MOMENTS AND DISTRIBUTION OF CENTRAL L-VALUES OF QUADRATIC TWISTS OF ELLIPTIC CURVES

MAKSYM RADZIWIŁŁ AND K. SOUNDARARAJAN

1. Introduction

The last two decades have seen tremendous progress in understanding the moments of central values in families of L-functions. There are now precise, and widely believed, conjectured asymptotic formulae for moments in several important families (see [3], [9], [21], [22]), and these conjectures have been verified in a variety of cases (see for example [1], [4], [30]). Furthermore, the work of Rudnick and Soundararajan ([27], [28]), together with its extension by the authors in [25], produces lower bounds of the conjectured order of magnitude for all moments larger than the first, provided a little more than the first moment can be computed. In this paper, we enunciate a complementary principle, which (roughly speaking) establishes that if one can compute a little more than a particular moment for some family of L-functions, then upper bounds of the conjectured order of magnitude hold for all smaller moments. Conditional on the Generalized Riemann Hypothesis, the work of Soundararajan [31] together with its sharp refinement by Harper [13] establishes the conjectured upper bounds for moments in many families; our work may be viewed as an unconditional analog of such results, but for a restricted range of moments. We shall illustrate our method for the important and well-studied family of quadratic twists of an elliptic curve. Here the first moment for central L-values is known, but the second moment can (at present) only be calculated assuming GRH (by adapting the argument of [30]). However, there is enough flexibility for us to work out an upper bound for all moments below the first. These ideas also enable us to study the distribution of the logarithm of the central L-values (when these are nonzero) and establish a one sided central limit theorem; this supports a conjecture of Keating and Snaith [21], and is an analog of Selberg's theorem on the normal distribution of $\log|\zeta(\frac{1}{2}+it)|$. Finally, our work leads to a conjecture on the distribution of the order of the Tate-Shafarevich group for rank zero quadratic twists of an elliptic curve, and establishes the upper bound part of this conjecture (assuming the Birch-Swinnerton-Dyer conjecture).

Let us now describe our results more precisely. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N. Write the associated Hasse-Weil L-function as

$$L(s,E)=\sum_{n=1}^{\infty}a(n)n^{-s},$$

The first author was partially supported by NSF grant DMS-1128155. The second author is partially supported by NSF grant DMS-1001068, and a Simons Investigator award from the Simons Foundation.

where the coefficients are normalized such that the Hasse bound reads $|a(n)| \le d(n)$ for all n, and so the center of the critical strip is $\frac{1}{2}$. Recall that $L(s,E)$ has an analytic continuation to the entire complex plane and satisfies the functional equation

$$\Lambda(s,E) = \epsilon_E \Lambda(1-s,E),$$

where ϵ_E, the root number, is ± 1, and

$$\Lambda(s,E) = \Big(\frac{\sqrt{N}}{2\pi}\Big)^s \Gamma(s+\tfrac{1}{2}) L(s,E).$$

Throughout the paper, d will denote a fundamental discriminant coprime to $2N$, and $\chi_d = (\frac{d}{\cdot})$ the associated primitive quadratic character. Let E_d denote the quadratic twist of the elliptic curve E by d. The twisted L-function associated to d is

$$L(s,E_d) = \sum_{n=1}^{\infty} a(n)\chi_d(n) n^{-s}.$$

If $(d,N)=1$ then E_d has conductor Nd^2 and the completed L-function

$$\Lambda(s,E_d) = \Big(\frac{\sqrt{N}|d|}{2\pi}\Big)^s \Gamma(s+\tfrac{1}{2}) L(s,E_d)$$

is entire and satisfies the functional equation

$$\Lambda(s,E_d) = \epsilon_E(d)\Lambda(s,E_d)$$

with

$$\epsilon_E(d) = \epsilon_E \chi_d(-N).$$

Note that, by Waldspurger's theorem, $L(\frac{1}{2},E_d) \ge 0$. Of course $L(\frac{1}{2},E_d) = 0$ when $\epsilon_E(d) = -1$, and in this paper, we shall restrict attention to those twists with root number 1. Put therefore

$$\mathcal{E} = \{d : \quad d \text{ a fundamental discriminant with } (d,2N)=1 \text{ and } \epsilon_E(d)=1\}.$$

Our first result concerns the moments of $L(\frac{1}{2},E_d)$. Keating and Snaith [21] have conjectured that for all real numbers $k \ge 0$,

$$\sum_{\substack{|d|\le X \\ d\in\mathcal{E}}} L(\tfrac{1}{2},E_d)^k \sim C_0(k,E) X (\log X)^{\frac{k(k-1)}{2}},$$

for a specified non-zero constant $C_0(k,E)$. As indicated earlier, this conjecture is known for $k=1$, and on GRH for $k=2$. We establish a sharp upper bound for all k between 0 and 1.

Theorem 1. *Let $0 \le k \le 1$ be a real number. For all large X we have*

$$\sum_{\substack{|d|\le X \\ d\in\mathcal{E}}} L(\tfrac{1}{2},E_d)^k \le C(k,E) X (\log X)^{\frac{k(k-1)}{2}},$$

for a positive constant $C(k,E)$.

By choosing k small but positive in Theorem 1, we see that $L(\frac{1}{2}, E_d) = O((\log |d|)^{-\frac{1}{2}+\epsilon})$ for all but $o(X)$ fundamental discriminants $|d| \leq X$ with $d \in \mathcal{E}$. More is expected to be true, and Keating and Snaith [22] have conjectured that, for $d \in \mathcal{E}$, the quantity $\log L(\frac{1}{2}, E_d)$ has a normal distribution with mean $-\frac{1}{2}\log\log|d|$ and variance $\log\log|d|$; see [5] for numerical data towards this conjecture. Here we interpret $\log L(\frac{1}{2}, E_d)$ to be negative infinity when the L-value vanishes. This conjecture is an analog of Selberg's theorem on the normal distribution of $\log|\zeta(\frac{1}{2}+it)|$. However the Keating-Snaith conjecture appears quite difficult to prove; for example, it implies the well-known conjecture of Goldfeld [11] that $L(\frac{1}{2}, E_d) \neq 0$ for almost all $d \in \mathcal{E}$. We are able to prove part of the Keating-Snaith conjecture, and establish the conjectured upper bound for the proportion of $d \in \mathcal{E}$ with $\log L(\frac{1}{2}, E_d) + \frac{1}{2}\log\log|d| \geq V\sqrt{\log\log|d|}$ for any fixed real number V.

Theorem 2. *Let V be a fixed real number. For large X we have*

$$\Big|\Big\{d \in \mathcal{E},\ 20 < |d| \leq X : \quad \frac{\log L(\frac{1}{2}, E_d) + \frac{1}{2}\log\log|d|}{\sqrt{\log\log|d|}} \geq V\Big\}\Big|$$

is at most

$$|\{d \in \mathcal{E}, |d| \leq X\}|\Big(\frac{1}{\sqrt{2\pi}}\int_V^\infty e^{-\frac{x^2}{2}}dx + o(1)\Big).$$

The connection between moments and analogs of Selberg's theorem for central values in families of L-functions is discussed in [31], where the possibility of establishing upper bounds as in Theorem 2 conditional on the Generalized Riemann Hypothesis is mentioned. Furthermore, if in addition to GRH one assumes the one level density conjectures of Katz and Sarnak [20] then the full Keating-Snaith conjecture on the normality of $\log L(\frac{1}{2}, E_d)$ would follow. In certain families of L-functions, Hough [16] has established unconditionally analogs of our Theorem 2. Hough's method relies on zero density results which show that most zeros of the L-functions under consideration lie near the critical line. While such zero density results are known in a number of cases, the family of quadratic twists of an elliptic curve is an example where such results remain elusive. The method used here is different (and perhaps simpler) and uses only knowledge about the first moment (plus epsilon) in the family.

In view of the Birch and Swinnerton-Dyer conjectures, our work contributes to the understanding of the distribution of the order of the Tate-Shafarevich group for those quadratic twists with analytic rank zero. Define, for $d \in \mathcal{E}$,

$$S(E_d) = L(\tfrac{1}{2}, E_d)\frac{|E_d(\mathbb{Q})_{\rm tors}|^2}{\Omega(E_d)\mathrm{Tam}(E_d)},$$

where $|E_d(\mathbb{Q})_{\rm tors}|$ denotes the size of the rational torsion group of E_d, $\Omega(E_d)$ denotes the real period of a minimal model for E_d, and $\mathrm{Tam}(E_d) = \prod_p T_p(d)$ is the product of the Tamagawa numbers. If $L(\frac{1}{2}, E_d) \neq 0$ then the Birch and Swinnerton-Dyer conjecture predicts that $S(E_d)$ equals the order of the Tate-Shafarevich group $Ш(E_d)$. Now $\Omega(E_d)$ is about size $1/\sqrt{|d|}$, and the Tamagawa factors $T_p(d)$ are generically 1 and for $p|d$ equal one more than the number

of roots of $f(x) \pmod p$ if E is represented in Weierstrass form as $y^2 = f(x)$. Thus, the behavior of these quantities for large $|d|$ is relatively straightforward, and combining this with the Keating-Snaith conjecture for $L(\frac{1}{2}, E_d)$, we are led to formulate the following conjecture.

Conjecture 1. *Let E be given by the model $y^2 = f(x)$ for a monic cubic polynomial f with integer coefficients. Let K denote the splitting field of f over $\mathbb{Q}$. Define the constants $\mu(E)$ and $\sigma(E)$ as follows: If $K = \mathbb{Q}$ so that E has full 2-torsion, set*

$$\mu(E) = -\tfrac{1}{2} - 2\log 2, \qquad \sigma(E)^2 = 1 + 4(\log 2)^2.$$

If $[K : \mathbb{Q}] = 2$ so that E has partial 2-torsion, set

$$\mu(E) = -\tfrac{1}{2} - \tfrac{3}{2}\log 2, \qquad \sigma(E)^2 = 1 + \tfrac{5}{2}(\log 2)^2.$$

If $[K : \mathbb{Q}] = 3$, then set

$$\mu(E) = -\tfrac{1}{2} - \tfrac{2}{3}\log 2, \qquad \sigma(E)^2 = 1 + \tfrac{4}{3}(\log 2)^2.$$

Lastly if $[K : \mathbb{Q}] = 6$, then set

$$\mu(E) = -\tfrac{1}{2} - \tfrac{5}{6}\log 2, \qquad \sigma(E)^2 = 1 + \tfrac{7}{6}(\log 2)^2.$$

As d ranges over $\mathcal{E}$, the distribution of $\log(|Ш(E_d)|/\sqrt{|d|})$ is approximately Gaussian with mean $\mu(E)\log\log|d|$ and variance $\sigma(E)^2\log\log|d|$. More precisely, for any fixed $V \in \mathbb{R}$ and as $X \to \infty$,

$$\Big|\Big\{d \in \mathcal{E}, 20 < |d| \le X : \quad \frac{\log(|Ш(E_d)|/\sqrt{|d|}) - \mu(E)\log\log|d|}{\sqrt{\sigma(E)^2\log\log|d|}} \ge V\Big\}\Big|$$

is

$$\sim |\{d \in \mathcal{E}, |d| \le X\}\Big(\frac{1}{\sqrt{2\pi}}\int_V^\infty e^{-\frac{x^2}{2}}dx\Big).$$

Previously, Delaunay [6] has studied the moments of orders of Tate-Shafarevich groups, and formulated analogs of the Keating-Snaith conjectures for the average values of $S(E_d)^k$. Our conjecture is naturally closely related to his work; see also the related papers [7] and [8]. In support of our conjecture, we are able to establish an upper bound for the distribution of values of $\log(S(E_d)/\sqrt{|d|})$ (as before, interpreting this quantity as $-\infty$ if $L(\frac{1}{2}, E_2) = 0$).

Theorem 3. *With notations as above, for fixed $V \in \mathbb{R}$ and as $X \to \infty$,*

$$\Big|\Big\{d \in \mathcal{E}, 20 < |d| \le X : \quad \frac{\log(|S(E_d)|/\sqrt{|d|}) - \mu(E)\log\log|d|}{\sqrt{\sigma(E)^2\log\log|d|}} \ge V\Big\}\Big|$$

is bounded above by

$$|\{d \in \mathcal{E}, |d| \le X\}\Big(\frac{1}{\sqrt{2\pi}}\int_V^\infty e^{-\frac{x^2}{2}}dx + o(1)\Big). \tag{1}$$

If the Birch and Swinnerton-Dyer conjecture for elliptic curves with analytic rank zero holds then the quantity in (1) *is an upper bound for*

$$\Big|\Big\{d\in\mathcal{E}, 20<|d|\le X:\quad L(\tfrac12,E_d)\neq 0,\quad \frac{\log(|Ш(E_d)|/\sqrt{|d|})-\mu(E)\log\log|d|}{\sqrt{\sigma(E)^2\log\log|d|}}\ge V\Big\}\Big|.$$

A lot of progress has been made on establishing the Birch and Swinnerton-Dyer conjecture in the analytic rank zero case, and thus the assumption in the final statement of our Theorem above seems plausibly within the reach of current technology (see [2] for results in a particular family of quadratic twists, and [24] for recent numerical verifications).

