriminant of f is non-zero.

Next, write $f(x) = \mathscr{C}(f) \cdot g(x)$, where $g(x)$ is primitive (that is to say its content is 1). Clearly,

$$\rho_f(\ell^r) = \ell^v \rho_g(\ell^{r-v}),$$

which reduces the lemma to the case when $\nu_\ell(\mathscr{C}(f)) = 0$. The result then follows by [37, Corollary 2 and eq. (44)] when $m \ge 2$, and trivially when $m = 1$.

Next, we show the general case. We argue by induction on d. Assume that the lemma holds for polynomials of $d-1$ variables. As in the case $d = 1$, writing $f(x_1, \dots, x_d) = \mathscr{C}(f) \cdot g(x_1, \dots, x_d)$ allows us to assume that f is primitive. There are polynomials $c_j(x_1, \dots, x_{d-1})$ of degree $\le m$ such that

$$f(x_1, \dots, x_d) = \sum_{j=0}^{m} c_j(x_1, \dots, x_{d-1}) x_d^j.$$

Clearly, since f is primitive, there must be at least one $j_0 \in \{0, 1, \dots, m\}$ such that the content of c_{j_0} is not divisible by ℓ. For each $a_1, \dots, a_{d-1} \in \mathbb{Z}$, we write $C(a_1, \dots, a_{d-1})$ for the greatest common divisor of the polynomial values $c_j(a_1, \dots, a_{d-1})$, $0 \le j \le m$. Then

$$\begin{aligned}\rho_f(\ell^r) &= \sum_{w=0}^{r} \sum_{\substack{0 \le a_1, \dots, a_{d-1} < \ell^r \\ \min\{r, \nu_\ell(C(a_1, \dots, a_{d-1}))\} = w}} \#\{0 \le x_d < \ell^r : f(a_1, \dots, a_{d-1}, x_d) = 0\} \\ &\le \sum_{w=0}^{r} \sum_{\substack{0 \le a_1, \dots, a_{d-1} < \ell^r \\ \min\{r, \nu_\ell(C(a_1, \dots, a_{d-1}))\} = w}} m\ell^{w/m + r(1-1/m)},\end{aligned}$$

by the base case (6.9). Note that if $\min\{r, \nu_\ell(C(a_1, \dots, a_{d-1}))\} = w$, then $\ell^w | c_{j_0}(a_1, \dots, a_{d-1})$. So the number of such $a_1, \dots, a_{d-1}$ mod ℓ^r is at most

$$\ell^{(d-1)(r-w)} \rho_{c_{j_0}}(\ell^w) \le m^{d-1}(w+1)^{d-2} \ell^{(d-1)(r-w) + w(d-1-1/m)} \le m^{d-1}(r+1)^{d-2} \ell^{(d-1)r - w/m},$$

by the induction hypothesis and our assumption that the content of c_{j_0} is not divisible by ℓ. Therefore

$$\rho_f(\ell^r) \le m^d(r+1)^{d-2}\sum_{w=0}^{r} \ell^{(d-1)r-w/m+w/m+(1-1/m)r} = m^d(r+1)^{d-1}\ell^{r(d-1/m)},$$

which completes the induction hypothesis and, hence, the proof of the lemma. □

Proof of Theorem 4.2 when $\Delta_\ell = 0$. Without loss of generality, we may assume that the parameter η lies in the interval $(0, 1/2]$. We first check that we can apply Theorem 4.1 under the hypothesis of Theorem 4.2 in this case. Conditions (1) and (2) hold by assumption. Condition (3') implies that condition (3) holds with $L_{\boldsymbol{a}} = L \cdot |D_1(\boldsymbol{a}) \cdots D_k(\boldsymbol{a})|$, and (5) holds since a non-zero integer n has $O(\log |n|)$ prime divisors. Finally, condition (4) is satisfied with

$$\mathcal{E}(\ell^r) = \{\boldsymbol{h} \in (\mathbb{Z}/\ell^r\mathbb{Z})^d : \ell^r | F(\boldsymbol{h})\},$$

since we have assumed that $\Delta_\ell = 0$ here and that $F(\boldsymbol{a}) \neq 0$ for $\boldsymbol{a} \in \mathcal{A}$ in condition (5'). In conclusion, Theorem 4.1 is applicable. We need to control the quantity S appearing in its statement. We will take $\lambda = 1 + 1/m$, where $m = \deg(F)$. Since the content of F is $\ll 1$ by condition (5'), Lemma 6.2(b) implies that

$$\rho_F(\ell^r) \ll (r+1)^{d-1}\ell^{r(d-1/m)} = \ell^{r(d-1)} \cdot (r+1)^{d-1}\ell^{r(1-1/m)}.$$

So

$$\frac{(|\mathcal{E}(\ell^r)|/\ell^{r(d-1)})^\lambda}{\ell^{r+1}} \le \frac{(\rho_F(\ell^r)/\ell^{r(d-1)})^\lambda}{\ell^{r+1}} \ll \frac{(r+1)^{\lambda(d-1)}}{\ell^{1+r(1-\lambda(1-1/m))}}.$$

Therefore, we see immediately that $S \ll 1$, and Theorem 4.2 follows in this special case by Theorem 4.1. □

The remainder of this section is devoted to showing that Theorem 4.2 can be indeed reduced to the special case when $\Delta_\ell = 0$. As before, we may assume that $\eta \in (0, 1/2]$. The key step is proving that the quantities Δ_ℓ in condition (4') satisfy the estimate

$$\Delta_\ell \ll \frac{1}{\ell^{3/2}} \quad (\ell \nmid LN), \tag{6.10}$$

where L is as in condition (3') and N is some appropriate non-zero integer of size $\le X^{O(1)}$. We will show how to construct N later in this section. For now, let us see how (6.10) allows us to reduce Theorem 4.2 to the case when $\Delta_\ell = 0$.

Deduction of Theorem 4.2 from (6.10). Note that $P = \prod_\ell (1 + \Delta_\ell)$ converges absolutely by (6.10). We define $\delta'_\ell(\boldsymbol{a})$ via the relation

$$\begin{cases} 1 + \delta_\ell(\boldsymbol{a}) = (1 + \delta'_\ell(\boldsymbol{a}))(1 + \Delta_\ell) & \text{if } \boldsymbol{a} \,(\mathrm{mod}\, \ell) \in \mathcal{G}(\ell), \\ \delta'_\ell(\boldsymbol{a}) = 0 & \text{otherwise,} \end{cases}$$

so that

$$\sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}} = P \cdot \sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} \gamma_{\boldsymbol{a}} \prod_\ell (1 + \delta'_\ell(\boldsymbol{a})),$$

where

$$\gamma_{\boldsymbol{a}} = \prod_{\substack{\ell \\ \boldsymbol{a}\,(\mathrm{mod}\,\ell)\notin\mathcal{G}(\ell)}} \frac{1}{1+\Delta_\ell} = \prod_{\substack{\ell > Q \\ \boldsymbol{a}\,(\mathrm{mod}\,\ell)\notin\mathcal{G}(\ell)}} \frac{1}{1+\Delta_\ell} \quad (\boldsymbol{a} \in \mathcal{A}),$$

since we have assumed that $\mathcal{A} \subset \{\boldsymbol{a} \in \mathbb{Z}^d : \boldsymbol{a}\,(\mathrm{mod}\,\ell) \in \mathcal{G}(\ell)\}$ for all $\ell \le Q$.

