MATHEMATICS OF COMPUTATION
Volume 92, Number 339, January 2023, Pages 385–408
https://doi.org/10.1090/mcom/3773
Article electronically published on September 12, 2022

FROM THE BIRCH AND SWINNERTON-DYER CONJECTURE TO NAGAO'S CONJECTURE

SEOYOUNG KIM AND M. RAM MURTY,
WITH AN APPENDIX BY ANDREW V. SUTHERLAND

ABSTRACT. Let E be an elliptic curve over $\mathbb{Q}$ with discriminant Δ_E. For primes p of good reduction, let N_p be the number of points modulo p and write $N_p = p + 1 - a_p$. In 1965, Birch and Swinnerton-Dyer formulated a conjecture which implies

$$\lim_{x\to\infty} \frac{1}{\log x} \sum_{\substack{p\le x \\ p\nmid \Delta_E}} \frac{a_p \log p}{p} = -r + \frac{1}{2},$$

where r is the order of the zero of the L-function $L_E(s)$ of E at $s = 1$, which is predicted to be the Mordell-Weil rank of $E(\mathbb{Q})$. We show that if the above limit exits, then the limit equals $-r + 1/2$. We also relate this to Nagao's conjecture. This paper also includes an appendix by Andrew V. Sutherland which gives evidence for the convergence of the above-mentioned limit.

1. INTRODUCTION

Let E be an elliptic curve over $\mathbb{Q}$ with discriminant Δ_E and conductor N_E. For each prime $p \nmid \Delta_E$, we write the number of points of $E \pmod p$ as

$$N_p := \#E(\mathbb{F}_p) = p + 1 - a_p, \tag{1.1}$$

where a_p satisfies Hasse's inequality $|a_p| \le 2\sqrt{p}$. For $p \mid \Delta_E$, we define $a_p = 0$ if E has additive reduction at p, $a_p = 1$ if E has split multiplicative reduction at p, and $a_p = -1$ if E has non-split multiplicative reduction at p (for precise definitions of this terminology, we refer the reader to [16, p. 449]).

The L-function attached to E, denoted as $L_E(s)$, is then defined as an Euler product:

$$L_E(s) = \prod_{p\mid\Delta_E} \left(1 - \frac{a_p}{p^s}\right)^{-1} \prod_{p\nmid\Delta_E} \left(1 - \frac{a_p}{p^s} + \frac{p}{p^{2s}}\right)^{-1}, \tag{1.2}$$

which converges absolutely for $\mathrm{Re}(s) > 3/2$ by virtue of Hasse's inequality. Moreover, the Euler product shows that $L_E(s)$ does not vanish for $\mathrm{Re}(s) > 3/2$. Expanding the Euler product into a Dirichlet series, we write

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}. \tag{1.3}$$

Received by the editor November 6, 2021, and, in revised form, May 19, 2022, and June 12, 2022.

2020 *Mathematics Subject Classification.* Primary: 11G40; Secondary: 14G10, 14D10, 14H52.

The first author was partially supported by a Coleman Postdoctoral Fellowship. The second author was partially supported by NSERC Discovery grant.

Dedicated to the memory of Professor John H. Coates.

If we write α_p, β_p as the eigenvalues of the Frobenius morphism at p, for $p \nmid \Delta_E$, we can write $a_p = \alpha_p + \beta_p$, and our L-function can be re-written as

$$L_E(s) = \prod_{p|\Delta_E} \left(1 - \frac{a_p}{p^s}\right)^{-1} \prod_{p\nmid\Delta_E} \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1}, \tag{1.4}$$

and by Hasse's inequality $|\alpha_p| = |\beta_p| = \sqrt{p}$.

By the elliptic modularity theorem (formerly the Taniyama conjecture) for semistable elliptic curves over $\mathbb{Q}$ by Wiles [21], and its complete extension to all elliptic curves over $\mathbb{Q}$ by Breuil, Conrad, Diamond, and Taylor [1], $L_E(s)$ extends to an entire function and satisfies a functional equation which relates $L_E(s)$ to $L_E(2-s)$. More precisely, if we define

$$\Lambda_E(s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s), \tag{1.5}$$

then $\Lambda_E(s)$ is entire and satisfies the following functional equation:

$$\Lambda_E(s) = w_E\Lambda_E(2-s), \tag{1.6}$$

where $w_E \in \{1, -1\}$ is the root number of E. As $L_E(s) \neq 0$ for $\mathrm{Re}(s) > 3/2$, the same is true for $\Lambda_E(s)$. Since $\Gamma(s)$ has simple poles at $s = 0, -1, \ldots$, we see that $L_E(s)$ has "trivial zeros" at $s = 0, -1, \ldots$. These zeros are simple by virtue of the functional equation and the non-vanishng of $L_E(s)$ for $\mathrm{Re}(s) > 3/2$. Thus, for $m = 0, 1, 2, \cdots$, we have

$$1 = \operatorname*{Res}_{s=-m} \frac{L_E'(s)}{L_E(s)} = \operatorname*{Res}_{s=-m} \left[\frac{\Lambda_E'(s)}{\Lambda_E(s)} - \frac{\Gamma'(s)}{\Gamma(s)}\right]. \tag{1.7}$$

This summarises our report on E from the analytic perspective.

From the algebraic perspective, a celebrated theorem of Mordell states that the group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group with rank r_M. In 1965, Birch and Swinnerton-Dyer [2] conjectured that $L_E(s)$ has a zero of order r_M at $s = 1$. In other words, the algebraic rank r_M equals the "analytic rank" which is the order of zero at $s = 1$ of $L_E(s)$. This conjecture is often referred to as the Birch and Swinnerton-Dyer conjecture. The first step towards this conjecture was taken by Coates and Wiles in 1977 when they studied the CM case.

However, before they formulated this conjecture in this form, Birch and Swinnerton-Dyer stated a stronger conjecture motivated by a heuristic "local-global" principle: the rank should be reflected by "modulo p" information for many primes p. More precisely, they conjectured that there is a constant C_E such that

$$\prod_{\substack{p<x \\ p\nmid\Delta_E}} \frac{N_p}{p} \sim C_E(\log x)^r, \tag{1.8}$$

as $x \to \infty$. We refer to this as the original Birch and Swinnerton-Dyer conjecture (or OBSD for short).

Several authors have noted the "severity" of this conjecture in that it implies the analog of the Riemann hypothesis for $L_E(s)$, and much more. This was first announced by Goldfeld [7]. Kuo and Murty [8, Theorem 2, Theorem 3], and K. Conrad [3, Theorem 1.3] independently noticed that (1.8) goes well beyond the analog of the Riemann hypothesis for $L_E(s)$. They proved that (1.8) is true if and

only if

$$\sum_{\substack{p^k \le x \\ p \nmid \Delta_E}} \frac{\alpha_p^k + \beta_p^k}{k} = o(x), \tag{1.9}$$

as $x \to \infty$, or equivalently

$$\sum_{\substack{p^k \le x \\ p \nmid \Delta_E}} (\alpha_p^k + \beta_p^k) \log p = o(x \log x), \tag{1.10}$$

as $x \to \infty$, whereas, the Riemann hypothesis for $L_E(s)$ is equivalent to the weaker assertion

$$\sum_{\substack{p^k \le x \\ p \nmid \Delta_E}} (\alpha_p^k + \beta_p^k) \log p = \mathcal{O}(x(\log x)^2), \tag{1.11}$$

as $x \to \infty$.

If we return to the heuristic "local-global" principle that perhaps motivated Birch and Swinnerton-Dyer to make their OBSD conjecture, we are led to formulate several gradations of their conjecture.

The first is that (1.8) is equivalent to

$$\sum_{\substack{p^k \le x \\ p \nmid \Delta_E}} \frac{\alpha_p^k + \beta_p^k}{kp^k} = -r \log\log x + A + o(1), \tag{1.12}$$

for some constant A, as $x \to \infty$. If we weight each prime power p^k by $\log p$ (following Chebysheff), we have that (1.8) implies via partial summation that

$$\sum_{\substack{p^k \le x \\ p \nmid \Delta_E}} \frac{\alpha_p^k + \beta_p^k}{kp^k} \log p = -r \log x + o(\log x), \tag{1.13}$$

which already implies the analog of the Riemann hypothesis for $L_E(s)$ and still leads to an analytic determination of the rank r using the "local" data a_p. The error term in (1.13) cannot be $\mathcal{O}(1)$ as will be shown in section 4.

There are good reasons to believe that (1.11) is not the optimal estimate. Montgomery [10] and Gallagher [6] have suggested in the context of the Riemann zeta function (but here applied to our context) that the error in (1.11) should be

$$\mathcal{O}(x(\log\log\log x)^2) \tag{1.14}$$

or even the "weaker" $\mathcal{O}(x(\log\log x)^2)$.

In either case, it is conceivable that OBSD is true, even though it goes well beyond the analog of the Riemann hypothesis for $L_E(s)$.

The purpose of this note is to show that if the limit

$$\lim_{x\to\infty} \frac{1}{\log x} \sum_{\substack{p^k \le x \\ p \nmid \Delta_E}} \frac{\alpha_p^k + \beta_p^k}{kp^k} \log p \tag{1.15}$$

exists, then the limit is $-r$. Moreover, this implies that if the limit

$$\lim_{x\to\infty} \frac{1}{\log x} \sum_{p<x} \frac{a_p \log p}{p} \tag{1.16}$$

exists, then the Riemann hypothesis for $L_E(s)$ is true, and the limit is $-r + 1/2$. We apply a technique of Cramér [4] to prove our theorem. We also relate the limit (1.16) to a conjecture of Nagao to formulate a conjecture which links the rank of an elliptic curve over $\mathbb{Q}(T)$ to its fibral elliptic curves (defined using the specialization).

In an appendix by Sutherland, we tabulate some numerical evidence that suggests the limit (1.16) always exists and equals our conjectured value. We respectfully dedicate this paper to Professor John H. Coates. Professor Coates asked the senior author back in 1989 if one can determine the rank effectively from a knowledge of the coefficients a_p alone. This paper is a partial answer to that question.

2. Preliminaries

For an elliptic curve E defined over $\mathbb{Q}$ with discriminant Δ_E and conductor N_E, we defined its L-function $L_E(s)$ in (1.2). Hence, we can write its logarithmic derivative as

$$-\frac{L_E'(s)}{L_E(s)} = \sum_{n=1}^{\infty} \frac{c_n \Lambda(n)}{n^s}, \tag{2.1}$$

where $\Lambda(n)$ is the von Mangoldt function, and

$$c_n = \begin{cases} \alpha_p^m + \beta_p^m, & \text{if } n = p^m \text{ and } p \nmid N, \\ a_p^m, & \text{if } n = p^m \text{ and } p \mid N, \\ 0, & \text{otherwise.} \end{cases} \tag{2.2}$$

Our first goal will be to derive a truncated explicit formula for

$$\sum_{n \le x} c_n \Lambda(n)$$

in terms of the non-trivial zeros of $L_E(s)$. The method for deriving this is standard (see for example, chapter 7 of [12]) where all the technical details are given in living colour. However, we will highlight the salient steps of the method. An important role is played by the following result which is of independent interest.

