Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

ON THE IDENTIFICATION OF ELLIPTIC CURVES THAT ADMIT INFINITELY MANY TWISTS SATISFYING THE BIRCH–SWINNERTON-DYER CONJECTURE

BARINDER S. BANWAIT AND XIAOYU HUANG

Abstract. Recent work of Burungale–Skinner–Tian–Wan established the first infinite families of quadratic twists of non-CM elliptic curves over $\mathbb{Q}$ for which the strong Birch–Swinnerton-Dyer (BSD) conjecture holds. Building on their results, we encode the required hypotheses into an explicit algorithm and apply it to the database of elliptic curves in the L-functions and Modular Forms Database (LMFDB), unconditionally identifying all elliptic curves E of conductor at most 500,000 that admit infinitely many quadratic twists satisfying the strong BSD conjecture. Our computations provide certain numerical evidence for a conjecture of Radziwiłł and Soundararajan predicting Gaussian behavior in the analytic order of the Shafarevich–Tate group, while also observing a positive bias within the BSD-satisfying subfamily.

1. Introduction

Significant progress has been made toward the Birch and Swinnerton-Dyer (BSD) conjecture from a statistical perspective. Through the work of Bhargava and Shankar on average ranks [3], combined with the Iwasawa-theoretic results of Skinner–Urban [37], Zhang [43], and others, it is now established that at least 66% of elliptic curves satisfy the rank part of the conjecture [4]. These results, however, are probabilistic in nature; they assure us that the conjecture holds frequently, but they do not necessarily tell us which specific curves satisfy the full BSD conjecture.

A complementary perspective is the algorithmic verification of the conjecture for specific curves up to a given conductor bound. As a result of an accumulation of works involving several people across many years [19, 32, 14, 31, 27], it is now known that the full BSD conjecture holds for all elliptic curves over $\mathbb{Q}$ with analytic rank 0 or 1 of conductor up to 5,000. At the most basic level, this is achieved by computing the order of the Shafarevich–Tate group $Ш(E)$ and showing it matches the other terms in the BSD conjectural formula (which are neatly packaged into a quantity $Ш(E)_{an}$ called the *analytic order of* $Ш(E)$). There are 31,073 elliptic curves with conductor less than 5,000; out of these, only 691 have analytic rank strictly greater than 1, meaning that the full BSD conjecture has been verified for $\approx 97.78\%$ of elliptic curves of conductor less than 5,000. We refer to the end of Section 5 of [27] for an account of how the multiple aforementioned works fit together to prove the stated result.

In this paper, we combine the algorithmic rigor of the second approach with the infinite scope of the first by identifying specific elliptic curves up to a conductor

2010 *Mathematics Subject Classification.* 11G05 (primary), 11Y16, 14Q05 (secondary).

bound that admit *infinitely many* quadratic twists satisfying the full BSD conjecture. Until recently, such families were known primarily for curves with Complex Multiplication (CM), thanks to the work of Coates–Wiles [12] and Rubin [35].

For non-CM curves, the landscape has expanded significantly with the recent work of Burungale–Skinner–Tian–Wan [6]. By establishing the p-part of the BSD conjecture at supersingular primes, together with earlier results in [37, 36, 7, 42] they proved the existence of infinite families of quadratic twists of non-CM elliptic curves satisfying the full BSD conjecture. In their work, they provided a list of such curves with conductor up to 150. While this list is given explicitly, details of the underlying algorithmic procedure for identifying these curves, as well as an implementation for verifying the requisite local conditions, are not made explicit.

Our first contribution is to translate the theoretical conditions of Burungale–Skinner–Tian–Wan into explicit, executable algorithms. We implement these checks and run them on the entire database of elliptic curves over $\mathbb{Q}$ in the L-functions and Modular Forms Database (LMFDB) [38]. This allows us to extend the list of known examples, identifying all elliptic curves of conductor $N < 500{,}000$ that unconditionally admit infinite families of BSD-satisfying twists.

Theorem 1.1. *Let $\mathcal{C}$ be the set of elliptic curves listed in* [2]*. For every $E \in \mathcal{C}$, there exists an explicit infinite family of quadratic twists $\{E_d\}$ such that each E_d satisfies the full Birch and Swinnerton-Dyer conjecture.*

The work [2] identifies 36,687 semistable elliptic curves admitting infinitely many quadratic twists satisfying the BSD conjecture, accounting for approximately 20.5% of optimal semistable analytic-rank-0 elliptic curves and 1.20% of all elliptic curves with conductor $N < 500{,}000$. We stress that unlike the probabilistic results, the BSD conjecture holds *unconditionally* for these families. This provides us with a unique dataset: a large collection of elliptic curves where the order of the Shafarevich–Tate group $|Ш(E_d)|$ is known unconditionally.

Our second contribution uses this dataset to study the statistical distribution of $Ш(E_d)$. A conjecture of Radziwiłł and Soundararajan [33], motivated by random matrix theory, predicts that for a fixed elliptic curve E, the values of $\log|Ш(E_d)| - \frac{1}{2}\log|d|$ (suitably normalized) should follow a standard Gaussian distribution as d varies. Previously, this conjecture could only be tested numerically by assuming the validity of BSD to interpret analytic L-values as actual group orders [15].

Because our dataset consists of families for which the full BSD conjecture is now unconditionally established, we are able to study the true order of $Ш(E_d)$ without relying on this assumption. We structure our analysis in two steps. First, to establish a baseline, we look at generic twists; assuming BSD for these twists, we recover the predicted Gaussian distribution. Second, we examine our specific, unconditionally BSD-verified families. Here, we observe a significant deviation: the true distribution for these families exhibits a positive bias compared to the generic Radziwiłł–Soundararajan prediction. This deviation is not unexpected: the BSD-verified twists form a constrained arithmetic subfamily, cut out by local congruence and splitting conditions on twist parameter d, rather than an unbiased sample of all quadratic twists.

Our work is supported by a code repository that is available here:

`https://github.com/cocoxhuang/ants_xvii`

We consider this repository a project that is built on top of the LMFDB, which we forked and are making use of in our work, all of which is contained in the `ants_xvii` folder. See the `README.md` at the top level of the repository for instructions on how to use the code to verify the claims made in this paper. Our algorithms are written in SageMath [39]. **All file paths in this paper will be relative to the `ants_xvii` directory of the above repository.**

Computing Environment. All computations reported here were carried out on a single laptop: an Apple MacBook Pro with an Apple M1 Pro processor (eight CPU cores) and 16 GB of unified memory, running macOS 26.4.1. The implementation uses SageMath 10.7, which bundles Python 3.13.3. Algorithm 1, executed against the full LMFDB elliptic-curve database at $N < 500{,}000$ (3,064,705 curves), runs to completion in 12 minutes and 26 seconds on this machine.

Acknowledgements. We thank the anonymous referees for their valuable comments and for suggesting recent work that led to improvements in Algorithm 1 as well as the exposition in general. We are grateful to Shuai Zhai for answering our questions regarding the curves listed in [6, Example 1]. We also thank Kannan Soundararajan for proposing the question of studying the empirical distribution of $|Ш(E_d)|$. We further thank Ashay Burungale, Chris Skinner, Ye Tian, and Xin Wan for answering our questions regarding their results. We would also like to thank Jaclyn Lang for helpful discussions.

2. Quadratic Twist Families That Satisfy the Full BSD Conjecture

The main contributions of this section are Algorithm 1 and Algorithm 2, which respectively (a) identify elliptic curves admitting infinitely many quadratic twists satisfying full BSD, and (b) determine these twists up to a bound on the twisting parameter. These algorithms are built upon many theoretical advances in the Iwasawa theory of elliptic curves, spanning the last 10 years, that establish the *p-part of BSD* (to be defined in Section 2.1) under various conditions. After discussing preliminaries, we discuss the p-part of BSD for odd primes p in Section 2.2, and the 2-part in Section 2.3. There is a certain set in Section 2.3 whose non-emptiness we need to understand for our algorithm to work; this is discussed in Section 2.4. We put the p-parts and 2-part together in Section 2.5 to obtain the mathematical statement Theorem 2.18. This result forms the basis of the algorithms, which are declared in pseudocode in Section 2.6. Finally in Section 2.7 we discuss the elliptic curves satisfying these conditions up to conductor 150, and compare our list with the corresponding list in [6, Example 1].

2.1. Notation and preliminaries.

In the sequel, we will use the notation $\mathrm{BSD}(E)$ to mean that the strong Birch–Swinnerton-Dyer conjecture has been established. Following Miller [32], we make the following definitions.

Definition 2.1. We define the **analytic order of** $Ш(E)$ as follows.

$$\#Ш(E)_{\mathrm{an}} := \frac{L^{(r)}(E,1)}{r!} \cdot \frac{|E(\mathbb{Q})_{\mathrm{tors}}|^2}{\Omega(E) \cdot \mathrm{Reg}(E) \cdot \prod_p c_p}, \tag{2.1}$$

where $r = r_{\mathrm{an}}(E)$, so that the leading factor $L^{(r)}(E,1)/r!$ is the leading nonzero Taylor coefficient of $L(E,s)$ at $s = 1$.

Definition 2.2. We denote by $\mathrm{BSD}(E/\mathbb{Q}, \infty)$ the assertion that the real number $\#Ш(E)_{\mathrm{an}}$ is positive.

Definition 2.3. We denote by $\mathrm{BSD}(E/\mathbb{Q}, p)$ the following assertions.

(1) The rank r of $E(\mathbb{Q})$ is equal to the analytic rank $r_{\mathrm{an}}(E)$.
(2) The p-primary part $Ш(E)(p)$ of the Shafarevich–Tate group is finite.
(3) The real number $\#Ш(E)_{\mathrm{an}}$ is rational.
(4) The conjectural formula holds at p; that is,

$$\mathrm{ord}_p(\#Ш(E)_{\mathrm{an}}) = \mathrm{ord}_p(\#Ш(E)(p)).$$

Write $M_{\mathbb{Q}} = \{\,\text{primes of } \mathbb{Q}\,\} \cup \{\infty\}$ for the set of places of $\mathbb{Q}$. The following is immediate from the definitions, since two positive rational numbers are equal if and only if they have the same v-adic valuation for every place v.

