A. C. Cojocaru *et al.* (2017) "Arithmetic Properties of the Frobenius Traces Defined by a Rational Abelian Variety (with two appendices by J-P. Serre)," International Mathematics Research Notices, Vol. 2017, No. 12, pp. 3557–3602
Advance Access Publication June 27, 2016
doi: 10.1093/imrn/rnw058

Arithmetic Properties of the Frobenius Traces Defined by a Rational Abelian Variety (with two appendices by J-P. Serre)

Alina Carmen Cojocaru[1,2,*], Rachel Davis[3], Alice Silverberg[4], and Katherine E. Stange[5]

[1]Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, IL 60607, USA, [2]Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania, [3]Department of Mathematics, Purdue University 150 N. University Street, West Lafayette, IN 47907, USA, [4]Department of Mathematics, University of California, Irvine, CA 92697-3875, USA and [5]Department of Mathematics, University of Colorado, Boulder, Campus Box 395, Boulder, 80305, CO, USA

[*]*Correspondence to be sent to: e-mail: cojocaru@uic.edu*

Let A be an abelian variety over $\mathbb{Q}$ of dimension g such that the image of its associated absolute Galois representation ρ_A is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. We investigate the arithmetic of the traces $a_{1,p}$ of the Frobenius at p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ under ρ_A. In particular, we obtain upper bounds for the counting function $\#\{p \leq x : a_{1,p} = t\}$ and we prove an Erdös–Kac-type theorem for the number of prime factors of $a_{1,p}$. We also formulate a conjecture about the asymptotic behaviour of $\#\{p \leq x : a_{1,p} = t\}$, which generalizes a well-known conjecture of Lang and Trotter from 1976 about elliptic curves.

Received September 25, 2015; Revised February 22, 2016; Accepted March 7, 2016

1 Introduction

Given an abelian variety $A/\mathbb{Q}$, its reductions $A_p/\mathbb{F}_p$ modulo primes encode deep arithmetic global information. A primary question related to these reductions concerns their p-Weil polynomials, in particular the coefficients of these polynomials.

In the simplest case when A has dimension 1, that is, when A is an elliptic curve over $\mathbb{Q}$, for each prime p of good reduction the p-Weil polynomial is $P_{A,p}(X) = X^2 - a_pX + p \in \mathbb{Z}[X]$, where $a_p := p + 1 - |A_p(\mathbb{F}_p)|$. The coefficient a_p satisfies the Weil bound $|a_p| < 2\sqrt{p}$ and is of major significance in number theory. For example, it appears as the pth Fourier coefficient in the expansion of the weight 2 newform associated to A. The study of a_p comes in several flavours, some having led to well-known problems in arithmetic geometry, such as the Sato–Tate Conjecture from the 1960s (now a theorem) and the Lang–Trotter Conjecture on Frobenius traces from the 1970s (still open).

Briefly, the Lang–Trotter Conjecture [35] on the behaviour of a_p predicts that for every elliptic curve $A/\mathbb{Q}$ and every integer $t \in \mathbb{Z}$, if $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ or $t \neq 0$, and if we write N_A for the product of the primes of bad reduction for A, then either there are at most finitely many primes p such that $a_p = t$ or there exists a constant $c(A,t) > 0$ such that, as $x \to \infty$,

$$\pi_A(x,t) := \#\left\{p \leq x : p \nmid N_A, a_p = t\right\} \sim c(A,t)\frac{\sqrt{x}}{\log x}. \tag{1}$$

The constant $c(A,t)$ has a precise heuristic description derived from the Chebotarev Density Theorem, combined with the Sato–Tate Conjecture when $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ and with a prime distribution law arising from works of Deuring and Hecke when $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \not\simeq \mathbb{Z}$.

While the Lang–Trotter Conjecture remains open, several remarkable related results have been proven. When $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \not\simeq \mathbb{Z}$ (the CM case) and $t \neq 0$, upper bounds of the right order of magnitude can be proved using sieve methods. When $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ and $t \neq 0$, weaker upper bounds, unconditional or conditional (upon the Generalized Riemann Hypothesis, GRH), can be proved using effective versions of the Chebotarev Density Theorem; such bounds were first obtained by Serre [42, Theorem 20]. The currently best unconditional upper bound, $\pi_A(x,t) \ll_A \frac{x(\log\log x)^2}{(\log x)^2}$, was obtained by V. K. Murty [38, Theorem 5.1] (see [48] for an earlier result), while the currently best upper bound under GRH, $\pi_A(x,t) \ll_A \frac{x^{\frac{4}{5}}}{(\log x)^{\frac{1}{5}}}$, was obtained by Murty, Murty, and Saradha [37, Theorem 4.2] (for very recent improvements on the exponent of the $\log x$ factor, see [52]). When $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$ and $t = 0$, stronger results are known; in particular, the unconditional bounds $\frac{\log\log\log x}{(\log\log\log\log x)^{1+\varepsilon}} \ll_\varepsilon$

$\pi_A(x,0) \ll x^{\frac{3}{4}}$ were obtained by Fouvry and M. R. Murty [22, Theorem 1] and, respectively, by Elkies [19] using, as a key tool, Deuring's characterization of supersingular primes [17].

Inspired by these works, the main goal of our article is to investigate the arithmetic of the Frobenius traces of a generic higher-dimensional abelian variety $A/\mathbb{Q}$; in particular:

(i) we will prove upper bounds for the generalization of the counting function $\pi_A(x,t)$ and deduce results on the growth of the Frobenius traces;
(ii) we will determine the normal order of the sequence defined by the prime divisor function of the Frobenius traces, and, more generally, we will prove an Erdös–Kac-type result for this sequence;
(iii) under suitable hypotheses, we will formulate a generalization of (1).

Our main results mark only the beginning of such investigations in higher dimensions and we hope shall stimulate further research.

Our main setting and notation are as follows. Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g. Let $\overline{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$ and let $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ denote the endomorphism ring of A over $\overline{\mathbb{Q}}$. Let N_A be the product of primes of bad reduction for A.

We denote by

$$\rho_A : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$$

the absolute Galois representation defined by the inverse limit of the representations

$$\bar{\rho}_{A,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$$

of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the m-torsion $A[m] \subset A(\overline{\mathbb{Q}})$ for each integer $m \geq 1$. For each prime ℓ we denote by

$$\rho_{A,\ell} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$$

the ℓ-adic representation, that is, the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the ℓ-adic Tate module $\varprojlim A[\ell^n]$.

For each prime $p \nmid N_A$, we consider the p-Weil polynomial $P_{A,p}(X)$ of A, which is uniquely determined by the property that

$$P_{A,p}(X) = \det\left(XI_{2g} - \rho_{A,\ell}\left(\mathrm{Frob}_p\right)\right) \tag{2}$$

for any prime $\ell \neq p$. In particular, we have

$$P_{A,p}(X) \equiv \det\left(XI_{2g} - \bar{\rho}_{A,m}\left(\mathrm{Frob}_p\right)\right) \pmod{m} \tag{3}$$

for any integer m coprime to p. We write

$$P_{A,p}(X) = X^{2g} + a_{1,p}X^{2g-1} + \cdots + a_{g,p}X^g + pa_{g-1,p}X^{g-1} + \cdots + p^{g-1}a_{1,p}X + p^g \in \mathbb{Z}[X],$$

where the integers $a_{i,p}$, $1 \leq i \leq g-1$, are independent of ℓ.

For any integer $t \in \mathbb{Z}$, we consider the function

$$\pi_A(x,t) := \#\left\{p \leq x : p \nmid N_A, a_{1,p} = t\right\}.$$

The reason we usually impose the restriction that our abelian varieties be principally polarized is for ease of notation. When the abelian variety is principally polarized, the image of the ℓ-adic representation $\rho_{A,\ell}$ lies in $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. Without the restriction on the polarization, the image lies in a group that can be defined by replacing the matrix J_{2g} of Section 2.1 below with a matrix that has a more complicated description, and our results could be modified accordingly; see, for example, Section 2.3 of [43] for the group of symplectic similitudes in this general setting.

Theorem 1. Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g and let $t \in \mathbb{Z}$. Assume that $\mathrm{Im}\,\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. Define

$$\alpha := \frac{1}{2g^2+g+1}, \qquad \beta := \begin{cases} \frac{1}{3} & \text{if } g = 1, \\ \frac{1}{2g^2-g+3} & \text{if } g \geq 2, \end{cases} \qquad \gamma := \begin{cases} \frac{1}{2} & \text{if } g = 1, \\ \frac{1}{8} & \text{if } g = 2, \\ \frac{1}{2g^2-g+1} & \text{if } g \geq 3. \end{cases}$$

For any $\varepsilon > 0$ we have:

(i1) unconditionally,

$$\pi_A(x,t) \ll_{A,\varepsilon} \frac{x}{(\log x)^{1+\alpha-\varepsilon}};$$

(i2) under GRH,

$$\pi_A(x,t) \ll_{A,\varepsilon} x^{1-\frac{\alpha}{2}+\varepsilon};$$

(ii) if $t \neq \pm 2g$, then *(i1)* and *(i2)* hold with α replaced by β;

(iii) if $t = 0$, then *(i1)* and *(i2)* hold with α replaced by γ. □

We will actually prove a more general result, stated as Theorem 14 in Section 4, and that the case $g = 1$ of Theorem 1 is [42, Theorem 20, p. 189].

An immediate consequence of Theorem 1 concerns the non-lacunarity of the sequence $(a_{1,p})_p$:

Corollary 2. We keep the setting and notation of Theorem 1. For any $\varepsilon > 0$ we have:

(i) unconditionally,

$$\#\left\{p \leq x : p \nmid N_A, |a_{1,p}| \geq (\log p)^{\alpha-\varepsilon}\right\} \sim \pi(x);$$

(ii) under GRH,

$$\#\left\{p \leq x : p \nmid N_A, |a_{1,p}| \geq p^{\frac{\alpha}{2}-\varepsilon}\right\} \sim \pi(x).$$ □

Recall that $\nu(n)$ denotes the number of distinct prime factors of a positive integer n and that an arithmetic function $f(\cdot)$ is said to have normal order $F(\cdot)$ if for all $\varepsilon > 0$, then $(1-\varepsilon)F(n) < f(n) < (1+\varepsilon)F(n)$ for all but a zero density subset of positive integers n. It is a classical result of Erdös, originating in work of Hardy and Ramanujan [25], that $\nu(p-1)$ has normal order $\log\log p$. More generally, Erdös and Kac [20] proved that $\nu(p-1)$ has a normal distribution. Variations of these results have also been obtained in arithmetic geometric contexts, including that of modular forms [36]. We now prove such results in the context of abelian varieties:

Theorem 3. Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g. Assume that $\operatorname{Im}\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. Under GRH we have that, for any $\tau \in \mathbb{R}$,

$$\lim_{x\to\infty} \frac{\#\left\{p \leq x : p \nmid N_A, a_{1,p} \neq 0, \nu(a_{1,p}) \leq \log\log p + \tau\sqrt{\log\log p}\right\}}{\pi(x)} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\tau} e^{-\frac{t^2}{2}}\, \mathrm{d}t. \quad (4)$$

In particular, $\nu(a_{1,p})$ has normal order $\log\log p$. □

The case $g = 1$ not only recovers but also generalizes the main theorem of [36] for weight 2 newforms that are not of CM type.

Finally, in Conjecture 4 below we propose a generalization of (1) to the case of higher-dimensional abelian varieties for which $\operatorname{Im}\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ and for which the following holds:

Equidistribution assumption: the normalized traces $\frac{a_{1,p}}{\sqrt{p}}$ are equidistributed on $[-2g, 2g]$ with respect to the projection by the trace map of the (normalized) Haar measure of the unitary symplectic group $\mathrm{USp}(2g)$.

The assumption that $\operatorname{Im}\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ gives rise to an integer $m_A \geq 1$ that is the smallest positive integer m such that

$$\rho_A(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \Pi^{-1}(\operatorname{Im}\bar{\rho}_{A,m}),$$

with $\Pi : \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ the natural projection.

The Equidistribution Assumption gives rise to a continuous function $\Phi : [-1,1] \longrightarrow [0,\infty)$, nonzero at 0, with the property that for every interval $I \subseteq [-1,1]$ we have

$$\lim_{x\to\infty} \frac{\#\left\{p \leq x : p \nmid N_A, \frac{a_{1,p}}{2g\sqrt{p}} \in I\right\}}{\pi(x)} = \int_I \Phi(t)\,\mathrm{d}t.$$

We propose:

Conjecture 4. Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g and let $t \in \mathbb{Z}$, $t \neq 0$. Assume that $\operatorname{Im}\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ and that the Equidistribution Assumption holds. Then, as $x \to \infty$,

$$\pi_A(x,t) \sim c(A,t)\frac{\sqrt{x}}{\log x},$$

where

$$c(A,t) := \frac{\Phi(0)}{g} \cdot \frac{m_{A,t}|C(m_{A,t},t)|}{|\operatorname{Im}\bar{\rho}_{A,m_{A,t}}|} \cdot \times \prod_{\ell\nmid m_A} \frac{\ell^{v_\ell(t)+1}\,|\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^{v_\ell(t)+1}\mathbb{Z}) : \operatorname{tr} M \equiv t (\mathrm{mod}\, \ell^{v_\ell(t)+1})\}|}{|\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^{v_\ell(t)+1}\mathbb{Z})|},$$

the integers $v_\ell(t) \geq 0$ are defined by $\ell^{v_\ell(t)} | t$, $\ell^{v_\ell(t)+1} \nmid t$, and

$$m_{A,t} := m_A \prod_{\ell | m_A} \ell^{v_\ell(t)},$$

$$C(m_{A,t},t) := \left\{M \in \operatorname{Im}\bar{\rho}_{A,m_{A,t}} : \operatorname{tr} M \equiv t (\mathrm{mod}\, m_{A,t})\right\}.$$

If $c(A,t)=0$, we interpret the asymptotic as saying that there are at most finitely many primes p such that $a_{1,p}=t$. □

For a discussion about the possible growth of $\pi_A(x,0)$, see Section 5.