Our method is flexible enough to allow the introduction of a sieve over the fundamental discriminants d; thus we are able to obtain sharp upper bounds for moments of $L(\frac12,E_d)$ where the discriminants are restricted to prime values of $|d|$. Below, define

$$\mathcal{E}'=\{d\in\mathcal{E}:|d|\text{ is prime}\}.$$

For the twists by these "prime" discriminants, the effect of the Tamagawa numbers in the Birch and Swinnerton-Dyer conjectures is negligible, and we have the following analog of the Keating-Snaith conjecture and Conjecture 1 above.

Conjecture 2. *As d ranges over $\mathcal{E}'$, the quantities $\log(|Ш(E_d)|/\sqrt{|d|})$ and $\log L(\frac12,E_d)$ are distributed like a Gaussian random variable with mean $-\frac12\log\log|d|$ and variance $\log\log|d|$. More precisely, for any fixed $V\in\mathbb{R}$ and as $X\to\infty$,*

$$\Big|\Big\{d\in\mathcal{E}':20<|d|\le X:\quad \frac{\log(|Ш(E_d)|/\sqrt{|d|})+\frac12\log\log|d|}{\sqrt{\log\log|d|}}\ge V\Big\}\Big|$$

and

$$\Big|\Big\{d\in\mathcal{E}':20<|d|\le X:\quad \frac{\log L(\frac12,E_d)+\frac12\log\log|d|}{\sqrt{\log\log|d|}}\ge V\Big\}\Big|$$

are both

$$\sim|\{d\in\mathcal{E}',|d|\le X\}\Big(\frac{1}{\sqrt{2\pi}}\int_V^\infty e^{-\frac{x^2}{2}}dx\Big).$$

Analogously to Theorems 1, 2 and 3, our methods would enable us to obtain sharp upper bounds for the k-th moment (with $0\le k\le 1$) in this family, and also the upper bound part of Conjecture 2 (unconditionally for the distribution of $\log L(\frac12,E_d)$, and restricted to twists with analytic rank zero and conditional on Birch and Swinnerton-Dyer for $\log(|Ш(E_d)|/\sqrt{|d|})$). We shall address these problems in a sequel paper.

With minor modifications, our work applies to the family of quadratic twists of any modular form. By Waldspurger's theorem, thus we may obtain an understanding of the Fourier coefficients of half-integer weight modular forms. Further, we could also consider the family of quadratic twists where the root number is -1, and study here the moments of the derivative $L'(\frac12,E_d)$. As mentioned earlier, the method developed here is general and whenever some moment (plus epsilon) is known in a family, our method produces sharp upper bounds for all smaller moments. For the Riemann zeta-function, where the fourth moment

(plus epsilon) is known (see [17]), we are thus able to establish sharp upper bounds for all moments below the fourth; previously such bounds were established by Heath-Brown [14] conditional on the Riemann Hypothesis. Another application of this circle of ideas is to the problem of the fluctuations of a quantum observable for the modular surface. More precisely, let ψ denote a fixed even Hecke-Maass form for $X = PSL_2(\mathbb{Z})\backslash\mathbb{H}$, and let ϕ_j denote an even Hecke-Maass form with eigenvalue $\lambda_j = \frac{1}{4} + t_j^2$. The problem is to understand the behavior of $\mu_j(\psi) = \int_X \psi(z)|\phi_j(z)|^2 \frac{dx\ dy}{y^2}$ as λ_j gets large. The mean of this quantity is approximately zero, and its variance is calculated in Zhao [32] (see also [23] for a holomorphic analog). It has been suggested in the physics literature that $\mu_j(\psi)$ has Gaussian fluctuations (see [10]). However, by Watson's formula, $|\mu_j(\psi)|^2$ is related to the central value $L(\frac{1}{2}, \psi \times \phi_j \times \phi_j)$ and the Keating-Snaith conjectures strongly suggest that $\mu_j(\psi)$ is not Gaussian (but instead $\log|\mu_j(\psi)|$ is). This is another instance where only the first moment (plus epsilon) can be calculated, and our work would give sharp upper bounds for all moments up to the first, and establish a one sided central limit theorem for $\log|\mu_j(\psi)|$. In particular, it would follow that $\lambda_j^{\frac{1}{4}}|\mu_j(\psi)| = o(1)$ for almost all eigenfunctions with $\lambda_j \le \lambda$.

It would be interesting to obtain lower bounds towards the Keating-Snaith conjectures, complementing the upper bounds established here. In work in progress, we have extended the ideas developed here to obtain a partial result in that direction provided one can control two moments in the family under consideration. Unfortunately this does not apply to the family of quadratic twists of an elliptic curve, but would apply for example to the family of quadratic Dirichlet L-functions, or to the family of newforms of weight 2 and large level N. Finally, we comment that the method developed here is related to the iterative method of Harper [13] (discovered independently) which yields sharp conditional estimates for moments.

2. Two technical propositions

We begin by introducing some notation that will be in place throughout the paper. Let N_0 denote the lcm of 8 and N. Let $\kappa = \pm 1$, and let $a \pmod{N_0}$ denote a residue class with $a \equiv 1$ or $5 \pmod 8$. We assume that κ and a are such that for any fundamental discriminant d of sign κ with $d \equiv a \pmod{N_0}$, the root number $\epsilon_E(d) = \epsilon_E\chi_d(-N)$ equals 1. Put

$$\mathcal{E}(\kappa, a) = \{d \in \mathcal{E} : \kappa d > 0, \quad d \equiv a \pmod{N_0}\},$$

so that $\mathcal{E}$ is the union of all such sets $\mathcal{E}(\kappa, a)$. Note that if $d \equiv a \pmod{N_0}$ then d is automatically $1 \pmod 4$ so that the condition of being a fundamental discriminant is simply that d is squarefree. Further, note that for $d \in \mathcal{E}(\kappa, a)$ the values $\chi_d(-1)$, $\chi_d(2)$, and $\chi_d(p)$ for all $p|N$ are fixed. Therefore, it is well defined (and convenient) to set, for $\mathrm{Re}(s) > 0$,

$$L_a(s) = \sum_{\substack{n=1 \\ p|n \Longrightarrow p|N_0}}^{\infty} \frac{a(n)}{n^s}\chi_d(n). \tag{2}$$

Lastly, let Φ denote a smooth, non-negative function compactly supported on $[1/2, 5/2]$ with $\Phi(x) = 1$ for $x \in [1, 2]$, and define, for any complex number s,

$$\check{\Phi}(s) = \int_0^\infty \Phi(x) x^s dx. \tag{3}$$

Throughout the paper, implied constants may depend upon E (and thus N_0) and Φ.

Our theorems rely upon two technical propositions which allow us to compute averages of short Dirichlet polynomials, as well as averages of $L(\frac{1}{2}, E_d)$ multiplied by short Dirichlet polynomials.

Proposition 1. *Let n and v be positive integers both coprime to N_0, with v square-free, and $(n, v) = 1$. Suppose that $v\sqrt{n} \leq X^{\frac{1}{2}-\epsilon}$. If n is a square then*

$$\sum_{\substack{d \in \mathcal{E}(\kappa, a) \\ v|d}} \chi_d(n) \Phi\Big(\frac{\kappa d}{X}\Big) = \check{\Phi}(0) \frac{X}{vN_0} \prod_{p|nv} \Big(1 + \frac{1}{p}\Big)^{-1} \prod_{p \nmid N_0} \Big(1 - \frac{1}{p^2}\Big) + O(X^{\frac{1}{2}+\epsilon}\sqrt{n}).$$

If n is not a perfect square, then

$$\sum_{\substack{d \in \mathcal{E}(\kappa, a) \\ v|d}} \chi_d(n) \Phi\Big(\frac{\kappa d}{X}\Big) = O(X^{\frac{1}{2}+\epsilon}\sqrt{n}).$$

Proposition 2. *Let u and v be positive integers with $(u, v) = 1$, $(uv, N_0) = 1$ and v square-free. Define*

$$\mathcal{S}(X; u, v) = \sum_{\substack{d \in \mathcal{E}(\kappa, a) \\ v|d}} L(\tfrac{1}{2}, E_d) \chi_d(u) \Phi\Big(\frac{\kappa d}{X}\Big). \tag{4}$$

Write $u = u_1 u_2^2$ with u_1 square free. Then

$$\mathcal{S}(X; u, v) = \frac{2Xa(u_1)}{vu_1^{\frac{1}{2}} N_0} \check{\Phi}(0) L_a(\tfrac{1}{2}) L(1, sym^2 E) \mathcal{G}(1; u, v) + O(X^{\frac{7}{8}+\epsilon} u^{\frac{3}{8}} v^{\frac{1}{4}}).$$

Here $\mathcal{G}(1; u, v)$ may be expressed as $Cg(u)h(v)$ where $C = C(E)$ is a non-zero constant, and g and h are multiplicative functions with $g(p^k) = 1 + O(1/p)$, and $h(p) = 1 + O(1/p)$.

The constant C and the functions g and h are described explicitly in the proof given in section 10. For our work here, we only need Proposition 2 in the case $v = 1$, but the general version above gives us the flexibility to introduce a sieve for the values of d, and thus enables us to obtain results over 'prime' discriminants; we will discuss this problem elsewhere. We postpone the proofs of these propositions to sections 7 and 10, and proceed now to outline the proofs of the main theorems.

3. Proof of Theorem 1

To prove Theorem 1 we first obtain good bounds for $L(\frac{1}{2}, E_d)^k$ in terms of a suitable short Dirichlet polynomial and $L(\frac{1}{2}, E_d)$ times another short Dirichlet polynomial. We next formulate a general such inequality.

3.1. **The key inequality.** Let ℓ be a non-negative integer, and x a real number. Define

$$E_\ell(x) = \sum_{j=0}^{\ell} \frac{x^j}{j!}. \tag{5}$$

Lemma 1. *Let ℓ be a non-negative even integer. The function $E_\ell(x)$ is positive valued and convex. Further, for any $x \le 0$ we have $E_\ell(x) \ge e^x$. Finally, if ℓ is a positive even integer and $x \le \ell/e^2$, we have*

$$e^x \le \Big(1 + \frac{e^{-\ell}}{16}\Big) E_\ell(x).$$

Proof. We prove the first assertion by induction on ℓ, the case $\ell = 0$ being clear. Since $E_\ell''(x) = E_{\ell-2}(x)$, it suffices to prove that $E_\ell(x)$ takes on positive values, and convexity follows at once. Consider a point x where E_ℓ takes a local minimum. Then $E_\ell'(x) = E_{\ell-1}(x) = 0$, so that $E_\ell(x) = E_{\ell-1}(x) + \frac{x^\ell}{\ell!} = \frac{x^\ell}{\ell!} > 0$, as desired. The second assertion that $E_\ell(x) \ge e^x$ for $x \le 0$ follows similarly by considering a local minimum for $E_\ell(x) - e^x$ on $(-\infty, 0)$.

Now we prove the final assertion, and we may assume that $0 \le x \le \ell/e^2$. Using $\ell! \ge e(\ell/e)^\ell$, we see that

$$e^x - E_\ell(x) \le \sum_{j=\ell+1}^{\infty} \frac{x^j}{j!} \le \frac{x^\ell}{\ell!} \sum_{j=\ell+1}^{\infty} \Big(\frac{x}{\ell}\Big)^{j-\ell} \le \frac{1}{6}\frac{x^\ell}{\ell!} \le \frac{1}{16} e^{-\ell},$$

and since $E_\ell(x) \ge 1$ for $x \ge 0$, the lemma follows. □

Lemma 2. *Let $y \ge 0$ be a real number. Suppose that $x_1, \dots, x_R$ are real numbers, and $\ell_1, \dots, \ell_R$ are positive even integers. Then, for any $0 \le k \le 1$ we have*

$$\begin{aligned} y^k \le Cky \prod_{j=1}^{R} E_{\ell_j}((k-1)x_j) + C(1-k) \prod_{j=1}^{R} E_{\ell_j}(kx_j) \\ + \sum_{r=0}^{R-1} \Big(Cky \prod_{j=1}^{r} E_{\ell_j}((k-1)x_j) + C(1-k) \prod_{j=1}^{r} E_{\ell_j}(kx_j) \Big) \Big(\frac{e^2 x_{r+1}}{\ell_{r+1}} \Big)^{\ell_{r+1}}, \end{aligned}$$

where $C = \exp((e^{-\ell_1} + \dots + e^{-\ell_R})/16)$.