We now show that we can apply Theorem 4.2 to the quantities $\delta'_\ell(\boldsymbol{a})$. Condition (1) holds for $\delta'_\ell(\boldsymbol{a})$ by definition. Conditions (4'c) and (4'd) imply that $\Delta_\ell \ll 1/\ell$. Since we also have that $|1+\Delta_\ell| \gg 1$ by (4'c), we deduce that

$$\delta'_\ell(\boldsymbol{a}) = \delta_\ell(\boldsymbol{a}) + O\left(\frac{1}{\ell}\right),$$

so that condition (2) holds for $\delta'_\ell(\boldsymbol{a})$ too by the same condition for $\delta_\ell(\boldsymbol{a})$. Condition (3') holds by (6.10) with L replaced by LN. Defining

$$1 + \Delta'_{\ell^r}(\boldsymbol{a}) = \frac{1+\Delta_{\ell^r}(\boldsymbol{a})}{1+\Delta_\ell},$$

we see that condition (4') holds for the ℓ^r-periodic function $\Delta'_{\ell^r}(\boldsymbol{a})$, which has average $\Delta'_\ell = 0$. Condition (5') is also easily seen to hold.

Applying Theorem 4.2 to the sequence $\delta'_\ell(\boldsymbol{a})$, with the weights $w_{\boldsymbol{a}}$ replaced by $w_{\boldsymbol{a}}\gamma_{\boldsymbol{a}}$, we get that

$$\sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}} P_{\boldsymbol{a}} = P \cdot \left(W' + O\left(\frac{\widetilde{W}'}{(\log X)^C} + M'X^\epsilon + (\log\log X)^{O(1)} \widetilde{W}'^{1-1/(m+1)} E'^{1/(m+1)} \right)\right),$$

where W', M' and E' are defined as W, M and E, with the difference that $w_{\boldsymbol{a}}$ is replaced by $w_{\boldsymbol{a}}\gamma_{\boldsymbol{a}}$, and $\widetilde{W}' := \widetilde{W} \cdot \max_{\boldsymbol{a}\in\mathcal{A}} |\gamma_{\boldsymbol{a}}|$.

We will show that $\gamma_{\boldsymbol{a}}$ is very close to 1 and, as a result, relate W' to W, M' to M, E' to E, and $\widetilde{W}'$ to $\widetilde{W}$. Note that

$$\sum_{\ell>Q} |\Delta_\ell| \ll \sum_{\ell>Q} \frac{1}{\ell^{1+\eta}} + \sum_{\substack{\ell>Q\\ \ell|LN}} \frac{1}{\ell} \ll \frac{1}{Q^\eta} + \frac{(\log X)^{O(1)}}{Q} \ll \frac{1}{(\log X)^{(m+1)C}},$$

by (6.10) and the fact that

$$\omega(LN) \le \omega(L) + \omega(N) \le \omega(L) + \frac{\log|N|}{\log 2} \ll (\log X)^{O(1)},$$

a consequence of condition (5'), and our assumption that $N \le X^{O(1)}$. Therefore,

$$\gamma_{\boldsymbol{a}} = 1 + O\left(\frac{1}{(\log X)^{(m+1)C}}\right).$$

So, we see immediately that

$$W' = \sum_{\boldsymbol{a}\in\mathcal{A}} w_{\boldsymbol{a}}\gamma_{\boldsymbol{a}} = W + O\left(\frac{\widetilde{W}}{(\log X)^{(m+1)C}}\right)$$

and, if E is as in the statement of Theorem 4.2, then relation (4.6) implies that

$$\begin{aligned}\sum_{q\le Q} q^{d-1} \max_{\boldsymbol{g}\in\mathcal{G}(q)} \left| \sum_{\substack{\boldsymbol{a}\in\mathcal{A}\\ \boldsymbol{a}\equiv\boldsymbol{g} \,(\mathrm{mod}\, q)}} w_{\boldsymbol{a}}\gamma_{\boldsymbol{a}} - \frac{W'}{|\mathcal{G}(q)|} \right| &\ll E + \sum_{q\le Q} q^{d-1} \cdot \frac{\widetilde{W}}{|\mathcal{G}(q)|(\log X)^{C(m+1)}} \\ &\ll E + \widetilde{W} \cdot \frac{(\log\log X)^{O(1)}}{(\log X)^{C(m+1)}},\end{aligned}$$

since $|\mathcal{G}(q)| \ge qe^{-O(\omega(q))}$ by (4.4) and the fact that $|\mathcal{G}(\ell^r)| = \ell^{(r-1)d}|\mathcal{G}(\ell)|$. This proves Theorem 4.2. □

The crucial result for the construction of the number N and the deduction of (6.10) is provided by the following theorem. Recall that $H(f)$ denotes the height of a polynomial f.

Theorem 6.3. *Let $f(x_1,\dots,x_d) \in \mathbb{Z}[x_1,\dots,x_d]$ of degree m. If f is not of the form $c \cdot g(x_1,\dots,x_d)^2$, where $c \in \mathbb{Q}$ and $g \in \mathbb{Q}[x_1,\dots,x_d]$, then there is some $B \in \mathbb{Z}$ such that $1 \le |B| \le H(f)^{O_{d,m}(1)}$ and for all primes $\ell \nmid B$,*

$$\sum_{x_1,\dots,x_d \in \mathbb{Z}/\ell\mathbb{Z}} \left(\frac{f(x_1,\dots,x_d)}{\ell}\right) \ll_{d,m} \ell^{d-1/2}.$$

Before proving Theorem 6.3, let us see how it can be used to construct N.

Proof of (6.10). We shall prove this relation with $N = \mathscr{C}(F)B_1\cdots B_k$, where B_j is the number B associated to the polynomial D_j by Theorem 6.3. Such a number exists because Gauss's lemma and our assumption that the polynomials $\pm D_j/\mathscr{C}(D_j)$ are not squares in $\mathbb{Z}[x_1,\dots,x_d]$ (see condition (5')) imply that D_j is not of the form $c\cdot g^2$, where $c \in \mathbb{Q}$ and g is a polynomial over $\mathbb{Q}$ in d variables. Moreover, $\mathscr{C}(F) \ll 1$ and $B_j \le H(D_j)^{O(1)} \le X^{O(1)}$, where we used condition (5) again. Therefore, $N \ll X^{O(1)}$, as claimed.