Remark 5. The image of ρ_A is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ for a large class of abelian varieties. Indeed, in [43, 44] Serre showed that this holds whenever $\mathrm{End}_{\overline{\mathbb{Q}}}(A)\simeq\mathbb{Z}$ and the dimension g of A is 1, 2, 6, or an odd number. An open image result also holds when $\mathrm{End}_{\overline{\mathbb{Q}}}(A)\simeq\mathbb{Z}$ and there exists a number field K such that the Néron model of A/K over the ring of integers of K has a semistable fibre of toric dimension 1; see [24]. As pointed out in [24, p. 704], for $g\geq 2$ the image of ρ_A is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ for most abelian g-folds that arise as Jacobians of hyperelliptic curves defined by $y^2=f(x)$ with the degree n of the monic polynomial $f\in\mathbb{Z}[x]$ equal to $2g+1$ or $2g+2$. Specifically, the hypotheses in Hall's Theorem are satisfied if the Galois group of f is S_n, or if there exists a rational prime p for which $f(\bmod p)$ has $n-1$ distinct zeroes over an algebraic closure, one of which is a double zero; see Kowalski's appendix in [24] and Zarhin's article [50]. □

Remark 6. When $\mathrm{Im}\,\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$, the Equidistribution Assumption is a very special case of a general conjecture explained in Section 13 of [45, Conjecture 13.5] that generalizes the Sato–Tate Conjecture. See also [15, pp. 173–174, 797–804, 906] and [40]. □

Remark 7. Generalizations of the Lang–Trotter Conjecture (1) have been previously considered by other authors. For example, in [39], V. K. Murty addressed generalizations in the setting of modular forms, while in [28, pp. 421–423], Katz addressed generalizations in the setting of abelian varieties arising as Jacobians of genus g curves. Our conjecture encompasses a generic class of abelian varieties A and is precise in terms of both the growth in x and the constant depending on A and t. The potential vanishing of the constant $c(A,t)$ is an important open problem in itself. In [28, p. 420], for instance, Katz discusses a general mechanism that leads to congruence obstructions for realizing $a_{1,p}=t$. We relegate this study to future work. □

The paper is structured as follows. In Section 2 we present some of the key results needed for proving Theorem 1, Corollary 2, and Theorem 3, and for arguing towards Conjecture 4. In Section 3 we prove Theorem 1 and Corollary 2 using the strategy of [42, Sections 7–8] and also with the help of the main result of Serre's Appendix 1 of this aricle. In Section 4 we prove Theorem 3 following a general strategy of [5]. In

Section 5 we provide our heuristic reasoning towards Conjecture 4 and address some connections with existing works. In Section 6 we provide computational data related to our theoretical investigations. J-P. Serre supplied two appendices: the first gives a result on the dimension of conjugacy classes in symplectic groups, while the second gives properties of a certain density function for unitary symplectic groups.

2 Generalities

2.1 Basic notation

Along with the standard analytic notation O, $\ll$, $\gg$, o, $\sim$,

$$\pi(x) := \#\{p \leq x : p \text{ prime}\},$$
$$\operatorname{li} x := \int_2^x \frac{1}{\log t}\, \mathrm{d}t,$$

we use p and ℓ to denote rational primes; we write $n|m^\infty$ to mean that all the prime divisors of n occur among the prime divisors of m, possibly with higher multiplicities; we write $n||m$ to mean that $n|m$, but $n^2 \nmid m$; we write $v_\ell(n)$ for the valuation of n at ℓ.

For a commutative, unitary ring R and a positive integer g, we denote by $R^\times$ its group of units, by $I_g \in M_g(R)$, $I_{2g} \in M_{2g}(R)$ the identity matrices, and by

$$J_{2g} := \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \in M_{2g}(R).$$

We recall that the *general symplectic group on* R is defined by

$$\mathrm{GSp}_{2g}(R) := \left\{M \in \mathrm{GL}_{2g}(R) : M^{\mathrm{t}} J_{2g} M = \mu J_{2g} \text{ for some } \mu \in R^\times\right\},$$

where M^{t} denotes the transpose of M, while

$$\mathrm{Sp}_{2g}(R) := \left\{M \in \mathrm{GL}_{2g}(R) : M^{\mathrm{t}} J_{2g} M = J_{2g}\right\}.$$

We note that $\mathrm{GSp}_2(R) = \mathrm{GL}_2(R)$. We recall that $\mathrm{GSp}_{2g}(R)$ has centre $\{\mu I_{2g} : \mu \in R^\times\}$ and that, as an algebraic group, it has dimension $2g^2 + g + 1$.

For $R = \mathbb{C}$, we recall that the *unitary symplectic group* is defined by

$$\mathrm{USp}(2g) := \left\{M \in \mathrm{Sp}_{2g}(\mathbb{C}) : \overline{M}^{\mathrm{t}} M = M\overline{M}^{\mathrm{t}} = I_{2g}\right\}.$$

2.2 The Chebotarev density theorem

2.2.1 Finite extensions of a number field

Let L/K be a finite Galois extension of number fields and let G be its Galois group. Let C be a non-empty subset of G that is stable under conjugation. For any $x > 0$, let

$$\pi_C(x, L/K) := \#\{\mathfrak{p} \text{ a place of } K, \text{ unramified in } L/K : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathrm{Frob}_{\mathfrak{p}} \subseteq C\}.$$

The Chebotarev Density Theorem states that

$$\pi_C(x, L/K) \sim \frac{|C|}{|G|}\pi(x).$$

We will use the following conditional effective version of this theorem:

Theorem 8 ([34]; for this version see [42, Theorem 4, p. 133]). Keep the above setting and notation. Assume GRH for the Dedekind zeta function of L. Then there exists an absolute constant $c > 0$ such that

$$\left|\pi_C(x, L/K) - \frac{|C|}{|G|}\pi(x)\right| \leq c\frac{|C|}{|G|}x^{\frac{1}{2}}\left(\log|\operatorname{disc}(L/\mathbb{Q})| + |L:\mathbb{Q}|\log x\right). \qquad \square$$

In order to apply this theorem, the following variation of a result of Hensel [26], proved in [42], is useful:

Proposition 9 ([42, Proposition 5, p. 129]). Keep the above setting and notation. Then

$$\log\left|N_{K/\mathbb{Q}}(\operatorname{disc}(L/K))\right| \leq (|L:\mathbb{Q}| - |K:\mathbb{Q}|)\left(\sum_{p\in\mathcal{P}(L/K)}\log p\right) + |L:\mathbb{Q}|\log|L:K|,$$

where

$$\mathcal{P}(L/K) := \{\text{primes } p : \text{there is a place } \mathfrak{p} \text{ of } K, \text{ ramified in } L/K, \text{ with } \mathfrak{p}|p\}. \qquad \square$$

2.2.2 ℓ-adic extensions of a number field

In [42], Serre used the effective versions of the Chebotarev Density Theorem of Lagarias and Odlyzko [34] to deduce upper bounds for $\pi_C(x, L/K)$ in the case of an ℓ-adic Galois extension L/K of a number field K. We recall his main results below.

Let K be a number field. Let ℓ be a rational prime and G a compact ℓ-adic Lie group of dimension D. Denote by $Z(G)$ the centre of G. Let $C \subseteq G$ be a non-empty closed subset of G that is stable under conjugation. In [42, Section 3] Serre explains what it

means for the *Minkowski dimension* $\dim_{\mathcal{M}} C$ of C to be $\leq d$. Let L/K be an infinite Galois extension, with Galois group G. For any $x > 0$, let

$$\pi_C(x, L/K) := \#\{\mathfrak{p} \text{ a place of } K, \text{ unramified in } L/K : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathrm{Frob}_{\mathfrak{p}} \subseteq C\}.$$

Following [42, p. 151], we define

$$\epsilon(x) := \frac{\log x}{(\log\log x)^2(\log\log\log x)} \quad \text{and} \quad \epsilon_R(x) := \frac{x^{\frac{1}{2}}}{(\log x)^2}.$$

Theorem 10 ([42, Theorem 10, p. 151]). Keep the above setting and notation. Let $0 \leq d < D$ be such that the Minkowski dimension of C satisfies $\dim_{\mathcal{M}} C \leq d$. Define $\alpha := \dfrac{D-d}{D}$.

(i) Unconditionally, we have

$$\pi_C(x, L/K) \ll_{K,L,C} \frac{\mathrm{li}\, x}{\epsilon(x)^{\alpha}}.$$

In particular, for any $\varepsilon > 0$, we have

$$\pi_C(x, L/K) \ll_{K,L,C,\varepsilon} \frac{x}{(\log x)^{1+\alpha-\varepsilon}}.$$

(ii) Under GRH for Dedekind zeta functions, we have

$$\pi_C(x, L/K) \ll_{K,L,C} \frac{\mathrm{li}\, x}{\epsilon_R(x)^{\alpha}}.$$

In particular, for any $\varepsilon > 0$, we have

$$\pi_C(x, L/K) \ll_{K,L,C,\varepsilon} x^{1-\frac{\alpha}{2}+\varepsilon}.$$ □

Serre obtains the following improvement in special cases:

Theorem 11 ([42, Theorem 12, p. 157]). Keep the above setting and notation. Let $0 \leq d < D$ be such that the Minkowski dimension of C satisfies $\dim_{\mathcal{M}} C \leq d$. Define

$$r_C := \inf_{M \in C} \dim \frac{G}{Z_G(M)},$$

where $Z_G(M)$ denotes the centralizer of M in G. Define

$$\beta_C := \frac{D-d}{D-\frac{r_C}{2}}.$$

Then (i) and (ii) of Theorem 10 hold with β_C in place of α. □

Note that $r_C \geq 0$, hence $\beta_C \geq \alpha$ and so Theorem 11 is Theorem 10 when $\beta_C = \alpha$. When $r_C \geq 1$, hence $\beta_C > \alpha$, Theorem 11 improves upon Theorem 10. This happens when $C \cap Z(G) = \emptyset$.

2.3 Abelian varieties

Let $A/\mathbb{Q}$ be an abelian variety of dimension g and let p be a prime of good reduction. Recall that for any root $\pi \in \mathbb{C}$ of $P_{A,p}(X)$ we have $|\pi| = \sqrt{p}$, hence

$$|a_{1,p}| < 2g\sqrt{p}. \tag{5}$$

Property (2) links the p-Weil polynomial $P_{A,p}(X)$ to the division fields of A, in particular to the Galois representation defining ρ_A.

For arbitrary integers $m \geq 1$ and t, we set

$$G(m) := \operatorname{Im} \bar{\rho}_{A,m},$$
$$C(m,t) := \{M \in G(m) : \operatorname{tr} M \equiv t \pmod m\}.$$

We recall that:

- by the Néron–Ogg–Shafarevich criterion,

$$\text{the extension } \mathbb{Q}(A[m])/\mathbb{Q} \text{ is unramified outside } mN_A; \tag{6}$$

- by the injectivity of the restriction of $\bar{\rho}_{A,m}$ to $\operatorname{Gal}(\mathbb{Q}(A[m])/\mathbb{Q})$,

$$|G(m)| \leq |\operatorname{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})| \leq m^{2g^2+g+1}. \tag{7}$$

In many cases, the image of the representation ρ_A is better understood. For example, as already mentioned in Remark 5 of Section 1, for several classes of abelian varieties $A/\mathbb{Q}$ with a trivial endomorphism ring, $\operatorname{Im} \rho_A$ is open in $\operatorname{GSp}_{2g}(\hat{\mathbb{Z}})$. In particular, for such A we have that:

- $\operatorname{Im} \rho_{A,\ell}$ is open in $\operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$ for all rational primes ℓ;
- $G(\ell) \simeq \operatorname{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ for all but finitely many rational primes ℓ.

Lemma 12 below gives further consequences of the openness of $\operatorname{Im} \rho_A$ in $\operatorname{GSp}_{2g}(\hat{\mathbb{Z}})$. To state the lemma, we introduce the following notation:

$$F_t(m) := \frac{m|C(m,t)|}{|G(m)|}, \qquad H_t(m) := \frac{m|\{M \in \operatorname{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}) : \operatorname{tr} M \equiv t \pmod m\}|}{|\operatorname{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})|};$$

for a sequence $(s_n)_n$,

$$\lim_{m \overset{\sim}{\to} \infty} s_m := \lim_{n \to \infty} s_{m_n} \text{ with } m_n := \prod_{\ell \le n} \ell^n.$$

Lemma 12. Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g such that $\operatorname{Im} \rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.

(i) There exists an integer $m \ge 1$ such that $\rho_A(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \Pi^{-1}(G(m))$, where we recall that

$$\Pi : \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$$

is the natural projection. Denote by m_A the least such integer.

(ii) For all positive integers m_1, m_2 with $m_1 | m_A^\infty$ and $(m_2, m_A) = 1$, we have

$$G(m_1 m_2) \simeq G(m_1) \times G(m_2) = G(m_1) \times \mathrm{GSp}_{2g}(\mathbb{Z}/m_2\mathbb{Z}).$$

(iii) For all $t \in \mathbb{Z}$ we have

$$\prod_{\ell} H_t(\ell) < \infty.$$

In particular, if $t \neq 0$, then

$$\prod_{\ell \nmid m_A} H_t\left(\ell^{v_\ell(t)+1}\right) < \infty.$$

(iv) For all $t \in \mathbb{Z}$, $t \neq 0$, we have

$$\lim_{m \overset{\sim}{\to} \infty} F_t(m) = F_t\left(m_A \prod_{\ell | m_A} \ell^{v_\ell(t)}\right) \cdot \prod_{\ell \nmid m_A} H_t\left(\ell^{v_\ell(t)+1}\right). \qquad \square$$

Proof. Parts (i) and (ii) are clear from the openness assumption on $\operatorname{Im} \rho_A$. For part (iii), let $\ell \nmid m_A$ and t be fixed. First, we will show that

$$\frac{\ell \, |C(\ell, t)|}{|\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} = 1 + O\left(\frac{1}{\ell}\right). \tag{8}$$

Recall that the multiplicator of $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ is the character of $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ with kernel $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$; we denote it by mult. Let $\mathrm{char}(M)$ denote the characteristic polynomial of a square matrix M. For $\gamma \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, define

$$\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})^\gamma := \mathrm{mult}^{-1}(\gamma),$$

$$C(\ell, t)^\gamma := C(\ell, t) \cap \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})^\gamma,$$

$$\mathcal{G}(\ell)^\gamma := \left\{\mathrm{char}(M) : M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})^\gamma\right\},$$
$$\mathcal{C}(\ell,t)^\gamma := \{M \in \mathcal{G}(\ell)^\gamma : \mathrm{tr}\, M = t\}.$$

By [1, Lemma 2.4, p. 631],

$$\left(\frac{\ell}{\ell+1}\right)^{2g^2+g} \frac{|\mathcal{C}(\ell,t)^\gamma|}{|\mathcal{G}(\ell)^\gamma|} \le \frac{|C(\ell,t)^\gamma|}{|\,\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} \le \left(\frac{\ell}{\ell-1}\right)^{2g^2+g} \frac{|\mathcal{C}(\ell,t)^\gamma|}{|\mathcal{G}(\ell)^\gamma|}.$$

Noting that $|\mathcal{C}(\ell,t)^\gamma| = \ell^{g-1}$ and $|\mathcal{G}(\ell)^\gamma| = \ell^g$, we deduce that

$$\left(\frac{\ell}{\ell+1}\right)^{2g^2+g} \cdot \frac{1}{\ell} \le \frac{|C(\ell,t)^\gamma|}{|\,\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} \le \left(\frac{\ell}{\ell-1}\right)^{2g^2+g} \cdot \frac{1}{\ell}.$$

Combining the above inequalities for all $\gamma \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ and multiplying by ℓ gives

$$\left(\frac{\ell}{\ell+1}\right)^{2g^2+g} \le \frac{\ell\,|C(\ell,t)|}{|\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} \le \left(\frac{\ell}{\ell-1}\right)^{2g^2+g}.$$

This completes the proof of (8).

Next we will prove that

$$\frac{\ell\,|C(\ell,t)|}{|\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} = 1 + \mathrm{O}\left(\frac{1}{\ell^2}\right). \tag{9}$$

This ensures the convergence of the infinite product $\prod_\ell H_t(\ell)$, proving (iii).