Proposition 2.4. $\mathrm{BSD}(E)$ *holds if and only if* $\mathrm{BSD}(E/\mathbb{Q}, v)$ *holds for all* $v \in M_{\mathbb{Q}}$.

We now specialise to the case $r_{\mathrm{an}}(E) \leq 1$, which is the only case occurring in this paper.

Theorem 2.5 (Gross–Zagier, Kolyvagin, Kohnen–Zagier)**.** *Suppose* $r_{\mathrm{an}}(E) \leq 1$. *Then assertions (1), (2), (3) of* $\mathrm{BSD}(E/\mathbb{Q}, p)$ *hold for every prime* p, *and* $\mathrm{BSD}(E/\mathbb{Q}, \infty)$ *holds. Consequently,*

$$\mathrm{BSD}(E) \iff \mathrm{ord}_p(\#Ш(E)_{\mathrm{an}}) = \mathrm{ord}_p(\#Ш(E)(p)) \quad \textit{for all primes } p.$$

Proof. The hypothesis $r_{\mathrm{an}}(E) \leq 1$ implies $r = r_{\mathrm{an}}(E)$ (assertion (1)) and the finiteness of $Ш(E)$ (assertion (2)), by Gross–Zagier [20] and Kolyvagin [25]. The rationality of $\#Ш(E)_{\mathrm{an}}$ (assertion (3)) follows from the rationality of $L(E,1)/\Omega(E)$ when $r_{\mathrm{an}} = 0$ [28] and from the Gross–Zagier formula when $r_{\mathrm{an}} = 1$. For $\mathrm{BSD}(E/\mathbb{Q}, \infty)$ we must show $L^{(r)}(E,1)/r! > 0$: if $r_{\mathrm{an}} = 0$, the non-negativity of the central value $L(E,1) \geq 0$ [24] together with $L(E,1) \neq 0$ gives $L(E,1) > 0$; if $r_{\mathrm{an}} = 1$, the Gross–Zagier formula expresses $L'(E,1)$ as a positive multiple of the Néron–Tate height of a non-torsion Heegner point, so $L'(E,1) > 0$.

By Proposition 2.4, and as assertions (1)–(3) and $\mathrm{BSD}(E/\mathbb{Q}, \infty)$ have now been verified, $\mathrm{BSD}(E)$ is equivalent to assertion (4) holding at every finite prime. Concretely, writing $\mathbb{Q}^\times \cong \{\pm 1\} \times \bigoplus_p p^{\mathbb{Z}}$, the finite valuations $(\mathrm{ord}_p q)_p$ of a nonzero rational q fix only its absolute value $|q| = \prod_p p^{\mathrm{ord}_p q}$ (the product formula); thus the equalities $\mathrm{ord}_p(\#Ш(E)_{\mathrm{an}}) = \mathrm{ord}_p(\#Ш(E)(p))$ pin down $\#Ш(E)_{\mathrm{an}}$ up to sign, and the positivity $\mathrm{BSD}(E/\mathbb{Q}, \infty)$ supplies the missing sign at the real place. □

Definition 2.6. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $\phi\colon X_0(N) \to E$ be a modular parametrization sending the cusp at infinity to the origin of E. We say that E is *optimal* if ϕ does not factor through any other elliptic curve in the isogeny class of E. If E is optimal and ω is the Néron differential on a global minimal Weierstrass equation for E, then the unique integer $\nu_E \in \mathbb{Q}^\times$ satisfying

$$\phi^*(\omega) = \nu_E f(\tau)\, d\tau,$$

where f is the normalized newform associated to E, is called the *Manin constant* of E.

See [1] for more on the Manin constant. It is conjectured to be 1 in all cases.

Definition 2.7. Let $E/\mathbb{Q}$ be an elliptic curve of analytic rank 0. We define the *algebraic L-value* as

$$L^{(\mathrm{alg})}(E,1) := \frac{L(E,1)}{\Omega(E)}.$$

2.2. **p-part of BSD for p odd.** Building on recent advances [37, Theorem 2], [6, Corollary 10.2], [36, Theorem C], and [6, Theorem 9.21], it is now known that a large class of elliptic curves E satisfy $\mathrm{BSD}(E,p)$ for odd primes p. The case relevant to our work is when the quadratic twists have rank zero.

We begin by isolating the following step to be used in the sequel. It is a slight strengthening of Ribet's level-lowering argument from [34].

Lemma 2.8. *Let $E/\mathbb{Q}$ be a semistable elliptic curve of conductor N, and let p be an odd prime of good ordinary reduction for E such that $\overline{\rho}_{E,p}$ is irreducible. Then there exists an* odd *prime $q \neq p$ with $q \parallel N$ at which $\overline{\rho}_{E,p}$ is ramified.*

Proof. Since E is semistable, N is squarefree, and at each prime $\ell \mid N$ the curve E has multiplicative reduction; thus $\overline{\rho}_{E,p}$ is ramified at such an $\ell \neq p$ if and only if $p \nmid \mathrm{ord}_\ell(\Delta_E)$, in which case its conductor exponent at ℓ is 1, and otherwise $\overline{\rho}_{E,p}$ is unramified at ℓ. At p itself, good reduction gives prime-to-p conductor. Consequently the (prime-to-p) Serre conductor $N(\overline{\rho}_{E,p})$ is the squarefree product of those primes $\ell \parallel N$, $\ell \neq p$, at which $\overline{\rho}_{E,p}$ ramifies; in particular $N(\overline{\rho}_{E,p}) \mid N$ and is squarefree and prime to p. Moreover, as p is a prime of good *ordinary* reduction, the Serre weight is $k(\overline{\rho}_{E,p}) = 2$.

Suppose, for contradiction, that $\overline{\rho}_{E,p}$ is unramified at every *odd* prime $q \parallel N$ with $q \neq p$. Then the only prime that can divide $N(\overline{\rho}_{E,p})$ is 2, so $N(\overline{\rho}_{E,p}) \in \{1, 2\}$. Since $\overline{\rho}_{E,p}$ is irreducible with p odd, Ribet's level-lowering theorem [34] (together with the modularity of E) produces a normalized eigenform of weight $k(\overline{\rho}_{E,p}) = 2$ on $\Gamma_0(N(\overline{\rho}_{E,p}))$, hence on $\Gamma_0(1)$ or $\Gamma_0(2)$, giving rise to $\overline{\rho}_{E,p}$. But the modular curves $X_0(1)$ and $X_0(2)$ both have genus 0, so $S_2(\Gamma_0(1)) = S_2(\Gamma_0(2)) = 0$; there are no such eigenforms, yielding the desired contradiction. □

Proposition 2.9. *Let p be an odd prime, E a semistable elliptic curve over $\mathbb{Q}$ with conductor N, and E_d the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, where $(d, N) = 1$. Write D for the discriminant of this quadratic field, and write N_{E_d} for the conductor of E_d. Suppose $L(E_d, 1) \neq 0$. Then p either divides d, or else is good ordinary, good supersingular, or multiplicative for E_d. In each of these four cases, if the following conditions hold, then $\mathrm{BSD}(E_d, p)$ holds.*

(1) If $p \mid d$:
  (a) $p \geq 5$ and p is a good ordinary prime for E;
  (b) $\overline{\rho}_{E,p}$ is irreducible.
(2) If $p \nmid d$ and is good ordinary: no further conditions.
(3) If $p \nmid d$ and is multiplicative:
  (a) $\overline{\rho}_{E_d,p}$ is irreducible;
  (b) there is a prime $q \neq p$ such that $q \parallel N_{E_d}$ and $\overline{\rho}_{E_d,p}$ is ramified at q.
(4) If $p \nmid d$ and p is supersingular:
  (a) $(D, N) = 1$;
  (b) if $p = 3$, then $a_3(E) = 0$.

Proof. The four cases correspond to the different reduction types for E_d at p, with $p \mid d$ being equivalent to E_d having additive reduction at p (because the primes dividing d divide the conductor of E_d to order at least 2).

(1) Since $p \mid d$, we have $p \mid D$, so this is the additive twist case of [6, Theorem 9.21(c)], applied with $K = \mathbb{Q}(\sqrt{d})$: conditions (a) and (b) supply

the hypotheses that $p \geq 5$ is ordinary for E with $\overline{\rho}_{E,p}$ irreducible (their $p \nmid 6N$ and $(\mathrm{irr}_{\mathbb{Q}})$). For their condition (ram_K), note that (a), (b), and the semistability of E are exactly the hypotheses of Lemma 2.8, which furnishes an odd prime $q \neq p$ with $q \parallel N$ at which $\overline{\rho}_{E,p}$ is ramified; since q is odd and $q \nmid d$, it does not divide D, giving (ram_K). The passage from the equality of Iwasawa ideals in [6, Theorem 9.21(c)] to the p-part of the BSD formula for E_d is Kato's rank-zero descent (cf. the $r = 0$ ordinary case in the proof of [6, Corollary 10.2], following [21, §14.20]).

(2) This case was first dealt with by Skinner–Urban [37, Theorem 3.33, Theorem 3.35] under the following additional conditions:
- surjectivity of the mod-p representation $\bar{\rho}_{E_d,p}$;
- the *ramified prime* condition: there exists a prime $q \mid\mid N_{E_d}$, $q \neq p$, such that $\bar{\rho}_{E_d,p}$ is ramified at q.

Subsequently, in [36, Theorem C], the surjectivity condition was weakened to the representation being irreducible.

