HEEGNER POINTS AT EISENSTEIN PRIMES AND TWISTS OF ELLIPTIC CURVES

DANIEL KRIZ AND CHAO LI

Abstract. Given an elliptic curve E over $\mathbb{Q}$, a celebrated conjecture of Goldfeld asserts that a positive proportion of its quadratic twists should have analytic rank 0 (resp. 1). We show this conjecture holds whenever E has a rational 3-isogeny. We also prove the analogous result for the sextic twists of j-invariant 0 curves (Mordell curves). To prove these results, we establish a general criterion for the non-triviality of the p-adic logarithm of Heegner points at an Eisenstein prime p, in terms of the relative p-class numbers of certain number fields and then apply this criterion to the special case $p = 3$. As a by-product, we also prove the 3-part of the Birch and Swinnerton-Dyer conjecture for many elliptic curves of j-invariant 0.

1. Introduction

1.1. **Goldfeld's conjecture.** Let E be an elliptic curve over $\mathbb{Q}$. We denote by $r_{\mathrm{an}}(E)$ its analytic rank. By the theorem of Gross–Zagier and Kolyvagin, the rank part of the Birch and Swinnerton-Dyer conjecture holds whenever $r_{\mathrm{an}}(E) \in \{0, 1\}$. One can ask the following natural question: how is $r_{\mathrm{an}}(E)$ distributed when E varies in families? The simplest (1-parameter) family is given by the quadratic twists family of a given curve E. For a fundamental discriminant d, we denote by $E^{(d)}$ the quadratic twist of E by $\mathbb{Q}(\sqrt{d})$. The celebrated conjecture of Goldfeld [Gol79] asserts that $r_{\mathrm{an}}(E^{(d)})$ tends to be as low as possible (compatible with the sign of the function equation). Namely in the quadratic twists family $\{E^{(d)}\}$, r_{an} should be 0 (resp. 1) for 50% of d's. Although $r_{\mathrm{an}} \geq 2$ occurs infinitely often, its occurrence should be sparse and accounts for only 0% of d's. More precisely,

Conjecture 1.1 (Goldfeld)**.** *Let*

$$N_r(E, X) = \{|d| < X : r_{\mathrm{an}}(E^{(d)}) = r\}.$$

Then for $r \in \{0, 1\}$,

$$N_r(E, X) \sim \frac{1}{2} \sum_{|d|<X} 1, \quad X \to \infty.$$

Here d runs over all fundamental discriminants.

Goldfeld's conjecture is widely open: we do not yet know a single example E for which Conjecture 1.1 is valid. One can instead consider the following weak version (replacing 50% by any positive proportion):

Conjecture 1.2 (Weak Goldfeld)**.** *For $r \in \{0, 1\}$, $N_r(E, X) \gg X$.*

Date: November 24, 2017.

2010 *Mathematics Subject Classification.* 11G05 (primary), 11G40 (secondary).

Key words and phrases. elliptic curves, Heegner points, Goldfeld's conjecture, Birch and Swinnerton-Dyer conjecture.

Remark 1.3. Heath-Brown ([HB04, Thm. 4]) proved Conjecture 1.2 *conditional* on GRH. Recently, Smith [Smi17] has announced a proof (*conditional* on BSD) of Conjecture 1.1 for curves with full rational 2-torsion by vastly generalizing the works of Heath-Brown [HB94] and Kane [Kan13].

Remark 1.4. Katz–Sarnak [KS99] conjectured the analogue of Conjecture 1.1 for the 2-parameter family $\{E_{A,B} : y^2 = x^3 + Ax + B\}$ of all elliptic curves over $\mathbb{Q}$. The weak version in this case is now known *unconditionally* due to the recent work of Bhargava–Skinner–W. Zhang [BSZ14]. However, their method does not directly apply to quadratic twists families.

The curve $E = X_0(19)$ is the first known example for which Conjecture 1.2 is valid (see James [Jam98] for $r = 0$ and Vatsal [Vat98] for $r = 1$). Later many authors have verified Conjecture 1.2 for infinitely many curves E (see [Vat99], [BJK09] and [Kri16]) using various methods. However, all these examples are a bit special, as they are all covered by our first main result:

Theorem 1.5 (Theorem 4.7)**.** *The weak Goldfeld Conjecture is true for any E with a rational 3-isogeny.*

In fact, in Theorem 4.7 we prove the same result for any abelian variety $A/\mathbb{Q}$ of GL_2-type with a rational 3-isogeny.

Remark 1.6. Theorem 1.5 gives so far the most general results for Conjecture 1.2. There is only one known example for which Conjecture 1.2 is valid and is not covered by Theorem 1.5: the congruent number curve $E : y^2 = x^3 - x$ (due to the recent work of Smith [Smi16] and Tian–Yuan–S. Zhang [TYZ14]).

Remark 1.7. For explicit lower bounds for the proportion in Theorems 1.5, see the more precise statements in Theorems 4.4, 4.5, Proposition 4.8, and Example 4.10.

For an elliptic curve E of j-invariant 0 (resp. 1728), one can also consider its cubic or sextic (resp. quartic) twists family. The weak Goldfeld conjecture in these cases asserts that for $r \in \{0, 1\}$, a positive proportion of (higher) twists should have analytic rank r. Our second main result verifies the weak Goldfeld conjecture for the sextic twists family. More precisely, consider the elliptic curve

$$E = X_0(27) : y^2 = x^3 - 432$$

of j-invariant 0 (isomorphic to the Fermat cubic $X^3 + Y^3 = 1$). For a 6th-power-free integer d, we denote by

$$E_d : y^2 = x^3 - 432d$$

the d-th sextic twist of E. These E_d's are also known as Mordell curves.

Theorem 1.8 (Corollary 5.8)**.** *The weak Goldfeld conjecture is true for the sextic twists family $\{E_d\}$. In fact, E_d has analytic rank 0 (resp. 1) for at least 1/6 of fundamental discriminants d.*

Remark 1.9. For a wide class of elliptic curves of j-invariant 0, we can also construct many (in fact $\gg X/\log^{7/8} X$) cubic twists of analytic rank 0 (resp. 1). However, these cubic twists do not have positive density. See the more precise statement in Theorem 6.1 and Example 6.3.

Remark 1.10. In a recent work, Bhargava–Elkies–Shnidman [BES16] prove the analogue of Theorem 1.8 for *3-Selmer ranks* 0,1, by determining the exact average size of 3-isogeny Selmer groups (its boundness was first proved by Fouvry [Fou93]). The same method also works for quadratic twists family of elliptic curves and GL_2-type abelian varieties with a 3-isogeny ([BKLS17], [Shn17]). We

remark that their method however does not have the same implication for analytic rank $r = 0, 1$ (or algebraic rank 1), since the p-converse to the theorem of Gross–Zagier and Kolyvagin is not known for p an additive and Eisenstein prime.