Proof. Suppose first that $|x_j| \le \ell_j/e^2$ for all $1 \le j \le R$. Recall Young's inequality: if a and b are non-negative and $p \ge 1$ with $1/p + 1/q = 1$ then $ab \le a^p/p + b^q/q$. Using this with $p = 1/k$, $q = 1/(1-k)$, $a = y^k \exp(k(k-1)(x_1 + \dots + x_R))$ and $b = \exp(k(1-k)(x_1 + \dots + x_R))$, we obtain

$$y^k \le ky \exp((k-1)(x_1 + \dots + x_R)) + (1-k)\exp(k(x_1 + \dots + x_R)).$$

Since $0 \le k \le 1$ and $|x_j| \le \ell_j/e^2$, it follows that $e^{(k-1)x_j} \le (1+e^{-\ell_j}/16)E_{\ell_j}((k-1)x_j)$ and that $e^{kx_j} \le (1+e^{-\ell_j}/16)E_{\ell_j}(kx_j)$. Using these inequalities we obtain

$$y^k \le Cky\prod_{j=1}^{R} E_{\ell_j}((k-1)x_j) + C(1-k)\prod_{j=1}^{R} E_{\ell_j}(kx_j).$$

This is one of the terms in the right hand side of our claimed inequality, and since all the terms are non-negative, the desired estimate follows in this case.

Now suppose that there exists $0 \le r \le R-1$ such that $|x_j| \le \ell_j/e^2$ for all $j \le r$, but $|x_{r+1}| > \ell_{r+1}/e^2$. As before, using Young's inequality we obtain

$$\begin{aligned} y^k &\le ky\exp((k-1)(x_1+\ldots+x_r)) + (1-k)\exp(k(x_1+\ldots+x_r)) \\ &\le Cky\prod_{j=1}^{r} E_{\ell_j}((k-1)x_j) + C(1-k)\prod_{j=1}^{r} E_{\ell_j}(kx_j). \end{aligned}$$

Since $|x_{r+1}| > \ell_{r+1}/e^2$ by assumption, multiplying the right hand side by $(e^2x_{r+1}/\ell_{r+1})^{\ell_{r+1}}$ only increases that quantity, and so our desired inequality follows in this case also. □

3.2. **Estimating $L(\frac{1}{2}, E_d)^k$.** We now specialize Lemma 2 to the situation at hand. Let d be an element of $\mathcal{E}(\kappa, a)$. Let R be a natural number and $\ell_1, \ldots, \ell_R$ be even natural numbers. Let $P_1, \ldots, P_R$ be disjoint subsets of primes p not dividing N_0. Define

$$\mathcal{P}_j(d) = \sum_{p\in P_j} \frac{a(p)}{\sqrt{p}}\chi_d(p). \tag{6}$$

Given a real number $0 \le k \le 1$, put

$$\mathcal{A}_j(d) = E_{\ell_j}((k-1)\mathcal{P}_j(d)), \tag{7}$$

and

$$\mathcal{B}_j(d) = E_{\ell_j}(k\mathcal{P}_j(d)). \tag{8}$$

Proposition 3. *With notations as above, we have*

$$\begin{aligned} \Big(\frac{L(\frac{1}{2},E_d)(\log|d|)^{\frac{1}{2}}}{L_a(\frac{1}{2})}\Big)^k \le Ck\frac{L(\frac{1}{2},E_d)(\log|d|)^{\frac{1}{2}}}{L_a(\frac{1}{2})}\Big(\prod_{j=1}^{R}\mathcal{A}_j(d) + \sum_{r=0}^{R-1}\prod_{j=1}^{r}\mathcal{A}_j(d)\Big(\frac{e^2\mathcal{P}_{r+1}(d)}{\ell_{r+1}}\Big)^{\ell_{r+1}}\Big) \\ + C(1-k)\Big(\prod_{j=1}^{R}\mathcal{B}_j(d) + \sum_{r=0}^{R-1}\prod_{j=1}^{r}\mathcal{B}_j(d)\Big(\frac{e^2\mathcal{P}_{r+1}(d)}{\ell_{r+1}}\Big)^{\ell_{r+1}}\Big), \end{aligned}$$

where $C = \exp((e^{-\ell_1}+\ldots+e^{-\ell_R})/16)$, as in Lemma 2.

Proof. The Proposition follows upon applying Lemma 2 with $y = L(\frac{1}{2}, E_d)(\log|d|)^{\frac{1}{2}}/L_a(\frac{1}{2})$, and $x_j = \mathcal{P}_j(d)$. □

3.3. **Estimation of terms arising from the key inequality.** Suppose now that X is large and $X/2 \le |d| \le 5X/2$. Define a sequence of even natural numbers ℓ_j by setting $\ell_1 = 2\lceil 100 \log\log X\rceil$ and for $j \ge 1$ put $\ell_{j+1} = 2\lceil 100 \log \ell_j\rceil$. Let R be the largest natural number with $\ell_R > 10^4$. Note that the sequence ℓ_j is monotone decreasing for $1 \le j \le R$, and indeed we have $\ell_j > \ell_{j+1}^2$ in this range. Now define P_1 to be the set of primes below X^{1/ℓ_1^2} that do not divide N_0. For $2 \le j \le R$ define P_j to be the primes lying in the interval $(X^{1/\ell_{j-1}^2}, X^{1/\ell_j^2}]$. Next define $\mathcal{P}_j(d)$, $\mathcal{A}_j(d)$ and $\mathcal{B}_j(d)$ as in (6), (7) and (8) above. We shall invoke Proposition 3 with this choice of parameters, and use Propositions 1 and 2 to estimate the terms that arise.

Proposition 4. *With notations as above,*

$$\sum_{d\in\mathcal{E}(\kappa,a)} \Big(\prod_{j=1}^{R}\mathcal{B}_j(d) + \sum_{r=0}^{R-1}\prod_{j=1}^{r}\mathcal{B}_j(d)\Big(\frac{e^2\mathcal{P}_{r+1}(d)}{\ell_{r+1}}\Big)^{\ell_{r+1}}\Big)\Phi\Big(\frac{\kappa d}{X}\Big) \ll X(\log X)^{\frac{k^2}{2}}.$$

Proposition 5. *With notations as above,*

$$\sum_{d\in\mathcal{E}(\kappa,a)} L(\frac12, E_d)\Big(\prod_{j=1}^{R}\mathcal{A}_j(d) + \sum_{r=0}^{R-1}\prod_{j=1}^{r}\mathcal{A}_j(d)\Big(\frac{e^2\mathcal{P}_{r+1}(d)}{\ell_{r+1}}\Big)^{\ell_{r+1}}\Big)\Phi\Big(\frac{\kappa d}{X}\Big) \ll X(\log X)^{\frac{k^2-1}{2}}.$$

The implied constants in Propositions 4 and 5 depend only on k, Φ, and E. We defer the proofs of these propositions to sections 8 and 9, and now complete the proof of Theorem 1.

3.4. **Completing the proof of Theorem 1.** Applying Propositions 3, 4, and 5 we obtain that

$$\sum_{d\in\mathcal{E}(\kappa,a)} L(\tfrac12, E_d)^k\Phi\Big(\frac{\kappa d}{X}\Big) \ll X(\log X)^{\frac{k(k-1)}{2}}.$$

Now summing over the different possibilities for a and κ, and breaking the range $|d| \le X$ into dyadic blocks, we obtain Theorem 1.

4. Proof of Theorem 2

We begin with a well-known result on the average size of $a(p)^2$, which will be useful throughout the paper. The proof of the lemma follows from the Rankin-Selberg theory for $L(s, E)$; see Chapter 5 of Iwaniec and Kowalski [19].

Lemma 3. *There exists a positive constant c such that*

$$\sum_{p\le x} a(p)^2\log p = x + O(x\exp(-c\sqrt{\log x})).$$

Further, there exists a constant B such that

$$\sum_{p\le x}\frac{a(p)^2}{p} = \log\log x + B + O\Big(\frac{1}{\log x}\Big).$$

Let X be large, and let P denote the set of primes below $X^{1/(\log\log X)^2}$ with $p \nmid N_0$. Let $d \in \mathcal{E}(\kappa, a)$ with $X \le |d| \le 2X$, and define

$$\mathcal{P}(d) = \sum_{p \in P} \frac{a(p)}{\sqrt{p}} \chi_d(p).$$

Proposition 6. *Let k be a given non-negative integer. Then, for large X and any $v \le X^{\frac{1}{2}-\epsilon}$,*

$$\sum_{\substack{d \in \mathcal{E}(\kappa,a) \\ v|d}} \mathcal{P}(d)^k \Phi\Big(\frac{\kappa d}{X}\Big) = \Big(\sum_{\substack{d \in \mathcal{E}(\kappa,a) \\ v|d}} \Phi\Big(\frac{\kappa d}{X}\Big)\Big)(\log\log X)^{\frac{k}{2}}(M_k + o(1)),$$

where M_k denotes the k-th Gaussian moment:

$$M_k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} x^k e^{-\frac{x^2}{2}} dx = \begin{cases} 0 & \text{if } k \text{ is odd} \\ \frac{k!}{2^{k/2}(k/2)!} & \text{if } k \text{ is even.} \end{cases}$$

Proof. Let P_v denote the set of primes in P that do not divide v. Expanding $\mathcal{P}(d)^k$, we obtain

$$\sum_{\substack{d \in \mathcal{E}(\kappa,a) \\ v|d}} \mathcal{P}(d)^k \Phi\Big(\frac{\kappa d}{X}\Big) = \sum_{p_1 \in P_v} \cdots \sum_{p_k \in P_v} \frac{a(p_1)\dots a(p_k)}{\sqrt{p_1 \cdots p_k}} \sum_{\substack{d \in \mathcal{E}(\kappa,a) \\ v|d}} \chi_d(p_1 \cdots p_k) \Phi\Big(\frac{\kappa d}{X}\Big). \tag{9}$$

Now we use Proposition 1. If $p_1 \cdots p_k$ is not a perfect square (which is always the case when k is odd) then the sum over d above is $O(X^{\frac{1}{2}+\epsilon}(p_1 \cdots p_k)^{\frac{1}{2}})$, and the contribution of these remainder terms to (9) is $O(X^{\frac{1}{2}+\epsilon})$. This proves the proposition in the case when k is odd.

When k is even, we have a main term arising from the case $p_1 \cdots p_k = \square$. This term contributes

$$\widehat{\Phi}(0) \frac{X}{vN_0} \prod_{p \nmid N_0} \Big(1 - \frac{1}{p^2}\Big) \prod_{p|v} \Big(1 + \frac{1}{p}\Big)^{-1} \sum_{\substack{p_1,\dots,p_k \in P_v \\ p_1 \dots p_k = \square}} \frac{a(p_1)\dots a(p_k)}{\sqrt{p_1 \cdots p_k}} \prod_{p | p_1 \cdots p_k} \Big(1 + \frac{1}{p}\Big)^{-1}. \tag{10}$$

Suppose $q_1 < q_2 < \ldots < q_s$ are the distinct primes in $p_1, \ldots, p_k$. Then each q_j appears an even number (say $a_j \ge 2$) of times among the p_j, and thus $s \le k/2$. The terms with $s < k/2$ contribute an amount

$$\ll \frac{X}{v} \Big(\sum_{p \in P_v} \frac{a(p)^2}{p}\Big)^s \ll X(\log\log X)^{\frac{k}{2}-1},$$

which is an acceptable error term. When $s = k/2$, all the a_j must equal 2, and so these terms contribute

$$\widehat{\Phi}(0) \frac{X}{vN_0} \prod_{p \nmid N_0} \Big(1 - \frac{1}{p^2}\Big) \prod_{p|v} \Big(1 + \frac{1}{p}\Big)^{-1} \frac{k!}{2^{k/2}(k/2)!} \sum_{\substack{q_1,\dots,q_{k/2} \in P_v \\ q_j \text{ distinct}}} \frac{a(q_1)^2 \cdots a(q_{k/2})^2}{(q_1+1)\cdots(q_{k/2}+1)}.$$

Appealing to Lemma 3, this establishes our proposition. □

Since the normal distribution is determined by its moments, by taking Φ to approximate the characteristic function of $[1,2]$, summing over dyadic blocks and then over all possibilities for κ and a, we find from Proposition 6 (with $v=1$) that for any fixed $V\in\mathbb{R}$ and as $X\to\infty$

$$\Big|\Big\{d\in\mathcal{E}, 20<|d|\le X:\ \frac{\mathcal{P}(d)}{\sqrt{\log\log X}}\ge V\Big\}\Big| \sim |\{d\in\mathcal{E}, 20<|d|\le X\}| \times\Big(\frac{1}{\sqrt{2\pi}}\int_V^\infty e^{-\frac{x^2}{2}}dx+o(1)\Big). \tag{11}$$

Now if $d\in\mathcal{E}$ with $X/\log X<|d|\le X$ satisfies $\log L(\frac12,E_d)+\frac12\log\log X\ge V\sqrt{\log\log X}$ then we must have one of the following three cases: (1) $\mathcal{P}(d)\ge (V-\epsilon)\sqrt{\log\log X}$, or (2) $\mathcal{P}(d)\le -\log\log X$, or (3) $-\log\log X\le\mathcal{P}(d)\le (V-\epsilon)\sqrt{\log\log X}$ but $L(\frac12,E_d)(\log X)^{\frac12}\exp(-\mathcal{P}(d))\ge\exp(\epsilon\sqrt{\log\log X})$.

