A CONDITIONAL DETERMINATION OF THE AVERAGE RANK OF ELLIPTIC CURVES

DANIEL FIORILLI

Abstract. Under a hypothesis which is slightly stronger than the Riemann Hypothesis for elliptic curve L-functions, we show that both the average analytic rank and the average algebraic rank of elliptic curves in families of quadratic twists are exactly $\frac{1}{2}$. As a corollary we obtain that under this last hypothesis, the Birch and Swinnerton-Dyer Conjecture holds for almost all curves in our family, and that asymptotically one half of these curves have algebraic rank 0, and the remaining half 1. We also prove an analogous result in the family of all elliptic curves. A way to interpret our results is to say that nonreal zeros of elliptic curve L-functions in a family have a direct influence on the average rank in this family. Results of Katz-Sarnak and of Young constitute a major ingredient in the proofs.

1. Introduction and statement of results

Let E be an elliptic curve over $\mathbb{Q}$ whose minimal Weierstrass equation is

$$y^2 = x^3 + ax + b \tag{1}$$

with $a, b \in \mathbb{Z}$ such that $p^4 \mid a \Rightarrow p^6 \nmid b$. It was first conjectured by Goldfeld [G] that the average analytic rank[1] over the family of quadratic twists of a fixed curve E should be exactly $\frac{1}{2}$. This follows from the widely believed Katz-Sarnak density conjecture, which asserts that this family has *orthogonal* symmetry. The family of all Weierstrass curves (1) is also believed to have orthogonal symmetry, and hence it is believed that the average rank of all elliptic curves ordered by height should also be $\frac{1}{2}$.

In the family of quadratic twists of a fixed elliptic curve, Goldfeld [G] showed under the Riemann Hypothesis for elliptic curve L-functions, which we will denote by ECRH (see below), that the average analytic rank is at most 3.25. It was then proved by Brumer [B] that in the family of all elliptic curves, the average analytic rank is at most 2.3, again under ECRH. Subsequently, Heath-Brown [HB] improved Goldfeld's upper bound to $\frac{3}{2}$, and Brumer's upper bound to 2. Heath-Brown also showed that the proportion of curves of rank at least R decays exponentially with R. Young [Y] showed under the Grand Riemann Hypothesis that the average analytic rank in the family of all curves is at most $\frac{25}{14}$, and as a corollary he obtained that the Birch and Swinnerton-Dyer Conjecture holds for a positive proportion of curves in his family. This last corollary is obtain from the deep results of Gross-Zagier [GZ], Kolyvagin [Ko], and others. Young also showed corresponding results for several other interesting families of elliptic curves. Finally, Bhargava and Shankar [BS] have recently shown unconditionally that the average algebraic rank in the family of all curves is at most 0.885.

Date: March 28, 2014.

[1]The analytic rank of E is the order of vanishing of $L(E, s)$ (see Section 2) at $s = 1$, and its algebraic rank is the rank of the abelian group of $\mathbb{Q}$-points on E.

Hypothesis ECRH. If E is an elliptic curve over $\mathbb{Q}$, then the Riemann Hypothesis holds for $L(E,s)$, that is all nontrivial zeros of $L(E,s+\frac{1}{2})$ lie on the line $\Re(s)=\frac{1}{2}$.

The goal of the current paper is to deduce Goldfeld's Conjecture from an assumption slightly stronger than ECRH, which is motivated by probabilistic arguments inspired by the work of Montgomery. This should be compared with the very recent paper of Bhargava, Kane, Lenstra, Poonen and Rains [BKLPR], in which the authors study a probability distribution on a certain set of short exact sequences and show that well-known conjectures on the average rank would follow from the assertion that short exact sequences arising from elliptic curves follow this distribution.

1.1. **Quadratic twists of a fixed elliptic curve.** We first consider families of quadratic twists, that is we fix E and consider for squarefree $d\neq 0$ the curve

$$E_d : dy^2 = x^3+ax+b. \tag{2}$$

For technical reasons we will mostly consider the values of d which are coprime with N_E. Our first main result is a conditional proof that the average analytic rank of E_d is exactly $\frac{1}{2}$. Here and throughout, $\sum_d^*$ will denote a sum over squarefree integers d and $N(D)$ will denote the number of squarefree integers $0<|d|\leq D$ with $(d,N_E)=1$.

Theorem 1.1. *Assume ECRH and assume that Hypothesis M below holds for some non-negative Schwartz weight function w with $w(0)>0$. Then the average of $r_{an}(E_d)$, the analytic rank of $L(E_d,s)$, is exactly $\frac{1}{2}$:*

$$\lim_{D\to\infty}\frac{1}{N(D)}\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1}} r_{an}(E_d)=\frac{1}{2}.$$

Hypothesis M is a statement about nonreal zeros of elliptic curve L-functions which is only slightly stronger than ECRH. Theorem 1.1 thus asserts that the imaginary parts of these nonreal zeros have a direct influence on the average order of vanishing of $L(E,s)$ at the central point.

We translate Theorem 1.1 into a statement about algebraic ranks using the deep results of Gross-Zagier [GZ] and Kolyvagin [Ko].

Corollary 1.2. *Assume ECRH and Hypothesis M for some non-negative Schwartz function w with $w(0)>0$. Then the Birch and Swinnerton-Dyer Conjecture holds for almost all curves E_d (with $\mu^2(d)=1$, $(d,N_E)=1$), and asymptotically one half of these curves have algebraic rank 0, and one half have algebraic rank 1.*

Remark 1.3. One can adapt the arguments of Theorem 1.1 to show that under similar hypotheses[2] we have

$$\lim_{D\to\infty}\frac{1}{N_0(D)}\sideset{}{^*}\sum_{0<|d|\leq D} r_{an}(E_d)=\frac{1}{2},$$

where $N_0(D)$ denotes the number of squarefree integers $0<|d|\leq D$. If N_E is squarefree, then Lemma 5.3 shows that the root number is equidistributed in the family $\{E_d:\mu^2(d)=1\}$, and hence asymptotically one half of these curves have algebraic rank 0, and one half have algebraic rank 1.

[2]The needed hypotheses are ECRH and the statement that (3) holds without the restriction $(d,N_E)=1$ in the sum over d.

Our working hypothesis is slightly stronger than ECRH, but only by one logarithm. We will see that Montgomery's probabilistic arguments predict a much stronger estimate. Here and throughout, $w(t)$ will denote a fixed non-negative Schwartz[3] test function such that $w(0) > 0$; this weight function will facilitate the analysis.

Hypothesis M. *There exists $0 < \delta < 1$ such that in the range[4] $D^{2-\delta} \leq x \leq 2D^{2-\delta}$ we have the following estimate:*

$$\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right) \sum_{\rho_d \notin \mathbb{R}} \frac{x^{\rho_d}}{\rho_d(\rho_d+1)} = o(Dx^{\frac{1}{2}}), \tag{3}$$

where ρ_d runs over the nontrivial zeros of $L(E_d, s+\frac{1}{2})$.

Remark 1.4. The Riemann Hypothesis for $L(E_d, s)$ implies that the left hand side of (3) is $O(Dx^{\frac{1}{2}} \log(DN_E))$, hence Hypothesis M is stronger, but only by one logarithm. A probabilistic argument which will be sketched in Appendix A suggests the stronger bound

$$\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right) \sum_{\rho_d \notin \mathbb{R}} \frac{x^{\rho_d}}{\rho_d(\rho_d+1)} = O_{\epsilon,E}(D^{\frac{1}{2}+\epsilon} x^{\frac{1}{2}}), \tag{4}$$

when x is large enough in terms of D. This is based on Montgomery's Conjecture on primes in arithmetic progressions. We will see in Corollary 1.8 that such an estimate implies a quantitative bound for the number of elliptic curves of rank ≥ 2. It will actually be sufficient to assume the weaker Hypothesis M(δ,η) (see below), for some $0 < \delta < 1$ and $0 < \eta < \frac{1}{2}$.

Remark 1.5. An important fact used in Appendix A to conjecture (4) as well as (7) is the fact that the families of elliptic curves we are considering contain at most a bounded number of isogenous elliptic curves. Indeed we are considering families of minimal[5] Weierstrass equations, which implies that no pairs of curves in these families are isomorphic. Moreover, a Theorem of Mazur states that at most a bounded number of such elliptic curves can be isogenous, and it follows from the Isogeny Theorem (see Lemma A.1) that at most a bounded number of elliptic curves in this family have the same L-function.

Remark 1.6. In (3), one can replace $1/\rho_d(\rho_d+1)$ by the Mellin Transform of any function satisfying appropriate decay conditions (see Property D in Section 2) evaluated at ρ_d, and the same results will follow (see the proof of Lemmas 2.2 and 2.3, and Propositions 3.1 and 4.3). We made the specific choice $h(x) = \max(1-x, 0)$ in (3) for simplicity, keeping in mind that (3) is more likely to hold if the Mellin Transform of h decays on vertical lines.

A weaker version of (4) is the following.

Hypothesis M(δ,η). *In the range $D^{2-\delta} \leq x \leq 2D^{2-\delta}$ we have the following estimate:*

$$\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right) \sum_{\rho_d \notin \mathbb{R}} \frac{x^{\rho_d}}{\rho_d(\rho_d+1)} = O_E(D^{1-\eta} x^{\frac{1}{2}}), \tag{5}$$

where ρ_d runs over the nontrivial zeros of $L(E_d, s+\frac{1}{2})$ and the constant implied in the error term might depend on δ and η.

[3]Hence $w(t)$ is smooth and rapidly decaying.
[4]It is actually sufficient to assume that (3) holds for the specific value $x = D^{2-\delta}$ only.
[5]E_d can be rewritten as $y^2 = x^3 + d^2ax + d^3b$, which is minimal for $d \neq 0$ squarefree.

We now show that the sharper bound (5) implies a more precise estimate for the average rank. We will assume the Riemann Hypothesis for some symmetric power L-functions of E_d.

Hypothesis ECRH$^+$. *The Riemann hypothesis holds for $\zeta(s)$, and holds for $L(Sym^k E, s)$ for every elliptic curve E over $\mathbb{Q}$ and $1 \leq k \leq 3$.*

Theorem 1.7. *Assume ECRH$^+$ and Hypothesis $M(\delta,\eta)$ for some $0<\delta<1$ and $0<\eta<\frac{1}{2}$, for some non-negative Schwartz weight w with $w(0)>0$. Then for any fixed $\epsilon>0$ we have*

$$\frac{1}{N(D)} \sideset{}{^*}\sum_{\substack{0<|d|\leq D \\ (d,N_E)=1}} r_{an}(E_d) = \frac{1}{2} + O_{\epsilon,E}(D^{1-\frac{\delta}{4}+\epsilon} + D^{1-\eta}), \tag{6}$$

where D^* denotes the number of squarefree integers in the interval $[1,D]$.

Corollary 1.8. *Under ECRH$^+$ and Hypothesis $M(\delta,\eta)$ for some $0<\delta<1$ and $0<\eta<\frac{1}{2}$, we have the following bound for the number of curves E_d of rank ≥ 2:*

$$\sideset{}{^*}\sum_{\substack{0<|d|\leq D \\ r_{al}(E_d)\geq 2 \\ (d,N_E)=1}} 1 \ll_{\epsilon,E} D^{1-\min(\frac{\delta}{4},\eta)+\epsilon}, \qquad \sideset{}{^*}\sum_{\substack{0<|d|\leq D \\ r_{an}(E_d)\geq 2 \\ (d,N_E)=1}} 1 \ll_{\epsilon,E} D^{1-\min(\frac{\delta}{4},\eta)+\epsilon}.$$

In particular, the proportion of elliptic curves E_d with $0<|d|\leq D$ squarefree for which the Birch and Swinnerton-Dyer Conjecture does not hold is $\ll D^{-\min(\frac{\delta}{4},\eta)+o(1)}$.

Remark 1.9. This should be compared with the following conjecture of Sarnak:

$$V_E(D) := \sideset{}{^*}\sum_{\substack{0<|d|\leq D \\ \epsilon(E)\chi_d(-N_E)=1 \\ r_{\rm an}(E_d)\geq 2}} 1 \approx D^{\frac{3}{4}},$$

where $\epsilon(E)$ denotes the root number of $L(E,s)$. Using random matrix theory, Conrey, Keating, Rubinstein and Snaith [CKRS] refined this conjecture to $V_E(D) \sim c_E D^{\frac{3}{4}} (\log D)^{b_E}$. Here, b_E can be made explicit [DW]. Interestingly, if we set $\eta = \frac{1}{2}-\epsilon$ and $\delta = 1-\epsilon$ in Hypothesis M(δ,η), which we believe is best possible choice of η for which (5) holds (this corresponds to Montgomery's Conjecture for primes in arithmetic progressions, see Appendix A), then in Corollary 1.8 we recover the upper bound in Sarnak's Conjecture: $V_E(D) \ll_\epsilon D^{\frac{3}{4}+\epsilon}$. Note also that if we wish to take $\delta>1$ in Hypothesis M(δ,η), then we have to add the error term $O_\epsilon(D^{\frac{1}{2}+\frac{\delta}{4}+\epsilon})$ in (6) (put $P=D^{2-\delta}$ in (23)), and hence the resulting bound on the number of curves of rank ≥ 2 can never be better than $O_\epsilon(D^{\frac{3}{4}+\epsilon})$.