Proposition 1. *If x is not an integer, then*

$$\sum_{\frac{1}{2}x < n < 2x} \left| \log \frac{x}{n} \right|^{-1} = \mathcal{O}\left(\frac{x \log x}{\|x\|} \right),$$

where $\|x\|$ is the distance of x to the nearest integer and the sum is over natural numbers n lying in the interval $(\frac{1}{2}x, 2x)$.

Proof. This is contained in Exercise 7.2.2 of [12]. □

We will also need an asymptotic formula for the number $N_E(T)$ of non-trivial zeros ρ of $L_E(s)$ with $|\mathrm{Im}(\rho)| < T$. A very general result of Selberg [15] can be specialized to our context. We record it below.

Proposition 2. *Let $N_E(T)$ be the number of zeros $\rho = \beta + i\gamma$ of $L_E(s)$ satisfying $0 < \gamma \le T$. Then*

$$N_E(T) = \frac{T}{\pi}(\log T + c) + \mathcal{O}(\log T), \tag{2.3}$$

where c is a constant which depends only on E.

We apply the previous proposition to estimate the following sums over non-trivial zeros of $L_E(s)$:

Proposition 3. *We have*

$$\sum_{|\gamma|<R} \frac{1}{|\rho|} = \mathcal{O}(\log^2 R),$$

and for any $\alpha > 1$, we have

$$\sum_{\rho} \frac{1}{|\rho|^\alpha} < \infty,$$

where the sums are over non-trivial zeros of $L_E(s)$.

Proof. By partial summation, the sum on the left hand side is dominated by

$$\ll \int_1^R \frac{N_E(t)}{t^2} dt \ll \int_1^R \frac{\log t}{t} dt \ll \log^2 R.$$

The second assertion also follows from partial summation and the convergence of the integral

$$\int_1^\infty \frac{\log t}{t^\alpha} dt.$$

□

3. The truncated explicit formula

We will now derive a truncated explicit formula alluded to in the previous section. Let $\mathcal{C}$ be the (oriented) rectangle with vertices $c - iR, c + iR, -U + iR, -U - iR$, and its edges denoted by I_1, I_2, I_3, and I_4 respectively, with $c = 2$ (R is chosen so that it is not the ordinate of a zero of $L_E(s)$, see [12, Ex. 7.2.5]) and U a positive non-integral number. We have by the Cauchy residue theorem,

$$\frac{1}{2\pi i} \int_{\mathcal{C}} -\frac{L_E'(s)}{L_E(s)} \frac{x^s}{s} ds = -\sum_{|\gamma|<R} n_\rho \frac{x^\rho}{\rho} - \sum_{m<U} \operatorname*{Res}_{s=-m} \left[\frac{L_E'(s)}{L_E(s)} \frac{x^s}{s} \right], \tag{3.1}$$

where the first sum is over all non-trivial zeros $\rho = \beta + i\gamma$ of $L_E(s)$, and n_ρ is the multiplicity of each ρ. The second sum is the contribution from the trivial zeros. Separating $m = 0$ and $m \geq 1$ in the second sum, and computing the residue for the term $m = 0$, we find

$$\frac{1}{2\pi i} \int_{\mathcal{C}} -\frac{L_E'(s)}{L_E(s)} \frac{x^s}{s} ds = -\sum_{|\gamma|<R} n_\rho \frac{x^\rho}{\rho} + \sum_{1 \leq m < U} \frac{x^{-m}}{m} - \log x. \tag{3.2}$$

On the other hand, for x not an integer, we have by the truncated Perron's formula (see Theorem 4.1.4 as well as Exercise 4.4.15 of [12]):

(3.3)

$$\sum_{n \leq x} c_n \Lambda(n) = \frac{1}{2\pi i} \int_{2-iR}^{2+iR} -\frac{L_E'(s)}{L_E(s)} \frac{x^s}{s} ds + \mathcal{O}\left(\sum_{n=1}^{\infty} \left(\frac{x}{n}\right)^2 |c_n \Lambda(n)| \cdot \min\left(1, \frac{1}{R|\log \frac{x}{n}|}\right)\right).$$

Injecting information from (3.2) for the integral on the right hand side, we get

(3.4)
$$\sum_{n\le x} c_n\Lambda(n) = -\sum_{|\gamma|<R} n_\rho \frac{x^\rho}{\rho} + \sum_{1\le m<U} \frac{x^{-m}}{m} - \log x + \frac{1}{2\pi i}\int_{C\setminus I_1} \frac{L_E'(s)}{L_E(s)}\frac{x^s}{s}ds$$

$$+\mathcal{O}\left(\sum_{n=1}^{\infty}\left(\frac{x}{n}\right)^2 |c_n\Lambda(n)|\cdot\min\left(1,\frac{1}{R|\log\frac{x}{n}|}\right)\right), \tag{3.5}$$

$$= -\sum_{|\gamma|<R} n_\rho\frac{x^\rho}{\rho} + \sum_{1\le m<U}\frac{x^{-m}}{m} - \log x + \frac{1}{2\pi i}\int_{C\setminus I_1}\frac{L_E'(s)}{L_E(s)}\frac{x^s}{s}ds + E(x,U,R), \text{ (say)} \tag{3.6}$$

where the first sum is over all non-trivial zeros $\rho=\beta+i\gamma$ of $L_E(s)$ (note that $\beta=1$ under the Riemann hypothesis for $L_E(s)$), and n_ρ is the multiplicity of each ρ. We note that $E(x,U,R)$ is the error term arising from the last term in (3.5). We first estimate the error term in (3.5) and (3.6):

$$E(x,U,R) = \mathcal{O}\left(\sum_{n=1}^{\infty}\left(\frac{x}{n}\right)^2 |c_n\Lambda(n)|\cdot\min\left(1,\frac{1}{R|\log\frac{x}{n}|}\right)\right).$$

We consider the following three parts of the sum in $E(x,U,R)$ separately:

$$\left(\sum_{n<x/2} + \sum_{x/2<n<2x} + \sum_{n>2x}\right)\left(\frac{x}{n}\right)^2 |c_n\Lambda(n)|\cdot\min\left(1,\frac{1}{R|\log\frac{x}{n}|}\right). \tag{3.7}$$

The first sum is for $n<x/2$, and hence we have $\log(x/n)>\log 2$, and

$$\sum_{n<x/2}\left(\frac{x}{n}\right)^2 |c_n\Lambda(n)|\cdot\min\left(1,\frac{1}{R|\log\frac{x}{n}|}\right) = \mathcal{O}\left(\frac{x^2}{R}\sum_{n<x/2}\frac{|c_n\Lambda(n)|}{n^2}\right) = \mathcal{O}\left(\frac{x^2}{R}\right), \tag{3.8}$$

for big enough R. Similarly, for the third sum of (3.7), the condition $n>2x$ implies $|\log(x/n)|>\log 2$, and hence

$$\sum_{n>2x}\left(\frac{x}{n}\right)^2 |c_n\Lambda(n)|\cdot\min\left(1,\frac{1}{R|\log\frac{x}{n}|}\right) = \mathcal{O}\left(\frac{x^2}{R}\right). \tag{3.9}$$

Now, it remains to compute the second sum of (3.7)

$$\sum_{x/2<n<2x}\left(\frac{x}{n}\right)^2 |c_n\Lambda(n)|\cdot\min\left(1,\frac{1}{R|\log\frac{x}{n}|}\right).$$

We observe that $x/2<n<2x$ implies that x/n is bounded and $c_n\Lambda(n)=\mathcal{O}(x^{1/2}\log x)$ for n in this range. Choosing $x=N+1/2$, an integer plus half, we see that $\|x\|=1/2$ and so, an application of Proposition 1 gives the result

$$\sum_{x/2<n<2x}\left(\frac{x}{n}\right)^2 |c_n\Lambda(n)|\cdot\min\left(1,\frac{1}{R|\log\frac{x}{n}|}\right) = \mathcal{O}\left(\frac{2x\sqrt{x}(\log x)^2}{R}\right). \tag{3.10}$$

In conclusion, we obtain from (3.8), (3.9), and (3.10),

$$E(x,U,R) = \mathcal{O}\left(\frac{x^2}{R}\right),$$

for $x=N+1/2$ (as above). The third term in (3.6)

$$\frac{1}{2\pi i}\int_{C\setminus I_1}\frac{L_E'(s)}{L_E(s)}\frac{x^s}{s}ds \tag{3.11}$$

can be estimated with the usual method (see, for example, [12, Ex. 7.2.7]). Again, as the method is standard, we indicate the main steps. The line integral has two horizontal paths and one vertical. Using the growth of the logarithmic derivative of the Γ-function along with the functional equation, one has

$$-\frac{L_E'(s)}{L_E(s)} \ll \log(2|s|) \qquad -U \le \mathrm{Re}(s) \le -1, \tag{3.12}$$

for U equal to $M + 1/2$ with M a positive integer and we exclude circles of a fixed (small) radius around the trivial zeros. (See Exercise 7.2.6 of [12].) The choice of R has been alluded to earlier and it is so chosen to have the estimate (by the method indicated on page 392 of [12]),

$$-\frac{L_E'(s)}{L_E(s)} \ll \log^2 R, \qquad -1 \le \mathrm{Re}(s) \le 2. \tag{3.13}$$

With these estimates in place, the top horizontal line integral in (3.11) is now easily estimated in two steps: first moving from $2+iR$ to $-1+iR$ and then from $-1+iR$ to $-U+iR$ and using (3.12) and (3.13) in the respective steps. The same holds true for the bottom horizontal line integral. Finally, the vertical line integral is estimated using (3.13). Putting everything together, we get

$$\mathcal{O}\left(\frac{x^2 \log^2 R}{R} + x^{-U} \log^2 R\right).$$

Letting U tend to infinity gives:

Proposition 4. *For $x > 3/2$ and R chosen as above, in essence, not equal to the ordinate of a non-trivial zero of $L_E(s)$, we have*

$$\psi_E(x) := \sum_{n \le x} c_n \Lambda(n) = -\sum_{|\gamma| < R} n_\rho \frac{x^\rho}{\rho} + \mathcal{O}(x^{1/2} \log x) + \mathcal{O}\left(\frac{x^2 \log^2 R}{R}\right). \tag{3.14}$$

Proof. The discussion preceding the statement of the theorem essentially contains the proof. We need to tie things up. Firstly, the contribution from the trivial zeros is

$$-\log x - \log\left(1 - \frac{1}{x}\right) = -\log(x-1).$$

This can easily be absorbed into the $\mathcal{O}(x^{1/2} \log x)$ term. In our discussion, we needed $x = N + \frac{1}{2}$. We can remove this restriction by noting that the summand on the left hand side is $\mathcal{O}(x^{1/2} \log x)$ and so

$$\psi_E(N + 1/2) - \psi_E(x) = \mathcal{O}(x^{1/2} \log x).$$

This completes the proof. □

We consider the following part of the sum from primes of good reduction:

$$\psi_E(t) = \sum_{n \le t} c_n \Lambda(n), \tag{3.15}$$

and similar to the estimation of Cramér [4], we have the following result:

Theorem 5. *Assuming the Riemann hypothesis for $L_E(s)$ is true, we obtain*

$$\lim_{x \to \infty} \frac{1}{\log x} \int_1^x \frac{\psi_E^2(t)}{t^3} dt = \sum_\rho \left|\frac{n_\rho}{\rho}\right|^2, \tag{3.16}$$

where the sum is over all non-trivial zeros ρ of $L_E(s)$, and n_ρ is the multiplicity of each ρ.