Now, fix a prime number $\ell \nmid LN$. Note that if $\ell \nmid F(\boldsymbol{n})D_1(\boldsymbol{n})\cdots D_k(\boldsymbol{n})$, then $\boldsymbol{n} \pmod{\ell} \in \mathcal{G}(\ell)$ and

$$\Delta_{\ell^r}(\boldsymbol{n}) = \delta_\ell(\boldsymbol{n}) = \frac{\lambda_1\left(\frac{D_1(\boldsymbol{n})}{\ell}\right) + \cdots + \lambda_k\left(\frac{D_k(\boldsymbol{n})}{\ell}\right)}{\ell} + O\left(\frac{1}{\ell^{1+\eta}}\right)$$

for all $r \ge 1$, by conditions (3') and (4'b). Set $D_0 = F$. Since $\|\Delta_{\ell^r}\|_\infty \ll 1/\ell$ and $\mathcal{G}(\ell^r) = \{\boldsymbol{g} \in \mathbb{Z}/\ell^r\mathbb{Z} : \boldsymbol{g} \pmod{\ell} \in \mathcal{G}(\ell)\}$, we have that

$$\begin{aligned}\frac{1}{|\mathcal{G}(\ell^r)|}\sum_{\boldsymbol{n}\in\mathcal{G}(\ell^r)}\Delta_{\ell^r}(\boldsymbol{n}) &= \frac{1}{|\mathcal{G}(\ell^r)|\ell}\sum_{j=1}^k\lambda_j\sum_{\boldsymbol{n}\in\mathcal{G}(\ell^r)}\left(\frac{D_j(\boldsymbol{n})}{\ell}\right)\\ &\quad + O\left(\frac{1}{\ell^{1+\eta}} + \sum_{j=0}^k\frac{\#\{\boldsymbol{n}\in(\mathbb{Z}/\ell^r\mathbb{Z})^d : \ell|D_j(\boldsymbol{n})\}}{|\mathcal{G}(\ell^r)|\ell}\right)\\ &= \frac{1}{|\mathcal{G}(\ell)|\ell}\sum_{j=1}^k\lambda_j\sum_{\boldsymbol{n}\in\mathcal{G}(\ell)}\left(\frac{D_j(\boldsymbol{n})}{\ell}\right) + O\left(\frac{1}{\ell^{1+\eta}} + \sum_{j=0}^k\frac{\rho_{D_j}(\ell)}{|\mathcal{G}(\ell)|\ell}\right).\end{aligned}$$

The polynomial D_0 is non-zero mod ℓ because $\ell \nmid \mathscr{C}(F) = \mathscr{C}(D_0)$, and the same is true for $D_1,\dots,D_k$, because $\ell \nmid B_1\cdots B_k$, whence

$$\sum_{j=0}^k\frac{\rho_{D_j}(\ell)}{|\mathcal{G}(\ell)|\ell} \ll \frac{1}{|\mathcal{G}(\ell)|\ell}.$$

Combining the above estimates with (4.7) that states that $|\mathcal{G}(\ell)| = \ell^d + O(\ell^{d-\eta})$, we conclude that

$$\frac{1}{|\mathcal{G}(\ell^r)|}\sum_{\boldsymbol{n}\in\mathcal{G}(\ell^r)}\Delta_{\ell^r}(\boldsymbol{n}) = \frac{1}{\ell^{d+1}}\sum_{j=1}^k\lambda_j\sum_{\boldsymbol{n}\in(\mathbb{Z}/\ell\mathbb{Z})^d}\left(\frac{D_j(\boldsymbol{n})}{\ell}\right) + O\left(\frac{1}{\ell^{1+\eta}}\right).$$

Finally, the condition that $\ell \nmid B_1 \cdots B_k$ implies that D_j cannot be of the form $cg^2 \bmod \ell$. Applying Theorem 6.3 and letting $r \to \infty$ then completes the proof of (6.10). □

In order to complete the proof of (6.10), and thus of Theorem 4.2, it remains to prove Theorem 6.3. We need a preliminary result.

Lemma 6.4. *Let $d, m \in \mathbb{N}$ and set $N = (2m+1)^d - (m+1)^d$. There are homogenous polynomials $S_1, \ldots, S_N$ over $\mathbb{Z}$ in $(2m+1)^d$ variables, depending at most on m and d, with the following property. If K is a field of characteristic different from 2 and*

$$f(x_1, \ldots, x_d) = \sum_{0 \le i_1, \ldots, i_d \le 2m} c_{i_1, \ldots, i_d} x_1^{i_1} \cdots x_d^{i_d} \in K[x_1, \ldots, x_d]$$

with $c_{0,\ldots,0} \neq 0$, then f is of the form $c \cdot g^2$, where $c \in K$ and g is an element of the ring $K[x_1, \ldots, x_d]$, if, and only if, $S_j(\{c_{i_1,\ldots,i_d} : 0 \le i_1, \ldots, i_d \le 2m\}) = 0$ for all $j \in \{1, \ldots, N\}$.

Proof. We shall denote $(i_1, \ldots, i_d)$ by $\boldsymbol{i}$, and $(0, \ldots, 0)$ by $\mathbf{0}$. Also, we write $\boldsymbol{i} \le \boldsymbol{j}$ if $i_n \le j_n$ for all $n \in \{1, \ldots, d\}$. Set $\tilde{f} = f/c_{\mathbf{0}}$. The coefficients of $\tilde{f}$ are the numbers $\tilde{c}_{\boldsymbol{i}} := c_{\boldsymbol{i}}/c_{\mathbf{0}}$. In particular, $\tilde{c}_{\mathbf{0}} = 1$. Clearly, f is of the form cg^2 if, and only if, $\tilde{f}$ is of the same form. If, now, $\tilde{f} = cg^2$, then we must have that $g(\mathbf{0})^2 = 1/c$. This means that we may restrict our attention to studying whether the equation $\tilde{f} = g^2$ has a solution with $g(\mathbf{0}) = 1$. This condition is equivalent to the existence of coefficients $a_{\boldsymbol{i}} \in K$, $0 \le i_1, \ldots, i_d \le m$, such that $a_{\mathbf{0}} = 1$ and

$$\sum_{\boldsymbol{i}+\boldsymbol{j}=\boldsymbol{k}} a_{\boldsymbol{i}} a_{\boldsymbol{j}} = \tilde{c}_{\boldsymbol{k}}, \tag{6.11}$$

for $0 \le k_1, \ldots, k_d \le 2m$. We claim that the conditions (6.11) for $k_1, \ldots, k_d \le m$ are altogether equivalent to having that

$$a_{\boldsymbol{i}} = P_{\boldsymbol{i}}(\{\tilde{c}_{\boldsymbol{r}} : \boldsymbol{r} \le \boldsymbol{i}\})$$

for $\boldsymbol{i} \neq \mathbf{0}$, where $P_{\boldsymbol{i}}$ is a polynomial in $(i_1+1)\cdots(i_d+1)$ variables, whose coefficients are of the form $2^v n$ with $n, v \in \mathbb{Z}$. Indeed, since $a_{\mathbf{0}} = 1$, we have that

$$2a_{\boldsymbol{k}} = \tilde{c}_{\boldsymbol{k}} - \sum_{\substack{\boldsymbol{i}+\boldsymbol{j}=\boldsymbol{k} \\ \boldsymbol{i},\boldsymbol{j} \neq \mathbf{0}}} a_{\boldsymbol{i}} a_{\boldsymbol{j}} \quad (k_1, \ldots, k_d \le m).$$