Corollary 1.8 also has an implication on the average algebraic rank. The implication is not direct, since one needs a bound on the algebraic rank of elliptic curves in families of quadratic twists (see Lemma 6.1).

Theorem 1.10. *Assume ECRH and assume that there exists $0<\delta<1$ such that in the range $D^{2-\delta} \leq x \leq 2D^{2-\delta}$, the left hand side of (3) is $o(Dx^{\frac{1}{2}}/\log\log D)$, for some non-negative Schwartz w with $w(0)>0$. Then the average algebraic rank of E_d is exactly $\frac{1}{2}$:*

$$\lim_{D\to\infty} \frac{1}{N(D)} \sideset{}{^*}\sum_{\substack{0<|d|\leq D \\ (d,N_E)=1}} r_{al}(E_d) = \frac{1}{2}.$$

Remark 1.11. Sarnak noticed[6] that Montgomery's Conjecture for primes in arithmetic progressions implies the Katz-Sarnak prediction for the 1-level density in the family of Dirichlet L-functions modulo q. In making the analogous conjecture in families of elliptic curve L-functions, one runs into the problem that if not excluded, zeros at the central point could give significant contributions to the sum on the left hand side of (3). In contrast with Dirichlet L-functions, many elliptic curve L-functions do vanish at the central point, and thus the direct analogue of Montgomery's Conjecture is not expected to hold. To fix this problem, we excluded the real zeros in (3); however the Katz-Sarnak prediction does not follow directly from (3), because of the absence of real zeros. Notice also that the range $x \asymp D^{2-\delta}$ in Hypothesis M corresponds in the Katz-Sarnak problem to test functions whose Fourier transform have small support, and this is not sufficient in order to deduce Goldfeld's Conjecture from an estimate on the 1-level density.

1.2. **The family of all elliptic curves.** We also give an analogue of Theorem 1.1 in the family of all elliptic curves. Here $w(t_1,t_2)$ will denote a fixed Schwartz test function on $\mathbb{R}^2$.

Hypothesis 1.12. *There exists $\delta>0$ such that in the range $X^{\frac{7}{9}-\delta} \leq x \leq 2X^{\frac{7}{9}-\delta}$ we have*

$$\sum_{a,b}{}^{*} w\left(\frac{a}{A},\frac{b}{B}\right) \sum_{\rho_{a,b}\notin\mathbb{R}} x^{\rho_{a,b}}\Gamma(\rho_{a,b}) = o(ABx^{\frac{1}{2}}), \tag{7}$$

where $A=X^{\frac{1}{3}}$, $B=X^{\frac{1}{2}}$ and $\rho_{a,b}$ runs through the zeros of $L(E_{a,b},s)$, the L-function of the elliptic curve $E_{a,b}: y^2=x^3+ax+b$. The star on the sum over (a,b) means that we are summing over the couples for which $p^4 \mid a \Rightarrow p^6 \nmid b$ (in particular $b\neq 0$).

Remark 1.13. As is the case with Hypothesis M, Hypothesis 1.12 is stronger than ECRH by only one logarithm, since ECRH implies the bound

$$\sum_{a,b}{}^{*} w\left(\frac{a}{A},\frac{b}{B}\right) \sum_{\rho_{a,b}\notin\mathbb{R}} x^{\rho_{a,b}}\Gamma(\rho_{a,b}) \ll ABx^{\frac{1}{2}}\log(ABN_E). \tag{8}$$

Hypothesis 1.12 is motivated by probabilistic considerations similar to those presented in Appendix A. An important requirement is that we only consider minimal Weierstrass Equations, since no two curves in this family are isomorphic[7], and by Lemma A.1, at most a bounded number of curves in this family have matching L-functions. It is then natural to conjecture that distinct L-functions (in this case L-functions of two non-isogenous elliptic curves) have distinct nonreal zeros.

Assuming Hypothesis 1.12, we will show using Young's results [Y] that the average analytic rank of the elliptic curve $E_{a,b}: y^2=x^3+ax+b$ is exactly $\frac{1}{2}$.

Theorem 1.14. *Assume ECRH, and assume that Hypothesis 1.12 holds for some non-negative Schwartz weight w. Then we have that*

$$\lim_{\substack{A,B\to\infty\\ A^3=B^2}} \frac{1}{W(A,B)} \sum_{a,b}{}^{*} w\left(\frac{a}{A},\frac{b}{B}\right) r_{an}(E_{a,b}) = \frac{1}{2},$$

where the sum is taken over the pairs (a,b) for which $p^4\mid a \Rightarrow p^6 \nmid b$, and $W(A,B)$ denotes the sum of $w\left(\frac{a}{A},\frac{b}{B}\right)$ over all such pairs.

[6]Private conversation.

[7]It follows from [Si, Section III] that two elliptic curves in Weierstrass Form $E: y^2=x^3+ax+b$ and $E': y^2=x^3+a'x+b'$ are isomorphic over $\mathbb{Q}$ if and only if $a'=u^4a$ and $b'=u^6b$ for some $u\in\mathbb{Q}^{\times}$.

If one also assumes the widely believed conjecture that the root number is equidistributed in the family of all elliptic curves, then the analogue of Corollary 1.2 follows.

2. Preliminaries and Prime Number Theorems

Fix an elliptic curve in Weierstrass form

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$, discriminant $\Delta_E = -16(4a^3 + 27b^2)$ and conductor N_E. For $p \nmid N_E$, consider the trace of the Frobenius automorphism $a_p(E) = p + 1 - \#E_p(\mathbb{F}_p)$, which satisfies Hasse's bound $|a_p(E)| \leq 2\sqrt{p}$. Here, E_p denotes the reduction of E modulo p. We extend the definition of $a_p(E)$ to all primes by setting

$$a_p(E) := \begin{cases} 1 \text{ if } E \text{ has split multiplicative reduction at } p \\ -1 \text{ if } E \text{ has nonsplit multiplicative reduction at } p \\ 0 \text{ if } E \text{ has additive reduction at } p, \end{cases}$$

and define the L-function of E as follows:

$$L(E, s) := \prod_{p \mid N_E} \left(1 - \frac{a_p(E)}{p^s}\right)^{-1} \prod_{p \nmid N_E} \left(1 - \frac{a_p(E)}{p^s} + \frac{p}{p^{2s}}\right)^{-1}.$$

One can see that the formula $a_p(E) = p+1-\#E_p(\mathbb{F}_p)$ still holds for primes dividing N_E [Kn, Section X.2]. It follows from the groundbreaking work of Wiles [Wi], Taylor and Wiles [TW], and Breuil, Conrad, Diamond, and Taylor [BCDT], that $L(E, s + \frac{1}{2}) = L(s, f_E)$ for some cuspidal self-dual newform f_E of weight 2 and level N_E. The gamma factor of $L(E, s + \frac{1}{2})$ is given by $\gamma(f_E, s) = \pi^{-s}\Gamma(\frac{s}{2} + \frac{1}{4})\Gamma(\frac{s}{2} + \frac{3}{4})$, and the completed L-function

$$\Lambda(f_E, s) := N_E^{\frac{s}{2}} \gamma(f_E, s) L(s, f_E)$$

satisfies the functional equation $\Lambda(f_E, s) = \epsilon(E)\Lambda(f_E, 1 - s)$. The trivial zeros of $L(f_E, s)$ are simple zeros at the points $s = -\frac{1}{2}, -\frac{3}{2}, -\frac{5}{2}, \ldots$ One can write

$$L(s, f_E) = L(E, s + \tfrac{1}{2}) = \prod_p \left(1 - \frac{\alpha_p(E)}{p^s}\right)^{-1} \left(1 - \frac{\beta_p(E)}{p^s}\right)^{-1},$$

where for $p \nmid N_E$ we have $|\alpha_p(E)| = |\beta_p(E)| = 1$, $\beta_p(E) = \overline{\alpha_p(E)}$ and $a_p(E)/\sqrt{p} = \alpha_p(E) + \beta_p(E)$, and for $p \mid N_E$ we have $\alpha_p(E) = a_p(E)/\sqrt{p}$ and $\beta_p(E) = 0$. The symmetric k-th power L-function of E is then defined as

$$L(s, \mathrm{Sym}^k f_E) = L(\mathrm{Sym}^k E, s + \tfrac{k}{2}) = \prod_p \prod_{j=0}^{k} \left(1 - \frac{\alpha_p(E)^j \beta_p(E)^{k-j}}{p^s}\right)^{-1}.$$

In the case $k = 2$, it was proven by Shimura [Sh] that $L(s, \mathrm{Sym}^2 f_E)$ can be analytically continued to an entire function of s. The gamma factor is given by $\gamma(\mathrm{Sym}^2 f_E, s) = \pi^{-\frac{3s}{2}}\Gamma(\frac{s+1}{2})^2\Gamma(\frac{s}{2} + 1)$, and the completed L-function

$$\Lambda(\mathrm{Sym}^2 f_E, s) := q(\mathrm{Sym}^2 f)^{\frac{s}{2}} \gamma(\mathrm{Sym}^2 f_E, s) L(s, \mathrm{Sym}^2 f_E),$$

where the conductor $q(\mathrm{Sym}^2 f_E) = N_E^2$, satisfies the functional equation $\Lambda(\mathrm{Sym}^2 f_E, s) = \epsilon(\mathrm{Sym}^2 E)\Lambda(\mathrm{Sym}^2 f_E, 1 - s)$ (see [IK, Section 5.12] and [CM]).

The Langlands Program predicts every symmetric power $L(\mathrm{Sym}^k E, s)$ to be the L-function of a self-dual $\mathrm{GL}(k+1)$ cuspidal automorphic form. In particular, it would follow that these L-functions have a analytic continuation to the whole s-plane (except for a possible pole at $s = 1$), have a functional equation, and are of order 1 (see [IK, Theorem 5.41]). A precise prediction of the conductor, root number and Gamma Factors of $L(\mathrm{Sym}^k E, s)$ is given in [CM]. The Riemann Hypothesis for $L(\mathrm{Sym}^k E, s + \frac{k}{2}) = L(s, \mathrm{Sym}^k f_E)$ states that all nontrivial zeros of this function have real part $\frac{1}{2}$.

The automorphy of $L(\mathrm{Sym}^k E, s)$ is currently known for $1 \leq k \leq 4$ by the work of Gelbart and Jacquet [GJ], Kim and Shahidi [KiS1, KiS2] and Kim [Ki]. In particular the Rankin-Selberg convolution $L(\mathrm{Sym}^k E \otimes \mathrm{Sym}^k E, s)$ exists, and thus we have a zero-free region [IK, Theorems 5.10 and 5.42], from which we will deduce a Prime Number Theorem. This will be essential, as the point of the present paper is to show how the average rank of elliptic curves is determined by the analytical properties of $L(\mathrm{Sym}^2 E, s)$; we believe this to hold in greater generality. Note that our error terms will be effective as Goldfeld, Hoffstein and Lieman have shown the non-existence of Landau-Siegel zeros for $L(\mathrm{Sym}^2 E, s)$.

Remark 2.1. One has to be careful with possible poles of $L(s, \mathrm{Sym}^k f_E)/L'(s, \mathrm{Sym}^k f_E)$ at $s = 1$. If E has no complex multiplication, then the work of Taylor, Clozel, Harris and Shepherd-Barron [T, CHT, HST] implies that $L(s, \mathrm{Sym}^k f_E)$ is holomorphic and nonzero at $s = 1$. In the CM case however, things are slightly different. Indeed at $s = 1$, the function $L(s, \mathrm{Sym}^k f_E)$ is holomorphic and nonzero for $k \equiv 1, 2, 3 \bmod 4$, but has a simple pole when $4 \mid k$.

The prime number theorems to appear in this section will be weighted by certain function, in order to obtain absolutely convergent sums over zeros. In the following we assume that $h : (0, \infty) \to \mathbb{R}$ is such that its Mellin Transform

$$\mathcal{M}h(s) := \int_0^\infty x^{s-1} h(x) dx$$

converges for $\Re(s) \geq 0$, and such that the following property holds.