Proof. From (3.14), we have for $t > 3/2$,

$$\frac{(\psi_E(t) - \mathcal{O}(t^{1/2}\log t))^2}{t^3} = \frac{1}{t^3}\left(\sum_\rho n_\rho \frac{t^\rho}{\rho} + \mathcal{O}\left(\frac{t^2\log^2 R}{R}\right)\right)^2$$
$$= \sum_\rho n_\rho \sum_{\rho'} n_{\rho'} \frac{t^{\rho+\rho'-3}}{\rho\rho'} + \mathcal{O}\left(\frac{t\log^4 R}{R^2}\right) + \mathcal{O}\left(\frac{\log^2 R}{R}\left|\sum_\rho n_\rho \frac{t^{\rho-1}}{\rho}\right|\right),$$

where the sums involving ρ and ρ' are taken over the zeros of $L_E(s)$ satisfying $|\mathrm{Im}(\rho)| < R$ and $|\mathrm{Im}(\rho')| < R$ (for simplifying the notation); we assume the same condition for such sums throughout the proof. Applying Proposition 3 to estimate the last error term above, we obtain assuming the Riemann hypothesis for $L_E(s)$ (that is, $\mathrm{Re}(\rho) = 1$), that the sum in absolute value is $\mathcal{O}(\log^2 R)$. Thus

$$\frac{(\psi_E(t) - \mathcal{O}(t^{1/2}\log t))^2}{t^3} = \sum_\rho n_\rho \sum_{\rho'} n_{\rho'} \frac{t^{\rho+\rho'-3}}{\rho\rho'} + \mathcal{O}\left(\frac{t\log^4 R}{R^2}\right) + \mathcal{O}\left(\frac{\log^4 R}{R}\right).$$

Both of the error terms can be combined to give

$$\frac{(\psi_E(t) - \mathcal{O}(t^{1/2}\log t))^2}{t^3} = \sum_\rho n_\rho \sum_{\rho'} n_{\rho'} \frac{t^{\rho+\rho'-3}}{\rho\rho'} + \mathcal{O}\left(\frac{t\log^4 R}{R}\right).$$

We integrate this equation from 1 to x. The left hand side is

$$\int_1^x \frac{\psi_E(t)^2}{t^3} dt + \mathcal{O}(1)$$

because $\psi_E(t) = \mathcal{O}(t\log^2 t)$ assuming the Riemann hypothesis for $L_E(s)$. To treat the right hand side, we use the relation $\rho(2-\rho) = |\rho|^2$ and $\overline{\rho} = 2 - \rho$, and thus obtain

$$\int_1^x \frac{\psi_E^2(t)}{t^3} dt = \sum_\rho \frac{n_\rho}{\rho} \sum_{\rho'} \frac{n_{\rho'}}{\rho'} \int_1^x t^{\rho+\rho'-3} dt + \mathcal{O}(1) + \mathcal{O}\left(\frac{x^2\log^4 R}{R}\right)$$
$$= \sum_\rho \frac{n_\rho}{\rho}\left[\sum_{\rho'=2-\rho} \frac{n_{\rho'}}{\rho'} \int_1^x t^{\rho+\rho'-3} dt + \sum_{\rho'\neq 2-\rho} \frac{n_{\rho'}}{\rho'} \int_1^x t^{\rho+\rho'-3} dt\right]$$
$$+ \mathcal{O}(1) + \mathcal{O}\left(\frac{x^2\log^4 R}{R}\right)$$
$$= \log x \sum_\rho \left|\frac{n_\rho}{\rho}\right|^2 + \sum_\rho \frac{n_\rho}{\rho} \sum_{\rho'\neq 2-\rho} \frac{n_{\rho'}}{\rho'} \cdot \frac{x^{\rho+\rho'-2} - 1}{\rho + \rho' - 2} + \mathcal{O}(1) + \mathcal{O}\left(\frac{x^2\log^4 R}{R}\right).$$

Note that $\rho' = 2 - \rho$ implies $\mathrm{Im}(\rho') = -\mathrm{Im}(\rho)$. We now estimate the second term:

$$\sum_\rho \frac{n_\rho}{\rho} \sum_{\rho'\neq 2-\rho} \frac{n_{\rho'}}{\rho'} \cdot \frac{x^{\rho+\rho'-2} - 1}{\rho + \rho' - 2}. \tag{3.17}$$

Let $\eta > 0$ be sufficiently small, which is independent of x, so that it is smaller than the smallest positive $|\gamma|$. We will estimate the sum separately for two different cases:

$$|\rho + \rho' - 2| \geq \eta \quad \text{and} \quad |\rho + \rho' - 2| < \eta.$$

In the first case, by symmetry, it is sufficient to show that the following two sums converge for all zeros satisfying $|\rho+\rho'-2|\geq\eta$ and $\rho'\neq 2-\rho$:

$$\sum_{\gamma>0}\frac{n_\rho}{|\rho|}\sum_{\gamma'>0}\frac{n_{\rho'}}{|\rho'|(\gamma+\gamma')}, \tag{3.18}$$

$$\sum_{\gamma>0}\frac{n_\rho}{|\rho|}\sum_{0<\gamma'\leq\gamma-\eta}\frac{n_{\rho'}}{|\rho'|(\gamma-\gamma')}. \tag{3.19}$$

Let us observe that both the cases $\gamma'>0$ and $\gamma'<0$ are covered by these cases by taking negative sign if necessary. Note also that all sums in (3.18) and (3.19) are over zeros which satisfy $|\rho+\rho'-2|\geq\eta$. The convergence of the first sum follows from Proposition 2 because by the arithmetic mean - geometric mean inequality, we have $(\gamma+\gamma')\geq 2(\gamma\gamma')^{1/2}$ and so,

$$\sum_{\gamma>0}\frac{n_\rho}{|\rho|}\sum_{\gamma'>0}\frac{n_{\rho'}}{|\rho'|(\gamma+\gamma')}\ll\left(\sum_\rho\frac{1}{|\rho|^{3/2}}\right)^2.$$

Now, we consider the second sum (3.19). We apply Propositions 2 and 3 to estimate the inner sum of (3.19) by breaking the sum into two parts:

$$\sum_{0<\gamma'\leq\gamma-\eta}\frac{n_{\rho'}}{|\rho'|(\gamma-\gamma')}=\left(\sum_{0<\gamma'\leq\gamma-\gamma^{\frac{2}{3}}}+\sum_{\gamma-\gamma^{\frac{2}{3}}<\gamma'\leq\gamma-\eta}\right)\frac{n_{\rho'}}{|\rho'|(\gamma-\gamma')}$$

In the first part, we observe that $|\gamma-\gamma'|\gg|\gamma|^{2/3}$, and by Proposition 3, we see it is

$$\ll\frac{\log^2\gamma}{\gamma^{2/3}}.$$

In the second part, $|\rho'|\gg|\gamma|$, and using the formula for the zero counting function (Proposition 2), we get

$$\ll\frac{1}{\gamma}\left(N_E(\gamma)-N_E(\gamma-\gamma^{2/3})\right)=\mathcal{O}\left(\frac{\log\gamma}{\gamma^{1/3}}\right),$$

for this part. Therefore, the sum in (3.19) converges since it is

$$\ll\sum_{\gamma>0}\frac{n_\rho}{|\rho|}\frac{\log\gamma}{\gamma^{1/3}}<\infty$$

by the second part of Proposition 3. Therefore, we can write the sum in (3.17) as

$$\sum_\rho\frac{n_\rho}{\rho}\sum_{\substack{\rho'\neq 2-\rho,\\ |\gamma+\gamma'|<\eta}}\frac{n_{\rho'}}{\rho'}\cdot\frac{x^{\rho+\rho'-2}-1}{\rho+\rho'-2}+\mathcal{O}(1).$$

Returning to our integral, and letting R tend to infinity, we therefore have

$$\begin{aligned}\int_2^x\frac{\psi_E^2(t)}{t^3}dt&=\log x\sum_\rho\left|\frac{n_\rho}{\rho}\right|^2+\sum_\rho\sum_{\substack{\rho'\neq 2-\rho\\ 0<|\gamma+\gamma'|<\eta}}\frac{n_\rho n_{\rho'}(x^{\rho+\rho'-2}-1)}{\rho\rho'(\rho+\rho'-2)}+\mathcal{O}(1)\\&=\log x\sum_\rho\left|\frac{n_\rho}{\rho}\right|^2+\sum_\rho\sum_{\substack{\rho'\neq 2-\rho\\ 0<|\gamma+\gamma'|<\eta}}\frac{n_\rho n_{\rho'}(x^{i(\gamma+\gamma')}-1)}{i\rho\rho'(\gamma+\gamma')}+\mathcal{O}(1).\end{aligned}$$

As the left hand side is real, we need only consider

(3.20)
$$\mathrm{Re}\left(\sum_{\rho}\sum_{\substack{\rho'\neq 2-\rho\\ 0<|\gamma+\gamma'|<\eta}}\frac{n_\rho n_{\rho'}(x^{i(\gamma+\gamma')}-1)}{i\rho\rho'(\gamma+\gamma')}\right)=-\sum_{\rho}\sum_{\substack{\rho'\neq 2-\rho\\ 0<|\gamma+\gamma'|<\eta}}\mathrm{Im}\left(\frac{n_\rho n_{\rho'}(x^{i(\gamma+\gamma')}-1)}{\rho\rho'(\gamma+\gamma')}\right).$$

The summand can be written as

$$\frac{n_\rho n_{\rho'}}{|\rho|^2|\rho'|^2(\gamma+\gamma')}\,\mathrm{Im}\left(\overline{\rho\rho'}(x^{i(\gamma+\gamma')}-1)\right).$$

Noting that $\rho=1+i\gamma$ and $\rho'=1+i\gamma'$, a routine calculation shows

$$\mathrm{Im}\left(\overline{\rho\rho'}(x^{i(\gamma+\gamma')}-1)\right)=-(\gamma+\gamma')\cos[(\gamma+\gamma')\log x]+(1-\gamma\gamma')\sin[(\gamma+\gamma')\log x].$$

Using the elementary inequality that $|\sin\theta|\le|\theta|$, we see for $x\ge 3$ that this quantity is bounded by

$$|\gamma+\gamma'|+|1+\gamma\gamma'||\gamma+\gamma'|\log x\le|\gamma+\gamma'|(2+|\gamma\gamma'|)\log x\le|\gamma+\gamma'|\left(\frac{2}{\eta^2}+1\right)|\gamma\gamma'|\log x,$$

because $|\gamma|,|\gamma'|>\eta$. Inserting this estimate into (3.20), we must bound

$$\left(\frac{2}{\eta^2}+1\right)\log x\sum_{\rho}\sum_{0<|\gamma+\gamma'|<\eta}\frac{n_\rho n_{\rho'}}{\gamma\gamma'}.$$

For a given constant $A>0$, we first consider the sum

$$\sum_{\gamma>A}\sum_{0<|\gamma+\gamma'|<\eta}\frac{n_\rho n_{\rho'}}{\gamma\gamma'}.$$