We first prove (9) for $t \neq 0$. For this, observe that for any $t_1, t_2 \in \mathbb{Z}$ we have

$$t_1 \equiv t_2 (\mathrm{mod}\, \ell) \;\Rightarrow\; C(\ell,t_1) = C(\ell,t_2)$$

and

$$t_1 \not\equiv 0 (\mathrm{mod}\, \ell),\; t_2 \not\equiv 0 (\mathrm{mod}\, \ell) \;\Rightarrow\; |C(\ell,t_1)| = |C(\ell,t_2)|.$$

Indeed, the first assertion is trivial, while the second assertion follows by noting that, if $t_1 \not\equiv 0 (\mathrm{mod}\, \ell)$ and $t_2 \not\equiv 0 (\mathrm{mod}\, \ell)$, then the endomorphism $\left[t_2 t_1^{-1}\right]$ of $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ defined by multiplication by $t_2 t_1^{-1}$ is a bijection satisfying that $\left[t_2 t_1^{-1}\right](C(\ell,t_1)) = C(\ell,t_2)$.

From the above observations,

$$|\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})| = |C(\ell,0)| + (\ell-1)\,|C(\ell,t)|.$$

It is now easy to show that (9) follows from this along with (8) for $|C(\ell,0)|$.

Now we prove (9) for $t = 0$. When $g = 1$, a straightforward calculation gives that

$$|C(\ell, 0)| = \ell^3 - \ell^2$$

and so

$$\frac{\ell |C(\ell,0)|}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} = \frac{\ell^3(\ell-1)}{\ell(\ell-1)(\ell^2-1)} = \frac{\ell^2}{\ell^2-1} = 1 + \mathrm{O}\left(\frac{1}{\ell^2}\right).$$

When $g \geq 2$, we proceed as follows. By [32, Theorem 5.3, p. 170],

$$|C(\ell, t)| = g(\ell) + \begin{cases} -\ell^{-1} f(\ell) & \text{if } t \neq 0, \\ \ell^{-1}(\ell-1) f(\ell) & \text{if } t = 0, \end{cases} \tag{10}$$

for some explicit polynomials $f(\ell)$ and $g(\ell)$ in ℓ. Of relevance to us is that the degree $d_{g(\ell)}$ of the leading term of $g(\ell)$ in ℓ satisfies

$$d_{g(\ell)} = 2g^2 + g, \tag{11}$$

and that the degree $d_{f(\ell)}$ of the leading term of $f(\ell)$ in ℓ, while less explicit, can be shown to satisfy

$$d_{f(\ell)} \leq \frac{3g^2}{2} + \frac{g}{2} + 1. \tag{12}$$

Before justifying this bound, let us complete the proof of (9) for $t = 0$, $g \geq 2$. From (10), we see that for any $t \neq 0$,

$$|C(\ell, 0)| = f(\ell) + |C(\ell, t)|.$$

Since we already know (9) for $t \neq 0$, it suffices to show that

$$\frac{\ell f(\ell)}{|\operatorname{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|} = \mathrm{O}\left(\frac{1}{\ell^2}\right).$$

This follows from (11) and (12), as well as the assumption that $g \geq 2$; indeed,

$$d_{g(\ell)} - d_{f(\ell)} \geq \frac{g^2}{2} + \frac{g}{2} - 1 \geq 2.$$

Consequently, (9) holds for $t = 0$, $g \geq 2$.

Finally, let us justify (12). The expression for $f(\ell)$ is rather delicate; indeed, Kim showed that

$$f(\ell) = \ell^{g^2-1} \sum_{b=0}^{\lfloor g/2 \rfloor} \ell^{b(b+1)} \prod_{m=0}^{2b-1} \frac{(\ell^{g-m}-1)}{(\ell^{2b-m}-1)} \prod_{j=1}^{b} (\ell^{2j-1}-1) \sum_{k=1}^{\lfloor (g-2b+2)/2 \rfloor} \ell^k$$
$$\times \sum_{\alpha \in \mathbb{F}_\ell^\times} K(\alpha)^{g-2b+2-2k} \sum_{\substack{j_1,\cdots j_{k-1} \\ 2k-1 \le j_{k-1} \le \cdots \le j_1 \le g-2b+1}} \prod_{v=1}^{k-1} (\ell^{j_v-2v}-1), \tag{13}$$

where $K(\alpha)$ is the ordinary Kloosterman sum

$$K(\alpha) = K(\lambda; \alpha, 1) := \sum_{a \in \mathbb{F}_q^\times} \lambda(a\alpha + a^{-1})$$

for any non-trivial additive character λ of $\mathbb{F}_q$.

To find the leading term, we first focus on

$$\sum_{\alpha \in \mathbb{F}_\ell^\times} K(\alpha)^r$$

for an arbitrary integer $r \ge 0$.

When $r = 0$, the sum is simply $\ell - 1$. When $r = 1$, by Weil's estimate on Kloosterman sums $|K(\alpha)| \le 2\sqrt{\ell}$, we deduce that $\left|\sum_{\alpha \in \mathbb{F}_\ell^\times} K(\alpha)\right| \le \ell^2$. When $r \ge 2$, Kim remarks that

$$\sum_{\alpha \in \mathbb{F}_\ell^\times} K(\alpha)^r = \ell^2 M_{r-1} - (\ell-1)^{r-1} + 2(-1)^{r-1},$$

where $M_0 := 1$ and for any integer $s \ge 1$,

$$M_s := \left|\left\{(\alpha_1, \ldots \alpha_s) \in (\mathbb{F}_\ell^\times)^s : \alpha_1 + \ldots + \alpha_s = 1 \text{ and } \alpha_1^{-1} + \cdots + \alpha_s^{-1} = 1\right\}\right|.$$

Note that $M_1 = 1$ and that for $s \ge 2$, the first of the two conditions defining M_s gives α_1 linearly in terms of the other α_i, while the second gives α_2 as a root of a quadratic in the remaining terms. Thus, if $s \ge 2$, then $M_s \le 2(\ell-1)^{s-2}$. It follows that when $r = 2$, the sum $\sum_{\alpha \in \mathbb{F}_\ell^\times} K(\alpha)^r$ is bounded by an expression of leading degree at most 2 in ℓ (by direct computation using M_1), and when $r \ge 3$, by an expression of leading degree at most $r-1$ in ℓ.

Using the above estimates, we now focus on the degree $d_{f(\ell)}$ of the leading term in (13); we deduce that

$$d_{f(\ell)} \le \max\left\{g^2 + 2bg - 2b^2 + b + k + kg - 2bk - k^2 + 1 : 0 \le b \le \left\lfloor \frac{g}{2} \right\rfloor, \right.$$
$$\left. 1 \le k \le \left\lfloor \frac{g - 2b + 2}{2} \right\rfloor \right\}.$$

The quadratic function above is maximized when $b = \lfloor \frac{g}{2} \rfloor$ and $k = \lfloor \frac{g-2b+2}{2} \rfloor = 1$, with maximal value $\frac{3g^2}{2} + \frac{g}{2} + 1$; the bound (12) follows. This proves (9), and therefore the first part of (iii).

To prove the second part of (iii), observe that $t \neq 0$ is divisible by at most finitely many primes, and so $\prod_{\ell \nmid m_A} H_t\left(\ell^{v_\ell(t)+1}\right)$ is a constant multiple of $\prod_{\ell} H_t(\ell)$, hence finite by the first part of (iii).

Now we prove (iv). Fix an arbitrary $t \in \mathbb{Z}$ with $t \neq 0$. For now, fix also a positive integer m such that $(m, m_A) = 1$ or $m_A | m$, and a prime divisor ℓ of m. Write $m = m_0 \ell^{v_\ell(m)}$, $t = t_0 \ell^{v_\ell(t)}$, where $m_0, t_0 \in \mathbb{Z}$ satisfy $\ell \nmid m_0$, $\ell \nmid t_0$, and note that $v_\ell(m) \ge 1$. For any $s \in \mathbb{Z}$ such that $s \equiv t \pmod{m\ell^{v_\ell(t)}}$, we have $v_\ell(s) = v_\ell(t)$ since $v_\ell(m) \ge 1$. Therefore we may write $s = s_0 \ell^{v_\ell(t)}$ with $s_0 \in \mathbb{Z}$ and $\ell \nmid s_0$. By the Chinese Remainder Lemma, there exists $u \in \mathbb{Z}$ such that $u \equiv t_0^{-1} s_0 \pmod{\ell}$ and $u \equiv 1 \pmod{m_0}$, hence such that

$$u\, t \equiv s \left(\mathrm{mod}\, \ell^{v_\ell(t)+1}\right), \tag{14}$$

$$u \equiv 1 (\mathrm{mod}\, m). \tag{15}$$

We have

$$uI_{2g} \in G(m), \tag{16}$$

since if $(m, m_A) = 1$ then by (ii) we have $G(m) = \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ and so $uI_{2g} \in G(m)$, while if $m_A | m$ then $u \equiv 1 (\mathrm{mod}\, m_A)$ (by (15)) and

$$\left\{M \in \mathrm{GSp}_{2g}\left(\hat{\mathbb{Z}}\right) : M \equiv 1 (\mathrm{mod}\, m_A)\right\} \subseteq \mathrm{Im}\, \rho_A$$

(by the definition of m_A) and thus $uI_{2g} \in G(m)$.

Using (14) and (16), we deduce that the multiplication by uI_{2g} map

$$C\left(m\, \ell^{v_\ell(t)+1}, t\right) \longrightarrow C\left(m\, \ell^{v_\ell(t)+1}, s\right)$$
$$M \mapsto uI_{2g}M$$

is a bijection; in particular,

$$\left|C\left(m\,\ell^{v_\ell(t)+1}, s\right)\right| = \left|C\left(m\,\ell^{v_\ell(t)+1}, t\right)\right|. \tag{17}$$

Now consider the natural projection

$$\Pi : G\left(m\,\ell^{v_\ell(t)+1}\right) \longrightarrow G\left(m\ell^{v_\ell(t)}\right)$$

and observe that

$$\left|\Pi^{-1}(I_{2g})\right| \cdot \left|G\left(m\ell^{v_\ell(t)}\right)\right| = \left|G\left(m\ell^{v_\ell(t)+1}\right)\right|. \tag{18}$$

Letting

$$S := \left\{s \left(\mathrm{mod}\, m\ell^{v_\ell(t)}\right) : s \equiv t \left(\mathrm{mod}\, m\ell^{v_\ell(t)}\right)\right\},$$

and using (17), we obtain

$$\begin{aligned}
\left|\Pi^{-1}(I_{2g})\right| \cdot \left|C\left(m\ell^{v_\ell(t)}, t\right)\right| &= \left|\Pi^{-1}\left(C\left(m\ell^{v_\ell(t)}, t\right)\right)\right| \\
&= \left|\bigcup_{s\left(\mathrm{mod}\, m\ell^{v_\ell(t)}\right)\in S} C\left(m\ell^{v_\ell(t)+1}, s\right)\right| \\
&= |S| \cdot \left|C\left(m\ell^{v_\ell(t)+1}, t\right)\right| \\
&= \ell \cdot \left|C\left(m\ell^{v_\ell(t)+1}, t\right)\right|,
\end{aligned}$$

giving

$$\left|\Pi^{-1}(I_{2g})\right| \cdot \left|C\left(m\ell^{v_\ell(t)}, t\right)\right| = \ell \cdot \left|C\left(m\ell^{v_\ell(t)+1}, t\right)\right|. \tag{19}$$

Putting together (18) and (19), we deduce that for all positive integers m such that $(m, m_A) = 1$ or $m_A | m$, and for all primes $\ell \mid m$, we have

$$F_t\left(m\ell^{v_\ell(t)+1}\right) = F_t\left(m\ell^{v_\ell(t)}\right)$$

and thus

$$F_t\left(m\ell^{k}\right) = F_t\left(m\ell^{v_\ell(t)}\right) \quad \text{for all } k \geq v_\ell(t).$$

Therefore for all $d \mid m_A$ we have

$$F_t\left(d\, m_A \prod_{\ell \mid m_A} \ell^{v_\ell(t)}\right) = F_t\left(m_A \prod_{\ell \mid m_A} \ell^{v_\ell(t)}\right) \tag{20}$$

and for all $k \geq 1$ and all primes $\ell \nmid m_A$ we have

$$F_t\left(\ell^{v_\ell(t)+k}\right) = F_t\left(\ell^{v_\ell(t)+1}\right). \tag{21}$$

Now for *any* positive integer m consider its unique factorization

$$m = m_1 \cdot m_2, \text{ with } m_1 | m_A^\infty \text{ and } (m_2, m_A) = 1.$$

By (ii),

$$F_t(m) = F_t(m_1) \prod_{\ell \mid m_2} H_t\left(\ell^{v_\ell(m_2)}\right).$$

Using (20) for the second line below and (21) for the third line, we have

$$\begin{aligned}
\lim_{m \overset{\sim}{\to} \infty} F_t(m) &= \lim_{m \overset{\sim}{\to} \infty} F_t(m_1) \prod_{\ell \mid m_2} H_t\left(\ell^{v_\ell(m_2)}\right) \\
&= F_t\left(m_A \prod_{\ell \mid m_A} \ell^{v_\ell(t)}\right) \cdot \lim_{x \to \infty} \prod_{\substack{\ell < x \\ \ell \nmid m_A}} \lim_{n \to \infty} H_t\left(\ell^n\right) \\
&= F_t\left(m_A \prod_{\ell \mid m_A} \ell^{v_\ell(t)}\right) \cdot \prod_{\ell \nmid m_A} H_t\left(\ell^{v_\ell(t)+1}\right),
\end{aligned}$$

which gives (iv). ■

Remark 13. As in the case $g = 1$, when $g = 2$ it is possible to derive closed formulae for the quotient $\frac{|C(\ell,t)|}{|\mathrm{GSp}_4(\mathbb{Z}/\ell\mathbb{Z})|}$; indeed, we have

$$|\mathrm{GSp}_4(\mathbb{Z}/\ell\mathbb{Z})| = \ell^4(\ell-1)(\ell^2-1)(\ell^4-1)$$

and

$$|C(\ell,t)| = \begin{cases} \ell^5(\ell-1)(\ell^4-\ell-1) & \text{if } t = 0, \\ \ell^4(\ell^6-\ell^5-\ell^4+\ell+1) & \text{if } t \neq 0. \end{cases} \tag{22}$$

We sketch a proof of the latter using arguments from [8]; we leave it as an exercise to the reader to derive these formulae using the aforementioned results of [32]. We will use these formulae in Remark 24.

Define

$$N_{\ell,t} := \left|\left\{(x,y,\delta) \in ((\mathbb{Z}/\ell\mathbb{Z})^\times)^3 : y \neq -\delta, \left(x+\frac{y}{x}\right)\left(1+\frac{\delta}{y}\right) = t\right\}\right|.$$

It follows from the proof of [8, Theorem 12] that

$$\left|\left\{M \in \mathrm{GSp}_4(\mathbb{Z}/\ell\mathbb{Z}) : \operatorname{tr} M \equiv t \pmod{\ell}\right\}\right|$$

equals

$$\ell^4\left((\ell-1)^2(\ell-2)+N_{\ell,t}\right) + \ell^4(\ell-1)(\ell^2-1)^2 + \ell^5(\ell-1)^2(\ell^3-\ell-1) + \begin{cases} (\ell^7-\ell^4)(\ell-1) & \text{if } t=0, \\ 0 & \text{if } t \neq 0. \end{cases}$$

We will now show that

$$N_{\ell,t} = \begin{cases} (\ell-1)(\ell-2) & \text{if } t=0, \\ (\ell-2)^2 & \text{if } t \neq 0, \end{cases}$$

which in turn confirms (22).