Proceeding by induction on $\sum_{n=1}^d k_n$ proves our claim about the polynomials P_i (where it is clear that the coefficients of P_i depends only on m and d). Finally, we substitute the expressions we have found for $a_{\boldsymbol{i}}$ to (6.11) when at least one of the k_n's is $> m$. This implies that relation (6.11) with $0 \le k_1, \ldots, k_d \le 2m$ is actually equivalent to the relations

$$\tilde{c}_{\boldsymbol{k}} = \sum_{\boldsymbol{i}+\boldsymbol{j}=\boldsymbol{k}} P_{\boldsymbol{i}}(\{\tilde{c}_{\boldsymbol{r}} : \boldsymbol{r} \le \boldsymbol{i}\}) \cdot P_{\boldsymbol{j}}(\{\tilde{c}_{\boldsymbol{r}} : \boldsymbol{r} \le \boldsymbol{j}\}) \quad (m < \max\{k_1, \ldots, k_d\} \le 2m).$$

Multiplying by a high enough power of $c_{\mathbf{0}}$ the above equations yields $(2m+1)^d - (m+1)^d$ homogeneous polynomial equations in the coefficients of f that are equivalent to f being of the form cg^2. This completes the proof of the lemma. □

Proof of Theorem 6.3. All implied constants might depend on d and m. It is easy to see by induction on d that there are integers $n_1, \ldots, n_d \in [0, m]$ such that $f(n_1, \ldots, n_d) \neq 0$. So, replacing f by $\tilde{f}(x_1, \ldots, x_d) = f(x_1 + n_1, \ldots, x_d + n_d)$, we may assume without loss of generality that $f(\mathbf{0}) \neq 0$. Since f is not of the form cg^2 over $\mathbb{Q}$, Lemma 6.4 implies that there is some integer polynomial expression in the coefficients of f, let's call it B', which is not zero. Moreover, if $\ell \nmid B'$, where ℓ is an odd prime, and $\ell \nmid f(0,\dots,0)$, then the same lemma implies that $f(x_1,\dots,x_d)$ is not of the form $c\cdot g(x_1,\dots,x_d)^2$ modulo ℓ. We will show that the theorem holds with $B = 2B'f(\mathbf{0}) = H(f)^{O(1)}$. So, we need to show that if $\ell \nmid B$, then

$$\sum_{x_1,\dots,x_d\in\mathbb{Z}/\ell\mathbb{Z}} \left(\frac{f(x_1,\dots,x_d)}{\ell}\right) \ll \ell^{d-1/2}. \tag{6.12}$$

It suffices to show that if ℓ is an odd prime such that $\ell \nmid f(\mathbf{0})$ and modulo which f is not of the form cg^2, then (6.12) is true. Fix such a prime ℓ. We argue by induction on d. If $d=1$, then this follows by [23, Theorem 11.13, p. 281] applied to the curve $y^2 = f(x_1)$. (Note that the condition there that the polynomial $y^2 - f(x_1)$ is absolutely irreducible is equivalent to f not being of the form cg^2.) Assume now that the theorem is true for polynomials of $< d$ variables. We write

$$f(x_1,\dots,x_d) = \sum_{j=0}^{m} c_j(x_1,\dots,x_{d-1})x_d^j. \tag{6.13}$$

We have that $c_0(\mathbf{0}) = f(\mathbf{0}) \not\equiv 0 \pmod{\ell}$. In particular, c_0 is non-zero mod ℓ. We distinguish two cases.

Case 1: $c_0 f$ is a perfect square mod ℓ. In this case, we can reduce to the case of $d-1$ variables: we have that

$$\begin{aligned}\sum_{x_1,\dots,x_d\in\mathbb{Z}/\ell\mathbb{Z}} \left(\frac{f(x_1,\dots,x_d)}{\ell}\right) &= \sum_{\substack{x_1,\dots,x_d\in\mathbb{Z}/\ell\mathbb{Z}\\ c_0(x_1,\dots,x_{d-1})\neq 0\\ f(x_1,\dots,x_d)\neq 0}} \left(\frac{c_0(x_1,\dots,x_{d-1})}{\ell}\right) + O(\ell\cdot\rho_{c_0}(\ell)+\rho_f(\ell))\\ &= \ell \sum_{x_1,\dots,x_{d-1}\in\mathbb{Z}/\ell\mathbb{Z}} \left(\frac{c_0(x_1,\dots,x_{d-1})}{\ell}\right) + O(\ell^{d-1}),\end{aligned}$$

by Lemma 6.2(a). Since $c_0 f$ is a perfect square and f is not of the form cg^2 mod ℓ, we must have that c_0 is not of the form cg^2 mod ℓ either. Moreover, $\ell \nmid c_0(\mathbf{0}) = f(\mathbf{0})$, and the induction hypothesis implies (6.12) in this case.

Case 2: $c_0 f$ is not a perfect square mod ℓ. We claim that in this case there are $O(\ell^{d-2})$ choices of $n_1,\dots,n_{d-1}\in\mathbb{Z}/\ell\mathbb{Z}$ such that the polynomial $f(n_1,\dots,n_{d-1},x_d)$ is of the form $c\cdot g(x_d)^2$ mod ℓ as a polynomial of x_d. This suffices to deduce (6.12). Indeed, if $n_1,\dots,n_{d-1}$ are such that $f(n_1,\dots,n_{d-1},x_d)$ is not of the form $c\cdot g(x_d)^2$ mod ℓ, then applying (6.12) with $d=1$ implies that

$$\sum_{x_d\in\mathbb{Z}/\ell\mathbb{Z}} \left(\frac{f(n_1,\dots,n_{d-1},x_d)}{\ell}\right) \ll \ell^{1/2},$$

and the proof of the inductive step is completed. Thus, it suffices to prove our claim.