By partial summation, we see that this is bounded by

$$\sum_{\gamma>A}\frac{n_\rho}{\gamma}\int_{-\gamma-\eta}^{-\gamma+\eta}\frac{N_E(t)}{t^2}dt\ll\sum_{\gamma>A}\frac{n_\rho}{\gamma}\int_{-\gamma-\eta}^{-\gamma+\eta}\frac{\log|t|}{t}dt\ll\sum_{\gamma>A}\frac{n_\rho\log|\gamma|}{\gamma^2}.$$

Applying Proposition 3, and choosing A large, we can make this arbitrarily small. It remains to consider $\gamma<A$ and the contribution from γ' such that $0<|\gamma+\gamma'|<\eta$. The set of such $\gamma\neq\gamma'$ is a finite set and we choose η smaller than any of the elements $|\gamma+\gamma'|$ so that the sum is vacous. This proves that for any $\epsilon>0$, there is an $\eta>0$ such that

$$\left|\sum_{\rho}\sum_{\substack{\rho'\neq 2-\rho\\ 0<|\gamma+\gamma'|<\eta}}\frac{n_\rho n_{\rho'}(x^{\rho+\rho'-2}-1)}{\rho\rho'(\rho+\rho'-2)}\right|<\epsilon\log x.$$

Dividing by $\log x$ and letting x tend to infinity, we obtain

$$\lim_{x\to\infty}\frac{1}{\log x}\int_2^x\frac{\psi_E^2(t)}{t^3}dt=\sum_{\rho}\left|\frac{n_\rho}{\rho}\right|^2. \tag{3.21}$$

□

Corollary 6. *Let $c>0$. For sufficiently large $x>0$, there exists $t\in[x,2x]$ which satisfies*

$$|\psi_E(t)|<ct\sqrt{\log t}. \tag{3.22}$$

Proof. Note that Theorem 5 implies

$$\int_x^{2x} \frac{\psi_E^2(u)}{u^3}\, du = o(\log x). \tag{3.23}$$

Assume that for every $t \in [x, 2x]$, we have $|\psi_E(t)| \geq ct\sqrt{\log t}$. This implies

$$\int_x^{2x} \frac{\psi_E^2(u)}{u^3} du \geq \int_x^{2x} \frac{c^2 u^2 \log u}{u^3} du \geq c^2 \log 2 \log x, \tag{3.24}$$

which contradicts (3.23). □

4. Birch and Swinnerton-Dyer conjecture and related works

The Birch and Swinnerton-Dyer conjecture describes the rank r_M of the Mordell-Weil group of E and relates it to the order of vanishing of its L-function. The conjecture has been improved over time with numerical evidence, and there are several ways to describe their conjecture. In this paper, we are interested in the following version of the conjecture from [2], which we previously introduced as "OBSD":

Conjecture 7 (Birch and Swinnerton-Dyer)**.** *For some constant C_E, we have*

$$\prod_{\substack{p<x \\ p \nmid \Delta_E}} \frac{N_p}{p} \sim C_E (\log x)^r, \tag{4.1}$$

where r is the order of the zero of the L-function $L_E(s)$ of E at $s = 1$.

Furthermore, Birch and Swinnerton-Dyer conjectured that the order of the zero of the L-function $L_E(s)$ of E is equal to the rank r_M of the Mordell-Weil group $E(\mathbb{Q})$ of E.

Kuo and Murty [8] and Conrad [3] independently showed that Conjecture 7 is equivalent to an asymptotic condition of a sum involving the eigenvalues of the Frobenius at each prime. We cite the result from [8, Theorem 2 and 3] and [3, Theorem 1.3]:

Theorem 8. *Conjecture 7 is true if and only if*

$$\sum_{\substack{p^k \leq x \\ p \nmid \Delta_E}} \frac{\alpha_p^k + \beta_p^k}{k} = o(x). \tag{4.2}$$

We also note that (4.2), and hence Conjecture 7, is equivalent to

$$\sum_{\substack{p^k \leq x \\ p \nmid \Delta_E}} (\alpha_p^k + \beta_p^k) \log p = o(x \log x). \tag{4.3}$$

As noted earlier, the Riemann hypothesis for $L_E(s)$ is equivalent to the following asymptotic condition of the sum (4.3):

$$\sum_{\substack{p^k \leq x \\ p \nmid \Delta_E}} (\alpha_p^k + \beta_p^k) \log p = \mathcal{O}(x(\log x)^2). \tag{4.4}$$

Hence, as Kuo and Murty [8] and Conrad [3] pointed out, Conjecture 7 is much deeper than the Riemann hypothesis for $L_E(s)$ according to our current knowledge.

Using Theorem 5, we prove the following result:

Theorem 9. *Assume the Riemann hypothesis is true for $L_E(s)$. Then there is a sequence $x_n \in [2^n, 2^{n+1}]$ such that*

$$\lim_{n\to\infty} \frac{1}{\log x_n} \sum_{p<x_n} \frac{a_p \log p}{p} = -r + \frac{1}{2}, \tag{4.5}$$

where r is the order of $L_E(s)$ at $s = 1$.

Proof. For $x > 1$, $d > 3/2$ and any real number a satisfying $d > a$, Perron's formula implies

$$\frac{1}{2\pi i} \int_{d-i\infty}^{d+i\infty} -\frac{L_E'(s)}{L_E(s)} \frac{x^s}{s-a}\, ds = x^a \sum_{n\le x} \frac{c_n \Lambda(n)}{n^a}, \tag{4.6}$$

where the last sum in (4.6) is weighted by $1/2$ if x is an integer. We consider the case when $a = 0, 1$, and $d = 2$, we get

$$\frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} -\frac{L_E'(s)}{L_E(s)} \frac{x^s}{s(s-1)}\, ds = x \sum_{n\le x} \frac{c_n \Lambda(n)}{n} - \sum_{n\le x} c_n \Lambda(n). \tag{4.7}$$

Noting that $L_E(s)$ has a simple zero at $s = 0$, we write the expansion of $\frac{L_E'(s)}{L_E(s)}$ at $s = 0$ and $s = 1$ as

$$\frac{L_E'(s)}{L_E(s)} = \frac{1}{s} + d' + \cdots, \quad \frac{L_E'(s)}{L_E(s)} = \frac{r}{s-1} + d + \cdots. \tag{4.8}$$

By following the residue computations as in [3, (6.8)], we have

$$\operatorname*{Res}_{s=\rho} \left(-\frac{L_E'(s)}{L_E(s)} \frac{x^s}{s(s-1)} \right) = \begin{cases} (\log x + 1) + d' & \text{if } \rho = 0, \\ -rx(\log x - 1) - dx & \text{if } \rho = 1. \end{cases} \tag{4.9}$$

As usual, we move the line of integration in (4.7) to the left (the methodology being similar to our derivation of the truncated explicit formula) and considering the contribution from the trivial and non-trivial zeros of $L_E(s)$, we get

$$-rx \log x + \mathcal{O}(x) = x \sum_{n\le x} \frac{c_n \Lambda(n)}{n} - \sum_{n\le x} c_n \Lambda(n), \tag{4.10}$$

as x tends to infinity, and we get

$$\sum_{n\le x} \frac{c_n \Lambda(n)}{n} = -r \log x + \frac{\sum_{n\le x} c_n \Lambda(n)}{x} + \mathcal{O}(1), \tag{4.11}$$

where c_n is defined as in (2.2). On the other hand, we can separate the left hand side sum of (4.11)

$$\begin{aligned} \sum_{n\le x} \frac{c_n \Lambda(n)}{n} &= \sum_{p\le x} \frac{a_p \log p}{p} + \sum_{p^2\le x} \frac{(\alpha_p^2 + \beta_p^2) \log p}{p^2} + \mathcal{O}(1) \\ &= \sum_{p\le x} \frac{a_p \log p}{p} + \sum_{p\le \sqrt{x}} \frac{(a_p^2 - 2p) \log p}{p^2} + \mathcal{O}(1) \\ &= \sum_{p\le x} \frac{a_p \log p}{p} + \sum_{p\le \sqrt{x}} \frac{a_p^2 \log p}{p^2} - \sum_{p\le \sqrt{x}} \frac{2 \log p}{p} + o(\log x) \\ &= \sum_{p\le x} \frac{a_p \log p}{p} - \frac{1}{2} \log x + o(\log x). \end{aligned}$$

Note that the fourth equality follows from calculations in the proof of [8, Lemma 1] using the theory of the Rankin-Selberg convolution. The proof is similar to that in [8]. To treat our sum which is weighted by $\log p$, one needs the partial summation formula. Combining this with (4.11), we obtain

$$\sum_{p\le x}\frac{a_p\log p}{p}=\left(-r+\frac{1}{2}\right)\log x+\frac{\sum_{n\le x}c_n\Lambda(n)}{x}+o(\log x), \tag{4.12}$$

where r is the order of $L_E(s)$ at $s=1$.

Now, using Corollary 6, for $n\ge 2$, we can define a sequence by selecting $x_n\in[2^{n-1},2^n]$ such that

$$|\psi_E(x_n)|<cx_n\sqrt{\log x_n}. \tag{4.13}$$

From (4.11) and (4.13), we have

$$\sum_{p\le x_n}\frac{a_p\log p}{p}=\left(-r+\frac{1}{2}\right)\log x_n+\mathcal{O}(\sqrt{\log x_n})+o(\log x_n), \tag{4.14}$$

and

$$\frac{1}{\log x_n}\sum_{p\le x_n}\frac{a_p\log p}{p}\to -r+\frac{1}{2}\quad\text{as } n\to\infty, \tag{4.15}$$

where r is the order of $L_E(s)$ at $s=1$. □

Furthermore, Theorem 9 implies the following:

Corollary 10. *If the limit*

$$\lim_{x\to\infty}\frac{1}{\log x}\sum_{p<x}\frac{a_p\log p}{p} \tag{4.16}$$

exists, then the Riemann hypothesis for $L_E(s)$ is true, and the limit is $-r+1/2$.

Proof. From the assumption, we can write

$$\sum_{p<x}\frac{a_p\log p}{p}=K\log x+o(\log x), \tag{4.17}$$

for some constant K. Taking into account the contribution from the higher powers of primes on the left hand side of (4.11), we deduce that

$$\sum_{n\le x}\frac{c_n\Lambda(n)}{n}=(K-\frac{1}{2})\log x+o(\log x).$$

Equation (4.11) now implies

$$\sum_{n\le x}c_n\Lambda(n)=\mathcal{O}(x\log x),$$

which we have already noted, implies the Riemann hypothesis for $L_E(s)$. We can therefore apply Theorem 9. If the limit of the theorem exists, then any subsequence will also converge to the same limit. We therefore take for our subsequence the $x_m\in[2^m,2^{m+1}]$ provided by Theorem 9. For this subsequence, the limit is $-r+1/2$, as desired. □

Corollary 11. *If the limit*

$$\lim_{x\to\infty}\frac{1}{\log x}\sum_{p<x}\frac{a_p\log p}{p} \tag{4.18}$$

exists, then Conjecture 7 is true.