Remark 1.11. Recently, Browning [Bro17] has used Theorem 1.8 as key input in his argument to show that a positive proportion (when ordered by height) of smooth projective cubic surfaces of the form $f(x_0, x_1) = g(x_2, x_3)$, where f, g are binary cubic forms over $\mathbb{Q}$, have a $\mathbb{Q}$-rational point.

1.2. **Heegner points at Eisenstein primes.** The above results on weak Goldfeld conjecture are applications of a more general p-adic criterion for non-triviality of Heegner points on E (applied to $p = 3$). To be more precise, let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $K = \mathbb{Q}(\sqrt{d_K})$ denote an imaginary quadratic field of fundamental discriminant d_K. We assume that K satisfies the *Heegner hypothesis for N*:

$$\text{each prime factor } \ell \text{ of } N \text{ is split in } K.$$

For simplicity, we also assume that $d_K \neq -3, -4$ so that $\mathcal{O}_K^\times = \{\pm 1\}$, and that d_K is odd (i.e. $d_K \equiv 1 \pmod 4$). We denote by $P \in E(K)$ the corresponding Heegner point, defined up to sign and torsion with respect to a fixed modular parametrization $\pi_E : X_0(N) \to E$ (see [Gro84]). Let

$$f(q) = \sum_{n=1}^{\infty} a_n(E) q^n \in S_2^{\mathrm{new}}(\Gamma_0(N))$$

be the normalized newform associated to E. Let $\omega_E \in \Omega^1_{E/\mathbb{Q}} := H^0(E/\mathbb{Q}, \Omega^1)$ such that

$$\pi_E^*(\omega_E) = f(q) \cdot dq/q.$$

We denote by $\log_{\omega_E}$ the formal logarithm associated to ω_E. Notice ω_E may differ from the Néron differential by a scalar when E is not the optimal curve in its isogeny class.

For a finite order Galois character $\psi : G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}^\times$, we abuse notation and denote by $\psi : (\mathbb{Z}/f\mathbb{Z})^\times \to \mathbb{C}^\times$ the corresponding Dirichlet character, where f is its conductor. The generalized (first) Bernoulli number is defined to be

$$B_{1,\psi} := \frac{1}{f} \sum_{m=1}^{f} \psi(m) m. \tag{1}$$

Let ε_K be the quadratic character associated to K. We consider the even Dirichlet character

$$\psi_0 := \begin{cases} \psi, & \text{if } \psi \text{ is even,} \\ \psi\varepsilon_K, & \text{if } \psi \text{ is odd.} \end{cases}$$

Now suppose p is an *Eisenstein prime* for E (i.e., $E[p]$ is a reducible $G_{\mathbb{Q}}$-representation, or equivalently, E admits a rational p-isogeny), we prove the following criterion for the non-triviality of the p-adic logarithm of Heegner points, in terms of the p-indivisibility of Bernoulli numbers.

Theorem 1.12 (Theorem 2.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Suppose p is an odd prime such that $E[p]$ is a reducible $G_{\mathbb{Q}}$-representation. Write $E[p]^{\mathrm{ss}} \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi^{-1}\omega)$, for some character $\psi : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathbb{F}_p) \cong \mu_{p-1}$ and the mod p cyclotomic character ω. Assume that*

(1) $\psi(p) \neq 1$ and $(\psi^{-1}\omega)(p) \neq 1$.
(2) E has no primes of split multiplicative reduction.
(3) If $\ell \neq p$ is an additive prime for E, then $\psi(\ell) \neq 1$ and $(\psi^{-1}\omega)(\ell) \neq 1$.

Let K be an imaginary quadratic field satisfying the Heegner hypothesis for N. Let $P \in E(K)$ be the associated Heegner point. Assume p splits in K. Assume

$$B_{1,\psi_0^{-1}\varepsilon_K} \cdot B_{1,\psi_0\omega^{-1}} \neq 0 \pmod{p}.$$

Then

$$\frac{|\tilde{E}^{\mathrm{ns}}(\mathbb{F}_p)|}{p} \cdot \log_{\omega_E} P \neq 0 \pmod{p}.$$

In particular, $P \in E(K)$ is of infinite order and E/K has analytic and algebraic rank 1.

In fact, this is a specialization of the most general form of our main result given in Theorem 2.1, which addresses abelian varieties of GL_2-type over $\mathbb{Q}$.

Remark 1.13. When $E/\mathbb{Q}$ has CM by $\mathbb{Q}(\sqrt{-p})$ (of class number 1), Rubin [Rub83] proved a mod p congruence formula between the algebraic part of $L(E,1)$ and certain Bernoulli numbers. Notice that E admits a p-isogeny (multiplication by $\sqrt{-p}$), Theorem 1.12 specializes to provide a mod p congruence between the p-adic logarithm of the Heegner point on E and certain Bernoulli numbers, which can be viewed as a generalization of Rubin's formula from the rank 0 case to the *rank 1* case.

Notice that the two odd Dirichlet characters $\psi_0^{-1}\varepsilon_K$ and $\psi_0\omega^{-1}$ cut out two abelian CM fields (of degree dividing $p-1$). When the relative p-class numbers of these two CM fields are trivial, it follows from the relative class number formula that the two Bernoulli numbers in Theorem 1.12 are nonzero mod p (see §3), hence we conclude $r_{\mathrm{an}}(E/K) = 1$. When $p = 3$, the relative p-class numbers becomes the 3-class numbers of two quadratic fields. Our final ingredient to finish the proof of Theorems 1.5 and 1.12 is Davenport–Heilbronn's theorem ([DH71]) (enhanced by Nakagawa–Horie [NH88] with congruence conditions), which allows one to find a positive proportion of twists such that both 3-class numbers in question are trivial.

1.3. **A by-product: the 3-part of the BSD conjecture.** The Birch and Swinnerton-Dyer conjecture predicts the precise formula

$$\frac{L^{(r)}(E/\mathbb{Q},1)}{r!\Omega(E/\mathbb{Q})R(E/\mathbb{Q})} = \frac{\prod_p c_p(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})|}{|E(\mathbb{Q})_{\mathrm{tor}}|^2} \tag{2}$$

for the leading coefficient of the Taylor expansion of $L(E/\mathbb{Q},s)$ at $s=1$ (here $r = r_{\mathrm{an}}(E)$) in terms of various important arithmetic invariants of E (see [Gro11] for detailed definitions). When $r \leq 1$, both sides of the BSD formula (2) are known to be positive rational numbers. To prove that (2) is indeed an equality, it suffices to prove that it is an equality up to a p-adic unit, for each prime p. This is known as the *p-part of the BSD formula* (BSD(p) for short). Much progress has been made recently, but only in the case p is *semi-stable* and *non-Eisenstein*. We establish the following new results on BSD(3) for many sextic twists $E_d : y^2 = x^3 - 432d$, in the case $p = 3$ is *additive* and *Eisenstein*.