We now show that, when $\bar{\rho}_{E_d,p}$ is irreducible, the ramified prime condition follows from semistability of E. Since p is odd, $\overline{\rho}_{E_d,p} \cong \overline{\rho}_{E,p} \otimes \chi_d$, where χ_d is the quadratic character of $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$; twisting by a character preserves irreducibility, so $\overline{\rho}_{E,p}$ is irreducible as well. As $p \nmid d$ and $(d, N) = 1$, the prime p is one of good reduction for E, and it is good ordinary for E since it is so for E_d (ordinarity being preserved under quadratic twist away from p). Thus E, p satisfy the hypotheses of Lemma 2.8, which furnishes an odd prime $q \neq p$ with $q \parallel N$ at which $\overline{\rho}_{E,p}$ is ramified.

We claim this same q witnesses the ramified prime condition for E_d. Indeed, q is odd and $q \mid N$, while $(d, N) = 1$ forces $q \nmid d$; hence q does not divide D, so χ_d is unramified at q. Therefore $\overline{\rho}_{E_d,p}|_{I_q} = \overline{\rho}_{E,p}|_{I_q}$ is ramified, and the conductor exponent of E_d at q equals that of E, namely 1; that is, $q \parallel N_{E_d}$ with $\overline{\rho}_{E_d,p}$ ramified at q. This is precisely the ramified prime condition for E_d, and hence [36, Theorem C] gives $\mathrm{BSD}(E_d, p)$ in the irreducible case.

The reducible case was addressed for all odd primes by [10, Theorem D] (building on [9, Theorem F]) up to a certain condition on the isogeny character denoted ϕ in *loc. cit.*. This condition was removed by [23, Theorem C]. Thus, we have $\mathrm{BSD}(E_d, p)$ in both cases (irreducible and reducible).

(3) This is [36, Theorem C].

(4) Here $p \nmid d$ is supersingular for E_d, hence also for E, and $a_p(E_d) = \chi_d(p)\, a_p(E) = \pm\, a_p(E)$. We verify the hypotheses of [6, Corollary 10.2] for E, applied with the quadratic field $K = \mathbb{Q}(\sqrt{d})$. As E is semistable its conductor N is squarefree, and $p \nmid 2N$ since p is odd and of good reduction for E. The twisting field has discriminant D, which is coprime to Np by assumption (a). Finally we check $a_p(E) = 0$. If $p > 3$, supersingularity forces $a_p(E) = 0$ by the Hasse bound; and if $p = 3$ then $a_3(E) = 0$ by condition (b).

Thus E satisfies the hypotheses of [6, Corollary 10.2], which yields $\mathrm{BSD}(E, p)$; the final clause of that corollary, valid for quadratic twists by a field of discriminant coprime to Np, then gives $\mathrm{BSD}(E_d, p)$. □

Remark 2.10. The semistable condition in the above result is a strong restriction, and is needed for Item 4, Item 1, and for Item 2 when $\overline{\rho}_{E_d,p}$ is irreducible.

Item 4 relies on [6, Corollary 10.2], whose proof rests on the resolution of Kobayashi's main conjecture [6, Theorem 10.1] and which carries the squarefree condition on the conductor.

Item 1 uses semistability only to supply the *ramified prime* condition via Lemma 2.8; without it, one adds that condition as a hypothesis.

Item 3 holds for non-semistable curves since the underlying result [36, Theorem C] applies with no restriction on the conductor.

For Item 2, we first consider the case of reducible residual representation. If $\bar{\rho}_{E_d,p}$ is reducible, the result holds for non-semistable curves for every odd p, by [10, Theorem D] (with the condition on ϕ removed in [23, Theorem C]), just as in the above proof. When $\bar{\rho}_{E_d,p}$ is irreducible, however, our argument uses the semistability of E to produce the ramified prime via Lemma 2.8, which is unavailable for a non-semistable base curve. In that setting one may verify the ramified prime condition directly; or, for $p \geq 5$, there is work of Burungale–Castella–Skinner [5, Corollary 1.3.1], which establishes the irreducible case for non-semistable curves at the expense of further hypotheses: the curve being non-CM, and a condition on the image of $\bar{\rho}_{E_d,p}$.

Remark 2.11. It is important to point out the parts of the above Proposition that depend on unpublished results in the literature. These are Items 1 and 4, which depend on [6] and [8]; and the reducible case of 2, which depends on [23].

We briefly mention some other related unpublished works that could be useful for future possible algorithmic extensions.

- The preprint [17] deals with arbitrary reduction type under various assumptions on the mod-p Galois representation attached to E, as listed in Theorem 1.7 of *loc. cit.*. It is not immediately apparent how to algorithmically verify these conditions.
- The paper [41] is subsequent to [6], adopts a similar approach, and has already appeared in print. Their Corollary 1.4 deals with the good ordinary case for both analytic rank 0 and 1 under an assumption labeled '(Im)' appearing in their Theorem 1.2. For our purposes of analytic rank 0, since we don't have *any* additional conditions here, Corollary 1.4 of this paper does not provide an additional input. However, this could be useful for possible extensions of our algorithmic work to analytic rank 1, although, as with [17], it is not clear how to algorithmically verify the condition '(Im)'.

Since many of the results used in the proof of Proposition 2.9 apply to a general semistable curve E, we record what can be said about $\mathrm{BSD}(E,p)$ directly.

Proposition 2.12. *Let p be an odd prime, E a semistable elliptic curve over $\mathbb{Q}$ with conductor N, and suppose $L(E,1) \neq 0$. Then p is good ordinary, good supersingular, or multiplicative for E, and in each case $\mathrm{BSD}(E,p)$ holds under the following conditions.*

(1) If p is good ordinary: no further conditions.
(2) If p is multiplicative:
  (a) $\overline{\rho}_{E,p}$ is irreducible;
  (b) there is a prime $q \neq p$ with $q \parallel N$ at which $\overline{\rho}_{E,p}$ is ramified.
(3) If p is supersingular: no further conditions.

Proof. Since E is semistable it has no additive primes, leaving the three cases above. Each is the $d = 1$ specialization of the corresponding case of Proposition 2.9, with E in place of E_d, and we only indicate the (minor) differences.

For Item 1, the argument of Item 2 applies verbatim: when $\overline{\rho}_{E,p}$ is irreducible, Lemma 2.8 supplies a prime $q \parallel N$ at which it is ramified, whence [36, Theorem C] gives $\mathrm{BSD}(E, p)$; the reducible case is [10, Theorem D] (with the condition on ϕ removed in [23, Theorem C]). Item 2 is again [36, Theorem C].

For Item 3, if $p > 3$, or $p = 3$ with $a_3(E) = 0$, this is [6, Theorem 1.5] applied to E. The remaining case $p = 3$, $a_3(E) = \pm 3$ is [8, Theorem C], whose hypothesis that E admit no rational p-power isogeny is automatic: a rational p-isogeny would give a $G_{\mathbb{Q}_p}$-stable line in $E[p]$, contradicting the irreducibility of $\overline{\rho}_{E,p}|_{G_{\mathbb{Q}_p}}$ at a supersingular prime (tame inertia acting through the fundamental characters of level 2). □

Proposition 2.9 is used to establish the following result, which is a sharpened version of [6, Theorem 10.12].

Theorem 2.13. *Let E be a semistable elliptic curve over $\mathbb{Q}$ with conductor N, and $d > 1$ a squarefree integer. Let E_d denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ of discriminant D. Suppose the following conditions hold.*

- *(i)* $(D, 3N) = 1$.
- *(ii)* $L(E_d, 1) \neq 0$.
- *(iii)* $\mathrm{BSD}(E_d, 2)$ *is true.*
- *(iv)* $a_3(E) \in \{-2, -1, 0, 1, 2\}$.
- *(v) For $p \in \{3, 5, 7\}$, E does not admit a rational p-isogeny.*
- *(vi) For any prime $p|N$, there exists a multiplicative prime $q \neq p$ of E at which $E[p]$ is ramified.*
- *(vii) E has ordinary reduction at prime divisors of d.*

Then $\mathrm{BSD}(E_d)$ *is true.*

Proof. From Theorem 2.5 applied to E_d (which is permissible because of assumption (ii)), we need to show that $\mathrm{BSD}(E_d, p)$ holds for all p. Condition (iii) treats the prime 2, so we are reduced to showing $\mathrm{BSD}(E_d, p)$ for odd primes p.

First suppose that $p \mid d$. From Case 1 of Proposition 2.9, we need to show $p \neq 3$, p is a good ordinary prime for E, and $\bar{\rho}_{E,p}$ is irreducible. These follow from assumptions (i), (vii) and (v) respectively (noting that [30, Theorem 4] ensures irreducibility (even surjectivity) of the residual representation for semistable curves and $p \geq 11$).

If $p \nmid d$ and p is good ordinary, then there is nothing further to check.

If $p \nmid d$ and p is multiplicative, then the conditions in Case 3 follow from assumptions (v) and (vi) (noting again that [30, Theorem 4] ensures we only need to consider primes ≤ 7). Here assumption (vi) provides a multiplicative prime q of E at which $\overline{\rho}_{E,p}$ is ramified; since $q \mid N$ and $(D, N) = 1$ we have $q \nmid D$, so χ_d is unramified at q. Hence $q \parallel N_{E_d}$ and $\overline{\rho}_{E_d,p}|_{I_q} = \overline{\rho}_{E,p}|_{I_q}$ is ramified, so q witnesses the ramified prime condition of Case 3 for E_d.

If $p \nmid d$ and p is supersingular, then the required conditions are established by assumptions (i) and (iv). □

2.3. **2-part of BSD for E_d.** Theorem 2.13 has a major condition of knowing $\mathrm{BSD}(E_d, 2)$. In this section we collect the conditions under which $\mathrm{BSD}(E_d, 2)$ can be established, which will feed into Theorem 2.13 in Section 2.5.