Proof. From (4.11), we observe that

$$\sum_{\substack{p^k\le x\\ p\nmid\Delta_E}}(\alpha_p^k+\beta_p^k)\log p=\sum_{n\le x}c_n\Lambda(n)=x\sum_{n\le x}\frac{c_n\Lambda(n)}{n}+rx\log x+\mathcal{O}(x), \tag{4.19}$$

where the last equality follows from (4.11). Using the theory of Rankin-Selberg convolution (as in the proof of [8, Lemma 1]), we obtain

$$\begin{aligned}\sum_{n\le x}c_n\Lambda(n)&=x\sum_{p\le x}\frac{a_p\log p}{p}-\frac{1}{2}x\log x+rx\log x+\mathcal{O}(x)\\&=\left(-r+\frac{1}{2}\right)x\log x+o(x\log x)-\frac{1}{2}x\log x+rx\log x+\mathcal{O}(x)\\&=o(x\log x),\end{aligned}$$

where r is the order of $L_E(s)$ at $s=1$ (as in (4.8)). This is equivalent to Conjecture 7, which is remarked as in Theorem 8. □

We make one final remark before concluding this section. This has to do with the fact that one can actually show that the statement

$$\sum_{n\le x}\frac{c_n\Lambda(n)}{n}=-r\log x+\mathcal{O}(1)$$

is false. Indeed, if true, this would imply via (4.11) that

$$\sum_{n\le x}c_n\Lambda(n)=\mathcal{O}(x),$$

which is false by Theorem 6 of [11] which implies high oscillations of the error term tending to infinity. Thus the error term cannot be bounded.

5. Connections to Nagao's conjecture

We make here a few remarks that relate our results to Nagao's conjecture. Recall that this conjecture focuses on the elliptic surface

$$\mathcal{E}: y^2=x^3+A(T)x+B(T)$$

with $A(T), B(T)\in\mathbb{Z}[T]$ and $\Delta(T):=4A(T)^3+27B(T)^2\neq 0$. For each $t\in\mathbb{Z}$ such that $\Delta(t)\neq 0$, we have an elliptic curve $\mathcal{E}_t$ defined over $\mathbb{Q}$, and Nagao [13] defined the fibral average of the trace of Frobenius for each prime p as follows:

$$A_p(\mathcal{E}):=\frac{1}{p}\sum_{t=1}^{p}a_p(\mathcal{E}_t),$$

where $a_p(\mathcal{E}_t)$ is the trace of the Frobenius automorphism at p (that we have studied in the previous sections) of $\mathcal{E}_t$. In [13], Nagao conjectured that

$$-\lim_{X\to\infty}\frac{1}{X}\sum_{p\le X}A_p(\mathcal{E})\log p=\operatorname{rank}\mathcal{E}(\mathbb{Q}(T)). \tag{5.1}$$

Now the sum can be re-written as

$$\sum_{p\le X}\frac{1}{p}\sum_{t\le p}a_p(\mathcal{E}_t)\log p=\sum_{t\le X}\left(\sum_{t\le p\le X}\frac{a_p(\mathcal{E}_t)\log p}{p}\right), \tag{5.2}$$

and from our analysis, for a fixed t, the inner sum is (ignoring error terms)

$$\left(-r_t+\frac{1}{2}\right)\log\frac{X}{t},$$

where $r_t=\operatorname{rank}\ \mathcal{E}_t(\mathbb{Q})$. Thus, one may expect

$$-\frac{1}{X}\sum_{p\le X}A_p(\mathcal{E})\log p\sim\frac{1}{X}\sum_{t\le X}\left(r_t-\frac{1}{2}\right)\log\frac{X}{t}.$$

This suggests the following (modified) form of Nagao's conjecture:

$$\lim_{X\to\infty}\frac{1}{X}\sum_{t\le X}\left(r_t-\frac{1}{2}\right)\log\frac{X}{t}=\operatorname{rank}\ \mathcal{E}(\mathbb{Q}(T)). \tag{5.3}$$

Now, note that

$$\sum_{t\le X}\log\frac{X}{t}=X+\mathcal{O}(\log X)$$

by a simple application of Stirling's formula. Thus, it would seem that

$$\lim_{X\to\infty}\frac{1}{X}\sum_{t\le X}r_t\log\frac{X}{t}=\operatorname{rank}\ \mathcal{E}(\mathbb{Q}(T))+\frac{1}{2}.$$

By letting $R(u)=\sum_{t\le u}r_t$, using Abel summation formula, it is not difficult to see that

$$\sum_{t\le X}r_t\log\frac{X}{t}=\int_1^X\left(\sum_{t\le u}r_t\right)\frac{du}{u}.$$

Thus, perhaps we have

$$\int_1^X\frac{R(u)}{u}du\sim\left(\operatorname{rank}\ \mathcal{E}(\mathbb{Q}(T))+\frac{1}{2}\right)X,$$

as $X\to\infty$.

We now invoke the following elementary lemma: if $f(x)$ is a positive nondecreasing function such that as $x\to\infty$

$$\int_1^x\frac{f(u)}{u}du\sim x,$$

then $f(x)\sim x$ as $x\to\infty$ [18, 3.7, Page 54]. Thus, our question becomes: is it true that

$$\sum_{t\le X}r_t\sim\left(\operatorname{rank}\mathcal{E}(\mathbb{Q}(T))+\frac{1}{2}\right)X \tag{5.4}$$

as $X\to\infty$, which can be viewed as a variant of Nagao's conjecture?

Remark 12. The upper bound of the sum (5.4) has been studied by several authors assuming various standard conjectures. For instance, assuming OBSD (Conjecture 7), the Riemann hypothesis for L-series attached to elliptic curves, and Tate's conjecture for elliptic surfaces, Michel [9] proved the upper bound

$$\frac{1}{2X}\sum_{|t|\le X}r_t\le\left(\deg\Delta(T)+\deg N(T)-\frac{3}{2}\right)(1+o(1)) \tag{5.5}$$

as $X \to \infty$, where $N(T)$ denotes the conductor of $\mathcal{E}$. Moreover, assuming the same standard conjectures as Michel's result [9], Silverman [17] obtained the upper bound

$$\frac{1}{2X}\sum_{|t|\le X} r_t \le \left(\deg N(T) + \operatorname{rank}\mathcal{E}(\mathbb{Q}(T)) + \frac{1}{2}\right)(1+o(1)) \tag{5.6}$$

as $X \to \infty$. Besides, Fermigier [5] studied (93 different) one-parameter families of elliptic curves of generic rank $r = \operatorname{rank}\mathcal{E}(\mathbb{Q}(T))$ with $0 \le r \le 4$. More precisely, let t be an integer, then 32% of the specialized curves $\mathcal{E}_t$ (defined over $\mathbb{Q}$) had rank r, 48% had rank $r+1$, 18% had rank $r+2$, and only 2% of the specialized curves had rank $r+3$. For every family of elliptic curves and bound which are considered in [5], Fermigier found the quantity

$$\frac{1}{2X}\sum_{|t|\le X} \operatorname{rank}\mathcal{E}_t(\mathbb{Q}) - \operatorname{rank}\mathcal{E}(\mathbb{Q}(T)) - \frac{1}{2} \tag{5.7}$$

ranges from 0.08 to 0.54 and averages around 0.35. This suggests that the quantity $1/2$ appearing in our question (5.4) may have to be modifed by a small amount.

Remark 13. The following one parameter family of elliptic curves was studied by Washington [19]:

$$\mathcal{E} : y^2 = x^3 + Tx^2 - (T+3)x + 1, \tag{5.8}$$

then $j(T) = 256(T^2+3T+9)$, and $\mathcal{E}$, viewed as an elliptic curve defined over $\mathbb{Q}(T)$ has $\operatorname{rank}\mathcal{E}(\mathbb{Q}(T)) = 1$. Interestingly, Rizzo [14, Theorem 1] proved that the family has extreme bias in its fibral root numbers. More precisely, the root number (defined in (1.6)) of each fiber is

$$w_{\mathcal{E}_t} = -1, \quad \text{for every } t \in \mathbb{Z}.$$

Hence, via the parity conjecture (or the Birch and Swinnerton-Dyer conjecture), we can expect the rank of all fibers will be odd and, in particular, positive with infinitely many rational points. On the other hand, via Silverman's specialization theorem, it is known that $\operatorname{rank}\mathcal{E}(\mathbb{Q}(T)) \le \operatorname{rank}\ \mathcal{E}_t(\mathbb{Q})$ for all but finitely many t. Furthermore, one conjectures that $\operatorname{rank}\mathcal{E}_t(\mathbb{Q})$ is equal to either $\operatorname{rank}\mathcal{E}(\mathbb{Q}(T))$ or $\operatorname{rank}\mathcal{E}(\mathbb{Q}(T))+1$ up to a zero density subset of $\mathbb{Q}$, depending on the parity given by the root numbers. This tells us that, outside of a zero density subset of $\mathbb{Q}$, the fibers of $\mathcal{E}$ have odd rank, and most likely have rank 1. Therefore, it is likely that

$$\lim_{X\to\infty}\frac{1}{2X}\sum_{|t|\le X}\operatorname{rank}\mathcal{E}_t(\mathbb{Q}) = \operatorname{rank}\mathcal{E}(\mathbb{Q}(T)), \tag{5.9}$$

where the extra $1/2$ disappears since the fibral parity of the family $\mathcal{E}$ has large bias.

Based on the heuristics suggested as in (5.4), Remark 13, and in [5,17], the above remark, we propose Conjecture 14:

Conjecture 14. *We define*

$$\mathcal{T} := \left\{t \in \mathbb{Z} : w_{\mathcal{E}_t} = (-1)^{\operatorname{rank}\mathcal{E}(\mathbb{Q}(T))+1}\right\}. \tag{5.10}$$

Then we have

$$\lim_{X\to\infty}\frac{1}{2X}\sum_{|t|\le X} r_t = \operatorname{rank}\mathcal{E}(\mathbb{Q}(T)) + \delta(\mathcal{T}) \tag{5.11}$$

where $\delta(\mathcal{T})$ is the natural density of $\mathcal{T}$ as a subset of $\mathbb{Z}$.

Note that the conjecture reflects the heuristic (5.3), Remark 13, as well as the experimental results of Fermigier: more precisely, the results in [5, Tableau 2] show that the quantity (5.7) does not tend to depend significantly as the other invariants of the elliptic curves change, such as rank $\mathcal{E}(\mathbb{Q}(T))$, $\deg N(T)$, and $\deg \Delta(T)$, which appear in the known upper bounds, as in (5.5) and (5.6). The work of Fermigier also suggests that the average of the error term in (5.2) is bounded.

A curious consequence of this conjecture is that the specializations $\mathcal{E}_t$ with r_t large are very rare. It may be possible to prove such consequences of the conjecture by other methods.

Also, note that the bounds (5.5) and (5.6) have been also considered for a family of abelian varieties over $\mathbb{Q}$ by Wazir [20]. More concretely, let $\pi : \mathcal{A} \to \mathbb{P}^1$ be a proper flat morphism of smooth projective varieties defined over $\mathbb{Q}$, with an abelian variety A over $\mathbb{Q}(T)$ as its generic fiber. Then, by assuming standard conjectures as in [17], Wazir obtains the following bound

$$\frac{1}{2X}\sum_{|t|\le X} \operatorname{rank} \mathcal{A}_t(\mathbb{Q}) \le \left(\frac{\mathcal{L}_X}{2X\log X} + \operatorname{rank} \mathcal{A}(\mathbb{Q}(T)) + \frac{g}{2}\right)(1+o(1)) \tag{5.12}$$

as $X \to \infty$, where $\mathcal{A}_t$ is the fiber at $t \in \mathbb{P}^1$, which is an abelian variety defined over $\mathbb{Q}$, and

$$\mathcal{L}_X = \sum_{|t|\le X} \log N_{\mathcal{A}_t}, \tag{5.13}$$

where $N_{\mathcal{A}_t}$ is the conductor of $\mathcal{A}_t$. For a more detailed definition of $\mathcal{L}_X$ and the conductor, please refer to [20, 1.1]. Hence, one can expect a similar conjectural estimation as Conjecture 14 involving $g/2$ in place of $1/2$. We leave the details for future studies.