Property D.

- For any $N \geq 1$ and in the range $x \geq 1$, $h(x) \ll_N \frac{1}{x^N}$.
- $\mathcal{M}h(s)$ can be analytically continued to a meromorphic function with possible poles of order at most one at the points $s = 0, -1, -2, \ldots$
- Uniformly for $|\sigma| \leq 1$ and $|t| \geq 1$, $\mathcal{M}h(\sigma + it) \ll \frac{1}{t^2}$.

These properties hold for the typical examples $h(x) = \max(1 - x, 0)^k$ $(k \geq 1)$, and $h(x) = e^{-x}$. In fact they hold when h is any real Schwartz function on $(0, \infty)$.

Lemma 2.2. *Fix an elliptic curve E, and assume that h is a function satisfying Property D. Then there exists an effective absolute constant $c > 0$ such that*

$$\sum_p (\alpha_p(E)^2 + \beta_p(E)^2) h(p/x) \log p = -x\mathcal{M}h(1) + O(xe^{-c\log x/(\sqrt{\log x} + \log N_E)} (\log N_E)^2). \quad (9)$$

If we assume the Riemann Hypothesis for both $L(Sym^2 E, s+1)$ and $\zeta(s)$, then

$$\sum_p (\alpha_p(E)^2 + \beta_p(E)^2) h(p/x) \log p = -x\mathcal{M}h(1) + O(x^{\frac{1}{2}} \log N_E). \quad (10)$$

The constants implied in the error terms depend on h.

The estimate (10) will allow us to predict a quantitative bound for the number of elliptic curves of rank ≥ 2. The following Lemma, which is an application of the automorphy of $L(s, \mathrm{Sym}^3 f_E)$, will strengthen this quantitative bound.

Lemma 2.3. *Fix an elliptic curve E and assume that h is a function satisfying Property D, and assume the Riemann Hypothesis for both $L(Sym^3 E, s+\frac{3}{2})$ and $L(E, s+\frac{1}{2})$. Then we have the bound*

$$\sum_p (\alpha_p(E)^3 + \beta_p(E)^3) h(p/x) \log p \ll x^{\frac{1}{2}} \log N_E. \tag{11}$$

Proof of Lemma 2.2. It follows from the above discussion that the function $L(\mathrm{Sym}^2 E, s+1) = L(s, \mathrm{Sym}^2 f_E)$ is a degree-3 entire L-function in the sense of Iwaniec and Kowalski [IK, Chapter 5]. The logarithmic derivative of this L-function is given by

$$-\frac{L'(\mathrm{Sym}^2 E, s+1)}{L(\mathrm{Sym}^2 E, s+1)} = \sum_{k \geq 1} \sum_p \frac{(\alpha_p(E)^{2k} + \alpha_p(E)^k \beta_p(E)^k + \beta_p(E)^{2k}) \log p}{p^{ks}}.$$

As noted in Remark 2.1, this function is holomorphic at $s=1$. Applying Mellin Inversion we obtain

$$\sum_{\substack{p\\k\geq 1}} (\alpha_p(E)^{2k} + \alpha_p(E)^k \beta_p(E)^k + \beta_p(E)^{2k}) h(p^k/x) \log p = \frac{-1}{2\pi i} \int_{\Re(s)=2} \frac{L'(s, \mathrm{Sym}^2 f_E)}{L(s, \mathrm{Sym}^2 f_E)} x^s \mathcal{M}h(s) ds. \tag{12}$$

We have seen that the functional equation for $L(s, \mathrm{Sym}^2 f_E, s)$ takes the form $\Lambda(\mathrm{Sym}^2 f_E, s) = \epsilon(\mathrm{Sym}^2 E) \Lambda(\mathrm{Sym}^2 f_E, 1-s)$, that is

$$\begin{aligned}(\pi^3 q(\mathrm{Sym}^2 f_E))^{-\frac{s}{2}} &\Gamma(\tfrac{s+1}{2})^2 \Gamma(\tfrac{s}{2}+1) L(s, \mathrm{Sym}^2 f_E) \\ &= \epsilon(\mathrm{Sym}^2 E)(\pi^3 q(\mathrm{Sym}^2 f_E))^{-\frac{1-s}{2}} \Gamma(1-\tfrac{s}{2})^2 \Gamma(\tfrac{3-s}{2}) L(1-s, \mathrm{Sym}^2 f_E).\end{aligned}$$

This implies that the trivial zeros of $L(s, \mathrm{Sym}^2 f_E, s)$ are simple zeros at $s = -2m$ ($m \geq 1$) and double zeros at $s = 1-2n$ ($n \geq 1$). Pulling the contour of integration to the left in (12) until $\Re(s) = -\frac{1}{3}$ gives the following estimate (note that $L'(s, \mathrm{Sym}^2 f_E)/L(s, \mathrm{Sym}^2 f_E)$ is holomorphic at $s=1$):

$$\begin{aligned}\sum_{\substack{p\\k\geq 1}} (\alpha_p(E)^{2k} + \alpha_p(E)^k \beta_p(E)^k + \beta_p(E)^{2k}) h(p^k/x) \log p &= -\sum_{\rho_{E,2}} x^{\rho_{E,2}} \mathcal{M}h(\rho_{E,2}) \\ - c_h \frac{L'(0, \mathrm{Sym}^2 f_E)}{L(0, \mathrm{Sym}^2 f_E)} &+ O\left(x^{-\frac{1}{3}} \int_{\Re(s)=-\frac{1}{3}} \left| \frac{L'(s, \mathrm{Sym}^2 f_E)}{L(s, \mathrm{Sym}^2 f_E)} \right| \frac{|ds|}{|s|^2} \right),\end{aligned} \tag{13}$$

where $\rho_{E,2}$ runs through the nontrivial zeros of $L(s, \mathrm{Sym}^2 f_E)$ with multiplicity, and c_h denotes the residue at $s=0$ of $\mathcal{M}h(s)$, which might equal zero. To bound the terms on the right hand side of (13) we use the functional equation in the form

$$\frac{L'(s, \mathrm{Sym}^2 f_E)}{L(s, \mathrm{Sym}^2 f_E)} + \frac{\gamma'(\mathrm{Sym}^2 f_E, s)}{\gamma(\mathrm{Sym}^2 f_E, s)} = \log q(\mathrm{Sym}^2 f_E) + \frac{L'(1-s, \mathrm{Sym}^2 f_E)}{L(1-s, \mathrm{Sym}^2 f_E)} + \frac{\gamma'(\mathrm{Sym}^2 f_E, 1-s)}{\gamma(\mathrm{Sym}^2 f_E, 1-s)}.$$

On the line $\Re(s) = 4/3$ the logarithmic derivative of $L(s, \mathrm{Sym}^2 f_E)$ is bounded by an absolute constant. It follows from the functional equation and the asymptotic properties of the Digamma function[8] that

$$\frac{L'(-\frac{1}{3}+it, \mathrm{Sym}^2 f_E)}{L(-\frac{1}{3}+it, \mathrm{Sym}^2 f_E)} \ll \log(N_E|t|),$$

and thus the error term in (13) is at most a constant (which can depend on h) times $x^{-\frac{1}{3}} \log N_E$.

We first assume the Riemann Hypothesis for $L(s, \mathrm{Sym}^2 f_E)$ and $\zeta(s)$, and we show the conditional result (10). Combining [IK, (5.28)] and [IK, Theorem 5.33], we obtain the bound[9]

$$\frac{L'(1, \mathrm{Sym}^2 f_E)}{L(1, \mathrm{Sym}^2 f_E)} \ll \sum_{|\rho_{E,2}|<1} \frac{1}{|\rho_{E,2}|} + \log q(\mathrm{Sym}^2 f_E) \leq \sum_{|\rho_{E,2}|<1} 2 + \log q(\mathrm{Sym}^2 f_E) \ll \log N_E. \quad (14)$$

It then follows from the functional equation that

$$\frac{L'(0, \mathrm{Sym}^2 f_E)}{L(0, \mathrm{Sym}^2 f_E)} \ll \log N_E.$$

As for the sum over nontrivial zeros in (13), we apply the Riemann-von Mangoldt Formula [IK, (5.33)] to obtain the bound

$$\sum_{\rho_{E,2}} x^{\frac{1}{2}+i\gamma_{E,2}} \mathcal{M}h(\rho_{E,2}) \ll x^{\frac{1}{2}} \log q(\mathrm{Sym}^2 f_E) \ll x^{\frac{1}{2}} \log N_E.$$

Combining these bounds we obtain that

$$\sum_{\substack{p \\ k\geq 1}} (\alpha_p(E)^{2k} + \alpha_p(E)^k \beta_p(E)^k + \beta_p(E)^{2k}) h(p^k/x) \log p \ll x^{\frac{1}{2}} \log q(\mathrm{Sym}^2 f_E) \ll x^{\frac{1}{2}} \log N_E.$$

Note that $|\alpha_p(E)|, |\beta_p(E)| \leq 1$, and for $p \nmid N_E$, $\alpha_p(E)\beta_p(E) = 1$. We therefore have

$$\begin{aligned} &\sum_{\substack{p \\ k\geq 1}} (\alpha_p(E)^{2k} + \alpha_p(E)^k \beta_p(E)^k + \beta_p(E)^{2k}) h(p^k/x) \log p \\ &\quad = \sum_p (\alpha_p(E)^2 + 1 + \beta_p(E)^2) h(p/x) \log p + O\Big(\sum_{\substack{p^k \leq x \\ k\geq 2}} \log p + \sum_{p | N_E} \log p \Big) \qquad (15) \\ &\quad = x\mathcal{M}h(1) + \sum_p (\alpha_p(E)^2 + \beta_p(E)^2) h(p/x) \log p + O(x^{\frac{1}{2}} + \log N_E), \end{aligned}$$

by the Riemann Hypothesis for $\zeta(s)$. The proof follows.

We now prove the unconditional result (9), using the zero-free region of [IK, Theorem 5.44]. If E has no CM, then f_E is not the lift of a $GL(1)$ L-function and the work of Goldfeld, Hoffstein and Lieman [GHL] implies the nonexistence of Landau-Siegel zeros for

[8]The function $\psi(z) := \Gamma'(z)/\Gamma(z)$ satisfies $\psi(z) \sim \log z$, in the sector $\{z \in \mathbb{C} : |\arg(z-1)| < \pi - \delta\}$, for $\delta > 0$ fixed.

[9]Note that $\mathcal{M}h(s)$ might have a pole at $s = 0$, but each nontrivial zero is at a positive distance away from this point.

the associated L-function. It follows from [IK, Theorem 5.44] that for an absolute effective constant $c>0$ we have, without exception, the following bounds:

$$\frac{c}{\log(N_E(|\Im(\rho_{E,2})|+3))}<\Re(\rho_{E,2})<1-\frac{c}{\log(N_E(|\Im(\rho_{E,2})|+3))}.$$

These bounds also hold in the CM case, since in this situation the associated Hecke Grossencharacter $\xi_{E/K}$ is complex, and thus Landau-Siegel zeros do not exist.

Using this zero-free region and introducing a parameter $T\geq 1$, the sum over $\rho_{E,2}$ on the right hand side of (13) is at most (note that $\mathcal{M}h(s)$ might have a simple pole at $s=0$)

$$\sum_{|\Im(\rho_{E,2})|>T}\frac{x}{|\rho_{E,2}|^2}+\sum_{1<|\Im(\rho_{E,2})|\leq T}\frac{x^{1-\frac{c}{\log(N_E(|T|+3))}}}{|\rho_{E,2}|^2}+\sum_{\substack{|\Im(\rho_{E,2})|\leq 1\\ \Re(\rho_{E,2})>0}}\frac{x^{1-\frac{c}{\log(4N_E)}}}{|\rho_{E,2}|}$$
$$\ll x\frac{\log(TN_E)}{T}+(x^{1-\frac{c}{\log(N_E(T+3))}}+\log N_E)\log N_E.$$

Selecting $T=\exp(\sqrt{\log x})$, we obtain the error term on the right hand side of (9).

As for the term $L'(0,\mathrm{Sym}^2 f_E)/L(0,\mathrm{Sym}^2 f_E)$, we combine the zero-free region with [IK, 5.28], and (14) becomes

$$\frac{L'(1,\mathrm{Sym}^2 f_E)}{L(1,\mathrm{Sym}^2 f_E)}\ll\sum_{|\rho_{E,2}|<1}\frac{1}{(\log q(\mathrm{Sym}^2 f_E))^{-1}}+\log q(\mathrm{Sym}^2 f_E)\ll(\log N_E)^2, \qquad (16)$$

from which we get using the functional equation that $L'(0,\mathrm{Sym}^2 f_E)/L(0,\mathrm{Sym}^2 f_E)\ll(\log N_E)^2$.