The result [6, Theorem 10.12] does not explicitly enumerate all of the hypotheses under which one may conclude $\mathrm{BSD}(E_d, 2)$. The discussion there refers to [7, Theorem 1.5] and [42, Theorem 1]; however, in the latter reference the relevant results are presented as Theorems 1.1–1.9. These theorems address closely related situations but involve differing assumptions, notably concerning the sign of the discriminant and the presence or absence of rational 2-torsion. For the reader's convenience, we therefore provide the following result that collects the required hypotheses into a single, self-contained statement.

Theorem 2.14. *Let $E/\mathbb{Q}$ be an optimal elliptic curve over $\mathbb{Q}$ of conductor N with odd Manin constant and analytic rank 0. Let d be a squarefree integer coprime to N and congruent to 1 modulo 4, and suppose that every prime divisor of N splits in $\mathbb{Q}(\sqrt{d})$. Assume that the 2-part of BSD holds for E.*

If one of the following sets of conditions holds, then $L(E_d, 1) \neq 0$, and the 2-part of BSD holds for E_d.

1. *If $E(\mathbb{Q})[2] = 0$ and E has negative discriminant:*
   - (a) *for every $p|d$, p is inert in the number field $\mathbb{Q}[x]/(f(x))$, where $f(x)$ is the two-division polynomial of E.*
   - (b) $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = 0$.
2. *If $E(\mathbb{Q})[2] = 0$ and E has positive discriminant:*
   - (a) *for every $p|d$, p is inert in the number field $\mathbb{Q}[x]/(f(x))$, where $f(x)$ is the two-division polynomial of E.*
   - (b) $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = 0$.
   - (c) $d > 0$.
3. *If $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$:*
   - (a) *for every $p|d$, $p \equiv 1 \pmod 4$, and* $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$.
   - (b) $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = -1$.
   - (c) *2 splits in $\mathbb{Q}(\sqrt{d})$.*
   - (d) *$E'(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ and $Ш(E')[2] = 0$, where $E' := E/E(\mathbb{Q})[2]$ is the 2-isogenous curve of E.*

We stress that in this result it is assumed that one knows the 2-part of BSD for one elliptic curve.

Proof. This result is obtained by amalgamating Theorems 1.1 and 1.5 of [7] for the case $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$; Theorems 1.1 and 1.2 of [42] for the case $E(\mathbb{Q})[2] = 0$ and negative discriminant; and Theorems 1.3 and 1.4 of [42] for the case $E(\mathbb{Q})[2] = 0$ and positive discriminant. There are then some other conditions needed as follows:

(1) The requirement that E have rank 0 is needed due to the use of modular symbols [13, Chapter 3]. This is mentioned in [7, Section 1] and confirmed by Zhai in private communication.

(2) The condition in Item 2b is written as $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = 1$ in Zhai's paper because he is using a slightly different definition of $L^{(\mathrm{alg})}(E, 1)$ than that being used in [7]. In this paper we are using the same definition as in [7], so we need to subtract the 2-adic valuation of the number of connected components of $E(\mathbb{R})$, yielding 0.

(3) The condition $E'(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ in Item 3d is not explicitly written in the theorem statements of [7], but is mentioned in Remark 1.3 of *loc. cit.* as being a necessary condition for non-emptiness of the set

$$\mathcal{S} := \left\{ q \equiv 1 \pmod 4 : q \nmid N,\ \mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_q)) = 1 \right\}, \tag{2.2}$$

which will become the set of primes where the twists d are supported. □

Remark 2.15. We note that there are no analogues of Theorems 1.2 and 1.4 of [42] in the case $E(\mathbb{Q})[2] \neq 0$. There are such analogues for the case $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ in [7]. Therefore, we do not have such results in the full rational 2-torsion case, and it is for this reason that this case is missing in the above result.

2.4. **Condition for $\mathcal{S} \neq \emptyset$.** As explained in [7, Remark 1.3], once one has shown that the set $\mathcal{S}$ in Equation (2.2) is non-empty, then by Chebotarev density arguments, it must have positive density, yielding infinitely many twists in the case $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. However, there remains the problem that it may be empty, meaning that there may be no such twists in this case. This section deals with this scenario.

We note that Item 3d of Theorem 2.14 is not sufficient (only necessary) to ensure non-emptiness of $\mathcal{S}$. The curve `85a1` is an example of a curve that passes all of the above checks, yet for all primes $p \equiv 1 \pmod 4$ up to 10,000, we have $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) \geq 2$ (excluding the bad primes 5 and 17 where the valuation is zero). In this case, the existence of an isogenous curve over $\mathbb{Q}(i)$ with full 2-torsion (as stated on the curve's basechange page) explains why $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) \geq 2$ for all good primes $p \equiv 1 \pmod 4$.

In general, the main result of [22] applied to $E/\mathbb{Q}(i)$ shows that, if $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) \geq 2$ for all good primes $p \equiv 1 \pmod 4$, then this must be explained by the existence of an isogenous curve $E'/\mathbb{Q}(i)$ that has 4 dividing $\#E'(\mathbb{Q}(i))_{\mathrm{tors}}$. Whether or not this happens can be expressed in terms of $E/\mathbb{Q}$ itself, as follows.

Proposition 2.16. *Let $E/\mathbb{Q}$ be an elliptic curve with $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. Write*

$$E : y^2 = f(x),$$

and let $x_0 \in \mathbb{Q}$ be such that $(x_0, 0)$ is the rational point of order 2.

Then there exists a good prime $p \equiv 1 \pmod 4$ with $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$ if and only if none of $f'(x_0)$, $-f'(x_0)$, or $-\Delta$ are squares in $\mathbb{Q}$.

Before giving the proof, we recall the link between $f'(x_0)$ and divisibility of the 2-torsion point by 2 that arises in the Kummer theory input to the Weak Mordell–Weil theorem. Writing $f(x) = (x - x_0)(x - \alpha)(x - \beta)$ over $\overline{\mathbb{Q}}$, we have $f'(x_0) = (x_0 - \alpha)(x_0 - \beta)$. The halving criterion is that for a field K in which f splits as above with $x_0 \in K$, the point $P_0 = (x_0, 0)$ lies in $2E(K)$ if and only if $(x_0 - \alpha)(x_0 - \beta) = f'(x_0)$ is a square in K. Concretely, if $Q = (x_1, y_1)$ satisfies $2Q = P_0$, then the duplication formula forces $x_1 - x_0$ to be a square root of $f'(x_0)$ (up to a sign convention). We apply this criterion with $K = \mathbb{F}_p$ in condition (c) below.

Proof. ($\Longleftarrow$): Write $f(x) = (x - x_0)g(x)$ where g is a monic quadratic. Since $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$, the quadratic g has no rational root, so $\mathrm{disc}(g)$ is a non-square in $\mathbb{Q}$. We have $\Delta(E) = 16 f'(x_0)^2 \,\mathrm{disc}(g)$, whence Δ and $\mathrm{disc}(g)$ agree in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$; in particular, Δ is a non-square.

We seek a prime p satisfying:

(a) $p \equiv 1 \pmod 4$, i.e., -1 is a square mod p;
(b) Δ is a non-square mod p (so g is irreducible mod p, making $(x_0, 0)$ the only 2-torsion point of $\widetilde{E}(\mathbb{F}_p)$, and hence the 2-Sylow cyclic);
(c) $f'(x_0)$ is a non-square mod p, so that $(x_0, 0) \notin 2\widetilde{E}(\mathbb{F}_p)$ by the halving criterion applied over $\mathbb{F}_p$ as in the preamble (note that $f'(x_0) \in \mathbb{F}_p$ even though the roots of g are only in $\mathbb{F}_{p^2}$); hence the 2-Sylow has order exactly 2.

Equivalently, we want a prime that splits in $\mathbb{Q}(i)$ and is inert in both $\mathbb{Q}(\sqrt{f'(x_0)})$ and $\mathbb{Q}(\sqrt{\Delta})$.

Let $L = \mathbb{Q}(i, \sqrt{f'(x_0)}, \sqrt{\Delta})$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. The action on $(i, \sqrt{f'(x_0)}, \sqrt{\Delta})$ embeds $G \hookrightarrow \{\pm 1\}^3$. It suffices to show that $\sigma = (+1, -1, -1) \in G$: Chebotarev then produces infinitely many primes with $\mathrm{Frob}_p = \sigma$, each satisfying (a), (b), (c).

The image of G in $\{\pm 1\}^3$ is cut out by the multiplicative relations among $\{-1, f'(x_0), \Delta\}$ modulo squares in $\mathbb{Q}^*$. There are seven nontrivial products to consider:

- -1, $f'(x_0)$, Δ a square: ruled out (trivially, by hypothesis, and by the discriminant computation above, respectively);
- $-f'(x_0)$, $-\Delta$ a square: ruled out by hypothesis;
- $f'(x_0) \cdot \Delta$ or $-f'(x_0) \cdot \Delta$ a square: not ruled out by the hypothesis.

We check that the two relations not excluded by hypothesis are compatible with σ.

If $f'(x_0) \cdot \Delta$ is a square in $\mathbb{Q}$, then $\sqrt{\Delta} \in \mathbb{Q}(\sqrt{f'(x_0)})$, forcing every element of G to act with the same sign on $\sqrt{f'(x_0)}$ and $\sqrt{\Delta}$. Our σ acts as $(-1, -1)$ on this pair, so the relation is satisfied.

If $-f'(x_0) \cdot \Delta$ is a square, then $\sqrt{\Delta} \in \mathbb{Q}(i, \sqrt{f'(x_0)})$ with $\sqrt{\Delta} = i \cdot \alpha$ for some $\alpha \in \mathbb{Q}(\sqrt{f'(x_0)})$, so every element of G acts on $\sqrt{\Delta}$ by the product of its actions on i and $\sqrt{f'(x_0)}$. For σ, this product is $(+1)(-1) = -1$, matching its action on $\sqrt{\Delta}$.

Thus $\sigma \in G$, and Chebotarev density yields infinitely many good primes p with $\mathrm{Frob}_p = \sigma$. For each such p, conditions (a)–(c) hold, so $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$.