Acknowledgments

The authors would like to thank Marc Hindry and Joseph Silverman for their helpful suggestions. The authors also wish to thank the anonymous referee(s) for helpful suggestions on the earlier version of this paper.

References

[1] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939, DOI 10.1090/S0894-0347-01-00370-8. MR1839918

[2] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108, DOI 10.1515/crll.1965.218.79. MR179168

[3] K. Conrad, *Partial Euler products on the critical line*, Canad. J. Math. **57** (2005), no. 2, 267–297, DOI 10.4153/CJM-2005-012-6. MR2124918

[4] H. Cramér, *Ein Mittelwertsatz in der Primzahltheorie* (German), Math. Z. **12** (1922), no. 1, 147–153, DOI 10.1007/BF01482072. MR1544509

[5] S. Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur* **Q** (French, with English and French summaries), Experiment. Math. **5** (1996), no. 2, 119–130. MR1418959

[6] P. X. Gallagher, *Some consequences of the Riemann hypothesis*, Acta Arith. **37** (1980), 339–343, DOI 10.4064/aa-37-1-339-343. MR598886

[7] D. Goldfeld, *Sur les produits partiels eulériens attachés aux courbes elliptiques* (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. **294** (1982), no. 14, 471–474. MR679556

[8] W. Kuo and M. R. Murty, *On a conjecture of Birch and Swinnerton-Dyer*, Canad. J. Math. **57** (2005), no. 2, 328–337, DOI 10.4153/CJM-2005-014-0. MR2124920

[9] P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate* (French, with English summary), Monatsh. Math. **120** (1995), no. 2, 127–136, DOI 10.1007/BF01585913. MR1348365
[10] H. L. Montgomery, *The zeta function and prime numbers*, Proceedings of the Queen's Number Theory Conference, 1979 (Kingston, Ont., 1979), Queen's Papers in Pure and Appl. Math., vol. 54, Queen's Univ., Kingston, Ont., 1980, pp. 1–31. MR634679
[11] M. R. Murty, *Oscillations of Fourier coefficients of modular forms*, Math. Ann. **262** (1983), no. 4, 431–446, DOI 10.1007/BF01456059. MR696516
[12] M. R. Murty, *Problems in analytic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 206, Springer, New York, 2008. Readings in Mathematics. MR2376618
[13] K.-i. Nagao, $\mathbf{Q}(T)$*-rank of elliptic curves and certain limit coming from the local points*, Manuscripta Math. **92** (1997), no. 1, 13–32, DOI 10.1007/BF02678178. With an appendix by Nobuhiko Ishida, Tsuneo Ishikawa and the author. MR1427665
[14] O. G. Rizzo, *Average root numbers for a nonconstant family of elliptic curves*, Compositio Math. **136** (2003), no. 1, 1–23, DOI 10.1023/A:1022669121502. MR1965738
[15] A. Selberg, *Old and new conjectures and results about a class of Dirichlet series*, Proceedings of the Amalfi Conference on Analytic Number Theory (Maiori, 1989), Univ. Salerno, Salerno, 1992, pp. 367–385. MR1220477
[16] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009, DOI 10.1007/978-0-387-09494-6. MR2514094
[17] J. H. Silverman, *The average rank of an algebraic family of elliptic curves*, J. Reine Angew. Math. **504** (1998), 227–236, DOI 10.1515/crll.1998.109. MR1656771
[18] E. C. Titchmarsh, *The theory of the Riemann zeta-function*, 2nd ed., The Clarendon Press, Oxford University Press, New York, 1986. Edited and with a preface by D. R. Heath-Brown. MR882550
[19] L. C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), no. 177, 371–384, DOI 10.2307/2007897. MR866122
[20] R. Wazir, *A bound for the average rank of a family of abelian varieties* (English, with English and Italian summaries), Boll. Unione Mat. Ital. Sez. B Artic. Ric. Mat. (8) **7** (2004), no. 1, 241–252. MR2044269
[21] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551, DOI 10.2307/2118559. MR1333035

Appendix

by Andrew V. Sutherland[1]

Let $a_p(E)$ denote the Frobenius trace of an elliptic curve $E/\mathbb{Q}$ at a prime p. Figures 1, 2, 3 plot the sums

$$S(x) := \frac{1}{\log x} \sum_{p \le x,\ p \nmid \Delta_E} \frac{a_p(E) \log p}{p}$$

for elliptic curves E of discriminant Δ_E and various ranks; See Table 1 for a list of the curves and their sources. These sums are conjectured to converge to $r - 1/2$ as $x \to \infty$, where r is the analytic rank of $L_E(s)$. The ranks r_E listed in Table 1 are lower bounds on the Mordell-Weil rank that are also upper bounds on the analytic rank under the Generalized Riemann Hypothesis (GRH), and equal to both the Mordell-Weil rank and the analytic rank under the Birch and Swinnerton–Dyer conjecture (BSD). Ranks listed with no asterisk are equal to the Mordell-Weil rank; for those marked with a single (resp. double) asterisk this equality is conditional on GRH (resp. GRH and BSD). Lower bounds on the Mordell-Weil rank were confirmed by verifying the existence of r_E independent points using the Néron-Tate

[1]Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Ave., Cambridge, MA 02139, USA; email: drew@math.mit.edu, URL: https://math.mit.edu/~drew. Supported by Simons Foundation grant 550033.

height pairing, while GRH-based upper bounds on the analytic rank were confirmed using Bober's method [3]. GRH-based upper bounds on the Mordell-Weil rank were confirmed using `magma` [1] for $r_E \le 19$; for $r_E \ge 20$ we rely on the results of [22]. Exact values of Mordell-Weil ranks were confirmed using Cremona's `mwrank` [8] package for $r_E \le 11$; for ranks $r_E \ge 12$ with no asterisk we rely on computations reported in the listed sources. The curves of rank $r_E \le 11$ have conductors N_E that are close to the smallest possible [16]. This is not likely to be true for the curves for rank $r_E \ge 12$, but we chose curves of smaller conductor when several were available. In many cases the curves we list are not the first known curve of that rank; see [10] for a history of rank records.

The sums $S(x)$ plotted for $x \le B = 10^{12}$ in Figure 1 were computed using the `smalljac` software library [21] with some further optimizations described in [38,39]. The expected time complexity of this approach is $O(B^{5/4}\log B\log\log B)$. This is asymptotically worse than both the $O(B(\log B)^{4+o(1)})$ expected time complexity (under GRH) of using the Schoof-Elkies-Atkin algorithm [40] and the $O(B(\log B)^3)$ time complexity of an average polynomial-time approach [20], but it is practically much faster for $B = 10^{12}$; it took approximately 100 core-days per curve to compute the $S(x)$ plots shown in Figure 1.

Figures 2 and 3 show similar plots for Mordell curves $y^2 = x^3 + k$ of ranks $r_E = 0, 1, 2, \cdots, 17$ and congruent number curves $y^2 = x^3 - n^2x$ of ranks $r_E = 0, 1, 2, \ldots, 7$. The corresponding curves listed in Table 1 were chosen to minimize the conductor among those of a given rank which have appeared in the literature, which generally means $|k|$ and n are among the smallest known. These are not necessarily the first curves of these forms found to achieve these ranks; see [24, 34, 42] for some earlier examples, and see [41] for unsuccessful attempts to extend the list of congruent number curves beyond $r_E = 7$.

The Mordell curves and congruent number curves have j-invariants $0, 1728$ (respectively), and thus admit (potential) complex multiplication by the ring of integers $\mathcal{O}$ of $K = \mathbb{Q}(\zeta_3), \mathbb{Q}(i)$. To efficiently compute $a_p(E) = \mathrm{tr}(\psi_E(\mathfrak{p}))$ we compute the trace of the Hecke character ψ_E corresponding to E evaluated at a prime $\mathfrak{p}$ of K above p; this trace is necessarily zero when p is inert. For each prime $p \le B$ of good reduction for E that splits in $\mathcal{O}$ we use Cornacchia's algorithm to compute all integer solutions (t, v) to the norm equation $4p = t^2 - v^2\mathrm{disc}(\mathcal{O})$. We then apply the algorithm of Rubin and Silverberg [37] to determine the correct choice of $t = a_p$. The algorithm in [37] determines the correct twist of an ordinary elliptic curve over $\mathbb{F}_p$ with a given j-invariant, endomorphism ring and Frobenius trace, but it can also be used to determine the Frobenius trace of an ordinary elliptic curve over $\mathbb{F}_p$ whose endomorphism ring is known. This yields an algorithm to compute $a_p(E)$ in $O((\log p)^2\log\log p)$ expected time, meaning we can compute $S(x)$ for $x \le B$ in $O(B\log B\log\log B)$ expected time. This makes it feasible to plot $S(x)$ for $x \le B = 10^{15}$ in Figures 2 and 3 in roughly the same time required for $B = 10^{12}$ in Figure 1, about 100 core-days per curve.

We end with a note of caution regarding the interpretation of these plots as evidence supporting the conjectured convergence of $S(x)$. The methods used to find the higher rank curves shown in these plots typically use $S(x)$ or a closely related sum as a heuristic method to identify elliptic curves of potentially high rank; see [5, 28, 32]. Most of the curves of rank $r_E \ge 12$ listed in Table 1 were discovered precisely because a partial sum related to $S(x)$ suggested they should

have large ranks. This is less of a concern for the lower rank curves where searches have been more exhaustive in an effort to minimize N_E, $|k|$, or n.