Note that

$$\left|\left\{(x,y,\delta) \in ((\mathbb{Z}/\ell\mathbb{Z})^\times)^3 : y \neq -\delta\right\}\right| = (\ell-1)^2(\ell-2)$$

and

$$N_{\ell,0} = \left|\left\{(x,y,\delta) \in ((\mathbb{Z}/\ell\mathbb{Z})^\times)^3 : y \neq -\delta, \left(x+\frac{y}{x}\right)\left(1+\frac{\delta}{y}\right) = 0\right\}\right| = (\ell-1)(\ell-2),$$

since, for any given x, the defining conditions of these sets determine y uniquely, provided that $\delta \neq -y$. Putting the two together, we obtain that

$$\left|\left\{(x,y,\delta) \in ((\mathbb{Z}/\ell\mathbb{Z})^\times)^3 : y \neq -\delta, \left(x+\frac{y}{x}\right)\left(1+\frac{\delta}{y}\right) \neq 0\right\}\right| = (\ell-1)(\ell-2)^2.$$

Dividing by $\ell-1$, we deduce that $N_{\ell,t} = (\ell-2)^2$ for any fixed nonzero t; this completes the proof of (22). □

3 Proof of Theorem 1

For a prime ℓ and an integer t, define:

$$\begin{aligned}
\mathbb{G}_\ell &:= \mathrm{GSp}_{2g}(\mathbb{Z}_\ell);\\
P\mathbb{G}_\ell &:= \mathbb{G}_\ell / Z(\mathbb{G}_\ell);\\
\Pi : \mathbb{G}_\ell &\longrightarrow P\mathbb{G}_\ell \text{ the canonical projection;}\\
G_\ell &:= \mathrm{Im}\,\rho_{A,\ell};\\
G'_\ell &:= \Pi(G_\ell);\\
\mathbb{C}_\ell(t) &:= \{M \in \mathbb{G}_\ell : \mathrm{tr}\, M = t\};\\
C_\ell(t) &:= \{M \in G_\ell : \mathrm{tr}\, M = t\};\\
C'_\ell(0) &:= \Pi\left(C_\ell(0)\right);\\
r_{C_\ell(t)} &:= \inf_{M \in C_\ell(t)} \dim \frac{G_\ell}{Z_{G_\ell}(M)};\\
r_{C'_\ell(0)} &:= \inf_{M \in C'_\ell(0)} \dim \frac{G'_\ell}{Z_{G'_\ell}(M)}.
\end{aligned}$$

We will deduce Theorem 1 from the following more general result:

Theorem 14. Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g and let $t \in \mathbb{Z}$.

(i) Assume that there exists a prime ℓ such that:
   (a) G_ℓ is open in $\mathbb{G}_\ell$;
   (b) $\exists\, 0 \le d < \dim \mathbb{G}_\ell$ such that $\dim_{\mathcal{M}} C_\ell(t) \le d$.

   Define

$$\alpha := \frac{\dim \mathbb{G}_\ell - d}{\dim \mathbb{G}_\ell}.$$

   Then for any $\varepsilon > 0$ we have:
   (i1) unconditionally,

$$\pi_A(x,t) \ll_{A,\ell,\varepsilon} \frac{x}{(\log x)^{1+\alpha-\varepsilon}}; \tag{23}$$

   (i2) under GRH,

$$\pi_A(x,t) \ll_{A,\ell,\varepsilon} x^{1-\frac{\alpha}{2}+\varepsilon}. \tag{24}$$

(ii) If $t \neq \pm 2g$, assume that there exists a prime ℓ such that:

(a) G_ℓ is open in $\mathbb{G}_\ell$;

(b) $\exists\, 0 \leq d < \dim \mathbb{G}_\ell$ such that $\dim_{\mathcal{M}} C_\ell(t) \leq d$;

(c) $v_\ell(\frac{t}{2g}) \neq 0$.

Define

$$\beta := \frac{\dim \mathbb{G}_\ell - d}{\dim \mathbb{G}_\ell - \frac{r_{C_\ell(t)}}{2}}.$$

Then $r_{C_\ell(t)} > 0$ and the equations (23) and (24) hold with α replaced by β.

(iii) If $t = 0$, assume that there exists a prime ℓ such that:

(a) G_ℓ is open in $\mathbb{G}_\ell$;

(b) $\exists\, 0 \leq d < \dim P\mathbb{G}_\ell$ such that $\dim_{\mathcal{M}} C'_\ell(0) \leq d$.

Define

$$\gamma := \frac{\dim \mathbb{G}_\ell - 1 - d}{\dim \mathbb{G}_\ell - 1 - \frac{r_{C'_\ell(0)}}{2}}.$$

Then $r_{C'_\ell(0)} > 0$ and the equations (23) and (24) hold with α replaced by γ. □

Proof. Throughout the proof we let $x > 0$, to be thought of as approaching ∞.

(i) Observe that, by (2), for any rational prime ℓ we have

$$\pi_A(x,t) \leq \pi_{C_\ell(t)}(x, L/\mathbb{Q}),$$

where

$$L := \overline{\mathbb{Q}}^{\operatorname{Ker}\rho_{A,\ell}}.$$

It remains to estimate $\pi_{C_\ell(t)}(x, L/\mathbb{Q})$, which we do by following the method of [42, Section 8].

We choose ℓ as in the hypothesis of (i). Since G_ℓ is open in $\mathbb{G}_\ell$, we have $\dim G_\ell = \dim \mathbb{G}_\ell$. We apply Theorem 10 to the extension $L/\mathbb{Q}$ and the conjugacy set $C_\ell(t)$ with $D := \dim \mathbb{G}_\ell$.

(ii) If $t \neq \pm 2g$, we choose ℓ as in the hypothesis of (ii). As before, $\dim G_\ell = \dim \mathbb{G}_\ell$. Moreover,

$$\mathbb{C}_\ell(t) \cap Z(\mathbb{G}_\ell) = \emptyset,$$

for, otherwise, recalling that $Z(\mathbb{G}_\ell) = \{\mu I_{2g} : \mu \in \mathbb{Z}_\ell^\times\}$, we would have that the ℓ-adic valuation of $\frac{t}{2g}$ satisfies $v_\ell\left(\frac{t}{2g}\right) = 0$, a contradiction.

In particular, for any $M \in \mathbb{C}_\ell(t)$,

$$Z_{\mathbb{G}_\ell}(M) \subsetneq \mathbb{G}_\ell. \tag{25}$$

Centralizers are closed subgroups, hence Lie subgroups, and $Z_{\mathbb{G}_\ell}(M)$ has a well-defined dimension. Since GSp_{2g} is connected as an algebraic group, (25) implies that

$$\dim Z_{\mathbb{G}_\ell}(M) < \dim \mathbb{G}_\ell = \dim G_\ell.$$

If $M \in C_\ell(t)$, then $\dim Z_{G_\ell}(M) \leq \dim Z_{\mathbb{G}_\ell}(M)$ and, by the above,

$$\dim \frac{G_\ell}{Z_{G_\ell}(M)} \geq \dim \mathbb{G}_\ell - \dim Z_{\mathbb{G}_\ell}(M) \geq 1.$$

Therefore we can improve upon the result of (i) by applying Theorem 11 to the extension $L/\mathbb{Q}$ and the conjugacy set $C_\ell(t)$ with $D := \dim \mathbb{G}_\ell$.

(iii) If $t = 0$, we choose ℓ as in the hypothesis of (iii) and with $\hat{\rho}_{A,\ell} := \Pi \circ \rho_{A,\ell}$ we consider

$$L' := \overline{\mathbb{Q}}^{\mathrm{Ker}\,\hat{\rho}_{A,\ell}},$$

a Galois extension of $\mathbb{Q}$ with Galois group G'_ℓ. Observing that

$$\pi_A(x, 0) \leq \pi_{C'_\ell(0)}(x, L'/\mathbb{Q}),$$

it remains to estimate the right-hand side.

Since G_ℓ is open in $\mathbb{G}_\ell$, we have that G'_ℓ is open in $P\mathbb{G}_\ell$ and so $\dim G'_\ell = \dim P\mathbb{G}_\ell = \dim \mathbb{G}_\ell - 1$. Moreover, since $Z(P\mathbb{G}_\ell) = \{I_{2g}\}$, we have

$$\Pi(\mathbb{C}_\ell(0)) \cap Z(P\mathbb{G}_\ell) = \emptyset.$$

In particular, as in the proof of part (ii), for any $M \in \mathbb{C}_\ell(0)$,

$$Z_{P\mathbb{G}_\ell}(\Pi(M)) \subsetneq P\mathbb{G}_\ell,$$

thus

$$\dim Z_{P\mathbb{G}_\ell}(\Pi(M)) < \dim \mathbb{G}_\ell - 1.$$

If $M \in C_\ell(0)$, then $\dim Z_{G'_\ell}(\Pi(M)) \le \dim Z_{P\mathbb{G}_\ell}(\Pi(M))$ and, by the above,

$$\dim \frac{G'_\ell}{Z_{G'_\ell}(\Pi(M))} \ge \dim P\mathbb{G}_\ell - \dim Z_{P\mathbb{G}_\ell}(\Pi(M)) \ge 1.$$

Therefore we can improve upon the result of (i) by applying Theorem 11 to the extension $L'/\mathbb{Q}$ and the conjugacy set $C'_\ell(0)$ with $D := \dim \mathbb{G}_\ell - 1$. ■

Proof of Theorem 1. In our setting, by the openness assumption on $\operatorname{Im}\rho_A$, hypothesis (a) of Theorem 14 holds for any prime ℓ. It remains to verify hypothesis (b) and to compute the values of α, β, and γ.

To verify hypothesis (b) of either parts (i) or (ii), observe that $\mathbb{C}_\ell(t)$ is a closed subvariety of the algebraic group GSp_{2g} and so $C_\ell(t)$ has a well-defined dimension strictly smaller than $\dim \mathbb{G}_\ell$. The bound applies to the Minkowski dimension $\dim_{\mathcal{M}} C_\ell(t)$ also by [42, Theorem 8]. Part (b) follows with $d := \dim \mathbb{G}_\ell - 1$.

To verify hypothesis (b) of part (iii), observe that $\Pi(\mathbb{C}_\ell(0))$ is a closed subvariety of the algebraic group $P\mathbb{G}_\ell$ and so $C'_\ell(0)$ has a well-defined dimension strictly smaller than $\dim P\mathbb{G}_\ell$. The bound applies to the Minkowski dimension $\dim_{\mathcal{M}} C'_\ell(0)$ also by [42, Theorem 8]. Part (b) follows with $d := \dim \mathbb{G}_\ell - 2$.

Recalling that $\dim \mathrm{GSp}_{2g} = 2g^2 + g + 1$, we see that $\alpha = \frac{1}{2g^2+g+1}$.

If $g = 1$, then $r_{C_\ell}(t)$ and $r_{C'_\ell}(0)$ are calculated as in [42, pp. 189–190], giving rise to $\beta = \frac{1}{3}$ and $\gamma = \frac{1}{2}$. If $g \ge 2$, then $r_{C_\ell}(t)$ and $r_{C'_\ell}(0)$ are estimated using Serre's Theorem A.1 in Appendix 1. Indeed, by this theorem and Remark 5 that follows its statement, for $M \in C_\ell(t)$ with t as in (ii) we have

$$r_{C_\ell(t)} = \inf_{M \in C_\ell(t)} \dim \frac{G_\ell}{Z_{G_\ell}(M)} = \inf_{M \in \mathbb{C}_\ell(t)} \dim \frac{\mathbb{G}_\ell}{Z_{\mathbb{G}_\ell}(M)} \ge 4g - 4,$$

which gives

$$\beta \ge \frac{1}{2g^2 - g + 3}.$$

To improve upon this bound when $t = 0$, we focus on estimating γ and use

$$\dim Z_{P\mathbb{G}_\ell}(\Pi(M)) = \dim Z_{\mathbb{G}_\ell}(M) - 1. \tag{26}$$

If $g = 2$, we use (26) and once again the first part of Theorem A.1 in Appendix 1 to deduce

$$\gamma \geq \frac{1}{(2g^2+g+1) - 1 - \frac{4g-4}{2}} = \frac{1}{8}.$$

If $g \geq 3$, we use (26) and the last part of Theorem A.1 in Appendix 1 to deduce

$$\gamma \geq \frac{1}{(2g^2+g+1) - 1 - \frac{4g-2}{2}} = \frac{1}{2g^2-g+1}.$$

This completes the proof of Theorem 1. ∎

Proof of Corollary 2. The proof of Corollary 2 is deduced easily from part (i) of Theorem 1 and the Prime Number Theorem, as follows. Unconditionally,

$$\begin{aligned}
\pi(x) &= \#\{p \leq x : p | N_A\} + \#\left\{p \leq x : p \nmid N_A, |a_{1,p}| \geq (\log p)^{\alpha-\varepsilon}\right\} \\
&\quad + \#\left\{p \leq x : p \nmid N_A, |a_{1,p}| < (\log p)^{\alpha-\varepsilon}\right\} \\
&= \#\left\{p \leq x : p \nmid N_A, |a_{1,p}| \geq (\log p)^{\alpha-\varepsilon}\right\} + O_A(1) + O\left(\sum_{\substack{t\in\mathbb{Z} \\ |t|<(\log x)^{\alpha-\varepsilon}}} \pi_A(x,t)\right) \\
&= \#\left\{p \leq x : p \nmid N_A, |a_{1,p}| \geq (\log p)^{\alpha-\varepsilon}\right\} + O_A(1) + O_{A,\varepsilon}\left(\frac{x}{(\log x)^{1+\alpha-\frac{\varepsilon}{2}}} \cdot (\log x)^{\alpha-\varepsilon}\right) \\
&= \#\left\{p \leq x : p \nmid N_A, |a_{1,p}| \geq (\log p)^{\alpha-\varepsilon}\right\} + o\left(\pi(x)\right).
\end{aligned}$$

Under GRH,

$$\begin{aligned}
\pi(x) &= \#\{p \leq x : p | N_A\} + \#\left\{p \leq x : p \nmid N_A, |a_{1,p}| \geq p^{\frac{\alpha}{2}-\varepsilon}\right\} + \#\left\{p \leq x : p \nmid N_A, |a_{1,p}| < p^{\frac{\alpha}{2}-\varepsilon}\right\} \\
&= \#\left\{p \leq x : p \nmid N_A, |a_{1,p}| \geq p^{\frac{\alpha}{2}-\varepsilon}\right\} + O_A(1) + O\left(\sum_{\substack{t\in\mathbb{Z} \\ |t|<x^{\frac{\alpha}{2}-\varepsilon}}} \pi_A(x,t)\right) \\
&= \#\left\{p \leq x : p \nmid N_A, |a_{1,p}| \geq p^{\frac{\alpha}{2}-\varepsilon}\right\} + O_A(1) + O_{A,\varepsilon}\left(x^{1-\frac{\alpha}{2}+\frac{\varepsilon}{2}} \cdot x^{\frac{\alpha}{2}-\varepsilon}\right) \\
&= \#\left\{p \leq x : p \nmid N_A, |a_{1,p}| \geq p^{\frac{\alpha}{2}-\varepsilon}\right\} + o\left(\pi(x)\right).
\end{aligned}$$

The uniformity in t of the bounds for $\pi_A(x,t)$ provided by Theorem 1 was crucial in the above estimates. ∎

4 Proof of Theorem 3

Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g such that $\operatorname{Im}\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. We will investigate $\nu(a_{1,p})$ via the method of moments, with the goal of proving:

Proposition 15. Assume GRH. Then

$$\frac{1}{\pi(x)} \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \left(\nu(a_{1,p}) - \log\log x\right)^k = c_k(\log\log x)^{\frac{k}{2}} + \mathrm{o}\left((\log\log x)^{\frac{k}{2}}\right) \tag{27}$$

for each integer $k \ge 1$, where

$$c_k := \begin{cases} \frac{k!}{2^{\frac{k}{2}}\left(\frac{k}{2}\right)!} & \text{if } k \text{ even} \\ 0 & \text{if } k \text{ odd} \end{cases}$$

is the kth moment of the standard Gaussian. □

With this, by adapting to our context the proof of the Erdös–Kac Theorem due to Billingsley [5] (see also [4] and the references therein for an accessible exposition), Theorem 3 is proved.