($\Longrightarrow$): If there exists such a prime p, it must satisfy $p \equiv 1 \pmod 4$ and be inert in both $\mathbb{Q}(\sqrt{f'(x_0)})$ and $\mathbb{Q}(\sqrt{\Delta})$. This means the Frobenius element $(+1, -1, -1)$ actually exists in the Galois group. If any of $f'(x_0)$, $-f'(x_0)$, or $-\Delta$ were squares in $\mathbb{Q}$, that specific Frobenius element would be algebraically impossible (it would force a contradiction in the signs). Thus, none of them can be squares. □

Remark 2.17. We have verified Proposition 2.16 computationally on every elliptic curve E that reaches this stage of our algorithm. Whenever E satisfies the algebraic criterion of the proposition, we exhibit an explicit prime $q \leq 10^4$ with $q \equiv 1 \pmod 4$, $q \nmid N$, and $\mathrm{ord}_2\big(\#E(\mathbb{F}_q)\big) = 1$, thereby witnessing $\mathcal{S} \neq \emptyset$. Conversely, whenever E fails the criterion, we have checked that no such prime exists in the range $q \leq 10^4$, verifying the conclusion $\mathcal{S} = \emptyset$.

The criterion in the above result will be used in the algorithms to follow to ensure non-emptiness of $\mathcal{S}$.

2.5. **Putting the parts together.** We now seek to combine Theorem 2.13 and Theorem 2.14. Specifically, Theorem 2.14 will give condition (iii) at the expense of additional assumptions on E and d. Moreover, we use Proposition 2.16 to strengthen Item 3d of Theorem 2.14 to an actual method for ensuring infinitude of d in that case. To keep track of the many such assumptions, we provide the following result that allows for an algorithmic implementation and justifies the title of this paper (specifically, the "infinitely many"). It separates the conditions on E from those on d, reflecting what is implicitly happening in [6, Theorem 1.7].

Theorem 2.18. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N that satisfies the following conditions:*

1. *E is semistable.*
2. *$a_3(E) \in \{-2, -1, 0, 1, 2\}$.*
3. *E does not admit a rational p-isogeny for $p \in \{3, 5, 7\}$.*
4. *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified.*
5. *E is optimal in its isogeny class.*
6. *E has analytic rank 0.*
7. *$\mathrm{BSD}(E, 2)$ is true.*
8. *One of the following two sets of conditions hold.*
   a. *$E(\mathbb{Q})[2] = 0$, $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = 0$*
   b. *$E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$; $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = -1$; writing $E : y^2 = f(x)$ and the 2-torsion point as $(x_0, 0)$, none of $f'(x_0)$, $-f'(x_0)$ or $-\Delta_E$ are squares in $\mathbb{Q}$; $Ш(E')[2] = 0$, where $E' := E/E(\mathbb{Q})[2]$ is the 2-isogenous curve of E.*

Then there exist infinitely many squarefree integers d satisfying the following:

1. *$(d, 3N) = 1$.*
2. *$d \equiv 1 \pmod 4$.*
3. *E has ordinary reduction at prime divisors of d.*
4. a. *in Item 8a, for every $p|d$, p is inert in the number field $\mathbb{Q}[x]/(f(x))$, where $f(x)$ is the two-division polynomial of E; for every $p \mid N$, p splits in $\mathbb{Q}(\sqrt{d})$; if $\Delta_E > 0$, then $d > 0$.*
   b. *in Item 8b, for every $p|d$, $p \equiv 1 \pmod 4$, and $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$; and for every $p \mid 2N$, p splits in $\mathbb{Q}(\sqrt{d})$.*

Therefore, by Theorem 2.13 and Theorem 2.14, such E as above admit infinitely many quadratic twists E_d that unconditionally satisfy BSD.

Note that we have dropped the condition that E has odd Manin constant, since the main theorem of [11] proves that it is 1 for optimal semistable curves. Also note that the condition $d \equiv 1 \pmod 4$ implies that $D = d$, so the condition $(d, 3N) = 1$ is equivalent to Item (i). The infinitude of d is stated in [6, Theorem 1.7] as relying on the two papers [7, 42]. These two papers establish infinitude of a family of twists by using the Chebotarev density theorem together with their modular symbols arguments. We provide some more details on this as follows.

Proof. Define

$$\mathcal{S}_0 := \{\ell \text{ prime} : \ell \nmid 6N,\ E \text{ ordinary at } \ell\}.$$

Since E is semistable over $\mathbb{Q}$, it is not CM; a theorem of Serre then gives that the supersingular set of E has density 0. Together with the finite exclusions, $\mathcal{S}_0$

has natural density 1. For any squarefree $d > 0$ whose prime factors lie in $\mathcal{S}_0$, conclusions (1) and (3) of the theorem therefore hold automatically.

We construct the family separately in cases 8a and 8b; in each, d will be a product of two primes drawn from an appropriate Chebotarev set derived from $\mathcal{S}_0$.

Case 8a. Since $E(\mathbb{Q})[2] = 0$, the 2-division polynomial f is irreducible of degree 3. Let $F = \mathbb{Q}[x]/(f(x))$ and $K_2 = \mathbb{Q}(E[2])$ its Galois closure. Then $\mathrm{Gal}(K_2/\mathbb{Q}) \in \{S_3, A_3\}$, and the condition "$\ell$ inert in F" is equivalent to "Frob_ℓ has order 3 in $\mathrm{Gal}(K_2/\mathbb{Q})$". Order-3 elements form a non-empty union of conjugacy classes in either of those two possibilities (S_3 and A_3), so by Chebotarev applied to $K_2/\mathbb{Q}$,

$$\mathcal{S} := \{\ell \in \mathcal{S}_0 : \ell \text{ inert in } F\}$$

has positive density. (This is the Chebotarev set used in [42, Theorems 1.1, 1.3].)

The splitting behaviour of an odd prime $p \mid N$ in $\mathbb{Q}(\sqrt{d})$ is controlled by the Legendre symbol $\left(\frac{d}{p}\right)$, and the splitting behaviour of 2 (relevant when $2 \mid N$) is controlled by d mod 8. For each $\ell \in \mathcal{S}$ we therefore record this data as the *signature*

$$\sigma(\ell) := \left(\ell \bmod 8,\ \left(\tfrac{\ell}{p}\right)_{p \mid N,\ p \text{ odd}}\right) \in (\mathbb{Z}/8\mathbb{Z})^\times \times \{\pm 1\}^{\omega_o(N)},$$

where $\omega_o(N)$ is the number of odd prime divisors of N. The codomain is finite, while $\mathcal{S}$ is infinite, so some value σ_0 is attained by infinitely many $\ell \in \mathcal{S}$; write $\mathcal{S}_{\sigma_0}$ for this infinite subset. Choose distinct $\ell_1, \ell_2 \in \mathcal{S}_{\sigma_0}$ and set $d := \ell_1\ell_2$. We verify the conclusions of the theorem in turn.

Both ℓ_1 and ℓ_2 lie in $\mathcal{S}$, so both are inert in F. Since $\ell_1 \equiv \ell_2 \pmod 8$, we have $d \equiv \ell_1^2 \pmod 8$, and every odd square is $\equiv 1 \pmod 8$; hence $d \equiv 1 \pmod 8$. This gives conclusion (2), and when $2 \mid N$ it also gives that 2 splits in $\mathbb{Q}(\sqrt{d})$. For each odd $p \mid N$, the Legendre symbol of the product is the product of the symbols, which are equal by construction, so $\left(\frac{d}{p}\right) = \left(\frac{\ell_i}{p}\right)^2 = 1$ and p splits in $\mathbb{Q}(\sqrt{d})$. Combined with the previous sentence, this gives the second half of conclusion (5a). Finally, $d = \ell_1\ell_2 > 0$, so the positivity clause of (5a) is automatic.

Letting (ℓ_1, ℓ_2) range over distinct pairs in $\mathcal{S}_{\sigma_0}$ produces infinitely many such d.

Case 8b. Since $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$, the 2-division polynomial factors as $f(x) = (x - x_0)g(x)$ with g an irreducible quadratic. The field $\mathbb{Q}(E[2])$ is the splitting field of g, and the discriminant identity $\Delta_E = 16f'(x_0)^2 \cdot \mathrm{disc}(g)$ shows that this is $\mathbb{Q}(\sqrt{\Delta_E})$. A similar direct computation with the explicit 2-isogeny gives $\mathbb{Q}(E'[2]) = \mathbb{Q}(\sqrt{f'(x_0)})$, where $E' := E/\langle(x_0, 0)\rangle$ is the 2-isogenous curve.

By [7, Remark 1.3], invoking [26, Lemma 4.1], for a prime $\ell \nmid 2N$ with $\ell \equiv 1 \pmod 4$, the condition $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_\ell)) = 1$ is equivalent to ℓ being inert in *both* $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E'[2])$. Set

$$\mathcal{S}' := \{\ell \in \mathcal{S}_0 : \ell \equiv 1 \pmod 4,\ \ell \text{ inert in } \mathbb{Q}(E[2]),\ \ell \text{ inert in } \mathbb{Q}(E'[2])\}.$$

The hypothesis that $-\Delta_E$, $f'(x_0)$, and $-f'(x_0)$ are not rational squares ensure that $\mathbb{Q}(\sqrt{\Delta_E})$ and $\mathbb{Q}(\sqrt{f'(x_0)})$ are both nontrivial quadratic extensions of $\mathbb{Q}$, and that both are distinct from $\mathbb{Q}(i)$. The fields $\mathbb{Q}(\sqrt{\Delta_E})$ and $\mathbb{Q}(\sqrt{f'(x_0)})$ may or may not coincide — they coincide precisely when $\Delta_E \cdot f'(x_0)$ is a rational square — but in either situation the conditions defining $\mathcal{S}'$ specify a single Frobenius element in $\mathrm{Gal}(\mathbb{Q}(i, \sqrt{\Delta_E}, \sqrt{f'(x_0)})/\mathbb{Q})$. By Chebotarev, $\mathcal{S}'$ has positive density. This is the set S of [7, Theorem 1.1].