Fix $n_1,\dots,n_{d-1}$ such that $f(n_1,\dots,n_{d-1},x_d)$ is of the form $c\cdot g(x_d)^2$ as a polynomial of x_d. The coefficients of $f(n_1,\dots,n_{d-1},x_d)$ as a polynomial of x_d are given by (6.13). By Lemma 6.2(a), there are only $O(\ell^{d-2})$ choices of $n_1,\dots,n_{d-1}$ such that $c_0(n_1,\dots,n_{d-1}) \equiv 0 \pmod{\ell}$. Assume, now, that $c_0(n_1,\dots,n_{d-1}) \not\equiv 0 \pmod{\ell}$. Then, following the proof of Lemma 6.4, we see that $F(x_d) = f(n_1,\dots,n_{d-1},x_d)/c_0(n_1,\dots,n_{d-1})$ must be of the form $(1 + a_1x_d + \cdots +$

$a_{m'}x_d^{m'})^2$, for certain integers a_j which are polynomial expressions in the coefficients of F, that is to say the a_j's are polynomials in the rational functions $c_i(n_1,\dots,n_{d-1})/c_0(n_1,\dots,n_{d-1})$, $1\le i\le d$. Multiplying through by $c_0(n_1,\dots,n_{d-1})^{2k}$ for a large enough k, we see that

$$c_0(n_1,\dots,n_{d-1})^{2k-1}f(n_1,\dots,n_{d-1},x_d)\equiv h(n_1,\dots,n_{d-1},x_d)^2 \pmod{\ell} \tag{6.14}$$

for all $x_d\in\mathbb{Z}/\ell\mathbb{Z}$, where h is some polynomial in $\mathbb{Z}[x_1,\dots,x_d]$. However, we know that the polynomial

$$c_0(x_1,\dots,x_{d-1})^{2k-1}f(x_1,\dots,x_d)-h(x_1,\dots,x_d)^2$$

is non-zero in the polynomial ring $(\mathbb{Z}/\ell\mathbb{Z})[x_1,\dots,x_d]$, by our assumption that c_0f is not a perfect square and the fact that $(\mathbb{Z}/\ell\mathbb{Z})[x_1,\dots,x_d]$ is a unique factorisation domain. Consequently, Lemma 6.2(a) implies that the number of $n_1,\dots,n_{d-1}$ for which (6.14) holds for all $x_d\in\mathbb{Z}/\ell\mathbb{Z}$ is $\ll \ell^{d-2}$. This completes the proof of our claim that there are $O(\ell^{d-2})$ choices of $n_1,\dots,n_{d-1}\in\mathbb{Z}/\ell\mathbb{Z}$ such that the polynomial $f(n_1,\dots,n_{d-1},x_d)$ is of the form $c\cdot g(x_d)^2$ as a polynomial of x_d. Hence, (6.12) follows in this last case too. This completes the proof of Lemma 6.3. □

7. An auxiliary result

We prove here the promised estimate needed to handle the main and the error term in the proof of Theorems 1.4 and 1.6. The main input to our result is the following estimate about primes in short arithmetic progressions, proven in [27].

Lemma 7.1. *Fix $\epsilon>0$ and $A\ge 1$. For $x\ge h\ge 2$ and $1\le Q^2\le h/x^{1/6+\epsilon}$, we have that*

$$\int_x^{2x}\sum_{q\le Q}E(y,h;q)\mathrm{d}y\ll\frac{xh}{(\log x)^A},$$

where $E(y,h;q)$ is defined by (1.6).

Lemma 7.2. *Fix $\epsilon>0$, $A\ge 1$ and two integers $d\ge 2$ and $m\in\{0,1,\dots,d\}$. Given a d-tuple $\boldsymbol{p}$ in the set*

$$\mathcal{P}_d'(x):=\{(p_1,\dots,p_d):x<p_1\le 2x,\ |p_{j+1}-p_j-1|<2\sqrt{p_j}\ (1\le j\le d)\ \text{with}\ p_{d+1}=p_1\},$$

we let

$$w_{\boldsymbol{p}}=\prod_{j=1}^m\frac{1}{\sqrt{p_j}}\sqrt{1-\left(\frac{p_j+1-p_{j+1}}{2\sqrt{p_j}}\right)^2}.$$

Then,

$$\sum_{q\le x^{1/6-\epsilon}}q^{d-1}\max_{\boldsymbol{a}\in((\mathbb{Z}/q\mathbb{Z})^*)^d}\left|\sum_{\substack{\boldsymbol{p}\in\mathcal{P}_d'(x)\\ \boldsymbol{p}\equiv\boldsymbol{a}\,(\mathrm{mod}\,q)}}w_{\boldsymbol{p}}-\frac{I_{d,m}}{\phi(q)^d}\cdot\int_x^{2x}\frac{u^{(d-m-1)/2}\mathrm{d}u}{(\log u)^d}\right|\ll_{A,\epsilon,d}\frac{x^{(d-m+1)/2}}{(\log x)^A}$$

for all $x\ge 3$, where

$$I_{d,m}=2^{d-1}\int\cdots\int_{\substack{|t_j|\le 1\ (1\le j\le d)\\ t_1+\cdots+t_d=0}}\prod_{j=1}^m\sqrt{1-t_j^2}\ \mathrm{d}t_1\cdots\mathrm{d}t_{d-1}.$$

Proof. We fix a parameter $B = B(A)$ and set $\eta = 1/(\log x)^B$. Furthermore, we set $N = \lfloor (\log x)^B \rfloor - 1$, so that $(N+1)\eta \le 1 < (N+2)\eta$. Note that if $\boldsymbol{p} \in \mathcal{P}_d'(x)$, then $|p_{j+1} - p_j| \ll \sqrt{p_j}$ for all j. In particular, $p_{j+1} \asymp p_j$, which implies that $p_j \asymp p_1 \asymp x$ for all j. So, we find that $|p_{j+1} - p_j| \ll \sqrt{x}$ and, consequently, $|p_j - p_1| \ll \sqrt{x}$ for all $j \in \{1, \dots, d\}$. In particular, $\sqrt{p_j} = \sqrt{p_1} + O(1)$ by the Mean Value Theorem. If we let

$$\mathcal{Q} = \{\boldsymbol{p} : x < p_1 \le (1 + N\eta)x, \quad |p_{j+1} - p_j| < 2\sqrt{p_1} N\eta \ (1 \le j \le d)\},$$

with the usual convention that $p_{d+1} = p_1$, then we see that $\mathcal{Q} \subset \mathcal{P}_d'(x)$ and that

$$\sum_{\substack{\boldsymbol{p} \in \mathcal{P}_d'(x) \setminus \mathcal{Q} \\ \boldsymbol{p} \equiv \boldsymbol{a} \pmod{q}}} \prod_{j=1}^{m} \frac{1}{\sqrt{p_j}} \sqrt{1 - \left(\frac{p_j + 1 - p_{j+1}}{2\sqrt{p_j}}\right)^2} \ll \frac{x^{(d-m+1)/2}}{q^d \cdot (\log x)^B}.$$

For each $\boldsymbol{r} \in ([1, N] \times [-N+1, N]^{d-1}) \cap \mathbb{Z}^d$ with $|r_2 + \cdots + r_d| \le N$, we define

$$\mathcal{Q}(\boldsymbol{r}) = \Bigg\{ \boldsymbol{p} : x(1 + (r_1 - 1)\eta) < p_1 \le x(1 + r_1\eta),$$
$$(r_{j+1} - 1)\eta < \frac{p_{j+1} - p_j}{2\sqrt{x(1 + r_1\eta)}} \le r_{j+1}\eta \ (1 \le j < d) \Bigg\}.$$

If $r_{d+1} := -(r_2 + \cdots + r_d)$, then

$$\frac{p_d - p_{d+1}}{2\sqrt{x(1 + r_1\eta)}} = \frac{p_d - p_1}{2\sqrt{x(1 + r_1\eta)}} = \sum_{j=1}^{d-1} \frac{p_{j+1} - p_j}{2\sqrt{x(1 + r_1\eta)}} = \sum_{j=2}^{d} r_j\eta + O(\eta) = -\eta r_{d+1} + O(\eta),$$