TABLE 1. Elliptic curves listed by Mordell-Weil rank. Asterisks (double asterisks) indicate ranks conditional on GRH (GRH and BSD).

r_E	$E(\mathbb{Q})_{\text{tors}}$	$\log N_E$	$[a_1, a_2, a_3, a_4, a_6]$	source
0	trivial	2.398	$[0, -1, 1, 0, 0]$	Birch, Kuyk, Swinnerton-Dyer 1972 [2]
1	trivial	3.611	$[0, 0, 1, -1, 0]$	Birch, Kuyk, Sinnwerton-Dyer 1972 [2]
2	trivial	5.964	$[0, 1, 1, -2, 0]$	Cremona 1997 [6]
3	trivial	8.532	$[0, 0, 1, -7, 6]$	Cremona 1997 [6]
4	trivial	12.365	$[1, -1, 0, -79, 289]$	APECS, Cremona 2012 [7], [23]
5	trivial	16.762	$[0, 0, 1, -79, 342]$	Brumer and McGuinness 1990 [4]
6	trivial	22.370	$[1, 1, 0, -2582, 48720]$	Elkies and Watkins 2004 [16]
7	trivial	26.670	$[0, 0, 0, -10012, 346900]$	Elkies and Watkins 2004 [16]
8	trivial	33.151	$[1, -1, 0, -106384, 13075804]$	Elkies and Watkins 2004 [16]
9	trivial	38.008	$[1, -1, 0, -135004, 97151644]$	Elkies and Watkins 2004 [16]
10	trivial	43.768	$[0, 0, 1, -16312387, 25970162646]$	Elkies and Watkins 2004 [16]
11	trivial	51.246	$[0, 0, 1, -16359067, 26274178986]$	Elkies and Watkins 2004 [16]
12*	trivial	67.767	$[0, 0, 1, -634\cdots647, 193\cdots036]$	Mestre 1982 [27]
13*	trivial	99.778	$[1, 0, 0, -560\cdots540, 529\cdots600]$	Nagao 1994 [32]
14*	trivial	86.484	$[0, 0, 1, -224\cdots757, 132\cdots406]$	Mestre 1986 [28]
15*	trivial	129.440	$[1, 0, 0, -209\cdots485, 266\cdots897]$	Mestre 1992 [29]
16	$\mathbb{Z}/2\mathbb{Z}$	139.095	$[1, 0, 0, 888\cdots054, 398\cdots0420]$	Dujella 2009 [9]
17*	trivial	136.210	$[0, 1, 0, -184\cdots145, 966\cdots743]$	Nagao 1992 [30]
18	$\mathbb{Z}/2\mathbb{Z}$	149.798	$[1, 0, 0, -171\cdots215, 445\cdots817]$	Elkies 2009 [9]
19*	trivial	149.986	$[1, -1, 1, -206\cdots978, 328\cdots881]$	Fermigier 1992 [17]
20*	trivial	170.088	$[1, 0, 0, -431\cdots166, 515\cdots196]$	Nagao 1993 [31]
21*	trivial	196.680	$[1, 1, 1, -215\cdots835 \ -194\cdots535]$	Nagao and Kouya 1994 [33]
22*	trivial	182.725	$[1, 0, 1, -940\cdots864, 107\cdots362]$	Fermigier 1996 [18]
23*	trivial	205.061	$[1, 0, 1, -192\cdots723, 326\cdots006]$	Martin and McMillen 1998 [25]
24*	trivial	219.927	$[1, 0, 1, -120\cdots374, 504\cdots116]$	Martin and McMillen 2000 [26]
25**	trivial	229.186	$[1, 0, 0, -122\cdots200, 523\cdots000]$	Elkies 2006 [15]
26**	trivial	247.860	$[1, 0, 0, -271\cdots190, 167\cdots092]$	Elkies 2006 [15]
27*	trivial	287.013	$[1, 0, 0, -556\cdots970, 161\cdots956]$	Elkies 2006 [22]
28*	trivial	368.407	$[1, -1, 1, -200\cdots502, 344\cdots429]$	Elkies 2006 [11]
0	$\mathbb{Z}/6\mathbb{Z}$	3.584	$[0, 0, 0, 0, 1]$	Birch, Kuyk, Swinnerton-Dyer 1972 [2]
1	trivial	7.455	$[0, 0, 0, 0, 2]$	Cremona 1997 [6]
2	trivial	9.478	$[0, 0, 0, 0, -11]$	Gebel, Petho, Zimmer 1998 [19]
3	trivial	14.137	$[0, 0, 0, 0, 113]$	Gebel, Petho, Zimmer 1998 [19]
4	trivial	18.872	$[0, 0, 0, 0, 2089]$	Gebel, Petho, Zimmer 1998 [19]
5	trivial	24.083	$[0, 0, 0, 0, -28279]$	Gebel, Petho, Zimmer 1998 [19]
6	trivial	31.540	$[0, 0, 0, 0, 1358556]$	Womack 2000 [42]
7	trivial	39.296	$[0, 0, 0, 0, -56877643]$	Womack 2000 [42]
8	trivial	45.493	$[0, 0, 0, 0, -2520963512]$	Womack 2000 [42]
9	trivial	52.637	$[0, 0, 0, 0, -44865147851]$	Elkies 2009 [12]
10	trivial	61.126	$[0, 0, 0, 0, 3612077876156]$	Elkies 2009 [12]
11	trivial	72.659	$[0, 0, 0, 0, -998820191314747]$	Elkies 2009 [12]
12	trivial	80.089	$[0, 0, 0, 0, 41025014649039529]$	Elkies 2009 [12]
13	trivial	87.294	$[0, 0, 0, 0, 481637455514868115 36]$	Elkies 2009 [12]
14	trivial	103.188	$[0, 0, 0, 0, 785\cdots336]$	Elkies 2009 [12]
15	trivial	122.905	$[0, 0, 0, 0, 469\cdots417]$	Elkies 2009 [12]
16	trivial	136.203	$[0, 0, 0, 0, 116\cdots888]$	Elkies 2016 [13]
17*	trivial	155.363	$[0, 0, 0, 0, -908\cdots363]$	Elkies 2016 [14]
0	$(\mathbb{Z}/2\mathbb{Z})^2$	3.466	$[0, 0, 0, -1^2, 0]$	Birch, Kuyk, Swinnerton-Dyer 1972 [2]
1	$(\mathbb{Z}/2\mathbb{Z})^2$	6.685	$[0, 0, 0, -5^2, 0]$	Cremona 1997 [6]
2	$(\mathbb{Z}/2\mathbb{Z})^2$	9.825	$[0, 0, 0, -34^2, 0]$	Cremona 1997 [6]
3	$(\mathbb{Z}/2\mathbb{Z})^2$	17.041	$[0, 0, 0, -1254^2, 0]$	Rogers 2000 [35]
4	$(\mathbb{Z}/2\mathbb{Z})^2$	23.341	$[0, 0, 0, -29274^2, 0]$	Rogers 2000 [35]
5	$(\mathbb{Z}/2\mathbb{Z})^2$	38.850	$[0, 0, 0, -48272239^2, 0]$	Rogers 2004 [36]
6	$(\mathbb{Z}/2\mathbb{Z})^2$	47.997	$[0, 0, 0, -6611719866^2, 0]$	Rogers 2004 [36]
7	$(\mathbb{Z}/2\mathbb{Z})^2$	58.275	$[0, 0, 0, -797507543735^2, 0]$	Rogers 2004 [36]

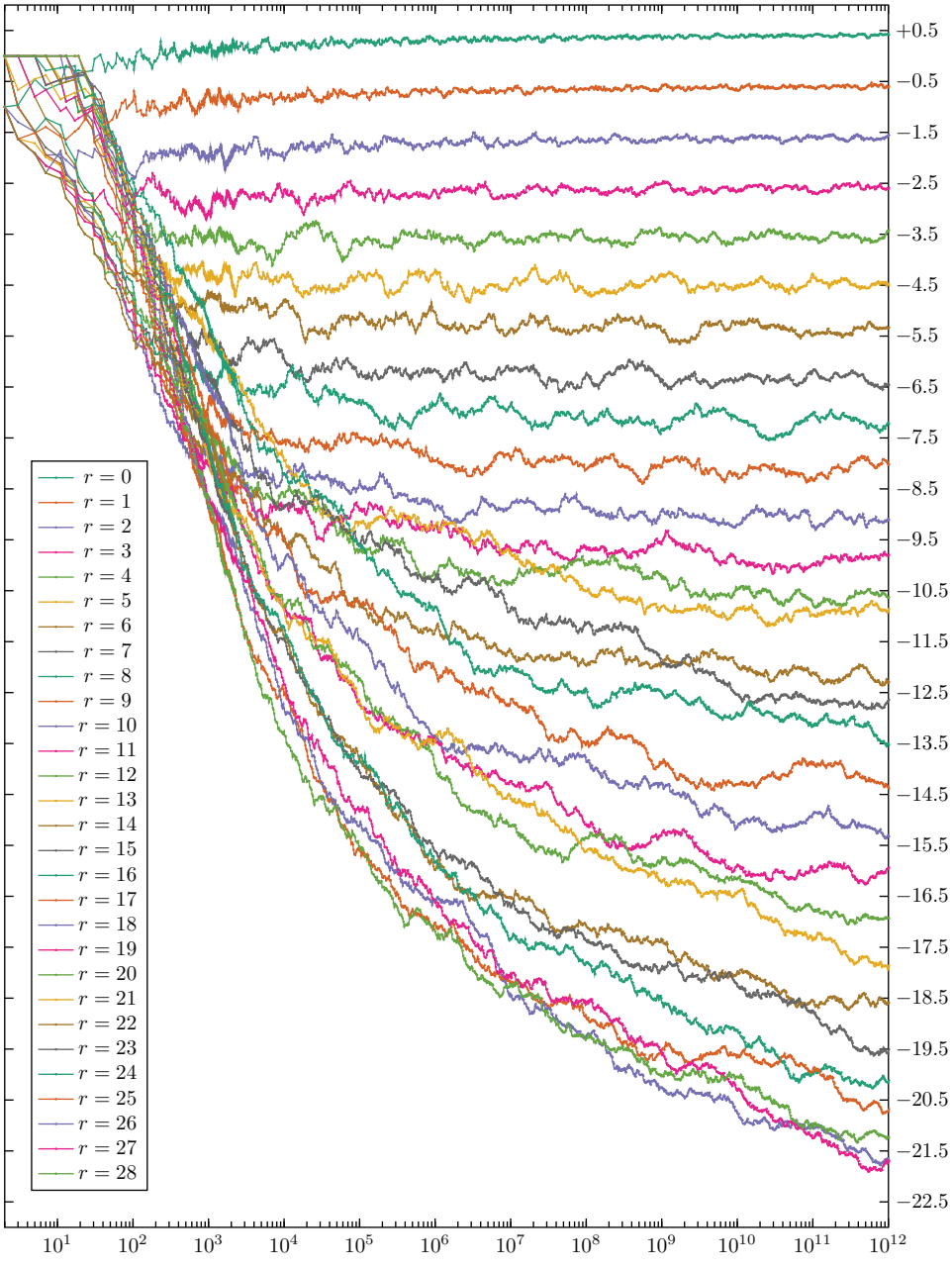

FIGURE 1. $S(x)$ plot for elliptic curves of rank $r = r_E$ listed in Table 1

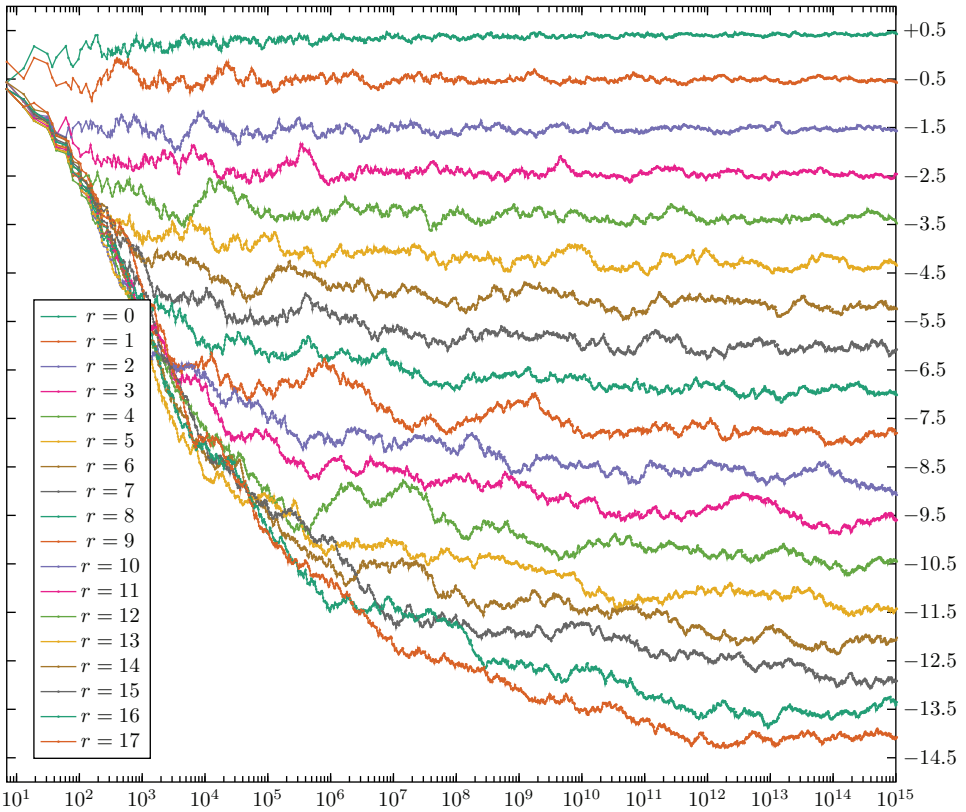

FIGURE 2. $S(x)$ plot for Mordell curves $y^2 = x^3 + k$ of rank $r = r_E$ listed in Table 1