As in case 8a, the splitting of 2 and of the odd primes $p \mid N$ in $\mathbb{Q}(\sqrt{d})$ is controlled by $d \bmod 8$ and by the Legendre symbols $\left(\frac{d}{p}\right)$, respectively. For each $\ell \in \mathcal{S}'$, define as before the signature

$$\sigma(\ell) := \left(\ell \bmod 8,\ \left(\tfrac{\ell}{p}\right)_{p\mid N,\ p \text{ odd}}\right) \in \{1,5\} \times \{\pm 1\}^{\omega_o(N)},$$

where the first coordinate is restricted to $\{1,5\}$ because $\ell \equiv 1 \pmod 4$. The codomain is finite while $\mathcal{S}'$ is infinite, so some value σ_0 is attained by infinitely many $\ell \in \mathcal{S}'$; write $\mathcal{S}'_{\sigma_0}$ for this infinite subset. Choose distinct $\ell_1, \ell_2 \in \mathcal{S}'_{\sigma_0}$ and set $d := \ell_1\ell_2$. We verify the conclusions of the theorem in turn.

Both ℓ_1 and ℓ_2 lie in $\mathcal{S}'$, so each satisfies $\ell_i \equiv 1 \pmod 4$ and $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_{\ell_i})) = 1$; this gives the first part of conclusion (5b). Since $\ell_1 \equiv \ell_2 \pmod 8$, we have $d \equiv \ell_1^2 \pmod 8$, and both possible values of $\ell_1 \bmod 8$ square to 1 (namely $1^2 = 1$ and $5^2 = 25 \equiv 1$); hence $d \equiv 1 \pmod 8$. This gives conclusion (2) and also that 2 splits in $\mathbb{Q}(\sqrt{d})$. For each odd $p \mid N$, the Legendre symbol of the product is the product of the symbols, which are equal by construction, so $\left(\frac{d}{p}\right) = \left(\frac{\ell_i}{p}\right)^2 = 1$ and p splits in $\mathbb{Q}(\sqrt{d})$. Combined with the splitting at 2, this gives the second part of conclusion (5b).

Letting (ℓ_1, ℓ_2) range over distinct pairs in $\mathcal{S}'_{\sigma_0}$ produces infinitely many d. □

2.6. **Algorithms.** Theorem 2.18 now readily translates into two algorithms: Algorithm 1, implemented in `infinite_bsd/Algorithm1.py`, that checks the conditions on E; and Algorithm 2, implemented in `infinite_bsd/Algorithm2.py`, that takes an E successfully checked by Algorithm 1, as well as a squarefree integer d, and `True`/`Unknown` depending on whether or not the pair (E, d) satisfies all the conditions listed in Theorem 2.18.

Algorithm 1 Filter Eligible Elliptic Curves

Require: Elliptic curve E
Check: N is squarefree and not prime
Check: $a_3(E) \in \{-2, -1, 0, 1, 2\}$
Check: $\forall p \in \{3, 5, 7\}$, E does not admit a rational p-isogeny
Check: $\forall p \mid N, \exists\ q \mid N,\ q \neq p$, s.t. $p \nmid \mathrm{ord}_q(\Delta_E)$
Check: E is optimal in its isogeny class
Check: $\mathrm{rank}(E) = 0$
if $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ **then**
    Check: $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = -1$
    Let $E' := E/E(\mathbb{Q})[2]$
    Check: $Ш(E')[2] = 0$ and $E'(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$
    Write $E : y^2 = f(x)$ and let $(x_0, 0) \in E(\mathbb{Q})[2]$
    Check: none of $f'(x_0)$, $-f'(x_0)$, or $-\Delta_E$ is a square in $\mathbb{Q}$
else if $E(\mathbb{Q})[2] = 0$ **then**
    Check: $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1))) = 0$
if 2-part of BSD holds **then**
    Accept E

Remark 2.19. (1) The requirement that N not be prime in Step 1 is forced by the ramified prime condition 4 in Theorem 2.18. By using the theory

of Tate curves, this condition is seen to be equivalent to Step 4. We are not claiming that N being composite ensures the ramified prime condition holds.

(2) The check on isogeny degrees and optimality are database checks, since this information is stored in the LMFDB for each curve. We refer to [13] for how these are computed.

(3) Step 15 certainly warrants some discussion. The suite of papers mentioned in the Introduction (those that established full BSD for all curves of analytic rank 0 or 1 up to conductor 5,000) furnished a very useful Sage function `prove_BSD` that attempts to unconditionally prove BSD for a given curve, and returns the primes where verification of $\mathrm{BSD}(E,p)$ fails. We extract the source code for this specifically for $p=2$ into a helper function `check_BSD_at_2` and run this at the end of the routine to minimize the number of curves we use this expensive function on. This function returns True if and only if $\mathrm{BSD}(E,2)$ can be unconditionally shown to be true via 2-descent. 2-descent alone settles $\mathrm{BSD}(E,2)$ only when $\mathrm{ord}_2(\#Ш_{\mathrm{an}}(E)) = 0$. Fortunately for us, this is the case for all curves in the LMFDB that reach this Step in the above algorithm. (In other words, $\#Ш_{\mathrm{an}}(E)$ is always odd for us.) For positive values of $\mathrm{ord}_2(\#Ш_{\mathrm{an}}(E))$, one would need to carry out higher 2-power descent.

For an elliptic curve E that is in the output of Algorithm 1, we next wish to identify the twists in a given range $[-B,B]$ that satisfy BSD. The conditions on d here listed in the second half of Theorem 2.18 can again be extracted into a procedural Algorithm 2 as follows.

Remark 2.20. For a fixed curve E, we do not claim to characterize all quadratic twists E_d satisfying BSD. What our results give is an explicit, effectively enumerable subfamily of such ds. Equivalently, one may generate admissible ds by choosing prime factors from the relevant Chebotarev sets and imposing the required congruence and splitting conditions using Algorithm 2. Thus the procedure is more structured than testing arbitrary squarefree d's one by one, although in bounded computations we still enumerate candidates within this explicitly described admissible set.

We executed these algorithms on all elliptic curves in the LMFDB database up to conductor 500,000; the output of doing this can be found at `infinite_bsd/output/twists_of_ec_labels_500k.txt` [2]. This lists, for each elliptic curve that passed Algorithm 1, the BSD-satisfying twists in the range $[-1000, 1000]$. Readers wishing to see only the elliptic curves and not the twists may refer to `infinite_bsd/output/ec_labels_500k.txt`.

Of the 3,064,705 elliptic curves in the LMFDB with conductor below 500,000, exactly 1,170,876 ($\approx 38.2\%$) have analytic rank 0. Of those, 274,888 ($\approx 23.5\%$ of the analytic-rank-0 curves, $\approx 9.0\%$ of all curves with $N < 500{,}000$) are semistable, and after restricting further to those whose conductor has at least two prime divisors and that are optimal representatives of their isogeny classes, 178,364 curves remain. Algorithm 1 accepts 36,687 of these — approximately 20.5% of the optimal semistable analytic-rank-0 candidates, and 1.20% of all elliptic curves in the LMFDB with $N < 500,000$.

Algorithm 2 Determine if E_d satisfies BSD

Require: Elliptic curve E output by Algorithm 1
Require: Squarefree integer d
$N \leftarrow \text{conductor}(E)$
Check: $(d, 3N) = 1$
Check: $\forall p|d,\ p \nmid a_p(E)$
if $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ **then**
    Check: $\forall p|d,\ p \equiv 1 \pmod 4$ and $\text{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$
    Check: $d \equiv 1 \pmod 8$ and if $p \mid N$ is odd, then $\left(\frac{\Delta_{\mathbb{Q}\sqrt{d}}}{p}\right) = 1$
    return True
else if $E(\mathbb{Q})[2] = 0$ **then**
    Check: $d \equiv 1 \pmod 4$
    $f(x) \leftarrow$ 2-division polynomial of E
    $F \leftarrow \mathbb{Q}[x]/(f(x))$
    Check: $\forall p|d$, p is inert in F
    Check: $\forall p|N$, $\left(\frac{\Delta_{\mathbb{Q}\sqrt{d}}}{p}\right) = 1$
    if $\Delta_E > 0$ **then**
        Check: $d > 0$
        return True
    else
        return True
return Unknown

2.7. **The curves up to conductor 150.** We list here the elliptic curve Cremona labels of the curves up to conductor 150 that our algorithm shows to admit infinitely many twists that unconditionally satisfy strong BSD. We present this in the same fashion as [6, Example 1], namely, two bullet points, the first for curves that use the results of [7] for establishing the 2-part of BSD for the twist, and the second for curves that use the results in [42]:

- 46a1, 69a1, 77c1, 94a1, 114b1, 141b1, 142c1;
- 106d1, 115a1, 118c1, 118d1, 141e1.

We compare these lists with the curves in [6, Example 1].

(1) The curves in our respective first bullet points match entirely.
(2) The curves in our second bullet form a strict subset of the curves in their second bullet point. The curves there that we are not listing here are those with Cremona label 62a1, 66b1, 105a1, and 141c1. To investigate the discrepancy, we implemented the script `diagnose_curve_discrepancy.py` that produces `output/discrepancy_report.txt` showing exactly which of the conditions are being violated. We find that all four fail for the same reason: the condition for non-emptiness of $\mathcal{S}$ in Proposition 2.16 is violated; i.e. the set $\mathcal{S}$ is empty. (This is also confirmed by searching for primes up to 10,000.) Since $\mathcal{S}$ is the set of prime support for the infinitely many twists, these four curves have not been shown to admit infinitely many twists satisfying BSD.