The core ingredient in our proof is the following application of (6)–(7), Theorem 8 (under GRH) and Proposition 9: for any positive integer m and any $x > 0$ (to be thought of as approaching infinity), we have

$$\pi_{C(m,0)}(x, \mathbb{Q}(A[m])/\mathbb{Q}) = \frac{|C(m,0)|}{|G(m)|}\pi(x) + \mathrm{O}\left(|C(m,0)|x^{\frac{1}{2}}\log(mN_Ax)\right). \tag{28}$$

Related to this, remark that by the openness assumption of $\operatorname{Im}\rho_A$ in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ and by (8) from the proof of part (iii) of Lemma 12, we have

$$\frac{|C(\ell,0)|}{|G(\ell)|} = \frac{1}{\ell} + \mathrm{O}\left(\frac{1}{\ell^2}\right) \tag{29}$$

for all $\ell \nmid m_A$. In particular, for any $y > 0$,

$$\sum_{\ell\le y} \frac{|C(\ell,0)|}{|G(\ell)|} = \log\log y + \mathrm{O}_A(1), \tag{30}$$

and, after using (29) and (7),

$$\sum_{\ell \le y} |C(\ell, 0)| \ll \frac{y^{2g^2+g+1}}{\log y}. \tag{31}$$

Crucial to the method is also the following simple observation. Let $x > 0$ and $0 < \delta < 1$ be fixed and let $y := x^{\delta}$. For any integer $m \ge 1$, we have

$$|\nu(m) - \nu_y(m)| \le \frac{\log m}{\delta \log x}, \tag{32}$$

where $\nu_y(m)$ denotes the number of distinct prime divisors $\ell \le y$ of m.

We now proceed with the proof of (27). For each prime ℓ, we define a random variable R_ℓ to be 1 with probability $\frac{1}{\ell}$ and 0 with probability $1 - \frac{1}{\ell}$. Upon taking $y := x^{\delta}$ for some fixed $0 < \delta < 1$ and $x \to \infty$, $R(y) := \sum_{\ell \le y} R_\ell$ becomes normally distributed with mean and variance each equal to $\log\log x$; by the Central Limit Theorem, for any integer $k \ge 1$ we have

$$\mathbb{E}\left((R(y) - \log\log x)^k\right) = c_k (\log\log x)^{\frac{k}{2}} + \mathrm{o}\left((\log\log x)^{\frac{k}{2}}\right). \tag{33}$$

By (29), R_ℓ models the event that $\ell | a_{1,p}$ for some p. Our strategy then is to prove (27) by comparing $\mathbb{E}\left((R(y) - \log\log x)^k\right)$ and $\frac{1}{\pi(x)} \sum_{\substack{p \le x \\ p \nmid N_A \\ a_{1,p} \ne 0}} (\nu_y(a_{1,p}) - \log\log x)^k$ for each $k \ge 1$.

We fix $x > 0$ and $k \ge 1$, choose a parameter $\delta = \delta(g, k)$ such that

$$0 < \delta < \frac{1}{2k\,(2g^2 + g + 1)} \tag{34}$$

and define $y := x^{\delta}$. In what follows, our O-estimates will reflect the growth of various functions as $x \to \infty$.

For each ℓ and each $p \nmid N_A$, we define

$$\delta_\ell(p) := \begin{cases} 1 & \text{if } \ell | a_{1,p}, \\ 0 & \text{else.} \end{cases}$$

Then, for each integer $1 \le j \le k$, upon applying (28)–(31) and (33), we obtain

$$\begin{aligned} &\sum_{\substack{p \le x \\ p \nmid N_A \\ a_{1,p} \ne 0}} \nu_y(a_{1,p})^j \\ &= \sum_{\substack{p \le x \\ p \nmid N_A \\ a_{1,p} \ne 0}} \sum_{\ell_1, \dots, \ell_j \le y} \delta_{\ell_1}(p) \dots \delta_{\ell_j}(p) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\ell_1,\dots,\ell_j \le Y} \#\left\{p \le x : p \nmid N_A, a_{1,p} \neq 0, \operatorname{lcm}\{\ell_1,\dots,\ell_j\} | a_{1,p}\right\} \\
&= \sum_{\ell_1,\dots,\ell_j \le Y} \#\left\{p \le x : p \nmid N_A, \operatorname{lcm}\{\ell_1,\dots,\ell_j\} | a_{1,p}\right\} + \mathrm{O}(\pi(y)^j\ \pi_A(x,0)) \\
&= \sum_{\ell_1,\dots,\ell_j \le Y} \#\left\{p \le x : p \nmid \operatorname{lcm}\{\ell_1,\dots,\ell_j\} N_A, \operatorname{lcm}\{\ell_1,\dots,\ell_j\} | a_{1,p}\right\} \\
&\quad + \sum_{\ell_1,\dots,\ell_j \le Y} \#\left\{p \le x : p \nmid N_A, p | \operatorname{lcm}\{\ell_1,\dots,\ell_j\} | a_{1,p}\right\} + \mathrm{O}(\pi(y)^j\ \pi_A(x,0)) \\
&= \sum_{\ell_1,\dots,\ell_j \le Y} \pi_{C(\operatorname{lcm}\{\ell_1,\dots,\ell_j\},0)}(x, \mathbb{Q}(A[\operatorname{lcm}\{\ell_1,\dots,\ell_j\}])/\mathbb{Q}) + \mathrm{O}\left(j\pi(y)^j\right) + \mathrm{O}\left(\pi_A(x,0)\ \pi(y)^j\right) \\
&= \mathbb{E}(R(y)^j)\ \pi(x) + \mathrm{O}_j\left(\pi(x)\ (\log\log y)^{j-1}\right) + \mathrm{O}_{A,j}\left(\frac{y^{j(2g^2+g+1)}}{(\log y)^j} x^{\frac{1}{2}} \log x\right) + \mathrm{O}_j\left(\pi(y)^j \pi_A(x,0)\right).
\end{aligned}
$$

By the binomial theorem and the above, we deduce

$$
\begin{aligned}
&\sum_{\substack{p \le x \\ p \nmid N_A \\ a_{1,p} \neq 0}} (\nu_y(a_{1,p}) - \log\log x)^k \\
&= \sum_{0 \le j \le k} \binom{k}{j} (-\log\log x)^{k-j} \sum_{\substack{p \le x \\ p \nmid N_A \\ a_{1,p} \neq 0}} \nu_y(a_{1,p})^j \\
&= \sum_{0 \le j \le k} \binom{k}{j} (-\log\log x)^{k-j}\ \mathbb{E}(R(y)^j)\ \pi(x) \\
&\quad + \mathrm{O}_{A,k}\left(y^{k(2g^2+g+1)} x^{\frac{1}{2}} (\log x)\ (\log\log x)^k\right) + \mathrm{O}_k\left(\pi(y)^k\ \pi_A(x,0)\ (\log\log x)^k\right).
\end{aligned}
$$

Recalling the choice of δ given in (34) and using part (i2) of Theorem 1, we see that the two O-terms above become $\mathrm{O}_{\varepsilon,A,k}\left(x^{1-\varepsilon}(\log x)(\log\log x)^k\right)$, which is $\mathrm{o}\left(\pi(x)(\log\log x)^{\frac{k}{2}}\right)$. Then, upon applying the binomial theorem once again in order to rewrite the first term, we deduce

$$
\frac{1}{\pi(x)} \sum_{\substack{p \le x \\ p \nmid N_A \\ a_{1,p} \neq 0}} (\nu_y(a_{1,p}) - \log\log x)^k \sim \mathbb{E}((R(y) - \log\log x)^k). \tag{35}
$$

Finally, recalling (5) and (32) and applying (33) and (35) several times, we deduce

$$\begin{aligned}
&\frac{1}{\pi(x)} \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \big(\nu(a_{1,p}) - \log\log x\big)^k \\
&= \frac{1}{\pi(x)} \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \left(\nu_Y(a_{1,p}) - \log\log x + \mathrm{O}\left(\frac{\log|a_{1,p}|}{\delta\log x}\right)\right)^k \\
&= \frac{1}{\pi(x)} \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \big(\nu_Y(a_{1,p}) - \log\log x\big)^k + \mathrm{O}_{k,g,\delta}\left(\sum_{0\le j\le k-1} \frac{1}{\pi(x)} \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \big|\nu_Y(a_{1,p}) - \log\log x\big|^j\right) \\
&= \frac{1}{\pi(x)} \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \big(\nu_Y(a_{1,p}) - \log\log x\big)^k + \mathrm{O}_k\left((\log\log x)^{\frac{k-1}{2}}\right) \\
&= c_k(\log\log x)^{\frac{k}{2}} + \mathrm{o}\left((\log\log x)^{\frac{k}{2}}\right).
\end{aligned}$$

This completes the proof of Theorem 3.

Remark 16. The first and second moments of $\nu(a_{1,p})$ may be estimated directly, without any comparison with the model defined by R_ℓ. The strategy originates in Turán's proof of the Hardy–Ramanujan Theorem, [47], and is summarized below. □

We choose $0 < \delta < \frac{1}{8g^2+4g+1}$ and let $y = x^\delta$. Then, proceeding as in the proof of Theorem 3 but without the model R_ℓ, we obtain

$$\begin{aligned}
&\sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \big(\nu(a_{1,p}) - \log\log x\big)^2 \\
&= \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \nu(a_{1,p})^2 - 2(\log\log x) \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \nu(a_{1,p}) + (\log\log x)^2 \#\{p\le x : p\nmid N_A, a_{1,p}\neq 0\} \\
&= \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \big(\nu_Y(a_{1,p}) + \mathrm{O}_A(1)\big)^2 \\
&\quad - 2(\log\log x) \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \big(\nu_Y(a_{1,p}) + \mathrm{O}_A(1)\big) + \pi(x)(\log\log x)^2 + \mathrm{O}(\pi_A(x,0)\ (\log\log x)^2)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \nu_Y(a_{1,p})^2 - 2(\log\log x) \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \nu_Y(a_{1,p}) + \pi(x)(\log\log x)^2 \\
&\quad + \mathrm{O}\left(\sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \nu_Y(a_{1,p}) \right) + \mathrm{O}(\pi(x)\log\log x) + \mathrm{O}(\pi_A(x,0)\ (\log\log x)^2) \\
&= \sum_{\substack{\ell_1,\ell_2\le y\\ \ell_1\neq\ell_2}} \frac{|C(\ell_1\ell_2,0)|}{|G(\ell_1\ell_2)|}\pi(x) + \mathrm{O}_A\left(\sum_{\ell_1,\ell_2\le y} |C(\ell_1\ell_2,0)| x^{\frac12}\log x \right) - 2(\log\log x)\sum_{\ell\le y}\frac{|C(\ell,0)|}{|G(\ell)|}\pi(x) \\
&\quad + \mathrm{O}_A\left(\sum_{\ell\le y} |C(\ell,0)| x^{\frac12}(\log x)(\log\log x) \right) + \pi(x)(\log\log x)^2 + \mathrm{O}_A\left(\sum_{\ell\le y}\frac{|C(\ell,0)|}{|G(\ell)|}\pi(x) \right) \\
&\quad + \mathrm{O}_A\left(\sum_{\ell\le y} |C(\ell,0)| x^{\frac12}\log x \right) + \mathrm{O}(\pi(x)\log\log x) + \mathrm{O}(\pi_A(x,0)\ (\log\log x)^2) \\
&= \pi(x)(\log\log x)^2 + \mathrm{O}_A\left(\frac{x^{2\delta(2g^2+g+1)}}{\log x} x^{\frac12} \right) - \ 2\pi(x)(\log\log x)^2 \\
&\quad + \mathrm{O}\left(x^{\delta(2g^2+g+1)}\ x^{\frac12}\log\log x \right) \\
&\quad + \ \pi(x)(\log\log x)^2 + \mathrm{O}_A\left(\pi(x)\log\log x\right) \\
&\quad + \mathrm{O}_A\left(x^{\delta(2g^2+g+1)}\ x^{\frac12}\log x \right) + \mathrm{O}_A\left(\pi_A(x,0)(\log\log x)^2 \right) \\
&= \mathrm{O}_A\left(\pi(x)\log\log x\right). \qquad (36)
\end{aligned}
$$

The cancellation of the $\pi(x)(\log\log x)^2$ terms is essential and that the choice of δ ensures that the largest emerging O-term depending on y, namely $\mathrm{O}_A\left(\frac{x^{2\delta(2g^2+g+1)}}{\log x}x^{\frac12}\right)$, is sufficiently small; precisely, it is $\ll_A \pi(x) \ll_A \pi(x)\log\log x$.

Remark 17. That $\nu(a_{1,p})$ has normal order $\log\log p$ can be deduced easily from the second moment estimate (36). In particular, this is an immediate consequence of the following variation of (36):

$$
\sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \left(\nu(a_{1,p}) - \log\log p\right)^2 \ll_A \pi(x)\log\log x.
$$

In turn, this is obtained by remarking that

$$\sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \big(\nu(a_{1,p})-\log\log p\big)^2 \ll \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \big(\nu(a_{1,p})-\log\log x\big)^2 + \sum_{\substack{p\le x\\ p\nmid N_A\\ a_{1,p}\neq 0}} \left(\log\frac{\log x}{\log p}\right)^2,$$

using (36) for the first sum and splitting the last sum over p into a sum over $p\le\sqrt{x}$ and one over $\sqrt{x}<p\le x$, followed by elementary estimates. □

Remark 18. The normal order of $\nu(a_{1,p})$ may also be obtained via the ubiquitous large sieve; see [33, Proposition 2.15] for generalities related to such works. Moreover, the kth moments (27) may be estimated more precisely via sieve methods by applying the general result [23, Proposition 3]. □

5 Heuristic Reasoning for Conjecture 4

We devote this section to arguing heuristically towards Conjecture 4. Our main setting will be that of a principally polarized abelian variety $A/\mathbb{Q}$ of dimension g for which $\mathrm{Im}\,\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ and which satisfies the Equidistribution Assumption. In particular, the function Φ introduced in Section 1 is bounded, continuous, and nonzero on $(-1,1)$; this was proved in more than one way in email communication between Katz [29] and Serre; in Appendix 2 we include a letter from Serre to Katz that contains such a proof.