The proof of (9) follows from combining these estimates with a similar calculation to (15), in which we replace the application of the Riemann Hypothesis for $\zeta(s)$ with the Prime Number Theorem.

□

Proof of Lemma 2.3. The proof is similar to that of Lemma 2.2. By the work of Kim and Shahidi [KiS2], $L(\mathrm{Sym}^3 E,s+\frac{3}{2})=L(s,\mathrm{Sym}^3 f_E)$ is the L-function of a cuspidal automorphic form on $GL(4)$. It follows that this function can be analytically continued to the whole complex plane, and the completed L-function [CM], given by

$$\Lambda(s,\mathrm{Sym}^3 f_E):=4q(\mathrm{Sym}^3 f_E)^{-\frac{s}{2}}(2\pi)^{-2s-2}\Gamma(s+\tfrac{1}{2})\Gamma(s+\tfrac{3}{2})L(s,\mathrm{Sym}^3 f_E),$$

satisfies the functional equation $\Lambda(s,\mathrm{Sym}^3 f_E)=\epsilon(\mathrm{Sym}^3 f_E)\Lambda(1-s,\mathrm{Sym}^3 f_E)$. Here, $q(\mathrm{Sym}^3 f_E)=N_E^3$ and $\epsilon(\mathrm{Sym}^3 f_E)=\pm 1$ [CM]. The logarithmic derivative of $\Lambda(s,\mathrm{Sym}^3 f_E)$ is given by

$$-\frac{L'(\mathrm{Sym}^3 E,s+\frac{3}{2})}{L(\mathrm{Sym}^2 E,s+\frac{3}{2})}=\sum_{k\geq 1}\sum_p\frac{(\alpha_p(E)^{3k}+\alpha_p(E)^{2k}\beta_p(E)^k+\alpha_p(E)^k\beta_p(E)^{2k}+\beta_p(E)^{3k})\log p}{p^{ks}}.$$

This function is holomorphic at $s=1$ whether or not E has complex multiplication (see Remark 2.1), hence arguing as in (13) we obtain that the Riemann Hypothesis for $L(s,\mathrm{Sym}^3 f_E)$ implies

$$\sum_{\substack{p\\ k\geq 1}}(\alpha_p(E)^{3k}+\alpha_p(E)^{2k}\beta_p(E)^k+\alpha_p(E)^k\beta_p(E)^{2k}+\beta_p(E)^{3k})h(p^k/x)\log p\ll x^{\frac{1}{2}}\log N_E.$$

The proof is achieved by trivially bounding the prime powers $k \geq 2$:

$$\sum_{\substack{p\\k\geq 2}} (\alpha_p(E)^{3k} + \alpha_p(E)^{2k}\beta_p(E)^k + \alpha_p(E)^k\beta_p(E)^{2k} + \beta_p(E)^{3k})h(p^k/x)\log p \ll x^{\frac{1}{2}};$$

and by the following computation:

$$\begin{aligned}
&\sum_p (\alpha_p(E)^3 + \alpha_p(E)^2\beta_p(E) + \alpha_p(E)\beta_p(E)^2 + \beta_p(E)^3)h(p^k/x)\log p \\
&\quad= \sum_p (\alpha_p(E)^3 + \beta_p(E)^3)h(p^k/x)\log p + \sum_p (\alpha_p(E) + \beta_p(E))h(p^k/x)\log p + O\Bigg(\sum_{p|N_E} \log p\Bigg) \\
&\quad= \sum_p (\alpha_p(E)^3 + \beta_p(E)^3)h(p^k/x)\log p + O(x^{\frac{1}{2}}\log N_E + \log N_E),
\end{aligned}$$

by the Riemann Hypothesis for $L(s, f_E)$.

$\square$

3. The average analytic rank in terms of a prime sum

Consider for $d \neq 0$ squarefree the quadratic twists

$$E_d : dy^2 = x^3 + ax + b.$$

The curve E_d has conductor dividing d^2N_E, and in the case where $(d, N_E) = 1$ its conductor is exactly d^2N_E. Moreover, the L-function of E_d is the Ranking-Selberg convolution of that of E and of $L(s, \chi_d)$, that is if $L(E, s + \frac{1}{2}) = L(s, f_E) = \sum_{n\geq 1} \lambda_E(n)n^{-s}$, then[10]

$$L(E_d, s + \tfrac{1}{2}) = L(s, f_E \otimes \chi_d) = \sum_{n\geq 1} \frac{\lambda_E(n)\chi_d(n)}{n^s}.$$

As is customary, we have denoted

$$\chi_d(n) := \left(\frac{d}{n}\right).$$

We fix $g : (0, \infty) \to \mathbb{R}$ a function satisfying Property D (see Section 2). Note that for $k \geq 1$, the function $g_k(x) := g(x^k)$ also satisfies Property D, since

$$\mathcal{M}g_k(s) = \int_0^\infty x^{s-1}g(x^k)dx = \frac{1}{k}\int_0^\infty t^{\frac{s}{k}-1}g(t)dt = \tfrac{1}{k}\mathcal{M}g(\tfrac{s}{k}), \tag{17}$$

which initially converges for $\Re(s) \geq 0$ and extends to a meromorphic function on $\mathbb{C}$ with possible simple poles at the points $s = 0, -k, -2k, ...$ The decay condition is trivial to check.

The central quantity we will study is the "prime sum"

$$S(D; P) := -\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\sum_{p\leq P} \frac{\chi_d(p)a_p(E)\log p}{\sqrt{p}}g(p/P). \tag{18}$$

---

[10]This follows from the following calculation:

$$a_p(E_d) = p + 1 - \#(E_d)_p(\mathbb{F}_p) = \sum_{x \bmod p} \left(\frac{d}{p}\right)\left(\frac{x^3 + ax + b}{p}\right) = \left(\frac{d}{p}\right)a_p(E).$$

In this section we apply Lemmas 2.2 and 2.3 to show that under either of Hypotheses M or M(δ,η) for some $0<\delta<1$ and $0<\eta<\frac12$, the quantity $S(D;P)$ is strongly linked with the average rank of E_d. Since these hypotheses are stated with a specific weight g, we will state the analogous bounds for a general function g satisfying Property D:

$$\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\sum_{\rho_d\notin\mathbb{R}} P^{\rho_d}\mathcal{M}g(\rho_d)=o(DP^{\frac12}); \tag{19}$$

$$\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\sum_{\rho_d\notin\mathbb{R}} P^{\rho_d}\mathcal{M}g(\rho_d)=O_E(D^{1-\eta}P^{\frac12}). \tag{20}$$

Proposition 3.1. *Assume that $L(E_d,s)$ has no real zeros in the critical strip, except possibly at the central point, and assume that (19) holds in the range $D^{2-\delta}\leq P\leq 2D^{2-\delta}$, for some $\delta>0$. Then in the same range we have*

$$P^{-\frac12}S(D;P)=\mathcal{M}g(\tfrac12)\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\left(r_{an}(E_d)-\frac12\right)+o_{D\to\infty}(D). \tag{21}$$

Assuming moreover that (20) holds for some $0<\eta<\frac12$, as well as the Riemann Hypothesis for $L(Sym^2E,s+1)$ and for $\zeta(s)$, we have in the same range the stronger estimate

$$P^{-\frac12}S(D;P)=\mathcal{M}g(\tfrac12)\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\left(r_{an}(E_d)-\frac12\right)+O_E(P^{-\frac16}D+D^{1-\eta}). \tag{22}$$

Finally, assume that (20) holds for some $0<\eta<\frac12$ in the range $D^{2-\delta}\leq P\leq 2D^{2-\delta}$ for some $0<\delta<1$, and assume the Riemann Hypothesis for $\zeta(s)$ and for $L(Sym^kE,s+\frac{k}{2})$ with $1\leq k\leq 3$. Then we have in the same range

$$P^{-\frac12}S(D;P)=\mathcal{M}g(\tfrac12)\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\left(r_{an}(E_d)-\frac12\right)+O_E(P^{-\frac14}D+D^{1-\eta}). \tag{23}$$

Remark 3.2. The dependence on E of the error terms in (21), (22) and (23) can be determined explicitly from the following proof, provided the dependence on E in (19) and (20) is known.

Remark 3.3. The error term $O_E(P^{-\frac14}D)$ in (23) comes from the Riemann Hypothesis for $L(\mathrm{Sym}^2E,s+\frac12)$, and thus assuming the Riemann Hypothesis for $L(\mathrm{Sym}^kE,s+\frac12)$ with $k\geq 4$ will not yield a better error term.

Proof. We first write the explicit formula for $L(E_d,s+\frac12)$. Note that

$$-\frac{L(E_d,s+\frac12)}{L(E_d,s+\frac12)}=\sum_{\substack{p\\k\geq1}}\frac{(\alpha_p(E_d)^k+\beta_p(E_d)^k)\log p}{p^{ks}},$$

hence as in the proof of Lemma 2.2 we obtain the formula

$$\sum_{\substack{p\\k\geq1}}\chi_d(p)^k(\alpha_p(E)^k+\beta_p(E)^k)g(p^k/P)\log p=-\sum_{\rho_d}P^{\rho_d}\mathcal{M}g(\rho_d)+O\left(\log(|d|N_E)\right). \tag{24}$$

Working on the left hand side of this equation, we use the bounds $|\alpha_p(E)|, |\beta_p(E)| \leq 1$ to obtain

$$\begin{aligned}\sum_{\substack{p\\k\geq 2}} \chi_d(p)^k(\alpha_p(E)^k+\beta_p(E)^k)g(p^k/P)\log p &= \sum_{p\nmid d}(\alpha_p(E)^2+\beta_p(E)^2)g(p^2/P)\log p + O(P^{\frac13})\\ &= \sum_p(\alpha_p(E)^2+\beta_p(E)^2)g_2(p/P^{\frac12})\log p + O(P^{\frac13}+\log|d|)\\ &= -\mathcal{M}g_2(1)P^{\frac12} + O(P^{\frac12}e^{-c\frac{\frac12\log P}{\sqrt{\frac12\log P+\log N_E}}}\log N_E+\log|d|),\end{aligned} \tag{25}$$

by Lemma 2.2. Note that $\mathcal{M}g_2(1) = \frac12\mathcal{M}g(\frac12)$ (see (17)), and hence it follows from (24), (25) and the identity $a_p(E)/\sqrt{p} = \alpha_p(E)+\beta_p(E)$ that

$$\begin{aligned}\sum_{p\leq P}\frac{\chi_d(p)a_p(E)\log p}{\sqrt{p}}g(p/P) = \tfrac12\mathcal{M}g(\tfrac12)P^{\frac12} - \sum_{\rho_d}P^{\rho_d}\mathcal{M}g(\rho_d)&\\ + O(P^{\frac12}e^{-\frac{c'\log P}{\sqrt{\log P+\log N_E}}}\log N_E+\log(|d|N_E)).&\end{aligned} \tag{26}$$

Note that the sum over zeros contains both real and nonreal zeros, however we are assuming that the only possible real zero ρ_d of $L(E_d, s+\frac12)$ is at the central point, that is $\rho_d = \frac12$, which gives a contribution of $-r_{\mathrm{an}}(E_d)P^{\frac12}\mathcal{M}g(\frac12)$. We then obtain by summing (26) over squarefree $0 < |d| \leq D$ against the smooth weight $w(d/D)$ the estimate

$$\begin{aligned}P^{-\frac12}S(D;P) = \mathcal{M}g(\tfrac12)\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\left(r_{\mathrm{an}}(E_d)-\frac12\right) + \sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\sum_{\rho_d\notin\mathbb{R}}P^{\rho_d-\frac12}\mathcal{M}g(\rho_d)&\\ + O\left(De^{-\frac{c'\log P}{\sqrt{\log P+\log N_E}}}\log N_E + \frac{D\log(DN_E)}{P^{\frac12}}\right).&\end{aligned} \tag{27}$$

The proof follows from applying (19).