Theorem 1.14 (Theorem 5.10)**.** *Suppose K is an imaginary quadratic field satisfies the Heegner hypothesis for $3d$. Assume that*

(1) d is a fundamental discriminant.
(2) $d \equiv 2, 3, 5, 8 \pmod 9$.
(3) If $d > 0$, $h_3(-3d) = h_3(d_K d) = 1$. If $d < 0$, $h_3(d) = h_3(-3d_K d) = 1$.
(4) The Manin constant of E_d is coprime to 3.

Then $r_{\mathrm{an}}(E_d/K) = 1$ and BSD(3) holds for E_d/K. (Here $h_3(D)$ denotes the 3-class number of $\mathbb{Q}(\sqrt{D})$.)

Remark 1.15. Since the curve E_d has complex multiplication by $\mathbb{Q}(\sqrt{-3})$, we already know that BSD(p) holds for $E_d/\mathbb{Q}$ if $p \neq 2, 3$ (when $r = 0$) and if $p \neq 2, 3$ is a prime of good reduction or potentially good ordinary reduction (when $r = 1$) thanks to the works [Rub91], [PR87], [Kob13], [PR04], [LLT16]. When $r = 0$, we also know BSD(3) for some quadratic twists of the two curves $X_0(27)$ and $X_0(36)$ of j-invariant 0, using explicit weight 3/2 modular forms ([Nek90], [Ono98], [Jam99]).

1.4. **Comparison with previous methods establishing the weak Goldfeld conjecture.**

(1) The work of James [Jam98] on weak Goldfeld for $r = 0$ uses Waldspurger's formula relating coefficients of weight 3/2 modular forms and quadratic twists L-values (see also Nekovář [Nek90], Ono–Skinner [OS98]). Our proof does not use any half-integral weight modular forms.

(2) When N is a prime different from p, Mazur in his seminal paper [Maz79] proved a congruence formula at an Eisenstein prime above p, between the algebraic part of $L(J_0(N), \chi, 1)$ and a quantity involving generalized Bernoulli numbers attached to χ, for certain odd Dirichlet characters χ. This was later generalized by Vatsal [Vat99] for more general N and used to prove weak Goldfeld for $r = 0$ for infinitely many elliptic curves.

(3) When N is a prime different from p, Mazur [Maz79] also constructed a point of infinite order on the Eisenstein quotient of $J_0(N)$, when certain quadratic class number is not divisible by p. This was later generalized by Gross [Gro84, II] to more general N, and became the starting point of the work of Vatsal [Vat98] and Byeon–Jeon–Kim [BJK09] on weak Goldfeld for $r = 1$.

(4) Our main congruence at Eisenstein primes (see §2.9) through which Theorem 1.12 is established can be viewed as a vast generalization of Mazur's congruence from $J_0(N)$ to *any* elliptic curve with a p-isogeny and to *both* rank 0 and rank 1 case. To achieve this, instead of working with L-functions directly, we use the p-adic logarithm of Heegner points as the p-adic incarnation of L-values (or L-derivatives).

(5) The recent work [Kri16] also uses p-adic logarithm of Heegner points. As we have pointed out, the crucial difference is that our proof uses a direct method of p-adic integration, and does not rely on the deep p-adic Gross–Zagier formula of [BDP13]. This is the key observation to remove *all* technical hypothesis appeared in previous works, which in particular makes the application to the sextic twists family possible.

(6) Although the methods are completely different, the final appearance of Davenport–Heilbronn type theorem is a common feature in all previous works ([Jam98], [Vat98], [Vat99], [BJK09], [Kri16]), and also ours.

1.5. **Strategy of the proof.** The proof of Theorem 1.12 (and the more general version Theorem 2.1) relies on the main congruence identity (§2.9) between the p-adic logarithm of Heegner points and a product of two Bernoulli numbers.

The starting point is that the prime p being Eisenstein produces a congruence between the modular form f and a weight 2 Eisenstein series g, away from the bad primes. We then apply certain Hecke operators (which we call *stabilization operators*) in order to produce a modified Eisenstein series $g^{(N)}$ whose entire q-expansion $g^{(N)}(q)$ is congruent to $f(q)$. Applying another p-stabilization operator and the Atkin-Serre derivatives θ^j, we obtain a p-adically continuously varying system of congruences $\theta^j f^{(p)}(q) \equiv \theta^j g^{(pN)}(q) \pmod{p}$. By the q-expansion principle and our assumption

that p splits in K, we can sum this congruence over CM points to obtain a congruence between a normalized CM period sum and a p-adic Katz L-value times certain Euler factors at bad primes.

Taking $j \to -1$ (p-adically), the CM period sums converge to the p-adic logarithm of the Heegner point times an Euler factor at p, by Coleman's integration. The Katz L-values converge to a product of two Bernoulli numbers, by Gross's factorization. We finally arrive at the main congruence identity.

1.6. **Structure of the paper.** In §2, we establish the non-triviality criterion for Heegner points at Eisenstein primes, in terms of p-indivisibility of Bernoulli numbers (Theorem 1.12). In §3, we explain the relation between the Bernoulli numbers and relative class numbers. In §4, we combine our criterion and the Nakagawa–Horie theorem to prove the weak Goldfeld conjecture for abelian varieties of GL_2-type with a 3-isogeny (Theorem 4.7). In §5, we give applications to the sextic twists family (Theorems 1.8 and 1.14). Finally, in §6, we give an application to cubic twists families (Theorem 6.1).

1.7. **Acknowledgments.** We are grateful to M. Bhargava, D. Goldfeld, B. Gross, B. Mazur, K. Prasanna, P. Sarnak, A. Shnidman, C. Skinner, E. Urban, X. Wan, A. Wiles and S. Zhang for helpful conversations or comments. The examples in this article are computed using Sage ([Sag16]).

2. Heegner points at Eisenstein primes

In this section, we carry out the p-adic integration which makes up the heart of Theorem 1.12. In the course of our argument, we recall certain Hecke operators from [KL16, Section 2] which we refer to as "stabilization operators". These operators will be used to modify q-expansions at bad primes to translate an isomorphism of mod p Galois representations to a system of congruences of p-adic modular forms. We begin by recalling some notation which will be used throughout this section.