Definition 19. For each integer $m\ge 1$ and prime p, define $c_{p,m}\in(0,\infty)$ by

$$c_{p,m}=\frac{|G(m)|}{m\displaystyle\sum_{\substack{\tau\in\mathbb{Z}\\ |\tau|<2g\sqrt{p}}}\Phi\left(\frac{\tau}{2g\sqrt{p}}\right)|C(m,\tau)|}$$

and define the function

$$f_p^{(m)}:\mathbb{Z}\longrightarrow[0,\infty),$$
$$f_p^{(m)}(\tau):=\begin{cases}\Phi\left(\frac{\tau}{2g\sqrt{p}}\right)\cdot\frac{m|C(m,\tau)|}{|G(m)|}\cdot c_{p,m} & \text{if } |\tau|<2g\sqrt{p},\\ 0 & \text{else.}\end{cases}$$ □

Note that

$$\sum_{\tau\in\mathbb{Z}} f_p^{(m)}(\tau)=1.$$

Lemma 20. For all integers $m \geq 1$ and $\tau_0 \in \mathbb{Z}$ we have

$$\lim_{p\to\infty} \frac{m}{2g\sqrt{p}} \sum_{\substack{\tau\in\mathbb{Z} \\ |\tau|<2g\sqrt{p} \\ \tau\equiv\tau_0 (\mathrm{mod}\, m)}} \Phi\left(\frac{\tau}{2g\sqrt{p}}\right) = 1. \qquad \square$$

Proof. This follows by viewing the expression inside the limit as a Riemann sum approximation of the integral $\int_{-1}^{1} \Phi(\tau)\, d\tau = 1$. For more details, see [35, pp. 31–32]. ■

Lemma 21. For all integers $m \geq 1$ we have

$$\lim_{p\to\infty} 2g\sqrt{p}\, c_{p,m} = 1. \qquad \square$$

Proof. By the definition of $c_{p,m}$ and Lemma 20,

$$\begin{aligned}
\lim_{p\to\infty} \frac{1}{2g\sqrt{p}\, c_{p,m}} &= \lim_{p\to\infty} \frac{1}{2g\sqrt{p}} \sum_{\tau_0=0}^{m-1} \sum_{\substack{\tau\in\mathbb{Z} \\ |\tau|<2g\sqrt{p} \\ \tau\equiv\tau_0 (\mathrm{mod}\, m)}} \Phi\left(\frac{\tau}{2g\sqrt{p}}\right) \frac{m\,|C(m,\tau)|}{|G(m)|} \\
&= \lim_{p\to\infty} \sum_{\tau_0=0}^{m-1} \frac{|C(m,\tau_0)|}{|G(m)|} \left(\frac{m}{2g\sqrt{p}} \sum_{\substack{\tau\in\mathbb{Z} \\ |\tau|<2g\sqrt{p} \\ \tau\equiv\tau_0 (\mathrm{mod}\, m)}} \Phi\left(\frac{\tau}{2g\sqrt{p}}\right) \right) \\
&= \sum_{\tau_0=0}^{m-1} \frac{|C(m,\tau_0)|}{|G(m)|} \\
&= 1. \qquad \blacksquare
\end{aligned}$$

Now let us fix $t \in \mathbb{Z}$ and assume that $\lim_{m\overset{\sim}{\to}\infty} f_p^{(m)}(t)$ models the likelihood of the event $a_{1,p} = t$, as guided by the Chebotarev law for all m-division fields and by the behaviour of $\frac{a_{1,p}}{2g\sqrt{p}}$ in the interval $(-1, 1)$. Then, recalling part (iv) of Lemmas 12 and 21, we reason *heuristically* as follows:

$$\begin{aligned}
&\#\{p \leq x : p \nmid N_A, a_{1,p} = t\} \\
&\quad \approx \lim_{m\overset{\sim}{\to}\infty} \sum_{p\leq x} f_p^{(m)}(t) \\
&\quad = \lim_{m\overset{\sim}{\to}\infty} \sum_{p\leq x} \Phi\left(\frac{t}{2g\sqrt{p}}\right) \cdot \frac{m|C(m,t)|}{|G(m)|} \cdot c_{p,m} \\
&\quad \approx \left(\lim_{m\overset{\sim}{\to}\infty} \frac{m|C(m,t)|}{|G(m)|} \right) \sum_{p\leq x} \Phi\left(\frac{t}{2g\sqrt{p}}\right) \cdot \frac{1}{2g\sqrt{p}} \\
&\quad = \left(\lim_{m\overset{\sim}{\to}\infty} F_t(m) \right) \sum_{p\leq x} \Phi\left(\frac{t}{2g\sqrt{p}}\right) \cdot \frac{1}{2g\sqrt{p}}.
\end{aligned}$$

Here, the symbol $\approx$ means equality deduced purely heuristically. The last line is simply notation, as introduced in Section 2.2.

To understand the growth of the last sum, we use the properties of the function Φ. For any $\varepsilon > 0$, by the continuity of Φ at 0, there exists a $\delta > 0$ such that

$$\left|\frac{t}{2g\sqrt{p}}\right| < \delta \;\Rightarrow\; \left|\Phi\left(\frac{t}{2g\sqrt{p}}\right) - \Phi(0)\right| < \varepsilon. \tag{37}$$

We thus split the sum over $p \le x$ according to the above δ-interval. By the boundedness of Φ, we obtain

$$\left|\sum_{p < \frac{t^2}{4g^2\delta^2}} \left(\Phi\left(\frac{t}{2g\sqrt{p}}\right) - \Phi(0)\right)\frac{1}{2\sqrt{p}}\right| \ll_{t,\varepsilon,g} 1.$$

By (37) and by noting that $\sum_{p\le x}\frac{1}{2\sqrt{p}} \sim \frac{\sqrt{x}}{\log x}$, we obtain

$$\left|\sum_{\frac{t^2}{4g^2\delta^2} < p \le x} \left(\Phi\left(\frac{t}{2g\sqrt{p}}\right) - \Phi(0)\right)\frac{1}{2\sqrt{p}}\right| \ll \frac{\varepsilon\sqrt{x}}{\log x}.$$

Taking $\varepsilon \to 0$ and returning to our heuristics, we are led to the possible prediction that

$$\#\{p \le x : p \nmid N_A, a_{1,p} = t\} \sim \frac{\Phi(0)}{g} \cdot \lim_{m \overset{\sim}{\to} \infty} F_t(m) \cdot \frac{\sqrt{x}}{\log x}. \tag{38}$$

When $t \neq 0$, we proved in parts (iii) and (iv) of Lemma 12 that the limit over $m \overset{\sim}{\to} \infty$ exists and equals an infinite product; in this case, we conjecture that

$$\#\{p \le x : p \nmid N_A, a_{1,p} = t\} \sim \frac{\Phi(0)}{g} \cdot \frac{m_{A,t}|C(m_{A,t}, t)|}{|G(m_{A,t})|} \cdot \prod_{\ell \nmid m_A} \frac{\ell^{v_\ell(t)+1}\,|\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^{v_\ell(t)+1}\mathbb{Z}) : \mathrm{tr}\, M \equiv t (\mathrm{mod}\, \ell^{v_\ell(t)+1})\}|}{|\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^{v_\ell(t)+1}\mathbb{Z})|} \cdot \frac{\sqrt{x}}{\log x}, \tag{39}$$

where we recall

$$m_{A,t} = m_A \prod_{\ell | m_A} \ell^{v_\ell(t)}.$$

When $t = 0$ and $g = 1$, the limit over $m \overset{\sim}{\to} \infty$ exists and equals an infinite product by [35, Lemma 2, p. 34]; see Remark 22 below. When $t = 0$ and $g \geq 2$, we are currently unable to make a similar statement and relegate such a study to future work.

We conclude this section with several remarks about the above conjecture.

Remark 22. Assume $g = 1$ and $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. Then $\mathrm{Im}\,\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ (see [41]) and the Equidistribution Assumption holds (see [3, 11, 12]). In this case, $\Phi(x) = \frac{2}{\pi}\sqrt{1-x^2}$ and (38) coincides with the formulation in (1) of the Lang–Trotter Conjecture on Frobenius traces of [35]. Combining this with the formula

$$|\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})| = \ell(\ell-1)\left(\ell^2-1\right)$$

and with [35, Lemma 2, p. 34], we obtain an equivalent reformulation of (38):

$$\pi_A(x,t) \sim \frac{2}{\pi} \cdot \frac{m_A |C(m_A,t)|}{|G(m_A)|} \cdot \prod_{\substack{\ell \nmid m_A \\ \ell \mid t}} \frac{\ell^2}{\ell^2-1} \cdot \prod_{\ell \nmid t m_A} \frac{\ell\left(\ell^2-\ell-1\right)}{(\ell+1)(\ell-1)^2} \cdot \frac{\sqrt{x}}{\log x}. \tag{40}$$

□

Remark 23. Assume $g = 2$ and $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$. Then $\mathrm{Im}\,\rho_A$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ ([43], [44]) and the Sato–Tate group of A is $\mathrm{USp}(4)$ [21, Theorem 4.3], while the Equidistribution Assumption is an open question. The function $\Phi(\cdot)$ may be calculated explicitly using the Weyl integration formula as in [31]. In particular, this calculation leads to the value

$$\Phi(0) = \frac{256}{15\pi^2}.$$

We explain the calculation of $\Phi(0)$ here briefly. Let $L_p(A,T) := T^4 P_{A,p}\left(\frac{1}{T}\right)$ be the p-Euler factor in the L-function of A and let $\bar{L}_p(A,T) = L_p\left(A, \frac{T}{\sqrt{p}}\right)$ be its normalization. Let

$$S := \left\{(x_1,x_2) \in \mathbb{R}^2 : x_2 \geq 2x_1 - 2, x_2 \geq -2x_1 - 2, x_2 \leq \frac{x_1^2}{4} + 2\right\}$$

and let $R(x_1)$ be the defining interval of x_2 imposed by the constraints of S. Recalling that the Sato–Tate group associated to A is $\mathrm{USp}(4)$, the conjectured joint density function of the normalized coefficients $\bar{a}_{1,p}$ and $\bar{a}_{2,p}$ is

$$\frac{1}{4\pi^2}\sqrt{\max\{\rho(\bar{a}_{1,p},\bar{a}_{2,p}),0\}},$$

where

$$\rho(x_1, x_2) := \left(x_1^2 - 4x_2 + 8\right)(x_2 - 2x_1 + 2)(x_2 + 2x_1 + 2),$$

with support in the region S where ρ is non-negative. Consequently, for any interval $I \subseteq [-4, 4]$, the set

$$\left\{p : \bar{a}_{1,p} \in I\right\}$$

is expected to have natural density

$$\int_I \int_{R(x_1)} \frac{1}{4\pi^2} \sqrt{\max\{\rho(x_1, x_2), 0\}}\, \mathrm{d}x_2\, \mathrm{d}x_1.$$

(For details, see the original source, specifically [21, p. 21 and p. 40].) Let

$$\Psi(x) = \frac{1}{4\pi^2} \int_{R(x)} \sqrt{\max\{\rho(x, x_2), 0\}}\, \mathrm{d}x_2.$$

In particular, $R(0) = [-2, 2]$ and

$$\Psi(0) = \frac{1}{4\pi^2} \int_{-2}^{2} \sqrt{(8 - 4x_2)(x_2 + 2)^2}\, \mathrm{d}x_2 = \frac{64}{15\pi^2}.$$

In our notation $\Phi(x) = \Psi(4x) \cdot 4$, since one can rescale the variable and account for the fact that both functions are assumed to have integral 1. Therefore, $\Phi(0) = \Psi(0) \cdot 4 = \frac{256}{15\pi^2}$. □

Remark 24. For $g = 2$, $t = \pm 1$, and $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathbb{Z}$, we have an equivalent reformulation of (39):

$$\pi_A(x, t) \sim \frac{128}{15\pi^2} \cdot \frac{m_A |C(m_A, t)|}{|G(m_A)|} \cdot \prod_{\ell \nmid m_A} \frac{\ell(\ell^6 - \ell^5 - \ell^4 + \ell + 1)}{(\ell - 1)(\ell^2 - 1)(\ell^4 - 1)} \cdot \frac{\sqrt{x}}{\log x}.$$

This is obtained by combining (22) with the value of $\Phi(0)$ from the previous remark and with the formula

$$|\,\mathrm{GSp}_4(\mathbb{Z}/\ell\mathbb{Z})| = \ell^4(\ell - 1)(\ell^2 - 1)(\ell^4 - 1).$$ □

Remark 25. For higher g, the function Φ is shown to have a certain general form in Appendix 2. It may again be calculated explicitly using, for example, [49, Theorem 7.8.B] and [30, 5.0.4] (see also the upcoming [7]). □

Remark 26. For $g = 1$, a more refined version of (1) was proposed in [2]; for higher g, similar refinements are relegated to future work. □

Remark 27. Variations of our Conjecture 4 may be formulated for non-generic classes of abelian varieties such as the case of a CM elliptic curve $E/\mathbb{Q}$ (which was already considered in [35]); in such cases, both the assumption on the image of ρ_A and the Equidistribution Assumption must be modified appropriately. We relegate such endeavours to future work. □

6 Computations

The Lang–Trotter Conjecture as formulated in (40) has been supported by numerical evidence (see [8, 13, 35]). Among the main ensuing difficulties are the computations of the integer m_A and of the quotient $\frac{m_A|C(m_A,t)|}{|G(m_A)|}$. These may be resolved for $g = 1$ by working with a Serre curve, that is, an elliptic curve for which $\left|\mathrm{GL}_2\left(\hat{\mathbb{Z}}\right) : \mathrm{Im}\,\rho_A\right| = 2$. For such a curve, the integer m_A is the least common multiple of 2 and the discriminant of $\mathbb{Q}\left(\sqrt{\Delta_A}\right)$, where Δ_A is the discriminant of any Weierstrass equation of A; see [27, Section 4, p. 1558]. As proved in [27] and later in [14], in more than one sense almost all elliptic curves are Serre curves. Examples of such curves, as exhibited by Serre in [41, pp. 310–311] and by Daniels in [16, p. 227], have been used for numerical computations in [13, 35].

For higher g, the investigation of m_A from a computational perspective is a solid problem in itself that remains to be tackled. In this section, while we do not provide numerical evidence for Conjecture 4, we do provide some computational data that complements our main theoretical results.

6.1 Values of $\pi_A(x,t)$

Figures 1 and 2 show the values of $\pi_A(x,t)$ graphed versus $\sqrt{x}/\log x$ for $t \in \{0,1\}$ and $A \in \{J_1, J_2, J_3\}$, where J_1, J_2, J_3 are the Jacobians of the hyperelliptic curves listed in Table 1. Prediction (38) would imply that these graphs approximate a straight line, whose slope is determined by the constant in front of $\sqrt{x}/\log x$; the graphs are indeed consistent with this implication.