To prove (22) and (23), we return to (25), but perform a more precise calculation:

$$\begin{aligned}&\sum_{\substack{p\\k\geq 2}} \chi_d(p)^k(\alpha_p(E)^k+\beta_p(E)^k)g(p^k/P)\log p\\ &= \sum_p(\alpha_p(E)^2+\beta_p(E)^2)g_2(p/P^{\frac12})\log p + \sum_p(\alpha_p(E_d)^3+\beta_p(E_d)^3)g_3(p/P^{\frac13})\log p\\ &\qquad + O(P^{\frac14}+\log|d|).\end{aligned} \tag{28}$$

(Note that for $p\nmid d$, $\chi_d(p)^2 = 1$, and $\chi_d(p)^3\alpha_p(E)^3 = \alpha_p(E_d)^3$.) Assuming the Riemann Hypothesis for $L(s, \mathrm{Sym}^2 f_E)$ and $\zeta(s)$, we obtain by an application of Lemma 2.2 and by trivially bounding the second sum that (28) equals

$$-\tfrac12\mathcal{M}g(\tfrac12)P^{\frac12} + O(P^{\frac14}\log N_E) + O(P^{\frac13}) + O(P^{\frac14}+\log|d|).$$

Following the steps above and applying (20) in (27) gives (22). As for (23), we follow the same procedure, except that we apply Lemmas 2.2 and 2.3 to (28), which gives that this quantity equals

$$-\tfrac12\mathcal{M}g(\tfrac12)P^{\frac12} + O(P^{\frac14}\log N_E) + O(P^{\frac16}\log(|d|N_E)) + O(P^{\frac14}+\log|d|).$$

$\square$

4. Quadratic twists: An upper bound for the prime sum $S(D;P)$

In this section we follow the arguments of Katz and Sarnak [KaS], which were inspired from Iwaniec's work [I1]. The goal is to give an upper bound on the prime sum $S(D;P)$ (see (18)), which by Proposition 3.1 will yield information about the average analytic rank of E_d. Let us first give a consequence of ECRH. We fix a function $g:(0,\infty)\to\mathbb{R}$ satisfying Property D (see Section 2).

Lemma 4.1. *Assume ECRH. We have for $m\neq 0$ and $P,t\geq 1$ the estimates*

$$\sum_{p\leq t}\frac{a_p(E)\log p}{\sqrt{p}}\left(\frac{m}{p}\right)\ll t^{\frac12}(\log t)\log(2t|m|N_E); \tag{29}$$

$$\sum_{p}\frac{a_p(E)\log p}{\sqrt{p}}\left(\frac{m}{p}\right)g(p/P)\ll P^{\frac12}\log(2|m|N_E). \tag{30}$$

Proof. First note that $a_p(E)\left(\frac{m}{p}\right)=a_p(E)$, where E_m is the quadratic twist $my^2=x^3+ax+b$. Note also that E_m is isomorphic to $E_{m'}$, where m' is the squarefree part of m. Applying the Riemann Hypothesis to $L(E_{m'},s)$, which is modular, we obtain by [IK, Theorem 5.15] that

$$\sum_{p\leq t}\frac{a_p(E_y)\log p}{\sqrt{p}}\ll t^{\frac12}(\log t)\log(2t|m|N_E).$$

The proof follows by bounding trivially the contribution of the primes dividing mN_E. As for (30), it follows along the similar lines, except that we use the following explicit formula:

$$\sum_{\substack{p\\ k\geq 1}}(\alpha_p(E)^k+\beta_p(E)^k)g(p^k/P)\log p=-\sum_{\rho_d}P^{\rho_d}\mathcal{M}g(\rho_d)+O(\log(|d|N_E)).$$

$\square$

We will need the following lemma of [FPS].

Lemma 4.2. *Fix $n\geq 1$ and $\epsilon>0$. Under the Riemann Hypothesis we have the estimate*

$$\sum_{(d,N_E)=1}^{*}w\left(\frac{d}{D}\right)\left(\frac{d}{n}\right)=\kappa(n)\frac{D}{\zeta(2)}\int_{\mathbb{R}}w(t)dt\prod_{p\mid N_E}\left(1+\frac{\left(\frac{p}{n}\right)}{p}\right)^{-1}\prod_{p\mid n}\left(1+\frac{1}{p}\right)^{-1} + O_\epsilon((N_E)^\epsilon|n|^{\frac38(1-\kappa(n))+\epsilon}D^{\frac14+\epsilon}),$$

where

$$\kappa(n):=\begin{cases}1 & \text{if } n=\square,\\ 0 & \text{otherwise.}\end{cases}$$

We are now ready to bound $S(D;P)$.

Proposition 4.3. *Assume ECRH and fix $0<\delta<1$. Then in the range $D^\delta\leq P\leq D^{2-\delta}$ we have*

$$P^{-\frac12}S(D;P)\ll_\epsilon N_E^\epsilon P^{\frac14+\epsilon}D^{\frac12}=o_{D\to\infty}(D).$$

Proof. The proof is an adaptation of that of [KaS, Theorem (B)]. We first turn the sum over squarefree d into a sum over all integers using the identities $\mu^2(d) = \sum_{a^2|d} \mu(a)$; $I_{(d,N_E)=1} = \sum_{c|(d,N_E)} \mu(c)$. We will use Lemma 4.2 to bound the contribution of $p = 2$ in (31). Denoting by $[a, c]$ the least common multiple of a and c, we compute

$$\begin{aligned} S(D;P) &= -\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right) \sum_p \frac{\chi_d(p) a_p(E) \log p}{\sqrt{p}} g(p/P) \\ &= -\sum_p \frac{a_p(E)\log p}{\sqrt{p}} g(p/P) \sum_{d\neq 0} \sum_{a^2|d} \mu(a) \sum_{c|(d,N_E)} \mu(c) w\left(\frac{d}{D}\right)\left(\frac{d}{p}\right) \qquad (31) \\ &= -\sum_{a\geq 1} \mu(a) \sum_{c|N_E} \mu(c) \sum_{p\nmid 2ac} \frac{a_p(E)\log p}{\sqrt{p}} g(p/P) \sum_{b\in\mathbb{Z}} w\left(\frac{[a^2,c]b}{D}\right)\left(\frac{[a^2,c]b}{p}\right) + O_\epsilon(D^{\frac12} N_E^\epsilon), \end{aligned}$$

since the primes dividing ac give a zero contribution, and the prime $p = 2$ contributes

$$\ll \sum_{a\leq D^{\frac12}} \tau(N_E) + \sum_{a > D^{\frac12}} \tau(N_E) \frac{D}{a^2} \ll \tau(N_E) D^{\frac12}.$$

We then have that (31) equals

$$T_1(A) + T_2(A) + O_\epsilon(D^{\frac12+\epsilon} N_E^\epsilon).$$

where, fixing a parameter $A \geq 1$,

$$T_2(A) := -\sum_{a>A} \mu(a) \sum_{c|N_E} \mu(c) \sum_{p\nmid 2ac} \frac{a_p(E)\log p}{\sqrt{p}} g(p/P) \sum_{b\in\mathbb{Z}} w\left(\frac{[a^2,c]b}{D}\right)\left(\frac{[a^2,c]b}{p}\right),$$

and $T_1(A)$ is the same sum with $a \leq A$. Applying Lemma 4.1 gives the bound

$$\begin{aligned} |T_2(A)| &\leq \sum_{a>A} \sum_{c|N_E} \sum_{b\in\mathbb{Z}} w\left(\frac{[a^2,c]b}{D}\right) \left| \sum_{p\neq 2} \left(\frac{[a^2,c]b}{p}\right) \frac{a_p(E)\log p}{\sqrt{p}} g(p/P) \right| \\ &\ll \sum_{a>A} \sum_{c|N_E} \sum_{b\in\mathbb{Z}} w\left(\frac{[a^2,c]b}{D}\right) (P^{\frac12} \log(abcN_E) + 1) \\ &\ll P^{\frac12} \tau(N_E) \sum_{a>A} \frac{D\log(ADN_E)}{a^2} \ll DP^{\frac12} \frac{\tau(N_E)\log(ADN_E)}{A}. \end{aligned}$$

To treat $T_1(A)$, we will use Gauss sums. Let $\epsilon_n = \frac{1+i}{2}\chi_0(n) + \frac{1-i}{2}\chi_1(n)$, where χ_0 and χ_1 are respectively the trivial and the nontrivial character modulo 4. Hence $\epsilon_p = 1$ if $p \equiv 1 \bmod 4$ and $-i$ if $p \equiv 3 \bmod 4$. Then, for any $a \geq 1$, $c \mid N_E$ and $p \nmid 2ac$ we have

$$\begin{aligned} \sum_{b\in\mathbb{Z}} w\left(\frac{[a^2,c]b}{D}\right)\left(\frac{[a^2,c]b}{p}\right) &= \sum_{b\in\mathbb{Z}} w\left(\frac{[a^2,c]b}{D}\right) \frac{\overline{\epsilon_p}}{p^{\frac12}} \sum_{x \bmod p} \left(\frac{x}{p}\right) e\left(\frac{[a^2,c]bx}{p}\right) \\ &= \frac{\overline{\epsilon_p}}{p^{\frac12}} \sum_{x \bmod p} \left(\frac{x}{p}\right) \sum_{b\in\mathbb{Z}} w\left(\frac{[a^2,c]b}{D}\right) e\left(\frac{[a^2,c]bx}{p}\right). \end{aligned}$$

We now transform the sum over b using Poisson summation:

$$\sum_{b\in\mathbb{Z}} w\left(\frac{[a^2,c]b}{D}\right) e\left(\frac{[a^2,c]bx}{p}\right) = \frac{D}{[a^2,c]}\sum_{m\in\mathbb{Z}} \hat{w}\left(D\left(\frac{m}{[a^2,c]}-\frac{x}{p}\right)\right).$$

Inserting this into the definition of $T_1(A)$ gives the identity

$$T_1(A) = -D\sum_{a\le A}\sum_{c\mid N_E}\frac{\mu(a)\mu(c)}{[a^2,c]}\sum_{p\nmid 2ac}\frac{\overline{\epsilon_p}a_p(E)\log p}{p}g(p/P)\sum_{x \bmod p}\left(\frac{x}{p}\right)\sum_{m\in\mathbb{Z}}\hat{w}\left(D\left(\frac{m}{[a^2,c]}-\frac{x}{p}\right)\right).$$

Note that as x runs through $\mathbb{Z}/p\mathbb{Z}$ and m runs through $\mathbb{Z}$, $y := pm-[a^2,c]x$ runs throught $\mathbb{Z}$. Indeed, $(p,ac)=1$ implies that the map $(x,m)\mapsto pm-[a^2,c]x$ is a bijection between $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}$ and $\mathbb{Z}$. We deduce that

$$T_1(A) = -D\sum_{a\le A}\sum_{c\mid N_E}\frac{\mu(a)\mu(c)}{[a^2,c]}\sum_{p\nmid 2ac}\frac{\overline{\epsilon_p}a_p(E)\log p}{p}g(p/P)\sum_{y\in\mathbb{Z}}\left(\frac{-[a^2,c]y}{p}\right)\hat{w}\left(\frac{Dy}{[a^2,c]p}\right) \quad (32)$$

$$= -D\sum_{a\le A}\sum_{c\mid N_E}\frac{\mu(a)\mu(c)}{[a^2,c]}\sum_{y\in\mathbb{Z}}\int_1^{P^{1+\epsilon/2}}\hat{w}\left(\frac{Dy}{[a^2,c]t}\right)dS_y(t) + O_N(\tau(N_E)DP^{-N}), \quad (33)$$

where

$$S_y(t) := \sum_{p\le t}\left(\frac{-4y[a^2,c]}{p}\right)\frac{\overline{\epsilon_p}a_p(E)\log p}{p}g(p/P),$$

and the error term comes from the decay of $g(x)$ in Property D. By the definition of ϵ_n and by applying summation by parts in Lemma 4.1, Hypothesis ECRH implies

$$S_y(t) \ll (\log t)\log(|acy|tN_E+2).$$

Moreover, since w is Schwartz we have the bounds

$$\hat{w}(\xi), \hat{w}'(\xi) \ll_\epsilon \min(\xi^{-1-\epsilon},\xi^{-2-\epsilon}).$$

Applying these bounds after a summation by parts, we obtain that the first term in (33) is

$$\begin{aligned}
&= -D\sum_{a\le A}\sum_{c\mid N_E}\frac{\mu(a)\mu(c)}{[a^2,c]}\sum_{y\in\mathbb{Z}}\hat{w}\left(\frac{Dy}{[a^2,c]t}\right)S_y(t)\Bigg|_1^{P^{1+\epsilon/2}} \\
&\qquad - D\sum_{a\le A}\sum_{c\mid N_E}\frac{\mu(a)\mu(c)}{[a^2,c]}\int_1^{P^{1+\epsilon/2}}\sum_{y\in\mathbb{Z}}\frac{DyS_y(t)}{[a^2,c]}\hat{w}'\left(\frac{Dy}{a^2t}\right)\frac{dt}{t^2} \\
&\ll_\epsilon D\sum_{a\le A}\frac{1}{a^2}\sum_{c\mid N_E}\sum_{y\in\mathbb{Z}}(\log(acP|y|N_E+2))(\log P)\left(\frac{Dy}{[a^2,c]P^{1+\epsilon/2}}\right)^{-1-\epsilon/3} \\
&\qquad + D^2\sum_{a\le A}\frac{1}{a^4}\sum_{c\mid N_E}\int_1^{P^{1+\epsilon/2}}\sum_{y\in\mathbb{Z}}y(\log(acP|y|N_E+2))(\log P)\left(\frac{Dy}{[a^2,c]t}\right)^{-2-\epsilon/2}\frac{dt}{t^2} \\
&\ll_\epsilon (AN_E)^{1+\epsilon}P^{1+\epsilon}\log N_E.
\end{aligned}$$

Combining our estimates for $T_1(A)$ and $T_2(A)$ we obtain that

$$\frac{S(D;P)}{DP^{\frac12}} = D^{-1}P^{-\frac12}(T_1(A)+T_2(A)+O_\epsilon(D^{\frac12}N_E^\epsilon))$$
$$\ll_\epsilon \frac{\tau(N_E)(\log ADN_E)^2}{A} + \frac{(AN_E)^{1+\epsilon}P^{\frac12+\epsilon}}{D}\log N_E + \frac{N_E^\epsilon}{P^{\frac12}D^{\frac12}}.$$

(The error term in (33) is absorbed by the error term $N_E^\epsilon/P^{\frac12}D^{\frac12-\epsilon}$). The claimed estimate follows from taking $A := D^{\frac12}P^{-\frac14} \geq 1$. □

5. Proof of the main results

We first give an effective equidistribution result for the root number $\epsilon(E_d)$.