2.1. **Notations and conventions.** Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and view all number fields L as embedded $L \subset \overline{\mathbb{Q}}$. Let h_L denote the class number of L, and let $\overline{\mathbb{Z}}$ denote the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$. Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ (which amounts to fixing a prime of $\overline{\mathbb{Q}}$ above p). Let $\mathbb{C}_p$ be the p-adic completion of $\overline{\mathbb{Q}}_p$, and let L_p denote the p-adic completion of $L \subset \mathbb{C}_p$. For any integers a, b, let (a, b) denote their (positive) greatest common divisor. Given ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_L$, let $(\mathfrak{a}, \mathfrak{b})$ denote their greatest common divisor.

All Dirichlet (i.e. finite order) characters $\psi : \mathbb{A}_{\mathbb{Q}}^{\times} \to \overline{\mathbb{Q}}^{\times}$ will be primitive, and we denote the conductor by $f(\psi)$, which as an ideal in $\mathbb{Z}$ identified with its unique positive generator. We may equivalently view ψ as a character $\psi : (\mathbb{Z}/f(\psi))^{\times} \to \overline{\mathbb{Q}}^{\times}$ via

$$\psi(x \mod f(\psi)) = \prod_{\ell \nmid f(\psi)} \psi_\ell(x) = \prod_{\ell \mid f(\psi)} \psi_\ell^{-1}(x)$$

where $\psi_\ell : \mathbb{Q}_\ell^{\times} \to \overline{\mathbb{Q}}^{\times}$ is the local character at ℓ. Following convention, we extend ψ to $\mathbb{Z}/f(\psi) \to \overline{\mathbb{Q}}$, defining $\psi(a) = 0$ if $(a, f(\psi)) \neq 1$. Given Dirichlet character ψ_1 and ψ_2, we let $\psi_1\psi_2$ denote the unique primitive Dirichlet character such that $\psi_1\psi_2(a) = \psi_1(a)\psi_2(a)$ for all $a \in \mathbb{Z}$ with $(a, f(\psi)) = 1$. Given a prime p, let $f(\psi)_p$ denotes the p-primary part of $f(\psi)$ and let $f(\psi)^{(p)}$ denote the prime-to-p part of $f(\psi)$.

We define the Gauss sum $\mathfrak{g}(\psi)$ of ψ and local Gauss sums $\mathfrak{g}_\ell(\psi)$ as in [Kri16, Section 1]. We will often identify a Dirichlet character $\psi : \mathbb{A}_{\mathbb{Q}}^{\times} \to \overline{\mathbb{Q}}^{\times}$ with its associated Galois character $\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}^{\times}$ via the (inverse of the) Artin reciprocity map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}} \xrightarrow{\sim} \hat{\mathbb{Z}}^{\times}$, using the arithmetic normalization (i.e. the normalization where Frob_ℓ, the Frobenius conjugacy

class at ℓ, gets sent to the idéle which is ℓ at the place of $\mathbb{Z}$ corresponding to ℓ and 1 at all other places). Throughout, for a given p, let $\omega : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mu_{p-1}$ denote the mod p cyclotomic character. Let $\mathbb{N}_{\mathbb{Q}} : \mathbb{A}_{\mathbb{Q}}^{\times} \to \mathbb{C}^{\times}$ denote the norm character, normalized to have infinity type -1. For a number field K, let $\mathrm{Nm}_{K/\mathbb{Q}} : \mathbb{A}_K^{\times} \to \mathbb{A}_{\mathbb{Q}}^{\times}$ denote the idèlic norm, and let $\mathbb{N}_K := \mathbb{N}_{\mathbb{Q}} \circ \mathrm{Nm}_{K/Q} : \mathbb{A}_K^{\times} \to \mathbb{C}^{\times}$. Suppose we are given an imaginary quadratic field K with fundamental discriminant d_K. Let $\varepsilon_K : (\mathbb{Z}/d_K)^{\times} \to \mu_2$ be the quadratic character associated with K. For any Dirichlet character ψ over $\mathbb{Q}$, let

$$\psi_0 := \begin{cases} \psi, & \text{if } \psi \text{ even}, \\ \psi\varepsilon_K, & \text{if } \psi \text{ odd}. \end{cases}$$

Throughout, let $E/\mathbb{Q}$ be an elliptic curve of conductor $N = N_{\mathrm{split}} N_{\mathrm{nonsplit}} N_{\mathrm{add}}$, where N_{split} is only divisible by primes of split multiplicative reduction, N_{nonsplit} is only divisible by primes of nonsplit multiplicative reduction, and N_{add} is only divisible by primes of additive reduction.

Finally, for any number field L, let h_L denote its class number. For any non-square integer D, we denote by $h_3(D) := |\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))[3]|$ the 3-class number of the quadratic field $\mathbb{Q}(\sqrt{D})$.

2.2. **Main theorem.** We will show, by direct p-adic integration, the following generalization of Theorem 13 of loc. cit.[1]Our generalization, in particular, does not require $p \nmid N$.

The most general form of our result will address GL_2-type abelian varieties attached to normalized newforms of weight 2. Let $f \in S_2(\Gamma_0(N))$ be a normalized newform, with associated q-expansion at ∞ given by $\sum_{n=1}^{\infty} a_n q^n$. Suppose λ is the prime above p in the ring of integers of the number field E_f generated by the Hecke eigenvalues of f which is fixed by our above choice of embeddings $E_f \subset \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Henceforth, let $\mathbb{F}_\lambda$ denote the residue field of E_f at λ. Let ρ_f be the semisimple λ-adic $G_{\mathbb{Q}}$-representation associated with f, and let $\bar{\rho}_f$ denote its mod λ reduction. We let A_f denote the GL_2-type abelian variety associated with f by Eichler-Shimura theory (defined uniquely up to isogeny over $\mathbb{Q}$). In the rest of the article, when we say A is an *abelian variety of* GL_2*-type*, we always mean A is chosen in its isogeny class so that A admits an action by the ring of integers of E_f. Let $\pi_f : J_0(N) \to A$ be a modular parametrization. Let $\omega_f := f(q)\frac{dq}{q} \in \Omega^1_{X_0(N)/\mathbb{Q}}$, and let $\omega_A \in \Omega^1_{A/\mathbb{Q}}$ be such that $\pi_f^* \omega_A = \omega_f$.

Henceforth, write $N = N_+ N_- N_0$, where

(1) $\ell | N_+ \implies a_\ell \equiv \psi(\ell) \pmod{\lambda}$,
(2) $\ell | N_- \implies a_\ell \equiv \psi^{-1}(\ell)\ell \pmod{\lambda}$,
(3) $\ell | N_0 \implies a_\ell \equiv 0 \pmod{\lambda}$.