Let $\mathcal{H}$ be the set of $\boldsymbol{r} \in ([1, N] \times [-N + C, N - C]^{d-1}) \cap \mathbb{Z}^d$ with $|r_{d+1}| \le N - C$, where C is some large constant, and call $\mathcal{Q}'$ the union of $\mathcal{Q}(\boldsymbol{r})$ over $\boldsymbol{r} \in \mathcal{H}$. If C is large enough, then it is easy to see that $\mathcal{Q}' \subset \mathcal{Q}$. Moreover, we have that

$$\sum_{\substack{\boldsymbol{p} \in \mathcal{Q} \setminus \mathcal{Q}' \\ \boldsymbol{p} \equiv \boldsymbol{a} \pmod{q}}} w_{\boldsymbol{p}} \ll \frac{x^{(d-m+1)/2}}{q^d \cdot (\log x)^B}.$$

Since $|\mathcal{H}| \asymp \eta^{-d}$, it suffices to show that

$$\sum_{q \le x^{1/6-\epsilon}} q^{d-1} \max_{\boldsymbol{a} \in ((\mathbb{Z}/q\mathbb{Z})^*)^d} \left| \sum_{\substack{\boldsymbol{p} \in \mathcal{Q}(\boldsymbol{r}) \\ \boldsymbol{p} \equiv \boldsymbol{a} \pmod{q}}} w_{\boldsymbol{p}} - \frac{2^{d-1} I(\boldsymbol{r})}{\phi(q)^d} \right| \ll \frac{\eta^d x^{(d-m+1)/2}}{(\log x)^A}, \tag{7.1}$$

where, for each $\boldsymbol{r} = (r_1, \dots, r_d) \in \mathcal{H}$, we define

$$x_1 = x + r_1\eta x$$

and

$$I(\boldsymbol{r}) = \int_{x_1 - \eta x}^{x_1} \frac{u^{(d-m-1)/2} \mathrm{d}u}{(\log u)^d} \underset{\substack{(r_{j+1}-1)\eta \le t_j \le r_{j+1}\eta \\ (1 \le j \le d-1) \\ t_1 + \cdots + t_d = 0}}{\int \cdots \int} \prod_{j=1}^{m} \sqrt{1 - t_j^2} \, \mathrm{d}t_1 \cdots \mathrm{d}t_{d-1}.$$

If $\boldsymbol{r}$ and x_1 are as above and $\boldsymbol{p} \in \mathcal{Q}(\boldsymbol{r})$, then

$$\frac{p_{j+1} - p_j - 1}{2\sqrt{p_j}} = \frac{\eta r_{j+1}\sqrt{x_1} + O(\eta\sqrt{x_1})}{(1 + O(\eta))\sqrt{x_1}} = \eta r_{j+1} + O(\eta) \quad (1 \le j \le d),$$

where we used the fact that $r_j \ll N \asymp 1/\eta$. Thus, if C is large enough, our assumption that $|r_j| \le N - C = 1/\eta - C + O(1)$ implies that $|1 - \eta|r_{j+1}| \gg \eta$. Applying the Mean Value Theorem we then find that

$$\begin{aligned}\prod_{j=1}^{m} \sqrt{1 - \left(\frac{p_{j+1} - p_j - 1}{2\sqrt{p_j}}\right)^2} &= \prod_{j=1}^{m} \sqrt{1 - (r_{j+1}\eta)^2} + O\left(\sum_{j=1}^{m} \frac{\eta}{\sqrt{1 - |r_{j+1}\eta|}}\right) \\ &= \frac{1}{\eta^{d-1}} \mathop{\int\cdots\int}_{\substack{(r_{j+1}-1)\eta \le t_j \le r_{j+1}\eta \\ (1 \le j \le d-1) \\ t_1 + \cdots + t_d = 0}} \prod_{j=1}^{m} \sqrt{1 - t_j^2}\, \mathrm{d}t_1 \cdots \mathrm{d}t_{d-1} + O(\sqrt{\eta})\end{aligned}$$

for all $\boldsymbol{p} \in \mathcal{Q}(\boldsymbol{r})$, where the condition $t_d = -(t_1 + \cdots + t_{d-1})$ comes from the fact that $r_{d+1} = -\sum_{j=2}^{d} r_j$. Moreover, we have that

$$\begin{aligned}\prod_{j=1}^{m} \frac{1}{\sqrt{p_j}} &= \frac{(\log p_1) \cdots (\log p_d)}{(\log x_1)^d x_1^{m/2}}(1 + O(\eta)) \\ &= \frac{1}{\eta x \cdot x_1^{(d-1)/2}} \left(\prod_{j=1}^{d} \log p_j\right) \int_{x_1 - \eta x}^{x_1} \frac{u^{(d-m-1)/2}}{(\log u)^d} \mathrm{d}u + O(\eta x^{-m/2}).\end{aligned}$$

Therefore, we conclude that

$$\sum_{\substack{\boldsymbol{p} \in \mathcal{Q}(\boldsymbol{r}) \\ \boldsymbol{p} \equiv a \pmod{q}}} \prod_{j=1}^{m} \frac{1}{\sqrt{p_j}} \sqrt{1 - \left(\frac{p_j + 1 - p_{j+1}}{2\sqrt{p_j}}\right)^2} = \frac{I(\boldsymbol{r}) \cdot S(\boldsymbol{r}; q, \boldsymbol{a})}{\eta^d x x_1^{(d-1)/2}} + O\left(\frac{\eta^{d+1/2} x^{(d-m+1)/2}}{q^d}\right),$$

where

$$S(\boldsymbol{r}; q, \boldsymbol{a}) = \sum_{\substack{\boldsymbol{p} \in \mathcal{Q}(\boldsymbol{r}) \\ \boldsymbol{p} \equiv \boldsymbol{a} \pmod{q}}} \prod_{j=1}^{d} \log p_j.$$

So, taking $B \ge 2A + 2$, we see that (7.1) is reduced to showing that

$$\sum_{q \le x^{1/6-\epsilon}} q^{d-1} \max_{\boldsymbol{a} \in ((\mathbb{Z}/q\mathbb{Z})^*)^d} \left| \frac{S(\boldsymbol{r}; q, \boldsymbol{a})}{\eta^d x x_1^{(d-1)/2}} - \frac{2^{d-1}}{\phi(q)^d} \right| \ll \frac{\eta^d x^{(d-m+1)/2}}{I(\boldsymbol{r}) \cdot (\log x)^A}.$$

Since

$$I(\boldsymbol{r}) \ll \frac{\eta^d x^{(d-m+1)/2}}{(\log x)^d},$$

it is enough to prove that

$$\sum_{q \le x^{1/6-\epsilon}} q^{d-1} \max_{\boldsymbol{a} \in ((\mathbb{Z}/q\mathbb{Z})^*)^d} \left| S(\boldsymbol{r}; q, \boldsymbol{a}) - \frac{2^{d-1} \eta^d x x_1^{(d-1)/2}}{\phi(q)^d} \right| \ll \frac{\eta^d x^{(d+1)/2}}{(\log x)^A}. \tag{7.2}$$