From (11) we already have a satisfactory estimate for the frequency with which the first case happens. Next using Proposition 6 with $v=1$ and $k=2$ we see that case (2) appears with frequency $o(X)$. Finally consider case 3. Put $\ell=20\lfloor\log\log X\rfloor$ so that ℓ is an even integer with $\ell\ge e^2|\mathcal{P}(d)|$. By Lemma 1 we must have $L(\frac12,E_d)(\log X)^{\frac12}E_\ell(-\mathcal{P}(d))\gg\exp(\epsilon\sqrt{\log\log X})$. Now, a small modification of Proposition 5 shows that

$$\sum_{\substack{d\in\mathcal{E}(\kappa,a)\\ X/\log X\le|d|\le X}} L(\tfrac12,E_d)(\log X)^{\frac12}E_\ell(-\mathcal{P}(d))\ll X\log\log X, \tag{12}$$

and so case (3) also occurs with frequency $o(X)$. This completes our proof.

5. Proof of Theorem 3

Recall that the elliptic curve E is given in Weierstrass form by $y^2=f(x)$ for a monic cubic polynomial f with integer coefficients, and that K is the splitting field of f over $\mathbb{Q}$. Let $c(p)$ denote 1 plus the number of solutions to $f(x)\equiv 0 \pmod p$, so that $c(p)=1$, 2, or 4. The Tamagawa number $\mathrm{Tam}(E_d)=\prod_p T_p(d)$ may be calculated using Tate's algorithm (see [26]). Primes dividing the discriminant of f make a bounded contribution, and for a prime not dividing the discriminant the factor $T_p(d)$ equals $c(p)$ if $p|d$, and $T_p(d)=1$ otherwise.

Lemma 4. *In the notation of Conjecture 1, we have*

$$\sum_{p\le x}\frac{\log c(p)}{p}=\Big(-\mu(E)-\frac12\Big)\log\log x+O(1),$$

and

$$\sum_{p\le x}\frac{(\log c(p))^2}{p}=(\sigma(E)^2-1)\log\log x+O(1).$$

Proof. Let us consider the case when $[K:\mathbb{Q}]=6$, so that the extension has Galois group S_3. The Chebotarev density theorem gives that $c(p)=4$ for a set of primes of density $1/6$,

$c(p) = 2$ on a set of primes of density $1/2$, and $c(p) = 1$ on a set of primes of density $1/3$. This proves the lemma in this case, and the other cases are similar. □

Let X be large and define $\mathcal{P}(d)$ as in Section 4. Further define, for primes $p \nmid N_0$,

$$C_p(d) = \begin{cases} \frac{p}{p+1}\log c(p) & \text{if } p|d \\ -\frac{1}{p+1}\log c(p) & \text{if } p \nmid d. \end{cases}$$

Put $z = X^{1/(\log\log X)^2}$ and set

$$\mathcal{C}(d) = \sum_{\log X \le p \le z} C_p(d) = \sum_{\log X \le p \le z} \Big(\log T_p(d) - \frac{\log c(p)}{p+1} \Big). \tag{13}$$

Since the real period $\Omega(E_d)$ is $\asymp 1/\sqrt{|d|}$, and $|E_d(\mathbb{Q})_{\text{tors}}|$ is bounded, in order to prove Theorem 3, it suffices to estimate

$$\Big| \Big\{ d \in \mathcal{E}, \frac{X}{\log X} \le |d| \le X : \ \frac{\log L(\frac{1}{2}, E_d) - \sum_{p|d} \log c(p) - \mu(E)\log\log X}{\sqrt{\sigma(E)^2 \log\log X}} \ge V \Big\} \Big|. \tag{14}$$

If d is a discriminant counted in (14) then one of the following four cases must happen: (1) $\mathcal{P}(d) - \mathcal{C}(d) \ge (V-\epsilon)\sqrt{\sigma(E)^2\log\log X}$, or (2) $\mathcal{P}(d) \le -\log\log X$, or (3) $-\log\log X \le \mathcal{P}(d) \le (V-\epsilon)\sqrt{\log\log X}$ but $L(\frac{1}{2}, E_d)(\log X)^{\frac{1}{2}} \exp(-\mathcal{P}(d)) \ge \exp(\epsilon\sqrt{\log\log X})$, or (4) $|\log \mathrm{Tam}(E_d) + (\mu(E) + \frac{1}{2})\log\log X - \mathcal{C}(d)| \ge \frac{\epsilon}{10}\sqrt{\log\log X}$.

From our work in Section 4, we know that cases 2 and 3 occur for at most $o(X)$ discriminants d. Now consider case 4. By Lemma 4

$$|\log \mathrm{Tam}(E_d) + (\mu(E) + \tfrac{1}{2})\log\log X - \mathcal{C}(d)| = \sum_{\substack{p|d \\ p < \log X}} \log c(p) + \sum_{\substack{p|d \\ p > z}} \log c(p) + O(\log\log\log X).$$

Summing the above over all $d \in \mathcal{E}$ with $X/\log X \le |d| \le X$ we get

$$\sum_{\substack{d \in \mathcal{E} \\ X/\log X \le |d| \le X}} |\log \mathrm{Tam}(E_d) + (\mu(E) + \tfrac{1}{2})\log\log X - \mathcal{C}(d)|$$

$$\ll X\log\log\log X + X \sum_{p < \log X} \frac{\log c(p)}{p} + X \sum_{X \ge p > z} \frac{\log c(p)}{p} \ll X \log\log\log X.$$

Therefore case 4 also occurs with frequency $o(X)$. It remains lastly to estimate the occurrence of case 1, which we achieve by computing the moments of $\mathcal{P}(d) - \mathcal{C}(d)$, and showing that these approximate the moments of a normal distribution with mean zero and variance $\sigma(E)^2 \log\log X$; our work here follows the argument in [12]. Since, as noted already, the Gaussian is determined by its moments, this completes the proof of Theorem 3.

Proposition 7. *Let k be a given non-negative integer. Then for large X we have*

$$\sum_{d \in \mathcal{E}(\kappa, a)} (\mathcal{P}(d) - \mathcal{C}(d))^k \Phi\Big(\frac{\kappa d}{X}\Big) = (\sigma(E)^2 \log\log X)^{\frac{k}{2}} (M_k + o(1)) \sum_{d \in \mathcal{E}(\kappa, a)} \Phi\Big(\frac{\kappa d}{X}\Big).$$

Proof. Expanding out our sum, we must evaluate

$$\sum_{j=0}^{k}\binom{k}{j}(-1)^j\sum_{(\log X)\le p_1,\dots,p_j\le z}\sum_{d\in\mathcal{E}(\kappa,a)}C_{p_1}(d)\cdots C_{p_j}(d)\mathcal{P}(d)^{k-j}\Phi\Big(\frac{\kappa d}{X}\Big). \tag{15}$$

Suppose that $q_1<q_2<\ldots<q_\ell$ are the distinct primes appearing in p_1, …, p_j and that q_i appears with multiplicity a_i. For such a choice of p_1, …, p_j, note that

$$C_{p_1}(d)\cdots C_{p_j}(d)=\prod_{i=1}^{\ell}C_{q_i}(d)^{a_i}=\sum_{v|(d,q_1\cdots q_\ell)}\Big(\sum_{rs=v}\mu(r)\prod_{i=1}^{\ell}C_{q_i}(s)^{a_i}\Big).$$

Therefore the inner sum over d in (15) equals

$$\sum_{v|q_1\cdots q_\ell}\Big(\sum_{rs=v}\mu(r)\prod_{i=1}^{\ell}C_{q_i}(s)^{a_i}\Big)\sum_{\substack{d\in\mathcal{E}(\kappa,a)\\ v|d}}\mathcal{P}(d)^{k-j}\Phi\Big(\frac{\kappa d}{X}\Big). \tag{16}$$

Using our work from Section 4, and in particular (10) there, we see that the sum over d above is

$$\check{\Phi}(0)\frac{X}{N_0}\prod_{p\nmid N_0}\Big(1-\frac{1}{p^2}\Big)\prod_{p|v}\Big(\frac{1}{p+1}\Big)\sum_{\substack{p_{j+1},\dots,p_k\in P_v\\ p_{j+1}\cdots p_k=\square}}\frac{a(p_{j+1})\cdots a(p_k)}{\sqrt{p_{j+1}\cdots p_k}}\prod_{p|p_{j+1}\cdots p_k}\Big(1+\frac{1}{p}\Big)^{-1}+O(X^{\frac12+\epsilon}).$$

Above, as in Section 4, P_v denotes the set of primes below z that do not divide N_0 or v. But the contribution of terms above with some p_i dividing v is easily seen to be $O(X(\log\log X)^k/(v\log X))$, since all the prime factors of v are larger than $\log X$. Thus removing the restriction that p_i do not divide v (for $j+1\le i\le k$), we see that the quantity in (16) is, up to an error $O(X(\log\log X)^k/(v\log X))$,

$$\check{\Phi}(0)\frac{X}{N_0}\prod_{p\nmid N_0}\Big(1-\frac{1}{p^2}\Big)\sum_{\substack{p_{j+1},\dots,p_k\in P\\ p_{j+1}\cdots p_k=\square}}\frac{a(p_{j+1})\cdots a(p_k)}{\sqrt{p_{j+1}\cdots p_k}}\prod_{p|p_{j+1}\cdots p_k}\Big(1+\frac{1}{p}\Big)^{-1}G(q_1^{a_1}\cdots q_\ell^{a_\ell}), \tag{17}$$

where

$$G(q_1^{a_1}\cdots q_\ell^{a_\ell})=\sum_{v|q_1\cdots q_\ell}\Big(\sum_{rs=v}\mu(r)\prod_{i=1}^{\ell}C_{q_i}(s)^{a_i}\Big)\prod_{p|v}\Big(\frac{1}{p+1}\Big).$$

Now it is easy to see that G is a multiplicative function and that

$$G(p^a)=(\log c(p))^a\Big(\frac{1}{p+1}\Big(1-\frac{1}{p+1}\Big)^a+\frac{p}{p+1}\Big(-\frac{1}{p+1}\Big)^a\Big).$$

Hence $G(q_1^{a_1}\cdots q_\ell^{a_\ell})$ is non-zero only if all the a_i are at least 2, and $G(p^a)\ll(\log c(p))^a/p$ for all $a\ge2$.