When $\bar{\rho}_f$ is reducible, such a decomposition always exists, by Theorem 34 of loc. cit. When f is attached to an elliptic curve $E/\mathbb{Q}$, for example, we can take $N_+ = N_{\mathrm{split}}, N_- = N_{\mathrm{nonsplit}}$ and $N_0 = N_{\mathrm{add}}$, where

(1) $\ell | N_{\mathrm{split}} \implies E$ has split multiplicative reduction at ℓ,
(2) $\ell | N_- \implies E$ has nonsplit multiplicative bad reduction at ℓ,
(3) $\ell | N_0 \implies E$ has additive bad reduction at ℓ.

Theorem 2.1. *Let $A/\mathbb{Q}$ be an abelian variety of GL_2-type (satisfying our assumptions above). Assume that $A[\lambda]$ is reducible, or equivalently, $A[\lambda]^{\mathrm{ss}} \cong \mathbb{F}_\lambda(\psi) \oplus \mathbb{F}_\lambda(\psi^{-1}\omega)$, for some character*

[1]Here our generalization also corrects a self-contained typo in the statement of Theorem 13 in loc. cit., where part of condition (3) was mistranscribed from Theorem 7 in loc. cit.: "$\ell \not\equiv -1 \mod p$" should be "$\ell \not\equiv \psi(\ell) \mod p$".

$\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\lambda^\times$. *Let K be an imaginary quadratic field satisfying the Heegner hypothesis for N. Suppose p splits in K. Suppose further that either the following conditions hold*

(1) $\psi(p) \neq 1$ *and* $(\psi^{-1}\omega)(p) \neq 1$,
(2) $N_+ = 1$,
(3) $8 \nmid f(\psi_0)$ *if* $p = 2$, *and* $p^2 \nmid f(\psi_0)$ *if* $p > 2$,
(4) $\ell \neq p, \ell | N_0$ *implies either* $\psi(\ell) \neq 1$ *and* $\ell \not\equiv \psi(\ell) \pmod{\lambda}$, *or* $\psi(\ell) = 0$,
(5) $p \nmid B_{1,\psi_0^{-1}\varepsilon_K} \cdot B_{1,\psi_0\omega^{-1}}$,

or the following conditions hold

(1) $\psi = 1$,
(2) $p | N$,
(3) $\ell | N, \ell \neq p$ *implies* $\ell || N, \ell \equiv -1 \pmod{p}, \ell \not\equiv 1 \pmod{p}$
(4) $\mathrm{ord}_\lambda \left(\frac{p-1}{2p} \log_p \overline{\alpha} \right) = 0$,

where $\alpha \in \mathcal{O}_K^\times$ *and* $(\alpha) = \mathfrak{p}^{h_K}$, $\overline{\alpha}$ *is its complex conjugate, and* $\log_p$ *is the Iwasawa p-adic logarithm.*

Let $P \in A(K)$ be the associated Heegner point. Then

$$\frac{1 + p - a_p}{p} \cdot \log_{\omega_A} P \neq 0 \pmod{p\mathcal{O}_{K_p}}.$$

In particular, $P \in A(K)$ is of infinite order and A/K has analytic and algebraic rank $\dim A$.

Remark 2.2. Suppose that $\psi \neq 1$, and $A = E$ is an elliptic curve (so that $\lambda = p$). Then one can show that condition (3) for the case $\psi \neq 1$ in the statement of Theorem 2.1, by the following argument.

If $p = 2$, then $\psi_0 = 1$ and $f(\psi_0) = 1$. If $p = 3$, then $\psi_0 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mu_2$ is quadratic, and so $9 \nmid f(\psi_0)$ (since $f(\psi_0)$ is squarefree outside of 2). If $p \geq 5$, then since $E[p]^{\mathrm{ss}} \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi^{-1}\omega)$, then $f(\psi) \cdot f(\psi^{-1}\omega) | N$. Since p splits in K, $f(\varepsilon_K)_p = 1$, and so $f(\psi_0)_p = f(\psi)_p$. Since $f(\omega) = p$, we have $f(\psi^{-1}\omega)_p = f(\psi^{-1})_p = f(\psi)_p$, and hence $f(\psi)_p^2 | N$. Now assume for the sake of contradiction that $p^2 | f(\psi_0)$. Then since $p^2 | f(\psi_0)_p = f(\psi)_p$, we have $p^4 | f(\psi)_p^2 | N$. However since N is the conductor of $E/\mathbb{Q}$ and $p \geq 5$, we have $\mathrm{ord}_p(N) \leq 2$, a contradiction.

Remark 2.3. When $p = 2$ and $A = E$ is an elliptic curve, we must have $\psi = 1$ (since $\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mu_{p-1} = \{1\}$). Note also that by (3) of the second part of Theorem 2.1, in this case N must be a power of 2.

Remark 2.4. Suppose $p = 3$, and that the GL_2-type abelian variety $A/\mathbb{Q}$ has a 3-isogeny defined over $\mathbb{Q}$ (i.e., $\mathbb{F}_\lambda \cong \mathbb{F}_3$). Then ψ is necessarily quadratic as is ψ_0, and so $9 \nmid f(\psi_0)$, and condition (3) in the case $\psi \neq 1$ of the statement of Theorem 2.1 is satisfied.

Remark 2.5. Note that when $p = 3$ and ψ is quadratic, condition (3) in case $\psi \neq 1$ of the statement of Theorem 2.1 is equivalent to

- $\ell | N_{\mathrm{add}}, \ell \equiv 1 \pmod{3}$ implies that $\psi(\ell) = -1$, and
- $\ell \neq 3, \ell | N_{\mathrm{add}}, \ell \equiv 2 \pmod{3}$ implies that $\psi(\ell) = 0$.

2.3. **Stabilization operators.** Here, we recall the definition of "stabilization operators", as in [KL16, §2.3]. We will use Katz's notion of p-adic modular forms as rules on the moduli space of isomorphism classes of ordinary test triples (see [KL16, Definition 2.1 and 2.2]). Let $\tilde{M}_k^{p\text{-adic}}(\Gamma_0(N))$ denote the space of weak p-adic modular forms of level N and $M_k^{p\text{-adic}}(\Gamma_0(N))$ the space of p-adic modular forms of level N, respectively. (See the paragraph after Definition 3.2 in loc. cit.) Note

that $M_k^{p\text{-adic}}(\Gamma_0(N)) \subset \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N))$. Fix $N^\# \in \mathbb{Z}_{>0}$ such that $N|N^\#$ (so that we may view $F \in M_k^{p\text{-adic}}(\Gamma_0(N^\#))$) and suppose that ℓ is a prime such that $\ell^2|N^\#$. Let V_ℓ be as defined in §3.3 of loc. cit.