Lemma 5.1. *Fix w a Schwartz function. We have the bounds*

$$\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\epsilon(E_d) \ll_\epsilon D^{\frac12+\epsilon}N_E^{\frac14+\epsilon}, \qquad \sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1}} \epsilon(E_d) \ll D^{\frac12}N_E^{\frac14}(\log N_E)^{\frac12}.$$

Remark 5.2. One can improve the dependence on N_E in these estimates by using Burgess's bound (see [GV]), however this is not important for our purposes since E is fixed.

Proof. We prove the second estimate; the first follows along similar lines. Note that by [IK, (23.48)], for $(d,N_E)=1$ we have $\epsilon(E_d) = (\frac{d}{-N_E})\epsilon_E$. Now,

$$\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1}} \left(\frac{d}{-N_E}\right) = \sum_{\substack{a\leq D^{\frac12}\\(a,N_E)=1}} \mu(a) \sum_{0<|\ell|\leq D/a^2} \left(\frac{\ell}{-N_E}\right).$$

We then split the sum into a sum over $a \leq A$ and $A < a \leq D^{\frac12}$, with $A = D^{\frac12}N_E^{-\frac14}(\log N_E)^{-\frac12}$. The first of these sums is bounded using the Polyà-Vinogradov Inequality, and the second using the trivial bound. □

Proof of Theorem 1.1 and Corollary 1.2. Let $\delta > 0$ be given by Hypothesis M, and for $D \geq 1$, set $P = P(D) = D^{2-\delta}$. Select $g(x) = \max(1-x,0)$, which satisfies Property D. On one hand, Proposition 3.1 gives the estimate

$$P^{-\frac12}S(D;P) = \mathcal{M}g(\tfrac12)\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\left(r_{\mathrm{an}}(E_d)-\frac12\right) + o_{D\to\infty}(D). \tag{34}$$

On the other hand, Proposition 4.3 shows that

$$P^{-\frac12}S(D;P) = o_{D\to\infty}(D).$$

It follows that

$$\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\left(r_{\mathrm{an}}(E_d)-\frac12\right) = o_{D\to\infty}(D). \tag{35}$$

We will use the following notation, for $k \geq 0$:

$$S_k(D) := \sideset{}{^*}\sum_{\substack{(d,N_E)=1\\ r_{\rm an}(E_d)=k}} w\left(\frac{d}{D}\right); \qquad S^{\rm odd}_{\geq k}(D) := \sideset{}{^*}\sum_{\substack{(d,N_E)=1\\ r_{\rm an}(E_d)\geq k\\ r_{\rm an}(E_d)\equiv 1 \bmod 2}} w\left(\frac{d}{D}\right),$$

and similarly for $S^{\rm even}_{\geq k}(D)$. Now, $r_{\rm an}(E_d)$ is even if $\epsilon(E_d)=1$, and odd if $\epsilon(E_d)=-1$. We now apply Lemma 5.1. Summing $(1+\epsilon(E_d))$ and $(1-\epsilon(E_d))$ against the weight $w(d/D)$ we obtain that

$$S^{\rm even}_{\geq 0}(D) \sim \frac{W(D)}{2}; \qquad S^{\rm odd}_{\geq 1}(D) \sim \frac{W(D)}{2}, \tag{36}$$

where

$$W(D) := \sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right) \sim D\int_{\mathbb{R}} w(t)dt.$$

We then have by (35) that

$$\begin{aligned}\frac{W(D)}{2} \sim \sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right) r(E_d) &\geq 0S_0(D) + S_1(D) + 2S^{\rm even}_{\geq 2}(D) + 3S^{\rm odd}_{\geq 3}(D)\\ &= 2S^{\rm even}_{\geq 2}(D) + S^{\rm odd}_{\geq 1}(D) + 2S^{\rm odd}_{\geq 3}(D),\end{aligned}$$

hence

$$2(S^{\rm even}_{\geq 2}(D) + S^{\rm odd}_{\geq 3}(D)) \leq \frac{W(D)}{2} - S^{\rm odd}_{\geq 1}(D) + o(W(D)) = o(D). \tag{37}$$

We now show that this implies that the proportion of curves of rank ≥ 2 is zero. Since $w(0) \neq 0$ and w is smooth, there exists $\eta > 0$ and $\theta > 0$ such that $w(x) \geq \theta$ for all $|x| \leq \eta$. We then have by nonnegativity of w that

$$\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\ (d,N_E)=1\\ r_{\rm an}(E_d)\geq 2}} 1 \leq \theta^{-1} \sideset{}{^*}\sum_{\substack{(d,N_E)=1\\ r_{\rm an}(E_d)\geq 2}} w\left(\frac{d}{\eta^{-1}D}\right) = \theta^{-1}o(\eta^{-1}D) = o(D), \tag{38}$$

by (37); hence the number of curves of rank ≥ 2 is negligible. Applying Lemma 5.1 again, one obtains

$$\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\ (d,N_E)=1\\ r_{\rm an}(E_d)=0}} 1 \sim \frac{N(D)}{2}; \qquad \sideset{}{^*}\sum_{\substack{0<|d|\leq D\\ (d,N_E)=1\\ r_{\rm an}(E_d)=1}} 1 \sim \frac{N(D)}{2}. \tag{39}$$

That is, 50% of the curves have rank 0 and the remaining 50% have rank 1.

To compute the average rank without the weight $w(d/D)$ we first see that

$$\begin{aligned}\sideset{}{^*}\sum_{\substack{(d,N_E)=1\\ r_{\rm an}(E_d)\geq 2}} w\left(\frac{d}{D}\right) r(E_d) &= \sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\left(r(E_d)-\frac{1}{2}\right) + \frac{W(D)}{2} - \sideset{}{^*}\sum_{\substack{(d,N_E)=1\\ r_{\rm an}(E_d)=1}} w\left(\frac{d}{D}\right)\\ &= o(D),\end{aligned}$$

by (35), (36) and (37). We then combine this with the fact that $w(x) \geq \theta$ for $|x| \leq \eta$:

$$\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1\\r_{\text{an}}(E_d)\geq 2}} r(E_d) \leq \theta^{-1} \sideset{}{^*}\sum_{\substack{(d,N_E)=1\\r_{\text{an}}(E_d)\geq 2}} w\left(\frac{d}{\eta^{-1}D}\right) r(E_d) = \theta^{-1}o(\eta^{-1}D) = o(D).$$

Combining this with (39) implies that the average rank is exactly 1/2.

Finally, the results of Gross-Zagier [GZ], Kolyvagin [Ko] and others imply that the Birch and Swinnerton-Dyer Conjecture holds for the curve E_d whenever $r_{\text{an}}(E_d) \leq 1$, and as we have shown in (39), this holds for almost all elliptic curves E_d.

□

Our results also apply to the family $\{E_d : \mu^2(d) = 1\}$. If N_E is squarefree, then we can show that the root number $\epsilon(E_d)$ is equidistributed in this family.

Lemma 5.3. *Assume that N_E is squarefree. Then we have*

$$\sideset{}{^*}\sum_{0<|d|\leq D} \epsilon(E_d) \ll_E D^{\frac{1}{2}}.$$

Proof. It follows from [IK, (23.48)] that if N_E is squarefree then we have the equality

$$\epsilon(E_d) = \chi_d(-N_E/(d,N_E))\mu((d,N_E))\lambda_E((d,N_E))\epsilon(E).$$

Here, $L(s,f_E) = \sum_n \lambda_E(n)n^{-s}$. We therefore have

$$\begin{aligned}\sideset{}{^*}\sum_{0<|d|\leq D} \epsilon(E_d) &= \epsilon(E)\sum_{a|N_E}\mu(a)\lambda_E(a) \sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=a}} \chi_d(-N_E/a)\\
&= \epsilon(E)\sum_{a|N_E}\mu(a)\lambda_E(a) \sideset{}{^*}\sum_{\substack{0<|k|\leq D/a\\(k,N_E)=1}} \left(\frac{ka}{-N_E/a}\right)\\
&= \epsilon(E)\sum_{a|N_E}\mu(a)\left(\frac{a}{-N_E/a}\right)\lambda_E(a)\sum_{\ell|N_E}\mu(\ell) \sideset{}{^*}\sum_{0<|m|\leq D/(a\ell)} \left(\frac{m\ell}{-N_E/a}\right)\\
&\ll D^{\frac{1}{2}}N_E^{\frac{1}{4}}\tau(N_E)^2(\log N_E)^{\frac{1}{2}},\end{aligned}$$

by Lemma 5.1. □

Proof of Theorem 1.7. Letting $P = D^{2-\delta}$ with $\delta = \delta_\eta > 0$ coming from Hypothesis M(η), Proposition 3.1 gives the following estimate:

$$\mathcal{M}g(\tfrac{1}{2}) \sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\left(r_{\text{an}}(E_d) - \frac{1}{2}\right) = P^{-\frac{1}{2}}S(D;P) + O_E(D^{\frac{1}{2}+\frac{\delta}{4}} + D^{1-\eta}).$$

With this choice of P, Proposition 4.3 yields the bound

$$\frac{4}{3}\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\left(r_{\text{an}}(E_d) - \frac{1}{2}\right) \ll_E D^{1-\frac{\delta}{4}+o(1)} + D^{\frac{1}{2}+\frac{\delta}{4}} + D^{1-\eta} \ll D^{1-\frac{\delta}{4}+o(1)} + D^{1-\eta},$$

since $\delta < 1$. The remaining of the proof is similar to that of Theorem 1.1.