We now use this evaluation of the inner sum over d in (15), and then perform the sum over p_1, …, p_j. First note that the error term incurred above leads to a total error of at most $O(X(\log\log X)^{2k}/(\log X))$, which is acceptable for the proposition. Now let us simplify the

main term that arose above. Given $q_1 < \ldots < q_\ell$ and $a_i \geq 2$ with $\sum a_i = j$, the number of choices for $p_1, \ldots, p_j$ is $j!/(a_1! \cdots a_\ell!)$. Thus the main term is

$$\check{\Phi}(0)\frac{X}{N_0}\prod_{p\nmid N_0}\Big(1-\frac{1}{p^2}\Big)\sum_{j=0}^{k}\binom{k}{j}(-1)^j \sum_{\substack{p_{j+1},\ldots,p_k\in P\\ p_{j+1}\cdots p_k=\square}}\frac{a(p_{j+1})\cdots a(p_k)}{\sqrt{p_{j+1}\cdots p_k}}\prod_{p\mid p_{j+1}\cdots p_k}\Big(1+\frac{1}{p}\Big)^{-1}$$

$$\times \sum_{\substack{\ell\\ a_1,\ldots a_\ell\geq 2\\ \sum a_i=j}}\frac{j!}{\prod_i a_i!}\sum_{\log X\leq q_1<\ldots<q_\ell<z} G(q_1^{a_1}\cdots q_\ell^{a_\ell}). \tag{18}$$

Now if any $a_i \geq 3$, then the sum over q_i above is seen to be $\ll (\log\log X)^{(j-1)/2}$, and the sum over $p_{j+1}, \ldots, p_k$ contributes $\ll (\log\log X)^{(k-j)/2}$, leading to a total of $\ll X(\log\log X)^{(k-1)/2}$. Thus the effect of such terms is negligible, and we are left with the case when all $a_i = 2$, so that $j = 2\ell$ is even. Since $G(p^2) \sim (\log c(p))^2/p$, using Lemma 4, these terms contribute

$$\sim \check{\Phi}(0)\frac{X}{N_0}\prod_{p\nmid N_0}\Big(1-\frac{1}{p^2}\Big)\sum_{\substack{j=0\\ j \text{ even}}}^{k}\binom{k}{j}\frac{j!}{2^{j/2}(j/2)!}((\sigma(E)^2-1)\log\log X)^{j/2}$$

$$\times \sum_{\substack{p_{j+1},\ldots,p_k\in P\\ p_{j+1}\cdots p_k=\square}}\frac{a(p_{j+1})\cdots a(p_k)}{\sqrt{p_{j+1}\cdots p_k}}\prod_{p\mid p_{j+1}\cdots p_k}\Big(1+\frac{1}{p}\Big)^{-1}.$$

Now, the sum over $p_{j+1}, \ldots, p_k$ is zero unless $k-j$ is even (so that k is even), and in that case, arguing as in Section 4, it equals $\sim \frac{(k-j)!}{2^{(k-j)/2}((k-j)/2)!}(\log\log X)^{(k-j)/2}$. Using this above, we conclude the proposition. □

6. Preliminary Lemmas

6.1. The approximate functional equation.

Lemma 5. *For $d \in \mathcal{E}(\kappa, a)$ we have*

$$L(\tfrac{1}{2}, E_d) = 2\sum_{\substack{n=1\\ (n,N_0)=1}}^{\infty}\frac{a(n)}{\sqrt{n}}\chi_d(n)W\Big(\frac{n}{|d|}\Big),$$

where for $\xi > 0$ and any $c > 0$ we define

$$W(\xi) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} L_a(s+\tfrac{1}{2})\Gamma(s)\Big(\frac{\sqrt{N}}{2\pi\xi}\Big)^s ds.$$

The function $W(\xi)$ is smooth in $\xi > 0$ and satisfies $W^{(k)}(\xi) \ll_k \xi^{-k}e^{-2\pi\xi/\sqrt{N}}$ for non-negative integers k and further we have $W(\xi) = L_a(\frac{1}{2}) + O(\xi^{\frac{1}{2}-\epsilon})$ as $\xi \to 0$.

Proof. We begin with, for $c > \frac{1}{2}$,

$$I = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\Big(\frac{\sqrt{N}|d|}{2\pi}\Big)^s\Gamma(s+1)L(s+\tfrac{1}{2},E_d)\frac{ds}{s}.$$

On the one hand, since

$$L(s+\tfrac{1}{2},E_d) = L_a(s+\tfrac{1}{2})\sum_{\substack{n=1\\(n,N_0)=1}}^{\infty}\frac{a(n)}{\sqrt{n}}\chi_d(n),$$

integrating term by term we see that

$$I = \sum_{\substack{n=1\\(n,N_0)=1}}^{\infty}\frac{a(n)}{\sqrt{n}}\chi_d(n)W\Big(\frac{n}{|d|}\Big).$$

On the other hand, moving the line of integration in I to $-c$ and using the functional equation (note that the sign is positive by assumption) we may see that

$$I = L(\tfrac{1}{2},E_d) - I,$$

and the stated identity follows. Now from the definition of W we see that

$$W(\xi) = \sum_{\substack{n=1\\p|n \implies p|N_0}}^{\infty}\frac{a(n)}{\sqrt{n}}\chi_d(n)e^{-2\pi\xi n/\sqrt{N}}.$$

From this it is clear that W is smooth in $\xi > 0$, and the stated bound on $W^{(k)}(\xi)$ follows. The last claim on the behavior of $W(\xi)$ as $\xi \to 0$ is obtained by moving the line of integration to $\mathrm{Re}(s) = -\frac{1}{2}+\epsilon$, and picking up the contribution of the pole at $s = 0$. □

6.2. **Poisson summation.** Here we apply the Poisson summation formula to understand real character sums. Let n be an odd integer and define the Gauss type sum $G_k(n)$ for any integer k by

$$G_k(n) = \Big(\frac{1-i}{2} + \Big(\frac{-1}{n}\Big)\frac{1+i}{2}\Big)\sum_{a \pmod n}\Big(\frac{a}{n}\Big)e\Big(\frac{ak}{n}\Big).$$

In addition to G_k, it is helpful to define the closely related sum

$$\tau_k(n) = \sum_{b \pmod n}\Big(\frac{b}{n}\Big)e\Big(\frac{kb}{n}\Big) = \Big(\frac{1+i}{2} + \Big(\frac{-1}{n}\Big)\frac{1-i}{2}\Big)G_k(n).$$

The Gauss type sum $G_k(n)$ has been calculated explicitly in Lemma 2.3 of [29] which we now quote.

Lemma 6. *If m and n are coprime odd integers then $G_k(mn) = G_k(m)G_k(n)$. If p^α is the largest power of p dividing k (setting $\alpha = \infty$ if $k = 0$) then*

$$G_k(p^\beta) = \begin{cases} 0 & \text{if } \beta \le \alpha \text{ is odd,} \\ \phi(p^\beta) & \text{if } \beta \le \alpha \text{ is even,} \\ -p^\alpha & \text{if } \beta = \alpha + 1 \text{ is even,} \\ (\frac{kp^{-\alpha}}{p})p^\alpha\sqrt{p} & \text{if } \beta = \alpha + 1 \text{ is odd,} \\ 0 & \text{if } \beta \ge \alpha + 2. \end{cases}$$

Lemma 7. *Let $r \pmod q$ be a given residue class, and let n be an odd natural number coprime to q. Let F be a smooth compactly supported function. Then*

$$\sum_{d \equiv r \pmod q} \Big(\frac{d}{n}\Big) F(d) = \frac{1}{qn}\Big(\frac{q}{n}\Big) \sum_k \widehat{F}\Big(\frac{k}{nq}\Big) e\Big(\frac{kr\overline{n}}{q}\Big)\tau_k(n),$$

where $\widehat{F}$ denotes the Fourier transform.

Proof. The desired sum is

$$\sum_{b \pmod n} \Big(\frac{b}{n}\Big) \sum_{\substack{d \equiv r \pmod q \\ d \equiv b \pmod n}} F(d).$$

Since q and n are coprime, the congruence conditions above may be expressed as $d \equiv bq\overline{q} + rn\overline{n} \pmod{qn}$ where $q\overline{q} \equiv 1 \pmod n$ and $n\overline{n} \equiv 1 \pmod q$. Thus, using Poisson summation the inner sum over d equals

$$\sum_{d \equiv bq\overline{q} + rn\overline{n} \pmod{qn}} F(d) = \frac{1}{qn} \sum_k \widehat{F}\Big(\frac{k}{nq}\Big) e\Big(\frac{kb\overline{q}}{n} + \frac{kr\overline{n}}{q}\Big).$$

Bringing back the sum over b we conclude that the desired sum equals

$$\frac{1}{qn} \sum_k \widehat{F}\Big(\frac{k}{nq}\Big) e\Big(\frac{kr\overline{n}}{q}\Big) \sum_{b \pmod n} \Big(\frac{b}{n}\Big) e\Big(\frac{kb\overline{q}}{n}\Big) = \frac{1}{qn}\Big(\frac{q}{n}\Big) \sum_k \widehat{F}\Big(\frac{k}{nq}\Big) e\Big(\frac{kr\overline{n}}{q}\Big)\tau_k(n).$$

□

7. Proof of Proposition 1

Since v is square-free and coprime to N_0, note that, (for d coprime to N_0, and d a multiple of v)

$$\sum_{\beta \mid (v, d/v)} \mu(\beta) \sum_{\substack{(\alpha, vN_0) = 1 \\ \alpha^2 \mid d/v}} \mu(\alpha) = \begin{cases} 1 & \text{if } d \text{ is a square-free multiple of } v \\ 0 & \text{otherwise.} \end{cases} \tag{19}$$

Thus, writing $d = kv\beta\alpha^2$, we obtain

(20)
$$\sum_{\substack{d\in\mathcal{E}(\kappa,a)\\ v|d}}\chi_d(n)\Phi\Big(\frac{\kappa d}{X}\Big) = \sum_{\beta|v}\sum_{(\alpha,vN_0)=1}\mu(\beta)\mu(\alpha)\Big(\frac{v\beta\alpha^2}{n}\Big)\sum_{k\equiv a\overline{v\beta\alpha^2}\pmod{N_0}}\Big(\frac{k}{n}\Big)\Phi\Big(\frac{\kappa kv\beta\alpha^2}{X}\Big).$$

Put $A = X^{\frac12-\epsilon}/(v\sqrt{n})$. Estimating the sum over k trivially, the terms in (20) with $\alpha > A$ contribute

$$\ll \sum_{\beta|v}\sum_{\alpha>A}\frac{X}{v\beta\alpha^2} \ll \frac{Xv^\epsilon}{vA} \ll X^{\frac12+\epsilon}\sqrt{n}. \tag{21}$$

For the terms with $\alpha \le A$, we use the Poisson summation as stated in Lemma 7, which gives

(22)
$$\sum_{k\equiv a\overline{v\beta\alpha^2}\pmod{N_0}}\Big(\frac{k}{n}\Big)\Phi\Big(\frac{\kappa kv\beta\alpha^2}{X}\Big) = \frac{X}{nN_0v\beta\alpha^2}\Big(\frac{\kappa N_0}{n}\Big)\sum_{\ell}\widehat{\Phi}\Big(\frac{X\ell}{nv\beta\alpha^2N_0}\Big)e\Big(\frac{\ell a\overline{v\beta\alpha^2n}}{N_0}\Big)\tau_\ell(n).$$

Since $X/(nv\beta\alpha^2N_0) \ge X^\epsilon/N_0$ and $\hat\Phi(\xi) \ll_K |\xi|^{-K}$ for any $K > 0$, we see that the terms with $\ell \ne 0$ above contribute (using the trivial bound $|\tau_\ell(n)| \le n$) an amount $\ll X^{-1}$ say. If n is not a perfect square, then the term $\ell = 0$ above vanishes, and we conclude that the quantity in (22) is $\ll X^{-1}$. Using this in (20) we see that the terms with $\alpha \le A$ contribute $\ll X^{-1+\epsilon}A$ in this case. Thus the proposition follows in the case when n is not a perfect square.

When n is a perfect square, the term $\ell = 0$ makes a contribution of $\hat\Phi(0)\frac{\phi(n)}{n}\frac{X}{vN_0\beta\alpha^2}$ in (22). Thus the terms with $\alpha \le A$ contribute to (20)

$$\begin{aligned}&\widehat{\Phi}(0)\frac{X}{vN_0}\frac{\phi(n)}{n}\sum_{\beta|v}\frac{\mu(\beta)}{\beta}\sum_{\substack{(\alpha,vnN_0)=1\\ \alpha\le A}}\frac{\mu(\alpha)}{\alpha^2} + O(AX^{-1+\epsilon})\\ =&\widehat{\Phi}(0)\frac{X}{vN_0}\frac{\phi(n)}{n}\sum_{\beta|v}\frac{\mu(\beta)}{\beta}\sum_{(\alpha,vnN_0)=1}\frac{\mu(\alpha)}{\alpha^2} + O(X^{\frac12+\epsilon}\sqrt{n}).\end{aligned}$$

It is easy to check that the main term above equals

$$\widehat{\Phi}(0)\frac{X}{vN_0}\prod_{p\nmid N_0}\Big(1-\frac{1}{p^2}\Big)\prod_{p|nv}\Big(1+\frac1p\Big)^{-1},$$

and so the proposition follows in the case when n is a perfect square, completing our proof.