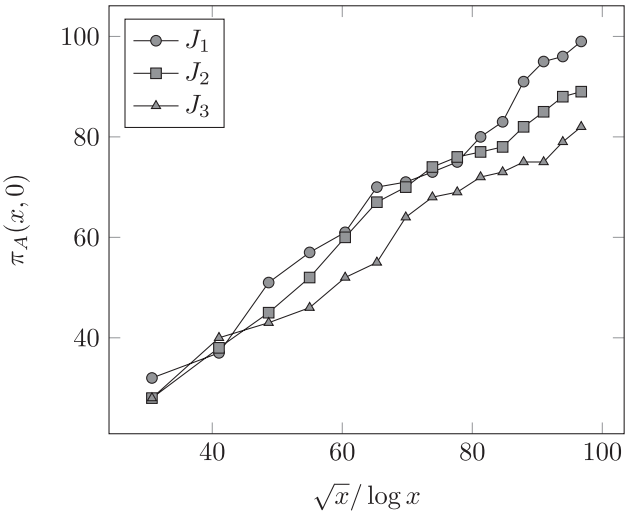

Fig. 1. Values of $\pi_A(x,0)$ versus $\sqrt{x}/\log x$ for various Jacobians of hyperelliptic curves.

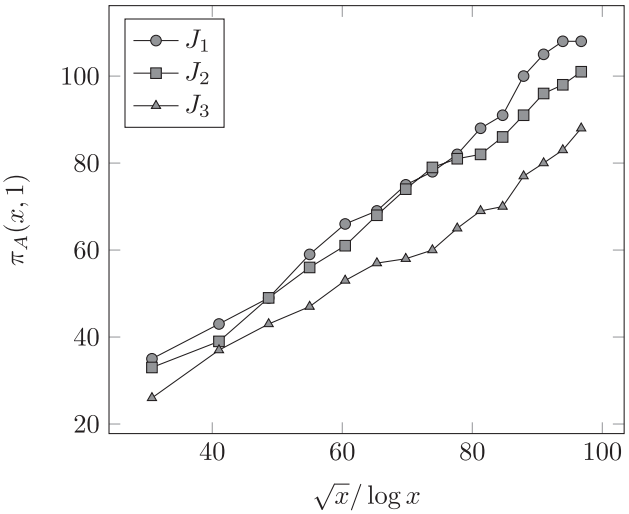

Fig. 2. Values of $\pi_A(x,1)$ versus $\sqrt{x}/\log x$ for various Jacobians of hyperelliptic curves.

6.2 Converging products of Lemma 12

In part (iii) of Lemma 12, we showed that the following infinite product converges for all integers t and all integers $g \geq 1$:

$$P_{g,t} := \prod_{\ell} \frac{\ell \cdot |\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}\, M \equiv t (\mathrm{mod}\, \ell)\}|}{|\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|}.$$

Table 1. Jacobians of hyperelliptic curves used in computations

Jacobian	Hyperelliptic curve	Genus	Comments
J_1	$y^2 = x^5 - x + 1$	2	Good reduction outside $\{2, 19, 151\}$, $\mathrm{End}(J_1) \cong \mathbb{Z}$ [18, p. 509]
J_2	$y^2 = 4x^7 - 12x - 35$	3	Everywhere semistable, $\mathrm{End}(J_2) \cong \mathbb{Z}$ [51, p. 2]
J_3	$y^2 = 4x^9 - 8x - 39$	4	Everywhere semistable, $\mathrm{End}(J_3) \cong \mathbb{Z}$ [51, p. 2]

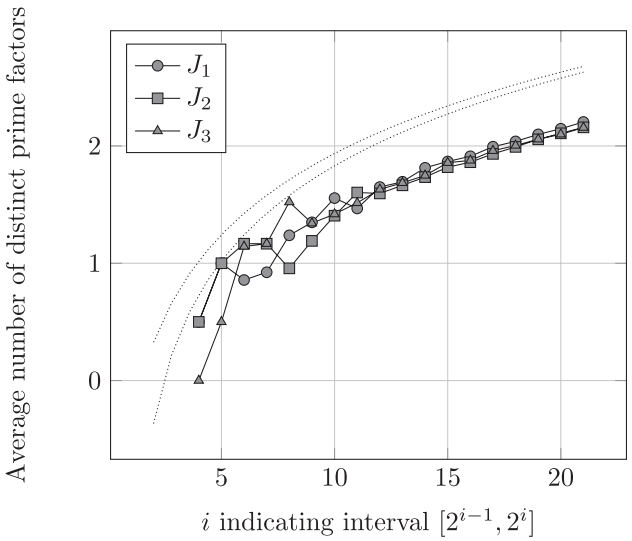

Fig. 3. Average number of $\nu(a_{1,p})$ for J_1, J_2, and J_3, in the intervals $[2^{i-1}, 2^i]$, $i = 2, \ldots, 21$. For comparison, the graphs of $\log(\log(2^i))$ and $\log(\log(2^{i-1}))$ are shown in dotted lines.

The numerical value of this product depends on the genus g and the primes dividing the trace t (more precisely, the numerator of each factor depends only on whether or not $\ell \mid t$). It is possible to compute its value for various g and t. For example, when $g = 2$ we can use the explicit formulae of Remark 13. In that case, for $t \in \{0, 1\}$, numerical computations show that the products appear to quickly converge to

$$P_{2,0} \approx 1.3547\ldots, \quad P_{2,1} \approx 0.7988\ldots.$$

6.3 The normal order of $\nu(a_{1,p})$

Figure 3 shows the average number of $\nu(a_{1,p})$ for J_1 of Table 1, for p in the intervals $[2^{i-1}, 2^i]$, $i = 2, \ldots, 21$. The graphs of $\log\log 2^i$ and $\log\log 2^{i-1}$ are shown for comparison.

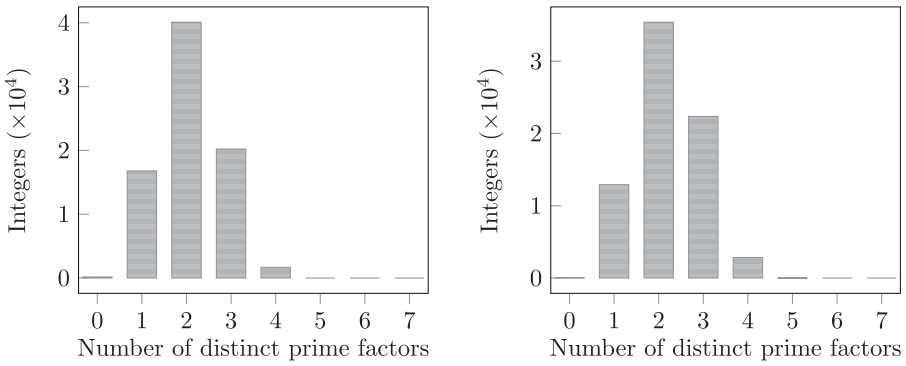

Fig. 4. Histograms of $\nu(a_{1,p})$ for J_1; on the left, the data are for primes $p < 2^{20}$, and on the right, the data are for primes $2^{20} < p < 2^{21}$. Primes of bad reduction and primes for which the trace is zero are excluded.

Figure 4 presents histograms of the values of $\nu(a_{1,p})$ for J_1 in two intervals: $[1, 2^{20}]$ and $[2^{20}, 2^{21}]$. The corresponding histograms for J_2 and J_3 are very similar.

Funding

This work was partially supported by the National Science Foundation under agreement No. DMS-0747724 (to A.C.C.), by the European Research Council under Starting Grant 258713 (to A.C.C.), by the Simons Collaborative Grant under Award No. 318454 (to A.C.C.), by the National Science Foundation under agreement CNS-0831004 (to A.S.), by the National Science Foundation MSPRF 0802915 (to K.E.S.), by the Natural Sciences and Engineering Research Council of Canada PDF 373333 (to K.E.S.), and by the National Security Agency under Grant H98230-14-1-0106 (to K.E.S.). The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein.

Acknowledgments

The authors thank Jeff Achter, Alina Bucur, Hao Chen, Francesc Fité, Nathan Jones, Kiran Kedlaya, Emmanuel Kowalski, Antonella Perucca, Karl Rubin, Jean-Pierre Serre, Drew Sutherland, Cassie Williams, and Jonathan Wise for valuable discussions related to this paper. They are grateful for the hospitality of the Banff International Research Station, Alberta, Canada, and the support of the organizers Chantal David, Matilde Lalín, and Michelle Manes of the conference *Women in Numbers 2* (2011), where this work was initiated. The last three authors thank the first author for her leadership and hard work on this project.

Appendix 1. Letter by J-P. Serre on Dimension of Conjugacy Classes in Symplectic Groups

Paris, May 8, 2015

Dear professor Cojocaru,

In case you want optimal estimates for the dimensions of conjugacy classes in **Sp** and **GSp**, here is what one can say:

Let us consider the algebraic groups $G = \mathbf{GSp}_{2n}$ or $\mathbf{Sp}_{2n}$ over a field k of characteristic 0 (there are some small changes in char. $p > 0$). Assume $n > 1$, since the case of $\mathbf{GL}_2$ and $\mathbf{SL}_2$ is obvious. If $g \in G(k)$, let $d(g)$ be the dimension of the conjugacy class of g, viewed as an algebraic subvariety of G; we have $d(g) = \dim G - \dim Z_G(g)$, where $Z_G(g)$ is the centralizer of g in G.

Theorem A.1. Assume that g is not of the form cu, where c is in the centre of G and u is unipotent. Then $d(g) \geqslant 4n-4$. If moreover $\mathrm{Tr}(g) = 0$ and $n > 2$, we have $d(g) \geqslant 4n-2$. □

A few remarks before giving the proof:

(1) This is a "geometric" statement: we may assume that the ground field is algebraically closed.

(2) We may assume that $G = \mathbf{Sp}_{2n}$; the case of $\mathbf{GSp}_{2n}$ follows by writing g as product of a scalar and an element of $\mathbf{Sp}_{2n}$; the dimension of the conjugacy class is the same.

(3) If $\mathrm{Tr}(g) = 0$, then the condition "$g \neq cu$" is satisfied, thanks to the fact that the characteristic does not divide $2n$.

(4) The bounds are optimal. One realizes them by using the obvious embedding $\iota : \mathbf{SL}_2 \to G$, fixing a non-degenerate subspace of codimension 2. If one chooses $g = \iota(-1)$, the centralizer of g in $\mathbf{Sp}_{2n}$ is $\mathbf{Sp}_{2n-2} \times \mathbf{SL}_2$; its dimension is $2(n-1)^2 + n - 1 + 3 = 2n^2 - 3n + 4$; hence the dimension of the conjugacy class of g is $\dim G - (2n^2 - 3n + 4) = 2n^2 + n - (2n^2 - 3n + 4) = 4n - 4$. If one chooses $g = \iota(x)$, where $x \in \mathbf{SL}_2$ is such that $\mathrm{Tr}(x) = 2 - 2n$ (this is always possible and gives a non-central element because $2 - 2n \neq \pm 2$), one gets an element of trace 0 with centralizer the product of $\mathbf{Sp}_{2n-2}$ by a group of dimension 1; its dimension is $2n^2 - 3n + 2$, and the dimension of its conjugacy class is $4n - 2$.

(5) In the ℓ-adic application, one needs the fact that, if $g \in \mathbf{GSp}_{2n}(\mathbf{Z}_\ell)$, the dimension (as an ℓ-adic manifold) of the conjugacy class of g is the same as its dimension in the sense of algebraic geometry.

For a given $t \in \mathbf{Z}$, with $t \neq \pm 2n$, one needs to choose ℓ so that no element of trace t of $\mathbf{GSp}_{2n}(\mathbf{Z}_\ell)$ can be of the forbidden shape cu ; as you explain in your paper, this is done by taking ℓ such that $v_\ell(t/2n) \neq 0$, which is always possible.

Proof of $d(g) \geqslant 4n - 4$.

We may assume that g is semisimple. Indeed, if we decompose g in Jordan form, as $g = su = us$, where s is semisimple and u is unipotent, the centralizer of g is contained in the centralizer of s, hence $d(g) \geqslant d(s)$.

Let us decompose the vector space $V = k^{2n}$ (with its chosen non-degenerate alternating form) as a direct sum of eigenspaces of g, say $V = \oplus V_\lambda$. These spaces have the following properties:

(a) V_1 and V_{-1} are non-degenerate, hence of even dimension;

(b) If $\lambda \neq 1, -1$, then V_λ is totally isotropic and in duality with $V_{\lambda^{-1}}$.

Put $n_\lambda = \dim V_\lambda$. The centralizer of g is :

$$Z_G(g) = \mathbf{Sp}_{n_1} \times \mathbf{Sp}_{n_{-1}} \times \Pi' \mathbf{GL}_{n_\lambda},$$

where the symbol Π' means a product on a set Λ such that $k^\times$ is the disjoint union of $\{1, -1\}, \Lambda$, and Λ^{-1}.

(It might be more efficient to use the orthogonal decomposition of V given by the eigenspaces of $g + g^{-1}$.)

This implies :

$$\dim Z_G(g) = \frac{1}{2}(n_1^2 + n_1 + n_{-1}^2 + n_{-1}) + \Sigma' n_\lambda^2, \tag{A.1}$$

where Σ' means a summation over $\lambda \in \Lambda$.

We also have:

$$2n = n_1 + n_{-1} + 2\Sigma' n_\lambda. \tag{A.2}$$

We now need to give an upper bound for the sum (A.1). Let us simplify the notation by putting $x = n_1/2, y = n_{-1}/2, z = \Sigma' n_\lambda$. Equation (A.2) becomes:

$$n = x + y + z, \tag{A.2'}$$

and equation (A.1) implies (using $(\Sigma' n_\lambda)^2 \geqslant \Sigma' n_\lambda^2$):

$$\dim Z_G(g) \leqslant 2x^2 + x + 2y^2 + y + z^2. \tag{A.3}$$

Consider first the case $z = 0$ (i.e., the case where g as order 2). In that case, (A.1) shows that $\dim Z_G(g) = 2x^2 + x + 2y^2 + y = 2n^2 + n - 4xy$. We have $xy \neq 0$, otherwise g would be central; hence x and y run between 1 and $n-1$. In that range the product xy is minimum when either x or y is equal to 1, in which case its value is $n-1$. Hence $\dim Z_G(g) \leqslant 2n^2 + n - 4(n-1)$, i.e., $d(g) \geqslant 4(n-1)$, as wanted.

Suppose $z \geqslant 1$; we have $x, y \geqslant 0$. With the relation (A.2′), this shows that the point $(x, y, z) \in \mathbf{R}^3$ belongs to the triangle with vertices the three points $(0, 0, n)$, $(0, n-1, 1)$, $(n-1, 0, 1)$. Since the function $2x^2+x+2y^2+y+z^2$ is convex, it attains its maximum at one of the vertices [6, Chapter II, Section 7.1, Proposition 1]; its values there are $n^2, 2n^2 - 3n + 2, 2n^2 - 3n + 2$. Since $n^2 \leqslant 2n^2 - 3n + 2$ for $n \geqslant 2$, this shows that $\dim Z_G(g) \leqslant 2n^2 - 3n + 2$, hence $d(g) \geqslant 4n - 2$, and *a fortiori* $d(g) \geqslant 4n - 4$, as wanted.