In order to prove (7.2), we start by observing that

$$S(\boldsymbol{r};q,\boldsymbol{a}) = \sum_{\substack{x_1-\eta x<p_1\le x_1\\ p_1\equiv a_1 \,(\mathrm{mod}\, q)}} (\log p_1) \sum_{\substack{r_2-1<\frac{p_2-p_1}{2\eta\sqrt{x_1}}\le r_2\\ p_2\equiv a_2 \,(\mathrm{mod}\, q)}} (\log p_2)\cdots \sum_{\substack{r_d-1<\frac{p_d-p_{d-1}}{2\eta\sqrt{x_1}}\le r_d\\ p_d\equiv a_d \,(\mathrm{mod}\, q)}} \log p_d$$

We replace the last sum by $2\eta\sqrt{x_1}/\phi(q)$, which introduces a total error term of size

$$\sum_{\substack{x_1-\eta x<p_1\le x_1\\ p_1\equiv a_1 \,(\mathrm{mod}\, q)}} (\log p_1) \sum_{\substack{r_2-1<\frac{p_2-p_1}{2\eta\sqrt{x_1}}\le r_2\\ p_2\equiv a_2 \,(\mathrm{mod}\, q)}} (\log p_2)\cdots \sum_{\substack{r_{d-1}-1<\frac{p_{d-1}-p_{d-2}}{2\eta\sqrt{x_1}}\le r_{d-1}\\ p_{d-1}\equiv a_{d-1} \,(\mathrm{mod}\, q)}} (\log p_{d-1})$$
$$\times E(p_{d-1}+2(r_d-1)\eta\sqrt{x_1}, 2\eta\sqrt{x_1}; q),$$

where $E(x,h;q)$ is defined by (1.6). We estimate this error term by fixing p_{d-1} and summing first over $p_1,\dots,p_{d-2}$. Note that p_{d-1} lies in an interval of size $O(\eta x)$ around x_1 and, given p_{d-1}, the primes $p_1,\dots,p_{d-2}$ lie in intervals of length $O(\eta\sqrt{x})$ around p_{d-1}. Using the Brun-Titschmarsh inequality for the sums over $p_1,\dots,p_{d-2}$, we find that the error term is bounded by some absolute constant times

$$\left(\frac{\eta\sqrt{x}}{\phi(q)}\right)^{d-2} \sum_{\substack{x_1-O(\eta x)<p_{d-1}\le x_1+O(\eta x)\\ p_{d-1}\equiv a_{d-1} \,(\mathrm{mod}\, q)}} (\log p_{d-1}) E(p_{d-1}+2(r_d-1)\eta\sqrt{x_1}, 2\eta\sqrt{x_1}; q).$$

For each y within $\eta^2\sqrt{x_1}$ of $p_{d-1}+2(r_d-1)\eta\sqrt{x_1}$, the Brun-Titschmarsh inequality implies that

$$E(y,2\eta\sqrt{x_1};q) - E(p_{d-1}+2(r_d-\eta)\sqrt{x_1}, 2\eta\sqrt{x}; q) \ll \frac{\eta^2\sqrt{x}}{\phi(q)}.$$

Therefore

$$E(p_{d-1}+2(r_d-\eta)\sqrt{x_1}, 2\eta\sqrt{x_1}; q) = \frac{1}{\eta^2\sqrt{x_1}} \int_{p_{d-1}+2(r_d-1)\eta\sqrt{x_1}}^{p_{d-1}+2(r_d-1)\eta\sqrt{x_1}+\eta^2\sqrt{x_1}} E(y,2\eta\sqrt{x_1};q)\mathrm{d}y$$
$$+O\left(\frac{\eta^2\sqrt{x}}{\phi(q)}\right).$$

for $y\in[p_{d-1}+2(r_d-1)\eta\sqrt{x_1}, p_{d-1}+2(r_d-1)\eta\sqrt{x_1}+\eta^2\sqrt{x_1}]$. Summing this over $p_{d-1}\in[x_1-O(\eta x), x_1+O(\eta x)]$ and reversing the sums, we find that the total error introduced by replacing the sum over p_d by $2\eta\sqrt{x_1}/\phi(q)$ in $S(\boldsymbol{r};q,\boldsymbol{a})$ is

$$\ll \frac{1}{\eta^2\sqrt{x}}\cdot\left(\frac{\eta\sqrt{x}}{\phi(q)}\right)^{d-2} \int_{x/2}^{3x} E(y,2\eta\sqrt{x_1};q) \sum_{\substack{-\eta^2\sqrt{x}\le p_{d-1}+2(r_d-1)\eta\sqrt{x_1}-y\le 0\\ p_{d-1}\equiv a_{d-1} \,(\mathrm{mod}\, q)}} \log p_{d-1}\,\mathrm{d}y$$
$$+\frac{\eta^{d+1}x^{(d+1)/2}}{\phi(q)^d}$$
$$\ll \frac{(\eta\sqrt{x})^{d-2}}{\phi(q)^{d-1}} \int_{x/2}^{3x} E(y,2\eta\sqrt{x_1};q)\mathrm{d}y + \frac{\eta^{d+1}x^{(d+1)/2}}{\phi(q)^d}.$$

In conclusion, we have proven that

$$S(\boldsymbol{r};q,\boldsymbol{a})=\frac{2\eta\sqrt{x_1}}{\phi(q)}\sum_{\substack{x_1-\eta x<p_1\le x_1\\ p_1\equiv a_1\,(\mathrm{mod}\,q)}}(\log p_1)\sum_{\substack{r_2-1<\frac{p_2-p_1}{2\eta\sqrt{x_1}}\le r_2\\ p_2\equiv a_2\,(\mathrm{mod}\,q)}}(\log p_2)\cdots\sum_{\substack{r_{d-1}-1<\frac{p_{d-1}-p_{d-2}}{2\eta\sqrt{x_1}}\le r_{d-1}\\ p_{d-1}\equiv a_{d-1}\,(\mathrm{mod}\,q)}}\log p_{d-1}$$
$$+O\left(\frac{(\eta\sqrt{x})^{d-2}}{\phi(q)^{d-1}}\int_{x/2}^{3x}E(y,2\eta\sqrt{x_1};q)\mathrm{d}y+\frac{\eta^{d+1}x^{(d+1)/2}}{\phi(q)^d}\right).$$