□

Proof of Corollary 1.8. The proof is very similar to that of Corollary 1.2. □

Proof of Theorem 1.14. The idea is very similar to the proof of Theorem 1.1. We fix a function g with Property D and study the following prime sum with two different techniques:

$$S(A,B;P) := -\sideset{}{^*}\sum_{a,b} w\left(\frac{a}{A},\frac{b}{B}\right)\sum_p \frac{a_p(E_{a,b})\log p}{\sqrt{p}} g(p/P). \tag{40}$$

We first add all prime powers to $S(A,B;P)$ in order to apply the Explicit Formula. The squares of primes are treated using $L(\mathrm{Sym}^2 E_{a,b},s)$, as in Lemma 2.2:

$$\sum_{\substack{p\\k\geq 1}}(\alpha_p(E_{a,b})^{2k}+\alpha_p(E_{a,b})^k\beta_p(E_{a,b})^k+\beta_p(E_{a,b})^{2k})g(p^{2k}/x^{2k})\log p$$
$$\ll xe^{-c\log x/(\sqrt{\log x}+\log(N_{E_{a,b}}))}\log(N_{E_{a,b}}),$$

from which we obtain using similar arguments that

$$\begin{aligned}\sum_p(\alpha_p(E_{a,b})^2+\beta_p(E_{a,b})^2)g(p^2/P)\log p &= -\sum_p g_2(p/P^{\frac12})\log p + o(P^{\frac12})\\ &= -\tfrac12\mathcal{M}g(\tfrac12)P^{\frac12}+o(P^{\frac12}),\end{aligned}$$

where as before $g_k(t)=g(t^k)$. Trivially bounding the higher prime powers, we obtain

$$\begin{aligned}-\sum_p \frac{a_p(E_{a,b})\log p}{\sqrt{p}}g(p/P) &= -\tfrac12\mathcal{M}g(\tfrac12)P^{\frac12}-\sum_{\substack{p\\k\geq1}}(\alpha_p(E_{a,b})^k+\beta_p(E_{a,b})^k)g(p^k/P)\log p+o(P^{\frac12})\\ &= -\tfrac12\mathcal{M}g(\tfrac12)P^{\frac12}+\sum_{\rho_{a,b}}\mathcal{M}g(\rho_{a,b})P^{\rho_{a,b}}+o(P^{\frac12})\\ &= \mathcal{M}g(\tfrac12)P^{\frac12}(r_{\mathrm{an}}(E_{a,b})-\tfrac12)+\sum_{\rho_{a,b}\notin\mathbb{R}}\mathcal{M}g(\rho_{a,b})P^{\rho_{a,b}}+o(P^{\frac12}).\end{aligned}$$

We then obtain by summing over a and b against the weight w that Hypothesis 1.12 implies the estimate

$$P^{-\frac12}S(A,B;P) = \mathcal{M}g(\tfrac12)\sideset{}{^*}\sum_{a,b} w\left(\frac{a}{A},\frac{b}{B}\right)(r_{\mathrm{an}}(E_{a,b})-\tfrac12)+o(AB). \tag{41}$$

We now show that $S(A,B;P)$ is negligible compared to AB, from which it will follow that the average analytic rank is $\frac12$, by arguments analogous to the proof of Theorem 1.1. This is a direct adaptation of [Y, Lemma 5.2]. The two differences between the prime sum $P(E;\phi)$ and the inner sum in (40) is that the test function in the current paper is of the form $g(p/P)$, whereas the test function in [Y] is of the form $\phi(\log p/\log P)$, and the support of e^{-t} is not compact. For these reasons, one cannot apply directly [Y, Lemma 5.2]. Instead we follow the proof, and see that the end result is the bound $S(A,B;P)\ll(AB)^{1-\eta}$, for some $\eta>0$ which depends on the value of δ for which Hypothesis 1.12 .

In our situation, the sum over primes is an infinite sum. We could have chosen a smooth test function having compact support, however we preferred to be specific since anyway the exponentially-decaying weight makes the terms with $p\geq P^{1+\epsilon}$ negligible:

$$\sum_{(a,b)\neq(0,0)} w\left(\frac{a}{A},\frac{b}{B}\right)\sum_{p\geq P^{1+\epsilon}}\frac{a_p(E_{a,b})\log p}{\sqrt{p}}e^{-p/P}\ll ABe^{-P^{\epsilon}}\ll_N X^{-N}.$$

Here the sum is over $a, b \geq 0$, not both zero. We will first bound this sum, and then argue as in [Y, Section 5.6] to bound $S(A, B; P)$.

The analogue of [Y, (14)] clearly follows from [Y, (15)]. In [Y, (20)], we need to replace $F(u, v)$ by

$$F(u,v) = \left(\frac{v}{P}\right)^{-\frac{3}{2}} g\left(\frac{ud_0}{H}, \frac{k}{K}, \frac{v}{V}\right) \widehat{w}\left(\frac{ud_0A}{v}, \frac{kB}{v}\right) e^{-v/P}.$$

The conditions of [Y, Lemma 5.7] are satisfied in a very analogous way. Indeed taking partial derivatives of $e^{-v/P}$ in v multiplies this quantity by P^{-1}. Moreover, $F(u, v)$ and its partial derivatives are exponentially small in X for $v > P^{1+\epsilon}$, and are bounded in a similar way as in [Y] in the range $v \leq P^{1+\epsilon}$. Also, [Y, Lemma 5.7] does not have a restriction on the support of $F(u, v)$, and therefore applies to our situation, that is we have the analogue of [Y, Corollary 5.3].

Having bounded the sum over primes, which was the only difference between our situation and that of [Y], we now look at Cases 1-4 in [Y]. Cases 1-3 depend only on [Y, (15)] and [Y, Corollary 5.3], and thus the proof remains identical. In Case 4 we can clearly restrict to dyadic intervals $Q < p \leq 2Q$ with $Q \leq P^{1+\epsilon}$. [Y, Lemma 5.4] then applies, from which the analogue of [Y, Corollary 5.5] follows. The sum over primes is now treated, and thus the rest of the proof is identical.

We conclude that

$$\sum_{(a,b)\neq(0,0)} w\left(\frac{a}{A}, \frac{b}{B}\right) \sum_p \frac{a_p(E_{a,b}) \log p}{\sqrt{p}} e^{-p/P} \ll (AB)^{1-\eta},$$

for some $\eta > 0$. The arguments of [Y, Section 5.6] then show that the following bound holds by similar arguments:

$$S(A, B; P) = o(AB).$$

Combining this with (41) and using the estimate $W(A, B) \asymp AB$, we deduce that the average analytic rank of the elliptic curves $E_{a,b}$ is exactly $\frac{1}{2}$. □

6. An upper bound on the algebraic rank of elliptic curves in families of quadratic twists

In this section we give an upper bound on the algebraic rank of the elliptic curve (over $\mathbb{Q}$)

$$E_d : dy^2 = x^3 + ax + b$$

which depends only on E. This was pointed out to me by Silverman. The bound in question is $r_{\mathrm{al}}(E_d) \leq 18\omega(d) + O_E(1)$, and consequently $r_{\mathrm{al}}(E_d) \ll_E \log\log d$ for almost all d. Note that for most d, this is sharper than Mestre's conditional bound on the analytic rank $r_{\mathrm{an}}(E_d) \ll_E \log d/\log\log d$.

Lemma 6.1. *Fix an elliptic curve E over $\mathbb{Q}$, and consider the quadratic twists E_d. Then one has the bound*

$$r_{al}(E_d) \leq 18\omega(d) + O_E(1).$$

Proof. Denote by $E[2]$ the 2-torsion of E (over $\mathbb{C}$), and let $K = \mathbb{Q}(E[2])$, which is a finite Galois extension of $\mathbb{Q}$ (since E is smooth). Considered as an elliptic curve over K, E satisfies the condition $E[2] \subset E(K)$. This condition is then automatically satisfied for all quadratic twists E_d (that is $E[2] \subset E_d(K)$), since a direct calculation shows that for $d \neq 0$, $\mathbb{Q}(E_d[2]) = \mathbb{Q}(E[2])$.

We will bound the rank of $E_d(K)$, which will be sufficient for our purposes since it gives an upper bound on the rank of $E_d(\mathbb{Q})$. Moreover, since $E_d(K) \simeq \mathbb{Z}^{r_{\mathrm{al}}(E_d(K))} \oplus E_d(K)_{\mathrm{tors}}$, it follows that $2^{r_{\mathrm{al}}(E_d(K))}$ is bounded above by the cardinality of $E_d(K)/2E_d(K)$. As for this last quantity, [Si, Exercise 8.1]) gives the bound

$$\#E_d(K)/2E_d(K) \leq 2^{2\#\{\mathfrak{p}\subset\mathcal{O}_K : E_d \text{ has bad reduction at } \mathfrak{p}\}+c_K} \leq 2^{2\omega(d^2N_E)[K:\mathbb{Q}]+c_K},$$

since the conductor of E_d divides d^2N_E. Notice that the constant c_K depends on the class number of K, and thus the fact that the base field K is independent of d is crucial in this proof. The splitting field of a cubic polynomial over $\mathbb{Q}$ has degree at most 9, and hence the result follows since K depends only on E.

□

We now deduce the result on the average algebraic rank.

Proof of Theorem 1.10. In a similar way to the proof of Theorem 1.1 and Theorem 1.7, our hypotheses imply that

$$\sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right)\left(r_{\mathrm{an}}(E_d) - \frac{1}{2}\right) = o\left(\frac{D}{\log\log D}\right).$$

Note that no hypothesis on symmetric power L-functions of E is needed, since we are not seeking a power-savings in the error term. Arguing as in the proof of Corollary 1.2, this implies the bound

$$\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1\\r_{\mathrm{an}}(E_d)\geq 2}} 1 = o\left(\frac{D}{\log\log D}\right).$$

The same bound holds for the algebraic rank by the work of Gross and Zagier [GZ] and Kolyvagin [Ko], and applying Lemma 5.1 we obtain

$$\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1\\r_{\mathrm{al}}(E_d)=0}} 1 = \frac{N(D)}{2} + o\left(\frac{D}{\log\log D}\right), \qquad \sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1\\r_{\mathrm{al}}(E_d)=1}} 1 = \frac{N(D)}{2} + o\left(\frac{D}{\log\log D}\right). \tag{42}$$

We now apply Hölder's Inequality and Lemma 6.1 to bound the average algebraic rank. Selecting $p = (1-\lfloor\log\log\log D\rfloor^{-1})^{-1} > 1$ and $q = (1-p^{-1})^{-1} = \lfloor\log\log\log D\rfloor$, we obtain that for any $\epsilon > 0$,

$$\begin{aligned}\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1\\r_{\mathrm{al}}(E_d)\geq 2}} r_{\mathrm{al}}(E_d) &\leq \Bigg(\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1\\r_{\mathrm{al}}(E_d)\geq 2}} 1\Bigg)^{\frac{1}{p}} \Bigg(\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1\\r_{\mathrm{al}}(E_d)\geq 2}} r_{\mathrm{al}}(E_d)^q\Bigg)^{\frac{1}{q}} \\ &\ll_{\epsilon,E} \left(\epsilon\frac{D}{\log\log D}\right)^{\frac{1}{p}} \Bigg(\sideset{}{^*}\sum_{\substack{0<|d|\leq D\\(d,N_E)=1}} (18+O_E(1))^q\omega(d)^q\Bigg)^{\frac{1}{q}}.\end{aligned} \tag{43}$$

The centered moments of $\omega(n)$ are estimated uniformly in [GS, Theorem 1]. This translates to a bound on the $q-$th moment as follows, for D large enough:

$$\begin{aligned}\sum_{d\le D}\omega(d)^q &= \sum_{j=0}^{q}\binom{q}{j}(\log\log D)^{q-j}\sum_{d\le D}(\omega(d)-\log\log D)^j\\ &\le 2D\sum_{j=0}^{q}\binom{q}{j}(\log\log D)^{q-\frac{j}{2}}\frac{\Gamma(j+1)}{2^{\frac{j}{2}}\Gamma(j/2+1)}\\ &\le 2D(\log\log D)^q\Big(1+\sum_{j=1}^{q}\frac{q^j}{j!}(\log\log D)^{-\frac{j}{2}}j^{\frac{j}{2}+1}\Big)\\ &\le 2D(\log\log D)^q\Big(1+\frac{q}{(\log\log D)^{\frac12}}+(e^{q^2(\log\log D)^{-\frac12}}-1)\Big)\\ &= 2D(\log\log D)^q(1+o(1)),\end{aligned}$$

since $q=\lfloor\log\log\log D\rfloor$. We obtain that (43) is

$$\ll_E \epsilon^{\frac12}D^{\frac1p}(\log\log D)^{-\frac1p}\big(3D(\log\log D)^q\big)^{\frac1q}\le 3\epsilon^{\frac12}D(\log\log D)^{\frac{1}{\lfloor\log\log\log D\rfloor}}\le 4e\epsilon^{\frac12}D.$$

Taking ϵ arbitrarily small and using (42), we obtain

$$\sideset{}{^*}\sum_{\substack{0<|d|\le D\\(d,N_E)=1}} r_{\mathrm{al}}(E_d)=\frac{N(D)}{2}+o(D)\sim\frac{N(D)}{2},$$

since $N(D)\asymp_E D$.

□

Appendix A. The distribution of $S(D;P)$

In this section we expand on the probabilistic study of $S(D;P)$. Before this, we show that the families of L-functions we are considering have a bounded number of repetitions.

Lemma A.1. *Fix E an elliptic curve over $\mathbb{Q}$. There exists an absolute constant C (see* [M, Theorem 5] *for the explicit value) such that at most C minimal Weierstrass Equations have the property that the L-functions of the associated elliptic curves match that of E.*

Proof. Let $y^2=x^3+ax+b$ be the minimal Weierstrass Equation of E. It is a well known fact that two elliptic curves with distinct minimal Weierstrass equations are not isomorphic (see for instance [Si, Section III]).

If two elliptic curves E' and E'' are isogenous, then their reductions have the same number of points and thus their L-functions are identical (see for instance [Kn, Theorem 11.67]). Conversely, if $L(E',s)=L(E'',s)$, then the reductions of these elliptic curves have the same number of local points, and thus their Frobenius elements have the same characteristic polynomial. It follows that their Tate Modules are isomorphic. The Isogeny Theorem, which follows from Falting's work [Fa], then implies that E' and E'' are isogenous.