(The proof also shows that $d(g) = 4n-4$ is only possible when g is an involution of type $\pm\iota(-1)$, as in Remark 4.)

Proof of $d(g) \geqslant 4n - 2$ *when* $\mathrm{Tr}(g) = 0$.

We use the same notation as in the above proof. The case $z = 0$ is possible only if n is even, with $x = y = n/2$. This gives a centralizer of dimension n^2+n, hence $d(g) = n^2$, which is $> 4n - 2$ when $n \geqslant 4$. Hence $z \geqslant 1$, in which case the computation given above shows that $d(g) \geqslant 4n - 2$.

Best wishes

J-P. Serre

Appendix 2. Letter by J-P. Serre on the Continuity of the Density Function

Paris, April 12, 2015

Dear Katz,

Thank you very much for your letter about the density problem for $\mathbf{USp}(2n)$.

After writing to you I found a different way of getting the same result, based on an integration formula which is a combination of Weyl's formula and a formula of Steinberg [46, Lemma 8.2].

Let me start with a simple simply connected group G. Let T be a maximal torus and define the roots, weights, fundamental weights as usual. I need to number the fundamental weights: $\omega_1, \ldots, \omega_n$, where n is the rank. Call χ_i the traces of the corresponding fundamental representations and call ψ_i their restrictions to T (I am copying Steinberg's notations). Steinberg's formula is a formula relating the n-differential forms on T given on one hand by the exterior product of the $d\psi_i$ and on the other hand by the exterior product of the $d\omega_i/\omega_i$ (invariant differential on the torus). The formula is as follow:

$$d\psi_1 \wedge \ldots \wedge d\psi_n = f.d\omega_1/\omega_1 \wedge \cdots \wedge d\omega_n/\omega_n, \tag{A.4}$$

where $f = \omega_0 \prod_{\alpha>0}(1-\alpha^{-1})$ and $\omega_0 = \prod \omega_i$.

(Note that, here, I am forced to use a multiplicative notation for the roots, since I view them as functions on T.)

We may write f^2 in a slightly simpler form:

$$f^2 = \prod_{\alpha>0}(\alpha + \alpha^{-1} - 2). \tag{A.5}$$

This shows that f^2 is real and invariant by the Weyl group. It can thus be written as a polynomial in the χ_i ; let me call D that polynomial (it is a kind of discriminant: it vanishes only on the singular elements of G). We thus have:

$$f^2 = D(\chi_1, \ldots, \chi_n). \tag{A.6}$$

This formula of Steinberg gives an integration formula over any local field. Here I shall stick to $\mathbf{R}$ but I have no doubt that the p-adic case should be useful, too. To simplify matters, I shall suppose that -1 is in the Weyl group W.

Let now call UG the compact form of G, and UT the corresponding torus. The roots α, and the characters ω_i are now viewed as functions on UT with complex values of absolute value 1. The χ_i are real-valued functions (because of my assumption on the Weyl group); let me call them x_i; they give a map $x : UG \to \mathbf{R}^n$ which is well known (since Elie Cartan [9, pp. 803–804]) to have the following properties:

(a) It gives a homeomorphism of the space $Cl(UG)$ on to a compact subset C of $\mathbf{R}^n$.

(When G has type G_2, the set C is the one I asked you to draw for me.)

(b) Let C_T be the standard fundamental domain of W (in the tangent space, it corresponds to the fundamental alcove); the map $C_T \to C$ is a homeomorphism; the boundary of C corresponds to the singular classes. (I see that by using topological arguments.)

(c) The function $D(x_1, \ldots, x_n)$ (where D is as above) is a polynomial whose restriction to C is zero on the boundary and nowhere else.

By combining this with H. Weyl's integration formula, one finds:

Theorem A.2. The image by $x : UG \to \mathbf{R}^n$ of the normalized Haar measure of G has a continuous density (with respect to the standard measure $dx_1 \cdots dx_n$), namely the function $\varphi(x_1, \ldots, x_n)$ which is equal to 0 outside C and to $(2\pi)^{-n}|D(x_1, \ldots, x_n)|^{1/2}$ on C. □

Corollary A.3. The equidistribution measure associated with a fundamental character of G has a continuous density. □

More precisely, the density at a number c of the fundamental character χ_1 is equal to $\int \varphi(c, x_2, \ldots, x_n) dx_2 \cdots dx_n$.

Curiously, this point of view does not seem to give the fact that such densities are real analytic outside a finite number of values (namely, those taken by the character at the points of finite order of G corresponding to the vertices of the alcove, i.e. the points of G of order 1 or 2 when $G = \mathbf{Sp}_{2n}$).

One can also say when the density is not 0; for instance, for the trace when $G = \mathbf{Sp}_{2n}$ the density is nonzero when the trace c is such that $-2n < c < 2n$.

When -1 is not in the Weyl group, some fundamental characters come in pairs of conjugate ones and instead of $\mathbf{R}^n$ one should take a product of copies of $\mathbf{R}$ and $\mathbf{C}$. The case of $\mathbf{SL}_3$ is especially nice; the compact C lies inside $\mathbf{C}$ and is the interior (+ boundary) of a "hypocycloid with 3 cusps" (*hypocycloïde à trois rebroussements*—as I learned when preparing the ENS competition in 1944–45).

Best wishes

J-P. Serre

PS—The explicit formula for φ in the case of $\mathbf{Sp}_4$ is given in the aritcle of Fité *et al.* [21]; see Table 5, last line. Their a_1 is my x_1 and their a_2 is my $x_2 + 1$.

References

[1] Achter, J., and J. Holden. "Notes on an analogue of the Fontaine-Mazur conjecture." *Journal de Théorie des Nombres de Bordeaux* 15, no. 3 (2003): 627–37.

[2] Baier, S., and N. Jones. "A refined version of the Lang–Trotter conjecture." *International Mathematics Research Notices* 2009, no. 3 (2009): 433–61.

[3] Barnet-Lamb, T., D. Geraghty, M. Harris, and R. Taylor. "A family of Calabi-Yau varieties and potential automorphy II." *Publications of the Research Institute for Mathematical Sciences* 47 (2011): 29–98.

[4] Billingsley, P. "On the central limit theorem for the prime divisor function." *The American Mathematical Monthly* 76 (1969): 132–39.

[5] Billingsley, P. "The probability theory of additive arithmetic functions." *Annals of Probability* 2, no. 5 (1974): 749–91.

[6] Bourbaki, N. *Topological Vector Spaces, Chapters 1–5*. Elements of Mathematics. Berlin: Springer, 1987.

[7] Bucur, A., F. Fité, and K. S. Kedlaya. "Some instances of the effective Sato–Tate conjecture." in preparation.

[8] Calkin, N., L. Huckaba, K. James, J. Joyner, J. Schwartz, and E. Smith. *Computing the Lang–Trotter Constant*. http://www.ces.clemson.edu/~kevja/REU/2008/LangTrotterPaper.pdf, 2008 preprint (accessed on 13 May 2016).

[9] Cartan, É. *Oeuvres Complètes*. Partie I. Vol. 2. Paris: Éditions du Centre National de la Recherche Scientifique (CNRS), 1984.

[10] Castryck, W., A. Folsom, H. Hubrechts, and A. V. Sutherland. "The probability that the number of points on the Jacobian of a genus 2 curve is prime." *Proceedings of the London Mathematical Society (3)* 104, no. 6 (2012): 1235–70.

[11] Clozel, L., M. Harris, and R. Taylor. "Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations." *Publications Mathématiques. Institut de Hautes Études Scientifiques* 108 (2008): 1–181.

[12] Clozel, L. "The Sato–Tate conjecture." In *Current Developments in Mathematics (2006)*, edited by D. Jerison, B. Mazur, T. Mrowka, W. Schmid, R. Stanley, & S.-T. Yau, 1–34. Somerville, MA: Int. Press, 2008.

[13] Cojocaru, A. C., M. Fitzpatrick, T. Insley, and H. Yilmaz. Reductions modulo primes of Serre curves, in preparation.

[14] Cojocaru, A. C., D. Grant, and N. Jones. "One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations." *Proceedings of the London Mathematical Society* 103, no. 3 (2011): 654–75.

[15] Colmez, P., and J-P. Serre, eds. *Correspondance Serre-Tate, vol. 1 (1956–1973)*. Société Mathématique de France vol. 13, 2015.

[16] Daniels, H. B. "An infinite family of Serre curves." *Journal of Number Theory* 155 (2015): 226–47.

[17] Deuring, M. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper." *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 14 (1941): 197–272.

[18] Dieulefait, L. V. "Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$." *Experimental Mathematics* 11, no. 4 (2002): 503–12.

[19] Elkies, N. D. "Distribution of supersingular primes." *Journées Arithmétiques (1989): Luminy, Astérisque* no. 198–200 (1991): 127–32.

[20] Erdös, P., and M. Kac. "The Gaussian law of errors in the theory of additive number theoretic functions." *American Journal of Mathematics* 62 (1940): 738–42.

[21] Fité, F., K. S. Kedlaya, V. Rotger, and A. V. Sutherland. "Sato–Tate distributions and Galois endomorphism modules in genus 2." *Compositio Mathematica* 148, no. 5 (2012): 1390–442.

[22] Fouvry, É., and M. R. Murty. "On the distribution of supersingular primes." *Canadian Journal of Mathematics* 48, no 1 (1996): 81–104.

[23] Granville, A. and K. Soundararajan. "Sieving and the Erdős-Kac theorem." In *Equidistribution in number theory, an introduction*, 15–27. NATO Sci. Ser. II Math. Phys. Chem. (237): Dordrecht: Springer, 2007.

[24] Hall, C. "An open image theorem for a general class of abelian varieties." *Bulletin of the London Mathematical Society* 43, no. 4 (2011): 703–11.

[25] Hardy, G. H. and S. Ramanujan. "The normal number of prime factors of a number n." *Quarterly Journal of Mathematics* 48 (1920): 76–92.

[26] Hensel, K. "Über die Entwicklung der algebraischen Zahlen in Potenzreihen." *Mathematische Annalen* 55 (1902): 301–36.

[27] Jones, N. "Almost all elliptic curves are Serre curves." *Transactions of the American Mathematical Society* 362 (2010): 1547–70.

[28] Katz, N. M. "Lang–Trotter revisited." *Bulletin of the American Mathematical Society. New Series* 46, no. 3 (2009): 413–57.

[29] Katz, N. M. *"Density comments."* Letter to J-P. Serre. 2015.

[30] Katz, N. M., and P. C. Sarnak, *Random Matrices, Frobenius Eigenvalues, and Monodromy*. American Mathematical Society Colloquium Publications 45. Providence, RI: American Mathematical Society, 1999.

[31] Kedlaya, K. S., and A. V. Sutherland. *Hyperelliptic Curves, L-Polynomials, and Random Matrices. Arithmetic, Geometry, Cryptography and Coding Theory (AGCT 2007)*, Contemporary Mathematics 487, Providence, RI: American Mathematical Society, 2009, 119–62.

[32] Kim, D. S. "Exponential sums for symplectic groups and their applications." *Acta Arithmetica* 88, no. 2 (1999): 155–71.

[33] Kowalski, E. *The Large Sieve and Its Applications*. Cambridge Tracts in Mathematics 175. Cambridge: Cambridge University Press, 2008.

[34] Lagarias, J. C., and A. M. Odlyzko. "Effective Versions of the Chebotarev Density Theorem." In *Algebraic Number Fields: L-Functions and Galois Properties, Proceedings of Symposium, University Durham*, Durham (1975). London: Academic Press, 1977: 409–64.

[35] Lang, S., and H. Trotter. *Frobenius Distributions in* $\mathbf{GL}_2$*-Extensions,* Lecture Notes in Mathematics 504. Berlin, New York: Springer-Verlag, 1976.

[36] Murty, M. R., and V. K. Murty. "Prime divisors of Fourier coefficients of modular forms." *Duke Mathematical Journal* 51, no. 1 (1984): 57–76.

[37] Murty, M. R., V. K. Murty, and N. Saradha. "Modular forms and the Chebotarev density theorem." *American Journal of Mathematics* 110, no. 2 (1988): 253–81.

[38] Murty, V. K. "Modular Forms and the Chebotarev Density Theorem II." In *Analytic Number Theory (Kyoto, 1996)*. London Mathematical Society Lecture Notes Series 247. Cambridge: Cambridge University Press, 1997, 287–308.

[39] Murty, V. K. "Frobenius distributions and Galois representations." In *Automorphic Forms, Automorphic Representations, and Arithmetic (Fort Worth, TX, 1996)*, Proceedings Symposium Pure Mathematics 66, Part 1, 193–211. Providence, RI: American Mathematical Society, 1999.

[40] Serre, J.-P. "Lettre à Armand Borel, 18 mai 1966." in *Frobenius Distributions: Lang–Trotter and Sato–Tate Conjectures*. Contemporary Mathematics, Providence, RI: American Mathematical Society, 2016: 1–10.

[41] Serre, J.-P. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." *Inventiones Math.* 15, no. 4 (1972): 259–331.

[42] Serre, J.-P. "Quelques applications du théorème de densité de Chebotarev." *Publications Mathématiques. Institut de Hautes Études Scientifiques* no. 54 (1981): 123–201.

[43] Serre, J.-P. "Résumé des cours de 1985–1986." In *Annuaire du Collège de France* (1986): 95–99. Oeuvres Collected Papers, vol. IV. Berlin: Springer-Verlag, 2003: 33–7.

[44] Serre, J.-P. *Lettre à Marie-France Vignéras du 10/2/1986*. Oeuvres Collected Papers, vol. IV, Berlin: Springer-Verlag, 2003: 38–55.

[45] Serre, J.-P. "Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques." in Motives (Seattle, WA, 1991), Proceedings Symposium Pure Mathematics 55, Part 1, 377–400. Providence, RI: American Mathematical Society, 1994.

[46] Steinberg, R. "Regular elements of semi-simple algebraic groups." *Publications Mathématiques. Institut de Hautes Études Scientifiques* no. 25 (1965): 49–80.

[47] Turán, P. "On a theorem of Hardy and Ramanujan." *Journal of the London Mathematical Society* 9 (1934): 274–6.

[48] Wan, D. "On the Lang–Trotter conjecture." *Journal of Number Theory* 35 (1990): 247–68.

[49] Weyl, H. *The Classical Groups: Their Invariants and Representations*. 2nd Revised edition. Princeton, N.J.: Princeton University Press, 1997.

[50] Zarhin, Yu. G. "Hyperelliptic Jacobians without complex multiplication." *Mathematical Research Letters* 7, no. 1 (2000): 123–32.

[51] Zarhin, Yu. G. "Galois Groups of Mori trinomials and hyperelliptic curves with big monodromy." *European Journal of Mathematics* 2 (2016): 360–81.

[52] Zywina, D. *Bounds for the Lang–Trotter Conjectures*. In SCHOLAR—a Scientific Celebration Highlighting Open Lines of Arithmetic Research, Contemporary Mathematics vol. 655, Providence, RI: American Mathematical Society, 2015: 235–56.