Next, we replace the sum over p_{d-1} by $2\eta\sqrt{x_1}/\phi(q)$. The total error term produced can be shown to be

$$\ll\frac{(\eta\sqrt{x})^{d-2}}{\phi(q)^{d-1}}\int_{x/2}^{3x}E(y,2\eta\sqrt{x_1};q)\mathrm{d}y+\frac{\eta^{d+1}x^{(d+1)/2}}{\phi(q)^d}$$

by following the above argument. We continue this way to deduce that

$$\begin{aligned}S(\boldsymbol{r};q,\boldsymbol{a})&=\left(\frac{2\eta\sqrt{x_1}}{\phi(q)}\right)^{d-1}\sum_{\substack{x_1-\eta x<p_1\le x_1\\ p_1\equiv a_1\,(\mathrm{mod}\,q)}}(\log p_1)\\&\quad+O\left(\frac{(\eta\sqrt{x})^{d-2}}{\phi(q)^{d-1}}\int_{x/2}^{3x}E(y,2\eta\sqrt{x_1};q)\mathrm{d}y+\frac{\eta^{d+1}x^{(d+1)/2}}{\phi(q)^d}\right)\\&=\frac{2^{d-1}\eta^d x x_1^{(d-1)/2}}{\phi(q)^d}+O\left(\frac{(\eta\sqrt{x})^{d-1}}{\phi(q)^{d-1}}E(x_1-\eta x,\eta x;q)\right)\\&\quad+O\left(\frac{(\eta\sqrt{x})^{d-2}}{\phi(q)^{d-1}}\int_{x}^{3x}E(y,2\eta\sqrt{x_1};q)\mathrm{d}y+\frac{\eta^{d+1}x^{(d+1)/2}}{\phi(q)^d}\right).\end{aligned}$$

In view of the above formula, relation (7.2) follows by the Bombieri-Vinogradov theorem and by Lemma 7.1 with $Q=x^{1/6-\epsilon}$. □

References

[1] J. D. Achter. The distribution of class groups of function fields. *J. Pure Appl. Algebra*, 204(2):316–333, 2006.

[2] J. D. Achter. Results of Cohen-Lenstra type for quadratic function fields. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 1–7. Amer. Math. Soc., Providence, RI, 2008.

[3] S. Baier and L. Zhao. The Sato-Tate conjecture on average for small angles. *Trans. Amer. Math. Soc.*, 361(4):1811–1832, 2009.

[4] A. Balog, A. Cojocaru, and C. David. Average twin prime conjecture for elliptic curves. *Amer. J. Math.*, 133(5):1179–1229, 2011.

[5] W. D. Banks and I. E. Shparlinski. Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height. *Israel J. Math.*, 173:253–277, 2009.

[6] B. J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968.

[7] V. A. Bykovskiĭ, V. A. Density theorems and the mean value of arithmetic functions on short intervals Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI). 212 (1994) Anal. Teor. Chisel i Teor. Funktsii. 12, 56–70, 196; translation in J. Math. Sci. (New York) 83 (1997), no. 6, 720–730

[8] W. Castryck and H. Hubrechts. The distribution of the number of points modulo an integer on elliptic curves over finite fields. *Ramanujan J.*, 30(2):223–242, 2013.

[9] V. Chandee, C. David, D. Koukoulopoulos, and E. Smith. The frequency of elliptic curve groups over prime finite fields. 05 2014.

[10] H. Davenport. *Multiplicative Number Theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1980. Revised by Hugh L. Montgomery.

[11] C. David and F. Pappalardi. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices*, 1999(4):165–183, 1999.

[12] C. David and E. Smith. Corrigendum to: Elliptic curves with a given number of points over finite fields. *Compos. Math.* (to appear).

[13] C. David and E. Smith. Elliptic curves with a given number of points over finite fields. *Compos. Math.*, 149(2):175–203, 2013.

[14] C. David and E. Smith. A Cohen-Lenstra phenomenon for elliptic curves. *J. London Math. Soc.*, 89(1):24–44, 2014.

[15] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[16] E. Fouvry and M. R. Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.

[17] S. D. Galbraith and J. McKee. The probability that the number of points on an elliptic curve over a finite field is prime. *J. London Math. Soc. (2)*, 62(3):671–684, 2000.

[18] P. X. Gallagher. On the distribution of primes in short intervals. *Mathematika*, 23(1):4–9, 1976.

[19] P. X. Gallagher. Corrigendum: "On the distribution of primes in short intervals" [Mathematika **23** (1976), no. 1, 4–9; MR **53** #13140]. *Mathematika*, 28(1):86, 1981.

[20] E.-U. Gekeler. Frobenius distributions of elliptic curves over finite prime fields. *Int. Math. Res. Not.*, (37):1999–2018, 2003.

[21] A. Granville and K. Soundararajan. The distribution of values of $L(1,\chi_d)$. *Geom. Funct. Anal.*, 13(5):992–1028, 2003.

[22] E. W. Howe. On the group orders of elliptic curves over finite fields. *Compositio Math.*, 85(2):229–247, 1993.

[23] H. Iwaniec and E. Kowalski. *Analytic Number Theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[24] N. Jones. Averages of elliptic curve constants. *Math. Ann.*, 345(3):685–710, 2009.

[25] —. Elliptic aliquot cycles of fixed length. *Pacific J. Math.*, 263(2):353–371, 2013.

[26] N. Katz. Lang-trotter revisited.

[27] D. Koukoulopoulos. Primes in short arithmetic progressions. *Int. J. Number Theory*, 11(5):1499–1521, 2015.

[28] E. Kowalski. Averages of Euler products, distribution of singular series and the ubiquity of Poisson distribution. *Acta Arith.*, 148(2):153–187, 2011.

[29] S. Lang and H. Trotter. *Frobenius Distributions in* GL_2*-extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[30] H. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987.

[31] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[32] J. Parks. Amicable pairs and aliquot cycles on average. (With an appendix by S. Giri.) Preprint. arXiv:1403.5810

[33] —. An asymptotic for the average number of amicable pairs for elliptic curves. Preprint. arXiv:1410.5888

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

[35] J. H. Silverman and K. E. Stange. Amicable pairs and aliquot cycles for elliptic curves. *Exp. Math.*, 20(3):329–357, 2011.

[36] K. Soundararajan and M. Young. The prime geodesic theorem. J. Reine Angew. Math. 676 (2013), 105–120.

[37] C. L. Stewart. On the number of solutions of polynomial congruences and Thue equations. *J. Amer. Math. Soc.*, 4(4):793–835, 1991.

[38] S. G. Vlăduţ. Cyclicity statistics for elliptic curves over finite fields. *Finite Fields Appl.*, 5(1):13–25, 1999.

[39] D. Zagier. Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields. Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976). pp. 105–169. Lecture Notes in Math., Vol. 627, Springer, Berlin, 1977.

(Chantal David) Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve West, Montréal, Québec, H3G 1M8, Canada
E-mail address: `cdavid@mathstat.concordia.ca`

(Dimitris Koukoulopoulos) Département de mathématiques et de statistique, Université de Montréal, CP 6128 succ. Centre-Ville, Montréal, QC H3C 3J7, Canada
E-mail address: `koukoulo@dms.umontreal.ca`

(Ethan Smith) Department of Mathematics, Liberty University, 1971 University Blvd, MSC Box 710052, Lynchburg, VA 24502
E-mail address: `ecsmith13@liberty.edu`