Now we define the stabilization operators as operations on rules on the moduli space of isomorphism classes of test triples. Let $F \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N))$ and henceforth suppose N is the *minimal* level of F. View $F \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N^\#))$, and let $a_\ell(F)$ denote the coefficient of the q^ℓ term in the q-expansion $F(q)$. Then up to permutation there is a unique pair of numbers $(\alpha_\ell(F), \beta_{\ell(F)}) \in \mathbb{C}_p^2$ such that $\alpha_\ell(F) + \beta_\ell(F) = a_\ell(F)$, $\alpha_\ell(F)\beta_\ell(F) = \ell^{k-1}$. We henceforth fix an ordered pair $(\alpha_\ell, \beta_\ell)$.

Definition 2.6. When $\ell \nmid N$, we define the $(\ell)^+$*-stabilization of* F as

$$F^{(\ell)^+} = F - \beta_\ell(F)V_\ell^* F, \tag{3}$$

the $(\ell)^-$*-stabilization of* F as

$$F^{(\ell)^-} = F - \alpha_\ell(F)V_\ell^* F, \tag{4}$$

and the $(\ell)^0$*-stabilization for* F as

$$F^{(\ell)^0} = F - a_\ell(F)V_\ell^* F + \ell^{k-1}V_\ell^* V_\ell^* F. \tag{5}$$

We have $F^{(\ell)^*} \in M_k^{p\text{-adic}}(\Gamma_0(N^\#))$ for $* \in \{+, -, 0\}$. On q-expansions, we have

$$F^{(\ell)^+}(q) := F(q) - \beta_\ell(F)F(q^\ell),$$

$$F^{(\ell)^-}(q) := F(q) - \alpha_\ell(F)F(q^\ell),$$

$$F^{(\ell)^0}(q) := F(q) - a_\ell(F)F(q^\ell) + \ell^{k-1}F(q^{\ell^2}).$$

It follows that if F is a T_n-eigenform where $\ell \nmid n$, then $F^{(\ell)^*}$ is still an eigenform for T_n. If F is a T_ℓ-eigenform, one verifies by direct computation that $a_\ell(F^{(\ell)^+}) = \alpha_\ell(F)$, $a_\ell(F^{(\ell)^-}) = \beta_\ell(F)$, and $a_\ell(F^{(\ell)^0}) = 0$.

When $\ell|N$, we define the $(\ell)^0$*-stabilization of* F as

$$F^{(\ell)^0} = F - a_\ell(F)V_\ell^* F. \tag{6}$$

Again, we have $F^{(\ell)^0} \in M_k^{p\text{-adic}}(\Gamma_0(N^\#))$. On q-expansions, we have

$$F^{(\ell)^0}(q) := F(q) - a_\ell(F)F(q^\ell).$$

It follows that if F is a U_n-eigenform where $\ell \nmid n$, then $F^{(\ell)^0}$ is still an eigenform for U_n. If F is a U_ℓ-eigenform, one verifies by direct computation that $a_\ell(F^{(\ell)^0}) = 0$.

Note that for $\ell_1 \neq \ell_2$, the stabilization operators $F \mapsto F^{(\ell_1)^*}$ and $F \mapsto F^{(\ell_2)^*}$ commute. Then for pairwise coprime integers with prime factorizations $N_+ = \prod_i \ell_i^{e_i}$, $N_- = \prod_j \ell^{e_j}$, $N_0 = \prod_m \ell_m^{e_m}$, we define the (N_+, N_-, N_0)*-stabilization of* F as

$$F^{(N_+,N_-,N_0)} := F^{\prod_i (\ell_i)^+ \prod_j (\ell_j)^- \prod_m (\ell_m)^0}.$$

2.4. **Stabilization operators at CM points.** Let K be an imaginary quadratic field satisfying the Heegner hypothesis with respect to $N^{\#}$. Assume that p splits in K, and let $\mathfrak{p}$ be prime above p determined by the embedding $K \subset \mathbb{C}_p$. Let $\mathfrak{N}^{\#} \subset \mathcal{O}_K$ be a fixed ideal such that $\mathcal{O}/\mathfrak{N}^{\#} = \mathbb{Z}/N^{\#}$, and if $p|N^{\#}$, we assume that $\mathfrak{p}|\mathfrak{N}^{\#}$. Let $A/\mathcal{O}_{\mathbb{C}_p}$ be an elliptic curve with CM by $\mathcal{O}_K$. By the theory of complex multiplication and Deuring's theorem, $(A, A[\mathfrak{N}^{\#}], \omega)$ is an ordinary test triple over $\mathcal{O}_{\mathbb{C}_p}$.

Given an ideal $\mathfrak{a} \subset \mathcal{O}_K$, we define $A_{\mathfrak{a}} = A/A[\mathfrak{a}]$, an elliptic curve over $\mathcal{O}_{\mathbb{C}_p}$ which has CM by $\mathcal{O}_K$. Let $\phi_{\mathfrak{a}} : A \to A_{\mathfrak{a}}$ denote the canonical projection. Note that there is an induced action of prime-to-$\mathfrak{N}^{\#}$ integral ideals $\mathfrak{a} \subset \mathcal{O}_K$ on the set of triples $(A, A[\mathfrak{N}^{\#}], \omega)$ given by of isomorphism classes $[(A, A[\mathfrak{N}^{\#}], \omega)]$, given by

$$\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega) = (A_{\mathfrak{a}}, A_{\mathfrak{a}}[\mathfrak{N}^{\#}], \omega_{\mathfrak{a}})$$

where $\omega_{\mathfrak{a}} \in \Omega^1_{A_{\mathfrak{a}}/\mathbb{C}_p}$ is the unique differential such that $\phi_{\mathfrak{a}}^* \omega_{\mathfrak{a}} = \omega$. Note that this action descends to an action on the set of isomorphism classes of triples $[(A, A[\mathfrak{N}^{\#}], \omega)]$ given by $\mathfrak{a} \star [(A, A[\mathfrak{N}^{\#}], \omega)] = [\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)]$. Letting $\mathfrak{N} = (\mathfrak{N}^{\#}, N)$, also note that for any $\mathfrak{N}' \subset \mathcal{O}_K$ with norm N' and $\mathfrak{N}|\mathfrak{N}'|N^{\#}$, the Shimura reciprocity law also induces an action of prime-to-$\mathfrak{N}'$ integral ideals on CM test triples and isomorphism classes of ordinary CM test triples of level N'.

The following is Lemma 2.6 of [KL16].