    Moreover, all four of these curves have $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. For this second bullet point, the authors of that paper are relying on the theorems in [42] to

establish the existence of infinitely many twists that unconditionally satisfy the 2-part of BSD; and while there are such theorems in the $E(\mathbb{Q})[2] = 0$ case, there are no such theorems in [42] that establish such a result in the case $E(\mathbb{Q})[2] \neq 0$, as also mentioned in Remark 2.15.[1]

3. Verifying the conjecture of Radziwiłł and Soundararajan

Having established an algorithm to identify families of quadratic twists where the full Birch and Swinnerton-Dyer (BSD) conjecture holds, we now consider the statistical behavior of the Shafarevich–Tate group $Ш(E_d)$ within these families. In particular, we investigate whether the distribution of the order of $Ш(E_d)$ conforms to the probabilistic predictions formulated by Radziwiłł and Soundararajan.

3.1. **Background on the Conjecture.** In [33], Radziwiłł and Soundararajan investigated the distribution of central L-values of quadratic twists of elliptic curves. Based on results from random matrix theory (specifically the Keating–Snaith conjecture), they formulated a conjecture describing the distribution of the size of $Ш(E_d)$ for rank zero twists, that we now briefly recall.

Let E be an elliptic curve over $\mathbb{Q}$ given by the model $y^2 = f(x)$ for a monic squarefree cubic polynomial $f \in \mathbb{Z}[x]$. Let K be the splitting field of f over $\mathbb{Q}$ and $G = \mathrm{Gal}(K/\mathbb{Q})$ viewed as a subgroup of S_3. For $g \in G$, let $c(g)$ denote $1 + |\mathrm{Fix}(g)|$, where $\mathrm{Fix}(g)$ is the number of fixed points of g acting on the roots of f. We define the arithmetic mean $\mu(E)$ and variance $\sigma(E)^2$ associated to the Galois action as:

$$\mu(E) = -\frac{1}{2} - \frac{1}{|G|}\sum_{g\in G} \log c(g) \quad \text{and} \quad \sigma(E)^2 = 1 + \frac{1}{|G|}\sum_{g\in G} (\log c(g))^2.$$

The Radziwiłł–Soundararajan conjecture predicts that as d ranges over those fundamental discriminants where the twist E_d has root number $+1$ (and hence even analytic rank), the distribution of the normalized values

$$Z_d = \frac{\log\left(|Ш(E_d)|/\sqrt{|d|}\right) - \mu(E)\log\log|d|}{\sqrt{\sigma(E)^2 \log\log|d|}}$$

converges to a standard Gaussian distribution $\mathcal{N}(0,1)$ as $|d| \to \infty$.

The above is sufficient for our purposes here, although we note that there is a more precise version given by the authors as Conjecture 1 in their paper.

3.2. **Verifying the conjecture.** We first wish to verify the Radziwill–Soundararajan conjecture numerically for all twists with root number $+1$, assuming BSD. We focus on the elliptic curve $E = \texttt{46a1}$ given by $y^2 = x^3 - 163x - 930$ that arises in Section 2.7; the other curves listed there exhibit the same pattern. For this curve, we compute

$$Z_d^{\mathrm{an}} := \frac{\log\left(|Ш(E_d)^{\mathrm{an}}|/\sqrt{|d|}\right) - \mu(E)\log\log|d|}{\sqrt{\sigma(E)^2 \log\log|d|}},$$

where as usual

$$|Ш(E_d)^{\mathrm{an}}| := \frac{L^{(r)}(E,1)/r! \cdot |E(\mathbb{Q})_{\mathrm{tors}}|^2}{\Omega(E)\cdot \prod_p c_p \cdot \mathrm{Reg}(E)}$$

[1]The closest statement is Theorem 1.6 of *loc. cit.*, which applies only to Neumann–Setzer curves; however, this case is excluded in our setting, since such curves necessarily have prime conductor, which is precluded as in Remark 2.19.

is the order of Ш(E_d) derived from the strong BSD formula.

Figure 3.1 displays the results for $X = 100{,}000$, where X is the bound on d (excluding 472 values where the computation for the order of Ш$(E)^{\mathrm{an}}$ took longer than 10 seconds and so was abandoned).

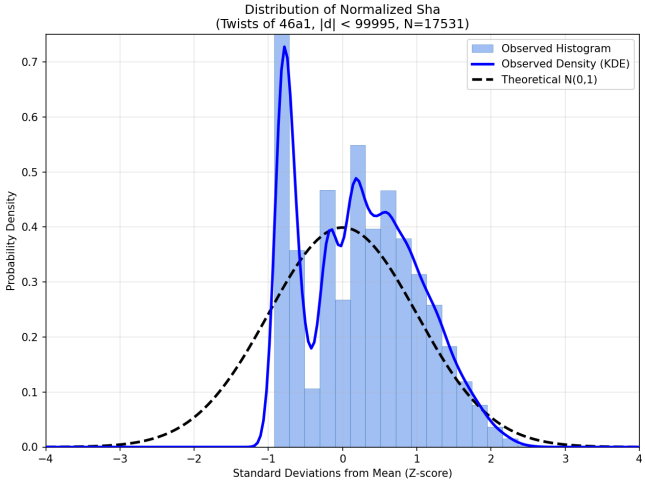
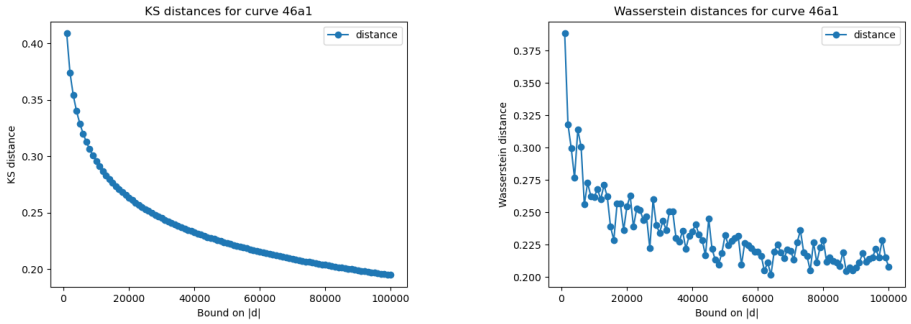


FIGURE 3.1. Distribution of 17,531 Z_d^{an} values for generic twists of `46a1` with $|d| \leq 100{,}000$. The histogram (light blue) shows the raw counts, while the Kernel Density Estimate (solid blue line) provides a smooth approximation that closely tracks the theoretical standard Gaussian prediction (black dashed). A time-lapse visualization of the convergence to $\mathcal{N}(0,1)$ is available at this link.

3.2.1. *Statistical Diagnostics for Normality.* To quantify the convergence of the empirical distributions of Z_d to $\mathcal{N}(0,1)$, we compute two standard metrics: the Kolmogorov–Smirnov (K–S) distance (cf. [29]) and the Wasserstein distance (cf. [40]). The KS distance measures the maximum vertical deviation between CDFs, whereas the Wasserstein distance quantifies the overall discrepancy between distributions by computing the minimal cost of transporting mass via optimal transport. Both are widely used measures of distributional discrepancy (cf. [16, 18]). At $X = 10{,}000$, both distances exhibit noticeable deviations from the standard normal distribution, consistent with finite-sample effects. However, as X increases, the K–S and Wasserstein distances decrease systematically across all examples, providing evidence of convergence toward the Gaussian limit predicted by Radziwiłł–Soundararajan.

Figure 3.2 illustrates this behavior for `46a1` as a representative case, where both distance metrics decrease as the discriminant bound grows to $X = 100{,}000$.

3.3. **Observed Deviation in the BSD Family.** Having validated the generic case, we now turn to our primary object of interest: the family of twists identified in Section 2. These are the twists for which the full BSD conjecture is unconditionally proven. We refer to this set of twists by $\mathcal{D}_{\mathrm{BSD}}$. We note that this set is defined by explicitly computable local conditions, implemented in the



(A) KS distance (B) Wasserstein distance

FIGURE 3.2. Goodness-of-fit diagnostics for curve 46a1 as functions of the truncation bound on $|d|$ where the maximum bound X increases to $100,000$. The KS and Wasserstein distances decrease with increasing bound indicating improved distributional agreement to normality.

`get_admissible_twists_CLZ` and `get_admissible_twists_Zhai` functions in `ants_xvii/infinite_bsd/Algorithm2.py`.

A natural question is whether the distribution of $|Ш(E_d)|$ for $d \in \mathcal{D}_{\mathrm{BSD}}$ follows the generic Radziwiłł–Soundararajan (RS) prediction. We take one example: for the elliptic curve `46a1`, we generated the set $\mathcal{D}_{\mathrm{BSD}} \cap [-X, X]$ with $X = 300,000$ using the criteria when $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ from [7], implemented in our Algorithm 2. This yielded a subset of $N = 1008$ fundamental discriminants. Recall that unlike the generic family, membership in $\mathcal{D}_{\mathrm{BSD}}$ requires satisfying stringent arithmetic constraints (see Algorithm 2). Specifically, for every $d \in \mathcal{D}_{\mathrm{BSD}}$, we require:

- d is squarefree and $d \equiv 1 \pmod 8$;
- Every prime factor $p \mid d$ satisfies $p \equiv 1 \pmod 4$;
- For all odd primes q dividing the conductor $N = 46$, the Legendre symbol satisfies $\left(\frac{d}{q}\right) = 1$.

In particular, these conditions imply that d must be positive: if d were negative, the condition on its prime factors would imply $d \equiv 3 \pmod 4$, contradicting the requirement that $d \equiv 1 \pmod 8$. Consequently, our family $\mathcal{D}_{\mathrm{BSD}}$ consists entirely of real quadratic twists, in contrast to the generic case which includes both real and imaginary fields.

As in [15, Section 8.1] we computed $|Ш(E_d)|$ from the BSD formula (which we know unconditionally for these values of d) for rank 0 curves (which we know to be the case from Algorithms 1 and 2 from Section 2) as follows:

$$|Ш(E_d)| = \frac{L(E,1) \cdot |E_d(\mathbb{Q})_{\mathrm{tors}}|^2}{\Omega(E) \cdot \prod_p c_p}.$$

We then computed Z_d; the resulting distribution is shown in Figure 3.3.