8. Proof of Proposition 4

Let $\tilde a(n)$ denote the completely multiplicative function defined on primes p by $\tilde a(p) = a(p)$. Let $w(n)$ be the multiplicative function defined by $w(p^\alpha) = \alpha!$ for prime powers p^α. For

$1 \le j \le R$ we may write

$$\mathcal{B}_j(d) = \sum_{n_j} \frac{\tilde{a}(n_j)}{\sqrt{n_j}} \frac{k^{\Omega(n_j)}}{w(n_j)} b_j(n_j)\chi_d(n_j), \tag{23}$$

where $\Omega(n_j)$ denotes the number of prime factors of n_j (counted with multiplicity), and $b_j(n_j) = 1$ if n_j is composed of at most ℓ_j primes, all from the interval P_j, and $b_j(n_j)$ is zero otherwise. In particular, note that $b_j(n_j) = 0$ unless $n_j < (X^{1/\ell_j^2})^{\ell_j} = X^{1/\ell_j}$, so that $\mathcal{B}_j(d)$ is a short Dirichlet polynomial. Write also

$$\frac{1}{\ell_j!}\mathcal{P}_j(d)^{\ell_j} = \sum_{n_j} \frac{\tilde{a}(n_j)}{w(n_j)\sqrt{n_j}} p_j(n_j)\chi_d(n_j), \tag{24}$$

where $p_j(n_j) = 1$ if n_j is composed of exactly ℓ_j primes (counted with multiplicity) all from the interval P_j, and $p_j(n_j) = 0$ otherwise. This too is a short Dirichlet polynomial supported only on $n_j \le X^{1/\ell_j}$. Thus note that $\prod_{j=1}^{R} \mathcal{B}_j(d)$ and $\prod_{j=1}^{r} \mathcal{B}_j(d)\mathcal{P}_{r+1}^{\ell_{r+1}}$ are all short Dirichlet polynomials, of length at most $X^{1/\ell_1+\ldots+1/\ell_R} < X^{1/1000}$.

Let $0 \le r \le R-1$ and consider one of the terms $\prod_{j=1}^{r} \mathcal{B}_j(d)\mathcal{P}_{r+1}^{\ell_{r+1}}$ that arises in our proposition. We expand this term using (23) and (24), and appeal to Proposition 1 (with $v = 1$ there). Since the Dirichlet polynomials $\mathcal{B}_j$ and ${\mathcal{P}_j}^{\ell_j}$ are short, the error terms arising from Proposition 1 contribute a negligible amount. We are thus left with the main term, which is

$$\frac{X}{N_0}\check{\Phi}(0) \prod_{p\nmid N_0}\Big(1-\frac{1}{p^2}\Big) \prod_{j=1}^{r}\Big(\sum_{n_j=\square} \frac{\tilde{a}(n_j)}{\sqrt{n_j}} \frac{k^{\Omega(n_j)}}{w(n_j)} \prod_{p\mid n_j}\Big(1+\frac{1}{p}\Big)^{-1} b_j(n_j)\Big)$$
$$\times \Big(\ell_{r+1}! \sum_{n_{r+1}=\square} \frac{\tilde{a}(n_{r+1})}{w(n_{r+1})\sqrt{n_{r+1}}} \prod_{p\mid n_{r+1}}\Big(1+\frac{1}{p}\Big)^{-1} p_{r+1}(n_{r+1})\Big).$$

Now, since all the terms involved are non-negative,

$$\sum_{n_j=\square} \frac{\tilde{a}(n_j)}{\sqrt{n_j}} \frac{k^{\Omega(n_j)}}{w(n_j)} \prod_{p\mid n_j}\Big(1+\frac{1}{p}\Big)^{-1} b_j(n_j) \le \prod_{p\in P_j}\Big(\sum_{t=0}^{\infty} \frac{a(p)^{2t}}{p^t}\frac{k^{2t}}{(2t)!}\Big) \ll \exp\Big(\frac{k^2}{2}\sum_{p\in P_j}\frac{a(p)^2}{p}\Big).$$

Similarly we find that

$$\sum_{n_{r+1}=\square} \frac{\tilde{a}(n_{r+1})}{w(n_{r+1})\sqrt{n_{r+1}}} \prod_{p\mid n_{r+1}}\Big(1+\frac{1}{p}\Big)^{-1} p_{r+1}(n_{r+1}) \le \frac{1}{(\ell_{r+1}/2)!}\Big(\sum_{p\in P_{r+1}}\frac{a(p)^2}{p}\Big)^{\ell_{r+1}/2}.$$

Putting all these observations together, we find that

$$\sum_{d\in\mathcal{E}(\kappa,a)}\prod_{j=1}^{r}\mathcal{B}_j(d)\Big(\frac{e^2\mathcal{P}_{r+1}}{\ell_{r+1}}\Big)^{\ell_{r+1}}\Phi\Big(\frac{\kappa d}{X}\Big)\ll X\exp\Big(\frac{k^2}{2}\sum_{j=1}^{r}\sum_{p\in P_j}\frac{a(p)^2}{p}\Big)$$
$$\times\Big(\Big(\frac{e^2}{\ell_{r+1}}\Big)^{\ell_{r+1}}\frac{\ell_{r+1}!}{(\ell_{r+1}/2)!}\Big(\sum_{p\in P_{r+1}}\frac{a(p)^2}{p}\Big)^{\ell_{r+1}/2}\Big).$$

Using Stirling's formula, Lemma 3, and that $\ell_{r+1}\geq 10^4$ we find that the above is

$$\ll Xe^{-\ell_{r+1}}(\log X)^{\frac{k^2}{2}}.$$

Arguing in the same way, we obtain

$$\sum_{d\in\mathcal{E}(\kappa,a)}\prod_{j=1}^{R}\mathcal{B}_j(d)\Phi\Big(\frac{\kappa d}{X}\Big)\ll X(\log x)^{\frac{k^2}{2}}.$$

Summing all these bounds, the proposition follows.

9. Proof of Proposition 5

Let $\tilde{a}(n)$, $w(n)$, $b_j(n)$ and $p_j(n)$ be defined as in Section 8. Then for $1\leq j\leq R$ we may write

$$\mathcal{A}_j(d)=\sum_{n_j}\frac{\tilde{a}(n_j)}{\sqrt{n_j}}\frac{(k-1)^{\Omega(n_j)}}{w(n_j)}b_j(n_j)\chi_d(n_j).$$

We shall also use the expression (24). Thus, as in Section 8, $\prod_{j=1}^{R}\mathcal{A}_j(d)$ and $\prod_{j=1}^{r}\mathcal{A}_j(d)\mathcal{P}_{r+1}^{\ell_{r+1}}$ are short Dirichlet polynomials of length at most $X^{1/1000}$.

Let $0\leq r\leq R-1$ and consider one of the terms $\prod_{j=1}^{r}\mathcal{A}_j(d)\mathcal{P}_{r+1}^{\ell_{r+1}}$ that arises in our proposition. We expand this term into its Dirichlet series, and appeal to Proposition 2 (with $v=1$ there). The error terms are negligible and we are left once again with the main term, which is

$$C(a,E)\check{\Phi}(0)X\prod_{j=1}^{r}\Big(\sum_{n_j}\frac{\tilde{a}(n_j)}{\sqrt{n_j}}\frac{a(n_{j1})}{\sqrt{n_{j1}}}\frac{(k-1)^{\Omega(n_j)}}{w(n_j)}b_j(n_j)g(n_j)\Big)$$
$$\times\Big(\ell_{r+1}!\sum_{n_{r+1}}\frac{\tilde{a}(n_{r+1})a(n_{(r+1)1})}{\sqrt{n_{r+1}n_{(r+1)1}}}\frac{g(n_{r+1})p_{r+1}(n_{r+1})}{w(n_{r+1})}\Big).\tag{25}$$

Here $C(a,E)$ is a constant, depending only on a and E; we write $n_j=n_{j1}n_{j2}^2$ with n_{j1} square-free; and g is the multiplicative function of Proposition 2.

Consider one of the terms with $1\leq j\leq r$ in (25) above. The factor $b_j(n_j)$ constrains n_j to have all prime factors in P_j, and also restricts $\Omega(n_j)$ to be at most ℓ_j. If we ignore the

restriction on $\Omega(n_j)$, the result would be given by the Euler product

$$\prod_{p\in P_j}\Big(\sum_{j=0}^{\infty}\frac{a(p)^{2j}}{p^j}\frac{(k-1)^{2j}}{(2j)!}g(p^{2j})+\sum_{j=0}^{\infty}\frac{a(p)^{2j+2}}{p^{j+1}}\frac{(k-1)^{2j+1}}{(2j+1)!}g(p^{2j+1})\Big); \tag{26}$$

the first sum above counts terms where n_j is divisible by an even power of p (so that n_{j1} is not a multiple of p), and the second sum counts those terms with an odd power of p dividing n_j (so that n_{j1} is divisible by p). The error in replacing the quantity in (25) by the Euler product of (26) comes from terms with $\Omega(n_j)>\ell_j$. We estimate this error using "Rankin's trick." Since $2^{\Omega(n_j)-\ell_j}\geq 1$ if $\Omega(n_j)>\ell_j$, the error in passing from (25) to (26) is at most

$$\sum_{n_j}\frac{|\tilde{a}(n_j)|}{\sqrt{n_j}}\frac{|a(n_{j1})|}{\sqrt{n_{j1}}}\frac{|k-1|^{\Omega(n_j)}}{w(n_j)}2^{\Omega(n_j)-\ell_j}g(n_j),$$

which is

$$\begin{aligned}&\leq 2^{-\ell_j}\prod_{p\in P_j}\Big(\sum_{j=0}^{\infty}\frac{a(p)^{2j}}{p^j}\frac{(k-1)^{2j}2^{2j}}{(2j)!}g(p^{2j})+\sum_{j=0}^{\infty}\frac{a(p)^{2j+2}}{p^{j+1}}\frac{|k-1|^{2j+1}2^{2j+1}}{(2j+1)!}g(p^{2j+1})\Big)\\&\ll 2^{-\ell_j}\exp\Big(4\sum_{p\in P_j}\frac{a(p)^2}{p}\Big).\end{aligned}$$

Since the quantity in (26) is $\gg\exp(\frac{k^2-1}{2}\sum_{p\in P_j}\frac{a(p)^2}{p})$ and, using Lemma 3 and the definition of ℓ_j, we may check that $\ell_j\geq 10\sum_{p\in P_j}a(p)^2/p$, we conclude that

$$\begin{aligned}&\sum_{n_j}\frac{\tilde{a}(n_j)}{\sqrt{n_j}}\frac{a(n_{j1})}{\sqrt{n_{j1}}}\frac{(k-1)^{\Omega(n_j)}}{w(n_j)}b_j(n_j)g(n_j)=(1+O(2^{-\ell_j/2}))\\&\qquad\times\prod_{p\in P_j}\Big(\sum_{j=0}^{\infty}\frac{a(p)^{2j}}{p^j}\frac{(k-1)^{2j}}{(2j)!}g(p^{2j})+\sum_{j=0}^{\infty}\frac{a(p)^{2j+2}}{p^{j+1}}\frac{(k-1)^{2j+1}}{(2j+1)!}g(p^{2j+1})\Big).\end{aligned}\tag{27}$$

Now consider the contribution of the n_{r+1} terms in (25). Note that the terms here satisfy $\Omega(n_{r+1})=\ell_{r+1}$, and we estimate these using Rankin's method again. Thus, the contribution of the n_{r+1} terms is

$$\leq \ell_{r+1}!10^{-\ell_{r+1}}\prod_{p\in P_{r+1}}\Big(\sum_{j=0}^{\infty}\sum_{j=0}^{\infty}\frac{a(p)^{2j}10^{2j}}{p^j(2j)!}g(p^{2j})+\sum_{j=1}^{\infty}\frac{a(p)^{2j+2}10^{2j+1}}{p^{j+1}(2j+1)!}g(p^{2j+1})\Big).$$

Since $\ell_{r+1}!\leq\ell_{r+1}(\ell_{r+1}/e)^{\ell_{r+1}}$, the above is, using Lemma 3 and the definition of ℓ_j,

$$\ll\ell_{r+1}\Big(\frac{\ell_{r+1}}{10e}\Big)^{\ell_{r+1}}\exp\Big(60\sum_{p\in P_{r+1}}\frac{a(p)^2}{p}\Big)\ll\ell_{r+1}\Big(\frac{\ell_{r+1}}{10e}\Big)^{\ell_{r+1}}\exp(\tfrac{3}{5}\ell_{r+1}).$$

Using the above estimate together with (25) and (27), we conclude that

$$\sum_{d\in\mathcal{E}(\kappa,a)} L(\tfrac12,E_d)\prod_{j=1}^{r}\mathcal{A}_j(d)\Big(\frac{e^2\mathcal{P}_{r+1}}{\ell_{r+1}}\Big)^{\ell_{r+1}}\Phi\Big(\frac{\kappa d}{X}\Big)$$
$$\ll Xe^{-\ell_{r+1}/2}\prod_{p\in\cup_{j=1}^{r}P_j}\Big(\sum_{j=0}^{\infty}\frac{a(p)^{2j}}{p^j}\frac{(k-1)^{2j}}{(2j)!}g(p^{2j})+\sum_{j=0}^{\infty}\frac{a(p)^{2j+2}}{p^{j+1}}\frac{(k-1)^{2j+1}}{(2j+1)!}g(p^{2j+1})\Big).$$

Using Lemma 3, we check that for all $0\le r\le R-1$ the above is

$$\ll X\exp(-\tfrac{\ell_{r+1}}{3})(\log X)^{\frac{k^2-1}{2}}.$$

A similar argument shows that

$$\sum_{d\in\mathcal{E}(\kappa,a)} L(\tfrac12,E_d)\prod_{j=1}^{R}\mathcal{A}_j(d)\Phi\Big(\frac{\kappa d}{X}\Big)\ll X(\log X)^{\frac{k^2-1}{2}},$$

and summing all these bounds, we obtain our proposition.