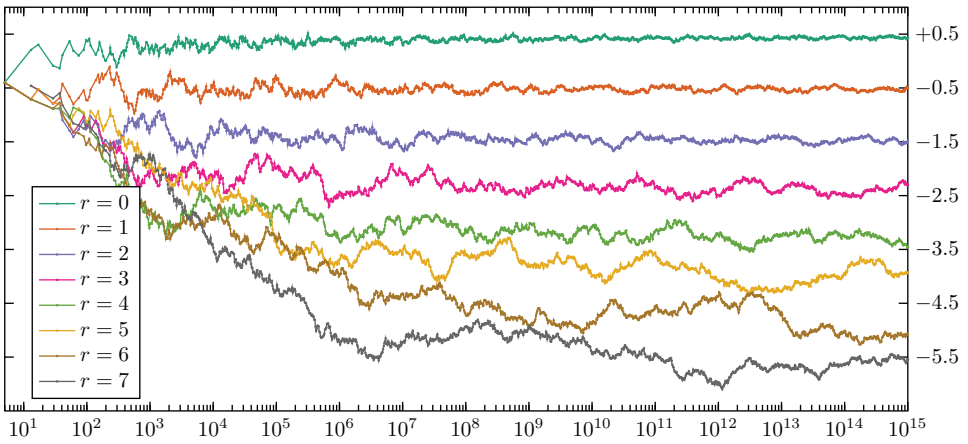

FIGURE 3. $S(x)$ plot for congruent number curves $y^2 = x^3 - n^2x$ of rank $r = r_E$ listed in Table 1

References

[1] W. Bosma, J.J. Cannon, C. Fieker, and A. Steel (Eds.), *Handbook of Magma functions*, v2.26-1, 2021.

[2] Bryan J. Birch and Willem Kuyk, *Table* 1, in *Modular Functions of One Variable IV, Proceedings of the International Summer School, University of Antwerp, RUCA, July 17–August 3, 1972*, Lecture Notes in Math. **476**, Springer,1975.

[3] J. W. Bober, *Conditionally bounding analytic ranks of elliptic curves*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 135–144, DOI 10.2140/obs.2013.1.135. MR3207411

[4] A. Brumer and O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 375–382, DOI 10.1090/S0273-0979-1990-15937-3. MR1044170

[5] G. Campbell, *Finding elliptic curves and families of elliptic curves over Q of large rank*, ProQuest LLC, Ann Arbor, MI, 1999. Thesis (Ph.D.)–Rutgers The State University of New Jersey - New Brunswick. MR2698708

[6] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR1628193

[7] John E. Cremona, *Minimal conductor of an elliptic curve over* $\mathbf{Q}$ *of rank* 4, NMBRTHRY listserv post, available at `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;6f6148dc.1204`, April 3, 2012.

[8] John E. Cremona, `eclib`, GitHub repository available at `https://github.com/JohnCremona/eclib`, accessed May 1, 2021.

[9] Andrej Dujella, *Elliptic curves of high rank with prescribed torsion (old version)*, including curves of rank 16 and 18 due to Dujella and Elkies (resp.), available at `https://web.math.pmf.unizg.hr/~duje/tors/z2old1415161718.html`, accessed May 1, 2021.

[10] Andrej Dujella, *History of elliptic curves rank records*, available at `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`, accessed May 1, 2021.

[11] Noam D. Elkies, $\mathbb{Z}^{28}$ *in* $E(\mathbb{Q})$*, etc.*, NMBRTHRY listerv post, available at `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;99f4e7cd.0605`, May 3, 2006.

[12] Noam D. Elkies, $j = 0$*, rank* 15*; also* 3*-rank* 6 *and* 7 *in real and imaginary quadratic fields*, NMBRTHRY listserv post, available at `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;6a3fad67.0912`, December 30, 2009.

[13] Noam D. Elkies, $j = 0$*, rank* 16*; also* 3*-rank* 7 *and* 8 *in real and imaginary quadratic fields*, NMBRTHRY listserv post, available at `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;fc0d1ed0.1602`, February 6, 2016.

[14] Noam D. Elkies, *How many points can a curve have?*, talk given at Arizona State University (Tempe), slides available at `http://math.harvard.edu/~elkies/many_pts_asu.pdf`, February 18, 2016.

[15] Noam D. Elkies, *Missing elliptic curve ranks*, personal email, received January 7, 2021.

[16] N. D. Elkies and M. Watkins, *Elliptic curves of large rank and small conductor*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 42–56, DOI 10.1007/978-3-540-24847-7_3. MR2137342

[17] S. Fermigier, *Un exemple de courbe elliptique définie sur* $\mathbf{Q}$ *de rang* ≥ 19 (French, with English and French summaries), C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), no. 6, 719–722. MR1183810

[18] Stefane Fermigier, *An elliptic curve of rank* ≥ 22 *over* $\mathbb{Q}$, NMBRTHRY listserv post, available at `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;5a3fefaa.9607`, July 7, 1996.

[19] J. Gebel, A. Pethö, and H. G. Zimmer, *On Mordell's equation*, Compositio Math. **110** (1998), no. 3, 335–367, DOI 10.1023/A:1000281602647. MR1602064

[20] D. Harvey and A. V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 127–147, DOI 10.1090/conm/663/13352. MR3502941

[21] K. S. Kedlaya and A. V. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 312–326, DOI 10.1007/978-3-540-79456-1_21. MR2467855

[22] Z. Klagsbrun, T. Sherman, and J. Weigandt, *The Elkies curve has rank 28 subject only to GRH*, Math. Comp. **88** (2019), no. 316, 837–846, DOI 10.1090/mcom/3348. MR3882286
[23] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, `http://www.lmfdb.org`, 2021.
[24] P. Llorente and J. Quer, *On the* 3*-Sylow subgroup of the class group of quadratic fields*, Math. Comp. **50** (1988), no. 181, 321–333, DOI 10.2307/2007934. MR917838
[25] Roland Martin and William McMillen, *An elliptic curve/*$\mathbb{Q}$ *of rank* 23, NMBRTHRY listserv post, available at `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;d3867479.9803`, March 16, 1998.
[26] Roland Martin and William McMillen, *An elliptic curve/*$\mathbb{Q}$ *of rank* 24, NMBRTHRY listserv post, available at `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;b8b5e7f2.0005`, May 2, 2000.
[27] J.-F. Mestre, *Construction d'une courbe elliptique de rang* ≥ 12 (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. **295** (1982), no. 12, 643–644. MR688896
[28] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques* (French), Compositio Math. **58** (1986), no. 2, 209–232. MR844410
[29] J.-F. Mestre, *Un exemple de courbe elliptique sur* $\mathbf{Q}$ *de rang* ≥ 15 (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. **314** (1992), no. 6, 453–455. MR1154385
[30] K.-i. Nagao, *Examples of elliptic curves over* $\mathbf{Q}$ *with rank* ≥ 17, Proc. Japan Acad. Ser. A Math. Sci. **68** (1992), no. 9, 287–289. MR1202634
[31] K.-i. Nagao, *An example of elliptic curve over* $\mathbf{Q}$ *with rank* ≥ 20, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), no. 8, 291–293. MR1249440
[32] K.-i. Nagao, *An example of elliptic curve over* $\mathbf{Q}(T)$ *with rank* ≥ 13, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), no. 5, 152–153. MR1291171
[33] K.-i. Nagao and T. Kouya, *An example of elliptic curve over* $\mathbf{Q}$ *with rank* ≥ 21, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), no. 4, 104–105. MR1276883
[34] J. Quer, *Corps quadratiques de* 3*-rang* 6 *et courbes elliptiques de rang* 12 (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. **305** (1987), no. 6, 215–218. MR907945
[35] N. F. Rogers, *Rank computations for the congruent number elliptic curves*, Experiment. Math. **9** (2000), no. 4, 591–594. MR1806294
[36] N. F. Rogers, *Elliptic curves x(3) + y(3) = k with high rank*, ProQuest LLC, Ann Arbor, MI, 2004. Thesis (Ph.D.)–Harvard University. MR2705989
[37] K. Rubin and A. Silverberg, *Choosing the correct elliptic curve in the CM method*, Math. Comp. **79** (2010), no. 269, 545–561, DOI 10.1090/S0025-5718-09-02266-2. MR2552240
[38] A. V. Sutherland, *Order computations in generic groups*, ProQuest LLC, Ann Arbor, MI, 2007. Thesis (Ph.D.)–Massachusetts Institute of Technology. MR2717420
[39] A. V. Sutherland, *Structure computation and discrete logarithms in finite abelian p-groups*, Math. Comp. **80** (2011), no. 273, 477–500, DOI 10.1090/S0025-5718-10-02356-2. MR2728991
[40] I. E. Shparlinski and A. V. Sutherland, *On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average*, LMS J. Comput. Math. **18** (2015), no. 1, 308–322, DOI 10.1112/S1461157015000017. MR3349320
[41] M. Watkins, S. Donnelly, N. D. Elkies, T. Fisher, A. Granville, and N. F. Rogers, *Ranks of quadratic twists of elliptic curves* (English, with English and French summaries), Numéro consacré au trimestre "Méthodes arithmétiques et applications", automne 2013, Publ. Math. Besançon Algèbre Théorie Nr., vol. 2014/2, Presses Univ. Franche-Comté, Besançon, 2015, pp. 63–98. MR3381037
[42] Tom Womack, *Minimal-known positive and negative k for Mordell curves of given rank*, web page snapshot available at `https://web.archive.org/web/20000925204914/http://tom.womack.net/maths/mordellc.htm`, September 25, 2000.

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario K7L 3N6, Canada
Email address: `sk206@queensu.ca`

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario K7L 3N6, Canada
Email address: `murty@queensu.ca`