It follows that $L(E',s)=L(E'',s)$ if and only if E' and E'' are isogenous. However Mazur proved [M, Theorem 5] that at most C isomorphism classes of elliptic curves are isogenous to a fixed curve E, for some absolute constant C. This concludes the proof.

□

We now give a probabilistic argument which supports (4). We will divide the left hand side of (4) by $x^{\frac{1}{2}}$ and put $x=e^y$, ending up in the quantity

$$T(D;y) := \sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right) \sum_{\rho_d \notin \mathbb{R}} \frac{e^{y(\rho_d-1/2)}}{\rho_d(\rho_d+1)}.$$

Our goal is to give arguments in favor of the bound $T(D;e^y) \ll_\epsilon D^{\frac{1}{2}+\epsilon}$. An important assumption is the following:

Hypothesis BM. The multiset $Z_E = \{\Im(\rho) \neq 0 : L(\rho, f_{E_d}) = 0, d \neq 0 \text{ is squarefree}\}$ has bounded multiplicity.[11]

We will see that under ECRH and BM, $T(D;y)$ has variance $\asymp D \log D$. It follows that $T(D;y)$ is normally $\ll_\epsilon D^{\frac{1}{2}+\epsilon}$, which justifies (4), as well as Hypothesis M and Hypothesis M(δ,η) for all $0<\eta<\frac{1}{2}$.

Proposition A.2. *Assume ECRH. Then $T(D;y)$ has a limiting distribution μ_D as $y \to \infty$. If we moreover assume BM, then the first two moments of this distribution satisfy*

$$\int_{\mathbb{R}} t d\mu_D(t) = 0 \qquad \int_{\mathbb{R}} t^2 d\mu_D(t) \asymp_E D \log D.$$

Proof. Hypothesis ECRH implies that $T(D;y)$ is a Besicovitch B^2 almost-periodic function of the form

$$T(D;y) = \sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right) \sum_{\gamma_d \neq 0} \frac{e^{iy\gamma_d}}{\rho_d(\rho_d+1)}.$$

The existence of the limiting distribution follows from [ANS]. To compute the first two moments of μ_D, we follow the arguments of [Fi]. As in [Fi, Lemma 2.5], ECRH implies that for $k \geq 1$,

$$\int_{\mathbb{R}} t^k d\mu_D(t) = \lim_{Y \to \infty} \frac{1}{Y} \int_2^Y T(D;y)^k dy.$$

The claim on the first moment follows from the fact that

$$\frac{1}{Y}\int_2^Y T(D;y)dy = \frac{1}{Y} \sideset{}{^*}\sum_{(d,N_E)=1} w\left(\frac{d}{D}\right) \sum_{\gamma_d \neq 0} \frac{e^{iy\gamma_d}}{i\gamma_d\rho_d(\rho_d+1)}\Bigg|_2^Y \ll_{E,D} \frac{1}{Y}.$$

For the variance we will apply Parseval's Identity for Besicovitch almost-periodic functions. Let W_E be the set Z_E without multiplicities. We have

$$T(D;y) = \sum_{\gamma \in W_E} \frac{e^{iy\gamma}}{(\frac{1}{2}+i\gamma)(\frac{3}{2}+i\gamma)} c_\gamma,$$

where c_γ is defined by the formula

$$c_\gamma := \sideset{}{^*}\sum_{\substack{d \neq 0 \\ (d,N_E)=1 \\ \exists \gamma_d = \gamma}} w\left(\frac{d}{D}\right) m_{\gamma_d},$$

[11] By this we mean that there exists an absolute constant C such that each element of E has multiplicity at most C.

with m_{γ_d} the multiplicity of $\frac{1}{2}+i\gamma_d$ as a zero of $L(s,f_{E_d})$. Parseval's Identity then reads

$$V_D := \int_{\mathbb{R}} t^2 d\mu_D(t) = \sum_{\gamma\in W_E} \frac{c_\gamma^2}{|\frac{1}{2}+i\gamma|^2|\frac{3}{2}+i\gamma|^2}.$$

We first give a lower bound on V_D. We have:

$$V_D \gg \sum_{\substack{\gamma\in W_E\\ |\gamma|\le 1}} c_\gamma^2 \ge \sum_{\substack{\gamma\in W_E\\ |\gamma|\le 1}} \sideset{}{^*}\sum_{\substack{d\neq 0\\ (d,N_E)=1\\ \exists\gamma_d=\gamma}} w\left(\frac{d}{D}\right)^2 \ge \sideset{}{^*}\sum_{\substack{d\neq 0\\ (d,N_E)=1}} w\left(\frac{d}{D}\right)^2 \sum_{\substack{\gamma_d\\ |\gamma_d|\le 1}} 1 \asymp_E D\log D.$$

As for the upper bound, we compute using Hypothesis BM:

$$\begin{aligned} V_D &\ll \sum_{\gamma\in W_E} \frac{1}{(\gamma+1)^4} \sideset{}{^*}\sum_{\substack{d_1,d_2\neq 0\\ (d_1d_2,N_E)=1\\ \exists\gamma_{d_1}=\gamma\\ \exists\gamma_{d_2}=\gamma}} w\left(\frac{d_1}{D}\right) w\left(\frac{d_2}{D}\right) \\ &\le \sideset{}{^*}\sum_{\substack{d_1\neq 0\\ (d_1,N_E)=1}} w\left(\frac{d_1}{D}\right) \sum_{\substack{\gamma\in W_E\\ \exists\gamma_{d_1}=\gamma}} \frac{1}{(\gamma+1)^4} \sideset{}{^*}\sum_{\substack{d_2\neq 0\\ (d_2,N_E)=1\\ L(E_{d_1},s)\text{ and }L(E_{d_2},s)\\ \text{have the common zero }\gamma}} w\left(\frac{d_2}{D}\right) \\ &\ll \sideset{}{^*}\sum_{\substack{d_1\neq 0\\ (d_1,N_E)=1}} w\left(\frac{d_1}{D}\right) \sum_{\substack{\gamma\in W_E\\ \exists\gamma_{d_1}=\gamma}} \frac{1}{(\gamma+1)^4} \\ &\ll \sideset{}{^*}\sum_{\substack{d_1\neq 0\\ (d_1,N_E)=1}} w\left(\frac{d_1}{D}\right) \sum_{\gamma_{d_1}} \frac{1}{(\gamma_{d_1}+1)^4} \asymp_E D\log D, \end{aligned}$$

from which the result follows. □

Acknowledgements

This work was supported by an NSERC Postdoctoral Fellowship, and was accomplished at the University of Michigan. I would like to thank Andrew Granville, Jeffrey Lagarias, James Maynard, James Parks, Kartik Prasanna, Ari Shnidman, Joseph Silverman, Anders Södergren and Matthew P. Young for their help and for inspiring conversations.

References

[ANS] Amir Akbary, Nathan Ng and Majid Shahabi, *Limiting distributions of the classical error terms of prime number theory*, arXiv:1306.1657.

[BKLPR] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra, Bjorn Poonen and Eric Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves.* arXiv:1304.3971 [math.NT]

[BS] Manjul Bhargava and Arul Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1.* arXiv:1312.7859 [math.NT]

[BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over Q: wild 3-adic exercises, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939

[B] Armand Brumer, *The average rank of elliptic curves. I.* Invent. Math. **109** (1992), no. 3, 445–472.

[CHT] L. Clozel, M. Harris and R. Taylor *Automorphy for some l-adic lifts of automorphic mod l representations.* Pub. Math. IHES **108** (2008), 1–181.

[CM] J. Cogdell, P. Michel, *On the complex moments of symmetric power L-functions at* $s = 1$. Int. Math. Res. Not. 2004, no. 31, 1561–1617.

[CKRS] J. B. Conrey, J. P. Keating, M. O. Rubinstein, N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions.* Number theory for the millennium, I (Urbana, IL, 2000), 301–315, A K Peters, Natick, MA, 2002.

[DW] C. Delaunay and M. Watkins, *The powers of logarithm for quadratic twists. In Ranks of elliptic curves and random matrix theory.* (J. B. Conrey, D. W. Farmer, F. Mezzadri and N. C. Snaith, ed.), London Mathematical Society Lecture Note Series, 341, 189–193, Cambridge University Press, Cambridge, 2007.

[Fa] Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73** (1983), no. 3, 349–366.

[Fi] Daniel Fiorilli, *Elliptic curves of unbounded rank and Chebyshev's Bias.* To appear, IMRN.

[FPS] Daniel Fiorilli, James Parks and Anders Södergren, *Low-lying zeros of elliptic curve L-functions: Beyond the Ratios Conjecture.* In preparation.

[GJ] S. Gelbart and H. Jacquet, *A relation between automorphic representations of GL(2) and GL(3).* Ann. Sci. École Norm. Sup. (4) **11** (1978), no. 4, 471–542.

[G] Dorian Goldfeld, *Conjectures on elliptic curves over quadratic fields.* Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), pp. 108–118, Lecture Notes in Math., 751, Springer, Berlin, 1979.

[GHL] Dorian Goldfeld, Jeffrey Hoffstein and Paul Lockhart, *Appendix to: Coefficients of Maass forms and the Siegel zero.* Ann. of Math. (2) **140** (1994), no. 1, 161–181.

[GS] Andrew Granville and Kannan Soundararajan, *Sieving and the Erdös-Kac theorem.* Equidistribution in number theory, an introduction, 15–27, NATO Sci. Ser. II Math. Phys. Chem., 237, Springer, Dordrecht, 2007.

[GV] Dorian Goldfeld and Carlo Viola, *Mean values of L-functions associated to elliptic, Fermat and other curves at the centre of the critical strip.* J. Number Theory **11** (1979), no. 3 S. Chowla Anniversary Issue, 305–320.

[GZ] Benedict H. Gross; Don B. Zagier, *Heegner points and derivatives of L-series.* Invent. Math. **84** (1986), no. 2, 225–320.

[HST] M. Harris, N. Shepherd-Barron and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy.* Ann. of Math. **171** (2010), 779–813.

[HB] D. R. Heath-Brown, *The average analytic rank of elliptic curves.* Duke Math. J. **122** (2004), no. 3, 591–623.

[I1] Henryk Iwaniec, *On the order of vanishing of modular L-functions at the critical point.* Sém. Théor. Nombres Bordeaux (2) **2** (1990), no. 2, 365–376.

[I2] Henryk Iwaniec, *Topics in classical automorphic forms.* Graduate Studies in Mathematics, 17. American Mathematical Society, Providence, RI, 1997. xii+259 pp. ISBN: 0-8218-0777-3

[IK] H. Iwaniec, E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004.

[KaS] N. M. Katz, P. Sarnak, *Zeroes of Zeta Functions, their Spaces and their Spectral Nature.* Preprint (1997).

[Ki] H. H. Kim, *Functoriality for the exterior square of GL4 and the symmetric fourth of* GL_2*. With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak.* J. Amer. Math. Soc. **16** (2003), no. 1, 139–183.

[KiS1] H. H. Kim and F. Shahidi, *Cuspidality of symmetric powers with applications.* Duke Math. J. **112** (2002), no. 1, 177–197.

[KiS2] H. H. Kim and F. Shahidi, *Functorial products for* $GL_2 \times GL_3$ *and the symmetric cube for* GL_2*. With an appendix by C. J. Bushnell and G. Henniart.* Ann. of Math. (2) **155** (2002), no. 3, 837–893.

[Ko] V. A. Kolyvagin, *Euler systems.* The Grothendieck Festschrift, Vol.II, 435–483, Progr.Math., 87, Birkhäuser Boston, Boston, MA, 1990.

[Kn] Anthony W. Knapp, *Elliptic curves.* Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992. xvi+427 pp. ISBN: 0-691-08559-5.

[M] Barry Mazur, *Rational isogenies of prime degree.* (with an appendix by D. Goldfeld). Invent. Math. **44** (1978), no. 2, 129–162.

[Sh] Goro Shimura, *On the holomorphy of certain Dirichlet series.* Proc. London Math. Soc. (3) **31** (1975), no. 1, 79–98.

[Si] Joseph H. Silverman, *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp. ISBN: 978-0-387-09493-9

[T] Richard Taylor, *Automorphy for some ℓ-adic lifts of automorphic mod l representations. II.* Pub. Math. IHES **108** (2008), 183–239.

[TW] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[Wi] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Y] Matthew P. Young, *Low-lying zeros of families of elliptic curves.* J. Amer. Math. Soc. **19** (2006), no. 1, 205–250.

Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor MI 48109 USA

E-mail address: `fiorilli@umich.edu`