10. Proof of Proposition 2

The proof of Proposition 2 follows the general plan of the arguments in [29] and [30] (see also [18]); therefore, in some places below we have been brief, and suppressed some details. Using Lemma 5 in (4) we obtain

$$\mathcal{S}(X;u,v)=2\sum_{\substack{n=1\\(n,N_0)=1}}^{\infty}\frac{a(n)}{\sqrt{n}}\sum_{\substack{d\in\mathcal{E}(\kappa,a)\\ v|d}}\chi_d(nu)W\Big(\frac{n}{\kappa d}\Big)\Phi\Big(\frac{\kappa d}{X}\Big). \tag{28}$$

The inner sum over d in (28) runs over multiples of v that are square-free and lying in the progression $a \pmod{N_0}$. Thus, using (19), and writing $d=kv\beta\alpha^2$, we see that the sum over d in (28) equals

$$\sum_{\beta|v}\sum_{(\alpha,vN_0)=1}\mu(\beta)\mu(\alpha)\Big(\frac{v\beta\alpha^2}{nu}\Big)\sum_{k\equiv a\overline{v\beta\alpha^2}\pmod{N_0}}\Big(\frac{k}{nu}\Big)W\Big(\frac{n}{\kappa kv\beta\alpha^2}\Big)\Phi\Big(\frac{\kappa kv\beta\alpha^2}{X}\Big). \tag{29}$$

Let $Y>1$ be a parameter to be chosen later. We distinguish the cases $\beta\alpha^2>Y$ and $\beta\alpha^2\le Y$. First we bound the contribution of the terms with $\beta\alpha^2>Y$; the main term will arise from the case $\beta\alpha^2\le Y$.

10.1. **The terms with $\alpha^2\beta>Y$.** Consider the contribution of the terms to (29) with $\alpha^2\beta>Y$ and sum that over n (as in (28)). Thus the total contribution of such terms to (28) is bounded by

$$\sum_{\beta|v}\sum_{\substack{(\alpha,vN_0)=1\\ \alpha^2\beta>Y}}\sum_{kv\beta\alpha^2\equiv a\pmod{N_0}}\Phi\Big(\frac{\kappa kv\beta\alpha^2}{X}\Big)\Big|\sum_{(n,N_0)=1}\frac{a(n)}{\sqrt{n}}\Big(\frac{kv\beta\alpha^2}{n}\Big)W\Big(\frac{n}{\kappa kv\beta\alpha^2}\Big)\Big|. \tag{30}$$

Now using the definition of W, the sum over n above can be rewritten as

$$\frac{1}{2\pi i}\int_{(\epsilon)} L_a(s+\tfrac{1}{2})\Gamma(s)\Big(\frac{\sqrt{N}\kappa k v\beta\alpha^2}{2\pi}\Big)^s \sum_{(n,N_0)=1}\frac{a(n)}{n^{\frac{1}{2}+s}}\Big(\frac{kv\beta\alpha^2}{n}\Big)ds. \tag{31}$$

Write the discriminant $4kv\beta\alpha^2$ as $k_1k_2^2$ with k_1 a fundamental discriminant. Note that $\alpha\beta$ must divide k_2. Since n is odd, $\chi_{kv\beta\alpha^2}(n)=\chi_{k_1k_2^2}(n)$, and so the sum over n above may be expressed as $L(\frac{1}{2}+s,E_{k_1})$ up to Euler factors coming from primes dividing k_2 and N_0 (and these factors are at most X^ϵ in size). Thus the quantity in (31) may be bounded by

$$\ll X^\epsilon\int_{(\epsilon)}|\Gamma(s)L(\tfrac{1}{2}+s,E_{k_1})||ds|.$$

Using this in (30) we obtain a bound

$$\ll X^\epsilon\sum_{\beta|v}\sum_{\alpha^2\beta>Y}\sum_{\alpha\beta|k_2}\sideset{}{^\flat}\sum_{|k_1|\le X^{1+\epsilon}/k_2^2}\int_{(\epsilon)}|\Gamma(s)L(\tfrac{1}{2}+s,E_{k_1})||ds|,$$

where the $\flat$ indicates a sum over fundamental discriminants. By an application of Heath-Brown's large sieve for quadratic characters (see [15], and also Corollary 2.5 of [30]) this is

$$\ll X^\epsilon\sum_{\beta|v}\sum_{\alpha^2\beta>Y}\sum_{\substack{\alpha\beta|k_2\\ k_2\le X^{\frac{1}{2}+\epsilon}}}\frac{X}{k_2^2}\ll X^{1+\epsilon}\sum_{\beta|v}\sum_{\alpha^2\beta>Y}\frac{1}{\alpha^2\beta^2}\ll\frac{X^{1+\epsilon}}{\sqrt{Y}}. \tag{32}$$

10.2. **The terms with $\beta\alpha^2\le Y$: Analysis of the main term.** Now we turn to the terms in (29) with $\beta\alpha^2\le Y$. Put

$$F(\xi;x,y)=W\Big(\frac{y}{\kappa\xi}\Big)\Phi\Big(\frac{\kappa\xi}{x}\Big).$$

Applying Poisson summation (Lemma 7) to the sum over k in (29) we get

$$\frac{1}{N_0nu}\Big(\frac{N_0}{nu}\Big)\sum_{\ell}\widehat{F}\Big(\frac{\ell}{N_0nu};\frac{X}{v\beta\alpha^2},\frac{n}{v\beta\alpha^2}\Big)\tau_\ell(nu)e\Big(\frac{\ell a\overline{v\beta\alpha^2nu}}{N_0}\Big). \tag{33}$$

The main term arises from $\ell=0$ in (33), which we now analyze. Note that $\tau_0(nu)=0$ unless nu is a perfect square when it equals $\phi(nu)$. Thus the main term for $\mathcal{S}(X;u,v)$ is

$$\frac{2}{N_0}\sum_{\beta|v}\sum_{\substack{(\alpha,uvN_0)=1\\ \beta\alpha^2\le Y}}\mu(\beta)\mu(\alpha)\sum_{\substack{(n,\alpha\beta N_0)=1\\ nu=\square}}\frac{\phi(nu)}{nu}\frac{a(n)}{\sqrt{n}}\widehat{F}\Big(0;\frac{X}{v\beta\alpha^2},\frac{n}{v\beta\alpha^2}\Big).$$

We add back the terms with $\alpha^2\beta>Y$ above. Since

$$\hat{F}\Big(0;\frac{X}{v\beta\alpha^2},\frac{n}{v\beta\alpha^2}\Big)=\frac{X}{v\beta\alpha^2}\int_0^\infty\Phi(\xi)W\Big(\frac{n}{X\xi}\Big)d\xi\ll\frac{X}{v\beta\alpha^2}e^{-n/(X\sqrt{N})},$$

the sum over n is at most $X^{1+\epsilon}/(\sqrt{u_1}v\beta\alpha^2)$ and adding this over the terms with $\beta\alpha^2 > Y$ contributes an error of $O(X^{1+\epsilon}/(\sqrt{u_1 Y}v))$. Note that this error is smaller than the error term in (32).

Next, using the definition of W, we obtain that for any $c > 0$

$$\hat{F}\Big(0; \frac{X}{v\beta\alpha^2}, \frac{n}{v\beta\alpha^2}\Big) = \frac{X}{v\beta\alpha^2}\frac{1}{2\pi i}\int_{(c)} \check{\Phi}(s) L_a(s+\tfrac{1}{2})\Gamma(s)\Big(\frac{\sqrt{N}X}{2\pi n}\Big)^s ds.$$

Thus the main term in $\mathcal{S}(X; u, v)$ (after extending the sums over α and β) equals

(34)
$$\frac{2X}{vN_0}\frac{1}{2\pi i}\int_{(c)} \check{\Phi}(s) L_a(s+\tfrac{1}{2})\Gamma(s)\Big(\frac{\sqrt{N}X}{2\pi}\Big)^s \sum_{\beta|v}\sum_{(\alpha, uvN_0)=1}\frac{\mu(\beta)\mu(\alpha)}{\beta\alpha^2}\sum_{\substack{(n,\alpha\beta N_0)=1\\ nu=\square}}\frac{a(n)}{n^{s+\frac{1}{2}}}\frac{\phi(nu)}{nu} ds.$$

A little calculation shows that, for a given n coprime to N_0,

$$\sum_{\substack{\beta|v\\(\beta,n)=1}}\frac{\mu(\beta)}{\beta}\sum_{(\alpha,uvnN_0)=1}\frac{\mu(\alpha)}{\alpha^2}\frac{\phi(nu)}{nu} = \prod_{p\nmid N_0}\Big(1-\frac{1}{p^2}\Big)\prod_{p|uvn}\Big(1+\frac{1}{p}\Big)^{-1}.$$

Thus

$$\sum_{\beta|v}\sum_{(\alpha,uvN_0)=1}\frac{\mu(\beta)\mu(\alpha)}{\beta\alpha^2}\sum_{\substack{(n,\alpha\beta N_0)=1\\ nu=\square}}\frac{a(n)}{n^{s+\frac{1}{2}}}\frac{\phi(nu)}{nu} = \prod_{p\nmid N_0}\Big(1-\frac{1}{p^2}\Big)\sum_{\substack{(n,N_0)=1\\ nu=\square}}\frac{a(n)}{n^{s+\frac{1}{2}}}\prod_{p|uvn}\Big(1+\frac{1}{p}\Big)^{-1}.$$

If $u = u_1u_2^2$ with u_1 square free then the condition that nu is a square is the same as writing $n = u_1m^2$. Thus the RHS above may be expressed as

$$\frac{a(u_1)}{u_1^{\frac{1}{2}+s}} L(1+2s, \mathrm{sym}^2 E)\mathcal{G}(1+2s; u, v) \tag{35}$$

where $\mathcal{G}(1+2s; u, v) = \prod_p \mathcal{G}_p(1+2s; u, v)$ is an Euler product defined as follows: If $p|N_0$ the Euler factor $\mathcal{G}_p$ is the inverse of the corresponding Euler factor for $L(1+2s, \mathrm{sym}^2 E)$. If $p|u_1$ then $\mathcal{G}_p(1+2s; u, v) = (1-1/p)(1-1/p^{1+2s})$. If $p|uv$ but $p\nmid u_1$, then $\mathcal{G}_p(1+2s; u, v) = (1-1/p)(1-1/p^{2+4s})$. Finally, if $p\nmid uvN_0$, then

$$\mathcal{G}_p(1+2s; u, v) = \Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{p^{1+2s}}\Big)\Big(1+\frac{1}{p}\Big(1-\frac{\alpha_p^2}{p^{2s+1}}\Big)\Big(1-\frac{\beta_p^2}{p^{2s+1}}\Big)+\frac{1}{p^{1+2s}}\Big),$$

where we wrote $a(p) = \alpha_p + \beta_p$ with $\alpha_p\beta_p = 1$. It follows that $\mathcal{G}(1+2s; u, v)$ admits an analytic continuation to the region $\mathrm{Re}(s) \geq -\frac{1}{4}+\epsilon$ and is bounded there by $(N_0uv)^\epsilon$.

Using the above remarks in (34), the integrand there is analytic in $\mathrm{Re}(s) > -\frac{1}{4}$ (except for a simple pole at $s = 0$) and therefore, by moving the line of integration to $\mathrm{Re}(s) = -\frac{1}{4}+\epsilon$ we obtain that our main term is

$$\frac{2Xa(u_1)}{vu_1^{\frac{1}{2}}N_0}\check{\Phi}(0)L_a(\tfrac{1}{2})L(1, \mathrm{sym}^2 E)\mathcal{G}(1; u, v) + O(X^{\frac{3}{4}+\epsilon}) + O\Big(\frac{X^{1+\epsilon}}{\sqrt{Y}}\Big). \tag{36}$$

This is the main term in our Theorem, and the decomposition of $\mathcal{G}(1;u,v)$ as a constant times $g(u)h(v)$ for appropriate multiplicative functions g and h follows from our remarks on the Euler factors of $\mathcal{G}$.