Lemma 2.7. *Suppose $F \in \tilde{M}_k^{p\text{-}adic}(\Gamma_0(N^{\#}))$, and let $\chi : \mathbb{A}_K^{\times} \to \mathbb{C}_p^{\times}$ be a p-adic Hecke character such χ is unramified (at all finite places of K), and $\chi_\infty(\alpha) = \alpha^k$ for any $\alpha \in K^{\times}$. Let $\{\mathfrak{a}\}$ be a full set of integral representatives of $\mathcal{C}\ell(\mathcal{O}_K)$ where each $\mathfrak{a}$ is prime to $\mathfrak{N}^{\#}$. If $\ell \nmid N$, we have*

$$\sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) F^{(\ell)^+}(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)) = \big(1 - \beta_\ell(F)\chi^{-1}(\overline{v})\big) \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) F(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)),$$

$$\sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) F^{(\ell)^-}(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)) = \big(1 - \alpha_\ell(F)\chi^{-1}(\overline{v})\big) \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) F(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)),$$

$$\sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) F^{(\ell)^0}(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)) = \left(1 - a_\ell(F)\chi^{-1}(\overline{v}) + \frac{\chi^{-2}(\overline{v})}{\ell}\right) \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) F(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega))$$

and if $\ell | N$, we have

$$\sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) F^{(\ell)^0}(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)) = \big(1 - a_\ell(F)\chi^{-1}(\overline{v})\big) \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) F(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)).$$

2.5. **The Eisenstein congruence.** We may assume without loss of generality that $\psi \neq \omega$ (otherwise, interchange ψ and $\psi^{-1}\omega$). As in the proof of Theorem 13 in [Kri16], the argument relies on establishing an Eisenstein congruence. More precisely, let $f \in S_2(\Gamma_0(N))$ be the normalized newform associated with A by modularity, and let A_f be the GL_2-type abelian variety associated with f by Eichler-Shimura theory, so that A is isogenous with A_f by Faltings' isogeny theorem. Also suppose (without loss of generality) that A_f satisfies our assumptions stated just before Theorem 2.1. Recall the weight 2 Eisenstein series $E_{2,\psi}$ defined by the q-expansion (at ∞)

$$E_{2,\psi}(q) := \delta(\psi)\frac{L(-1,\psi)}{2} + \sum_{n=1}^{\infty} \sigma^{\psi,\psi^{-1}}(n)q^n$$

where $\delta(\psi) = 1$ if $\psi = 1$ and $\delta(\psi) = 0$ otherwise, and

$$\sigma^{\psi,\psi^{-1}}(n) = \sum_{0<d|n} \psi(n/d)\psi^{-1}(d)d.$$

This determines a $\Gamma_0(f(\psi)^2)$-level algebraic modular form of weight 2, in Katz's sense (see [Kat76, Chapter II]).

Note that the minimal level of $E_{2,\psi}$ is $f(\psi)^2$. With respect to this level, take $N^{\#}$ as in §2.6 to be $N^{\#} = \mathrm{lcm}_{\ell|N}(\ell^2, f(\psi))$. We now consider $E_{2,\psi}$ as a form of level $N^{\#}$ and let $E_{2,\psi}^{(N_+,N_-,N_0)}$ denote the (N_+, N_-, N_0)-stabilization of $E_{2,\psi}$, with the choices $\alpha_\ell = \psi(\ell)$ and $\beta_\ell = \psi^{-1}(\ell)\ell$ as in Definition 2.6. . Thus, viewing f and $E_{2,\psi}^{(N_+,N_-,N_0)}$ as a p-adic $\Gamma_0(N)$-level modular forms over $\mathcal{O}_{\mathbb{C}_p}$, we have

$$\theta^j f(q) \equiv \theta^j E_{2,\psi}^{(N_+,N_-,N_0)}(q) \pmod{\lambda\mathcal{O}_{\mathbb{C}_p}}$$

for all $j \geq 1$.

Let A_0 be a fixed elliptic curve with complex multiplication by $\mathcal{O}_K$, and fix an ideal $\mathfrak{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{N} = \mathbb{Z}/N$ and $\mathfrak{p}|\mathfrak{N}$ if $p|N$. Since p is split in K, the q-expansion principle implies that the above congruences of q-expansions translate to congruences on points corresponding to curves with CM by $\mathcal{O}_K$. Let $P_f \in A_f(K)$ denote the Heegner point associated with A_f. As is explained in §2 of [KL16], by a generalization of Coleman's theorem ([LZZ15, Proposition A.1], see also [KL16, Theorem 2.8]), this implies that (for any generator $\omega \in \Omega^1_{A_0/\mathcal{O}_{\mathbb{C}_p}}$)

(7)

$$\begin{aligned}
\frac{1+p-a_p}{p} \cdot \log_{\omega_A} P &= \frac{1+p-a_p}{p} \cdot \log_{\omega_{A_f}} P_f \\
&= \sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1} f^{(1,1,p)}(\mathfrak{a} \star (A_0, A_0[\mathfrak{N}], \omega)) \\
&\equiv \sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1} E_{2,\psi}^{(N_+,N_-,pN_0)}(\mathfrak{a} \star (A_0, A_0[\mathfrak{N}], \omega)) \\
&= \prod_{\ell|N_+,\ell\neq p} (1-\psi^{-1}(\ell)) \prod_{\ell|N_-,\ell\neq p} \left(1-\frac{\psi(\ell)}{\ell}\right) \prod_{\ell|N_0,\ell\neq p} (1-\psi^{-1}(\ell)) \left(1-\frac{\psi(\ell)}{\ell}\right) \\
&\qquad \cdot \sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1} E_{2,\psi}^{(1,1,p)}(\mathfrak{a} \star (A_0, A_0[\mathfrak{N}], \omega)) \pmod{\lambda\mathcal{O}_{\mathbb{C}_p}}
\end{aligned}$$

where the final equality follows from Lemma 2.7, applied to successive stabilizations of $E_{2,\psi}$.

2.6. **CM period of Eisenstein series.** To evaluate (7) further, we need to study the period

$$\sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1}E_{2,\psi}^{(1,1,p)}(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega)) \pmod{\lambda\mathcal{O}_{\mathbb{C}_p}}.$$