The behaviour of the two distributions is clearly significantly different, with the main qualitative difference being that Figure 3.3 has shifted to a bimodal shape.

This anomaly need not be a failure of the Radziwiłł–Soundararajan heuristics, but rather a demonstration of their sensitivity to arithmetic progressions. The

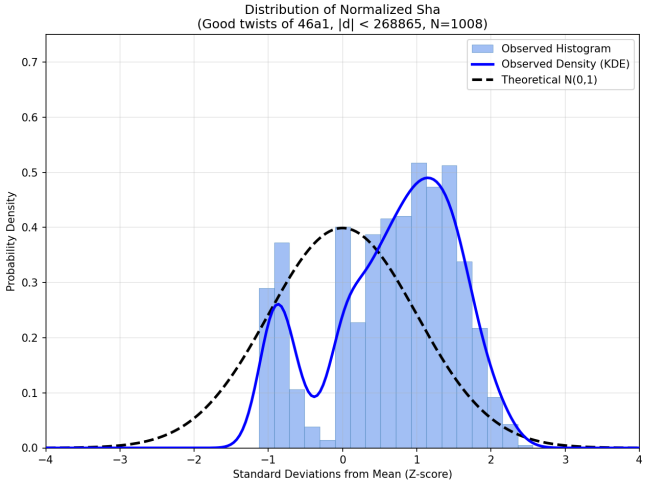


FIGURE 3.3. Distribution of normalized Z_d for 1008 of the unconditionally BSD-satisfying twists of `46a1`. The observed distribution (blue) is clearly shifted to the right of the generic Radziwiłł–Soundararajan prediction (black dashed). This shift reflects the bias introduced by restricting to real quadratic fields with split primes at the conductor. A time-lapse visualization of the convergence to $\mathcal{N}(0,1)$ is available at this link.

generic parameters $\mu(E)$ and $\sigma(E)$ are derived by averaging over the Galois group G under the assumption that Frobenius elements are equidistributed as d varies. However, our family $\mathcal{D}_{\mathrm{BSD}}$ explicitly restricts the factorization of d (forcing $p \equiv 1 \pmod 4$), fixes the sign of the discriminant (forcing real fields), and fixes the quadratic character at the conductor (forcing $\left(\frac{d}{23}\right) = 1$). These restrictions alter the density of primes where our twists are supported, necessitating a correction to the probabilistic model.

If we observed persistent deviations from Gaussian behavior in $|Ш(E_d)|$ across unconstrained, randomly sampled families of quadratic twists, such as the baseline family shown in Figure 3.1, this would provide more plausible evidence against the conjecture. However, we do not observe such a deviation in the baseline distribution. We also note that the introduction of Radziwiłł–Soundararajan mentions that their method "is flexible enough to allow the introduction of a sieve over the fundamental discriminants d"; this being the case, we could still expect the distribution in Figure 3.3 to become approximately Gaussian (with different mean and variance) with more data, and this would be worthy of further investigation.

REFERENCES

1. Amod Agashe, Kenneth Ribet, and William A Stein, *The Manin constant*, Pure and Applied Mathematics Quarterly **2** (2006), no. 2, 617–636.
2. Barinder Banwait and Xiaoyu Huang, *A list of elliptic curves that admit infinitely many twists satisfying the Birch–Swinnerton-Dyer conjecture up to conductor*

500,000, `https://github.com/cocoxhuang/ants_xvii/blob/main/ants_xvii/infinite_bsd/output/ec_labels_500k.txt`, 2026, GitHub repository `cocoxhuang/ants_xvii`.
3. Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Mathematics (2015), 191–242.
4. Manjul Bhargava, Christopher Skinner, and Wei Zhang, *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*, arXiv preprint arXiv:1407.1826 (2014).
5. Ashay Burungale, Francesc Castella, and Christopher Skinner, *Base change and 0iwasawa main conjectures for* GL_2, International Mathematics Research Notices **2025** (2025), no. 8, rnaf082.
6. Ashay Burungale, Christopher Skinner, Ye Tian, and Xin Wan, *Zeta elements for elliptic curves and applications*, arXiv preprint arXiv:2409.01350 (2024).
7. Li Cai, Chao Li, and Shuai Zhai, *On the 2-part of the Birch and Swinnerton-Dyer conjecture for quadratic twists of elliptic curves*, Journal of the London Mathematical Society **101** (2020), no. 2, 714–734.
8. Francesc Castella, Mirela Çiperiani, Christopher Skinner, and Florian Sprung, *On the Iwasawa main conjectures for modular forms at non-ordinary primes*, arXiv preprint arXiv:1804.10993 (2018).
9. Francesc Castella, Giada Grossi, Jaehoon Lee, and Christopher Skinner, *On the anticyclotomic Iwasawa theory of rational elliptic curves at Eisenstein primes*, Inventiones Mathematicae **227** (2022), no. 2, 517–580.
10. Francesc Castella, Giada Grossi, and Christopher Skinner, *Mazur's main conjecture at Eisenstein primes*, Mathematische Annalen **393** (2025), no. 2, 2451–2506.
11. Kęstutis Česnavičius, *The Manin constant in the semistable case*, Compositio Mathematica **154** (2018), no. 9, 1889–1920.
12. John Coates and Andrew Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Inventiones Mathematicae **39** (1977), no. 3, 223–251.
13. John E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1997.
14. Brendan Creutz and Robert L. Miller, *Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula*, Journal of Algebra **372** (2012), 673–701.
15. Andrzej Dąbrowski and Lucjan Szymaszkiewicz, *Behaviour of the order of Tate–Shafarevich groups for the quadratic twists of elliptic curves*, Journal of the Ramanujan Mathematical Society, To appear.
16. Luc Devroye, László Györfi, and Gábor Lugosi, *A probabilistic theory of pattern recognition*, vol. 31, Springer Science & Business Media, 2013.
17. Olivier Fouquet and Xin Wan, *The Iwasawa main conjecture for universal families of modular motives*, arXiv preprint arXiv:2107.13726 (2021).
18. Alison L. Gibbs and Francis Edward Su, *On choosing and bounding probability metrics*, International Statistical Review **70** (2002), no. 3, 419–435.
19. Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William Stein, and Corina Tarniţă, *Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves*, Mathematics of Computation **78** (2009), no. 268, 2397–2425.
20. Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.
21. Kazuya Kato, *p-adic hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290.
22. Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Inventiones Mathematicae **62** (1980), no. 3, 481–502.
23. Timo Keller and Mulun Yin, *On the anticyclotomic Iwasawa theory of newforms at Eisenstein primes of semistable reduction*, arXiv preprint arXiv:2402.12781 (2024).
24. Winfried Kohnen and Don Zagier, *Values of L-series of modular forms at the center of the critical strip*, Inventiones Mathematicae **64** (1981), no. 2, 175–198.
25. V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $Ш(E,\mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671, English translation in Math. USSR-Izv. **32** (1989), no. 3, 523–541.
26. Daniel Kriz and Chao Li, *Prime twists of elliptic curves*, Mathematical Research Letters **26** (2019), no. 4, 1187–1195.
27. Tyler Lawson and Christian Wuthrich, *Vanishing of some Galois cohomology groups for elliptic curves*, Elliptic Curves, Modular Forms and Iwasawa Theory — Conference in Honour

of the 70th Birthday of John Coates (David Loeffler and Sarah Livia Zerbes, eds.), Springer, 2016, pp. 373–399.
28. Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66, English translation in Math. USSR-Izv. **6** (1972), 19–64.
29. Frank J. Massey, Jr., *The Kolmogorov–Smirnov test for goodness of fit*, Journal of the American Statistical Association **46** (1951), no. 253, 68–78.
30. Barry Mazur, *Rational isogenies of prime degree*, Inventiones Mathematicae **44** (1978), no. 2, 129–162, With an appendix by Dorian Goldfeld.
31. Robert Miller and Michael Stoll, *Explicit isogeny descent on elliptic curves*, Mathematics of Computation **82** (2013), no. 281, 513–529.
32. Robert L. Miller, *Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one*, LMS Journal of Computation and Mathematics **14** (2011), 327–350.
33. Maksym Radziwiłł and Kannan Soundararajan, *Moments and distribution of central L-values of quadratic twists of elliptic curves*, Inventiones Mathematicae **202** (2015), no. 3, 1029–1068.
34. Kenneth A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Inventiones Mathematicae **100** (1990), no. 2, 431–476.
35. Karl Rubin, *p-adic L-functions and rational points on elliptic curves with complex multiplication*, Inventiones Mathematicae **107** (1992), no. 1, 323–350.
36. Christopher Skinner, *Multiplicative reduction and the cyclotomic main conjecture for* GL_2, Pacific Journal of Mathematics **283** (2016), no. 1, 171–200.
37. Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for* GL_2, Inventiones Mathematicae **195** (2014), 1–277.
38. The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2026, [Online; accessed 20 January 2026].
39. The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2026, `https://www.sagemath.org`.
40. Cédric Villani, *Optimal transport: Old and new*, vol. 338, Springer, 2008.
41. Xiaojun Yan and Xiuwu Zhu, *Main conjectures for non-CM elliptic curves at good ordinary primes*, Journal of Algebra (2026).
42. Shuai Zhai, *Non-vanishing theorems for quadratic twists of elliptic curves*, Asian Journal of Mathematics **20** (2016), no. 3, 475–502.
43. Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Cambridge Journal of Mathematics **2** (2014), no. 2, 191–253.

Barinder S. Banwait, London, UK
Email address: `barinder.s.banwait@gmail.com`

Xiaoyu Huang, Department of Mathematics, Temple University, Wachman Hall, Philadelphia, PA 19122, USA
Email address: `xiaoyu.huang@temple.edu`