10.3. **The terms with $\beta\alpha^2 \le Y$: Estimating the remainder terms.** Recall that the Fourier transform $\hat{F}(\lambda;x,y)$ (where λ, x and y are real numbers, with x and y positive) is given by

$$\widehat{F}(\lambda;x,y) = x\int_0^\infty \Phi(\xi)W\Big(\frac{y}{x\xi}\Big)e(-\kappa\lambda x\xi)d\xi.$$

Since $W(t)$ and its derivatives decrease rapidly as $t\to\infty$, we obtain that $|\hat{F}(\lambda;x,y)| \ll_A x(x/y)^A$ for any integer $A\ge 0$. Further, integrating by parts many times, we also find that $|\hat{F}(\lambda;x,y)| \ll_A x(|\lambda|y)^{-A}$. Thus we have

$$|\widehat{F}(\lambda;x,y)| \ll_A x\min\Big(\Big(\frac{x}{y}\Big)^A, \frac{1}{(|\lambda|y)^A}\Big). \tag{37}$$

For $\alpha^2\beta \le Y$ we must bound the contribution of the terms with $\ell\neq 0$ in (33) to the quantity in (28). This is

$$\ll \frac{1}{N_0u}\sum_{\beta|v}\sum_{\substack{(\alpha,vN_0)=1\\ \alpha^2\beta\le Y}}\Big|\sum_{\ell\neq 0}\sum_{(n,N_0)=1}\frac{a(n)}{n^{\frac32}}\Big(\frac{v\beta\alpha^2}{n}\Big)\widehat{F}\Big(\frac{\ell}{N_0nu};\frac{X}{v\beta\alpha^2},\frac{n}{v\beta\alpha^2}\Big)\tau_\ell(nu)e\Big(\frac{\ell a\overline{v\beta\alpha^2nu}}{N_0}\Big)\Big|. \tag{38}$$

First we show that the terms $|\ell| > N_0uvYX^\epsilon$ make a negligible contribution above. Using (37) we see that

$$\Big|\widehat{F}\Big(\frac{\ell}{N_0nu};\frac{X}{v\beta\alpha^2},\frac{n}{v\beta\alpha^2}\Big)\Big| \ll_A \frac{X}{v\beta\alpha^2}\Big(\frac{Nuv\beta\alpha^2}{|\ell|}\Big)^A\Big(\frac{X}{n}\Big)^2 \ll \frac{1}{X\ell^2n^2},$$

by choosing A appropriately large. Using this in (38), we deduce that the contribution of the terms with $|\ell| > N_0uvYX^\epsilon$ is $\ll X^{-1}$, which is indeed negligible.

Now suppose $1\le|\ell|\le N_0uvYX^\epsilon$, and consider the sum over n in (38). We remove the $e(\ell a\overline{v\beta\alpha^2nu}/N_0)$ term by introducing Dirichlet characters $\psi \pmod{N_0}$:

$$e\Big(\frac{\ell a\overline{v\beta\alpha^2nu}}{N_0}\Big) = \sum_{\psi \pmod{N_0}}\psi(n)\Big(\frac{1}{\phi(N_0)}\sum_{b \pmod{N_0}}\overline{\psi(b)}e\Big(\frac{\ell a\overline{v\beta\alpha^2bu}}{N_0}\Big)\Big).$$

Since the sum over b above is trivially bounded by $\phi(N_0)$, we are reduced to the problem of estimating

$$\sum_{\psi \pmod{N_0}}\Big|\sum_{(n,N_0)=1}\frac{a(n)}{n^{\frac32}}\Big(\frac{v\beta\alpha^2}{n}\Big)\psi(n)\tau_\ell(nu)\widehat{F}\Big(\frac{\ell}{N_0nu};\frac{X}{v\beta\alpha^2},\frac{n}{v\beta\alpha^2}\Big)\Big|. \tag{39}$$

Now we pass to Mellin transforms in order to handle the sum over n above. For a complex number s with $\mathrm{Re}(s) > 0$, put

$$\widetilde{F}(s;\ell,\beta\alpha^2) = \int_0^\infty \widehat{F}\Big(\frac{\ell}{N_0 tu}; \frac{X}{v\beta\alpha^2}, \frac{t}{v\beta\alpha^2}\Big) t^{s-1} dt, \tag{40}$$

which, using the definition of $\widehat{F}$, may be expressed as

$$\frac{X^{s+1}}{v\beta\alpha^2}\check{\Phi}(s)\int_0^\infty W\Big(\frac{1}{y}\Big) e\Big(-\frac{\kappa\ell y}{N_0 uv\beta\alpha^2}\Big)\frac{dy}{y^{s+1}}. \tag{41}$$

By Mellin inversion, the sum over n in (39) is, for any $c > 0$,

$$\frac{1}{2\pi i}\int_{(c)} \widetilde{F}(s;\ell,\beta\alpha^2) \sum_{(n,N_0)=1} \frac{a(n)}{n^{\frac{3}{2}+s}}\Big(\frac{v\beta\alpha^2}{n}\Big)\psi(n)\tau_\ell(nu) ds. \tag{42}$$

Now from (41), and using that $W(\xi) = L_a(\frac{1}{2}) + O(\xi^{\frac{1}{2}-\epsilon})$ as $\xi \to 0$, we may obtain an analytic continuation of $\widetilde{F}(s;\ell,\beta\alpha^2)$ to the region $\mathrm{Re}(s) > -\frac{1}{2}+\epsilon$, and that it is bounded in that region by $\ll_A X^{1+\mathrm{Re}(s)}/(v\beta\alpha^2(1+|s|)^A)$ for any $A > 0$. Furthermore, expressing τ_ℓ in terms of the multiplicative G_ℓ and $G_{-\ell}$ and using Lemma 5, we see that the sum over n above may be expressed in terms of $G_{\pm\ell}(u)$ times $L(1+s, E\times\psi\chi_{\pm v\beta\ell})$ times certain Euler factors at primes $p|N_0\ell v\beta\alpha^2$. Using the convexity bound for L-functions, we may bound this quantity in the region $\mathrm{Re}(s) > -\frac{1}{2}+\epsilon$ by $\ll uX^\epsilon(v\beta\ell(1+|s|))^{\frac{1}{2}+\epsilon}$. Therefore we conclude that the quantity in (42) is bounded by

$$\ll \frac{X^{\frac{1}{2}+\epsilon}}{v^{\frac{1}{2}}\beta^{\frac{1}{2}}\alpha^2} u\ell^{\frac{1}{2}+\epsilon}.$$

Using this estimate in (39) and summing over all $1 \le |\ell| \le N_0 uvYX^\epsilon$, we conclude that these terms contribute to (38) an amount bounded by $\ll u^{\frac{3}{2}}vY^{\frac{3}{2}}X^{\frac{1}{2}+\epsilon}$. We conclude that the contribution of the remainder terms arising from $\beta\alpha^2 \le Y$ is

$$\ll u^{\frac{3}{2}}vY^{\frac{3}{2}}X^{\frac{1}{2}+\epsilon} + X^{-1} \ll u^{\frac{3}{2}}vY^{\frac{3}{2}}X^{\frac{1}{2}+\epsilon}. \tag{43}$$

10.4. **Completion of the proof.** Choose $Y = X^{\frac{1}{4}}v^{-\frac{1}{2}}u^{-\frac{3}{4}}$, and the proposition follows in view of (32), (36) and (43).

References

[1] Vorrapan Chandee and Xiannan Li. The eighth moment of Dirichlet L-functions. *preprint, arXiv:1303.4482*, 2013.

[2] John Coates, Yongxiong Li, Ye Tian, and Shuai Zhai. Quadratic twists of elliptic curves. *preprint, arXiv:1312.3884*, 2013.

[3] J. B. Conrey, D. W. Farmer, J. P. Keating, M. O. Rubinstein, and N. C. Snaith. Integral moments of L-functions. *Proc. London Math. Soc. (3)*, 91(1):33–104, 2005.

[4] J. B. Conrey, H. Iwaniec, and K. Soundararajan. The sixth power moment of Dirichlet L-functions. *Geom. Funct. Anal.*, 22(5):1257–1288, 2012.

[5] J. B. Conrey, J. P. Keating, M. O. Rubinstein, and N. C. Snaith. Random matrix theory and the Fourier coefficients of half-integral-weight forms. *Experiment. Math.*, 15(1):67–82, 2006.

[6] Christophe Delaunay. Moments of the orders of Tate-Shafarevich groups. *Int. J. Number Theory*, 1(2):243–264, 2005.
[7] Christophe Delaunay. Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 323–340. Cambridge Univ. Press, Cambridge, 2007.
[8] Christophe Delaunay and Mark Watkins. The powers of logarithm for quadratic twists. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 189–193. Cambridge Univ. Press, Cambridge, 2007.
[9] Adrian Diaconu, Dorian Goldfeld, and Jeffrey Hoffstein. Multiple Dirichlet series and moments of zeta and L-functions. *Compositio Math.*, 139(3):297–360, 2003.
[10] Bruno Eckhardt, Shmuel Fishman, Jonathan Keating, Oded Agam, Jörg Main, and Kirsten Müller. Approach to ergodicity in quantum wave functions. *Phys. Rev. E*, 52:5893–5903, 1995.
[11] Dorian Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, volume 751 of *Lecture Notes in Math.*, pages 108–118. Springer, Berlin, 1979.
[12] Andrew Granville and K. Soundararajan. Sieving and the Erdős-Kac theorem. In *Equidistribution in number theory, an introduction*, volume 237 of *NATO Sci. Ser. II Math. Phys. Chem.*, pages 15–27. Springer, Dordrecht, 2007.
[13] A. J. Harper. Sharp conditional bounds for moments of the Riemann zeta function. *Preprint, arXiv:1305.4618*, 2013.
[14] D. R. Heath-Brown. Fractional moments of the Riemann zeta function. *J. London Math. Soc. (2)*, 24(1):65–78, 1981.
[15] D. R. Heath-Brown. A mean value estimate for real character sums. *Acta Arith.*, 72(3):235–275, 1995.
[16] R. D. Hough. The distribution of the logarithm in an orthogonal and a symplectic family of l-functions. *Forum Mathematicum*, 26:523–546, 2014.
[17] C. P. Hughes and Matthew P. Young. The twisted fourth moment of the Riemann zeta function. *J. Reine Angew. Math.*, 641:203–236, 2010.
[18] Henryk Iwaniec. On the order of vanishing of modular L-functions at the critical point. *Sém. Théor. Nombres Bordeaux (2)*, 2(2):365–376, 1990.
[19] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.
[20] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.
[21] J. P. Keating and N. C. Snaith. Random matrix theory and L-functions at $s = 1/2$. *Comm. Math. Phys.*, 214(1):91–110, 2000.
[22] J. P. Keating and N. C. Snaith. Random matrix theory and $\zeta(1/2+it)$. *Comm. Math. Phys.*, 214(1):57–89, 2000.
[23] Wenzhi Luo and Peter Sarnak. Quantum variance for Hecke eigenforms. *Ann. Sci. École Norm. Sup. (4)*, 37(5):769–799, 2004.
[24] Robert L. Miller. Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one. *LMS J. Comput. Math.*, 14:327–350, 2011.
[25] Maksym Radziwiłł and Kannan Soundararajan. Continuous lower bounds for moments of zeta and L-functions. *Mathematika*, 59(1):119–128, 2013.
[26] Karl Rubin. Fudge factors in the Birch and Swinnerton-Dyer conjecture. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 233–236. Cambridge Univ. Press, Cambridge, 2007.

[27] Z. Rudnick and K. Soundararajan. Lower bounds for moments of L-functions. *Proc. Natl. Acad. Sci. USA*, 102(19):6837–6838, 2005.
[28] Z. Rudnick and K. Soundararajan. Lower bounds for moments of L-functions: symplectic and orthogonal examples. In *Multiple Dirichlet series, automorphic forms, and analytic number theory*, volume 75 of *Proc. Sympos. Pure Math.*, pages 293–303. Amer. Math. Soc., Providence, RI, 2006.
[29] K. Soundararajan. Nonvanishing of quadratic Dirichlet L-functions at $s = \frac{1}{2}$. *Ann. of Math. (2)*, 152(2):447–488, 2000.
[30] K. Soundararajan and Matthew P. Young. The second moment of quadratic twists of modular L-functions. *J. Eur. Math. Soc. (JEMS)*, 12(5):1097–1116, 2010.
[31] Kannan Soundararajan. Moments of the Riemann zeta function. *Ann. of Math. (2)*, 170(2):981–993, 2009.
[32] Peng Zhao. Quantum variance of Maass-Hecke cusp forms. *Comm. Math. Phys.*, 297(2):475–514, 2010.

School of Mathematics, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ, 08540, USA
E-mail address: maksym@ias.edu

Department of Mathematics, Stanford University, 450 Serra Mall, Bldg. 380, Stanford, CA 94305-2125
E-mail address: ksound@math.stanford.edu