We will show that this period is interpolated by the Katz p-adic L-function. Indeed, let χ_j be the unramified Hecke character of infinity type $(h_Kj,-h_Kj)$ defined on ideals by

$$\chi_j(\mathfrak{a}) = (\alpha/\overline{\alpha})^j$$

where $(\alpha)=\mathfrak{a}^{h_K}$, and h_K is the class number of K. Let $\overline{\mathfrak{p}}$ denote the prime ideal of $\mathcal{O}_K$ which is the complex conjugate of $\mathfrak{p}$. For the remainder of the proof, in a slight abuse of notation, unless otherwise stated let $\mathbb{N}_K$ denote the p-adic Hecke character associated with the algebraic Hecke character giving rise to the complex Hecke character $\mathbb{N}_K : K^\times\backslash\mathbb{A}_K^\times\to\mathbb{C}^\times$. Then by looking at q-expansions and invoking the q-expansion principle, it is apparent that the above sum is given by

$$\begin{aligned}
&\sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1}E_{2,\psi}^{(1,1,p)}(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega))\\
&=\lim_{j\to 0}\sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)}(\chi_j^{-1}\mathbb{N}_K^{h_Kj})(\mathfrak{a})\theta^{-1+h_Kj}E_{2,\psi}^{(1,1,p)}(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega))\\
&=\lim_{j\to 0}(1-\psi^{-1}(p)\chi_j^{-1}(\overline{\mathfrak{p}}))(1-\psi(p)(\chi_j^{-1}\mathbb{N}_K)(\overline{\mathfrak{p}}))\\
&\qquad\qquad\cdot\sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)}(\chi_j^{-1}\mathbb{N}_K^{h_Kj})(\mathfrak{a})\theta^{-1+h_Kj}E_{2,\psi}(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega))
\end{aligned}\tag{8}$$

since $\chi_j^{-1}\mathbb{N}_K^{h_Kj}\to 1$ as $j\to 0=(0,0)\in\mathbb{Z}/(p-1)\times\mathbb{Z}_p$; here the last equality again follows from Lemma 2.7 applied to $F=E_{2,\psi}$.

2.7. **The Katz p-adic L-function.** We will now show that the terms in the above limit are interpolated by the Katz p-adic L-function (restricted to the anticyclotomic line). Let $\mathfrak{f}|\mathfrak{N}$ such that $\mathcal{O}/\mathfrak{f}=\mathbb{Z}/f(\psi)$. Choose a good integral model $\mathcal{A}_0$ of A_0 at p, choose an identification $\iota:\hat{\mathcal{A}}_0\xrightarrow{\sim}\hat{\mathbb{G}}_m$ (unique up to $\mathbb{Z}_p^\times$), and let $\omega_{\mathrm{can}}:=\iota^*\frac{du}{u}$ where u is the coordinate on $\hat{\mathbb{G}}_m$. This choice of ω_{can} determines p-adic and complex periods Ω_p and Ω_∞ as in Section 3 of [Kri16]. As an intermediate step to establishing the p-adic interpolation, we have the following identity of algebraic values.

Lemma 2.8. *We have the following identity of values in $\overline{\mathbb{Q}}$ for $j\geq 1$:*

$$\begin{aligned}
&\sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)}(\chi_j^{-1}\mathbb{N}_K^{h_Kj})(\mathfrak{a})\theta^{-1+h_Kj}E_{2,\psi}(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega_{\mathrm{can}}))\\
&=\left(\frac{\Omega_p}{\Omega_\infty}\right)^{2h_Kj}\cdot\frac{f(\psi)^2\Gamma(1+h_kj)\psi^{-1}(-\sqrt{d_K})(\chi_j^{-1}\mathbb{N}_K)(\bar{\mathfrak{f}})}{(2\pi i)^{1+h_Kj}\mathfrak{g}(\psi^{-1})(\sqrt{d_K})^{-1+h_Kj}}L((\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K,0)
\end{aligned}$$

where $\psi^{-1}(-\sqrt{d_K})$ denotes the Dirichlet character ψ^{-1} evaluated at the unique class $b\in(\mathbb{Z}/f(\psi))^\times$ such that $b+\sqrt{d_K}\equiv 0 \pmod{\mathfrak{f}}$. (In particular, note that the above complex-analytic calculation does not use the assumptions $p>2$ or $p\nmid f(\psi)$.)

Proof. View the algebraic modular form $E_{2,\psi}$ as a modular form over $\mathbb{C}$, and evaluate at CM triples $(A_0,A_0[\mathfrak{N}],2\pi idz)$ as a triple over $\mathbb{C}$ by considering the uniquely determined complex uniformization $\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z})\cong A_0$ for some τ in the complex upper half-plane, and identifying $A_0[\mathfrak{N}]$ with $\frac{1}{N}\mathbb{Z}\subset$

$\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z})$. By plugging $\psi_1=\psi_2^{-1}=\psi$ and $\mathfrak{u}=\mathfrak{t}=\mathfrak{f}$, $\mathfrak{N}'=\mathfrak{f}^2$ into Proposition 36 of loc. cit., we have the complex identity

$$\begin{aligned}&\sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)}(\chi_j^{-1}\mathbb{N}_K^{h_Kj})(\mathfrak{a})\partial^{-1+h_Kj}E_{2,\psi}(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],2\pi idz))\\&=\frac{f(\psi)^2\Gamma(1+h_kj)\psi^{-1}(-\sqrt{d_K})(\chi_j^{-1}\mathbb{N}_K)(\bar{\mathfrak{f}})}{(2\pi i)^{1+h_Kj}\mathfrak{g}(\psi^{-1})(\sqrt{d_K})^{-1+h_Kj}}L((\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K,0)\end{aligned}\tag{9}$$

where ∂ is the complex Maass-Shimura operator, and $\mathbb{N}_K:K^\times\backslash\mathbb{A}_K^\times\to\mathbb{C}^\times$ is the complex norm character over K. By definition of Ω_p and Ω_∞, we have

$$2\pi idz=\frac{\Omega_p}{\Omega_\infty}\cdot\omega_{\mathrm{can}}.$$

By Proposition 21 of loc. cit., we have the equality of *algebraic* values

$$\partial^{-1+h_kj}E_2(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega_{\mathrm{can}}))=\theta^{-1+h_kj}E_2(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega_{\mathrm{can}}))$$

for all $j\geq 1$. Moreover, since $\mathbb{N}_K(\mathfrak{a})\in\overline{\mathbb{Z}}$, we can identify this value of $\mathbb{N}_K$ with the value of its p-adic avatar, which again we also denote by $\mathbb{N}_K$, at $\mathfrak{a}$. Applying these identities to the identity of complex numbers (9), we get the desired identity of algebraic numbers. □

We now apply the interpolation property of the Katz p-adic L-function (see [HT93, Theorem II]) to our situation, taking the normalization as in [Gro80], thus arriving at the identity

$$\begin{aligned}&L_p^{\mathrm{Katz}}((\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K,0)=4\cdot\mathrm{Local}_{\mathfrak{p}}((\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K)\left(\frac{\Omega_p}{\Omega_\infty}\right)^{2h_Kj}\\&\cdot\left(\frac{2\pi i}{\sqrt{D_K}}\right)^{-1+h_Kj}\Gamma(1+h_Kj)(1-\psi(p)(\chi_j^{-1}\mathbb{N}_K)(\overline{\mathfrak{p}}))(1-\psi(p)\chi_j^{-1}(\overline{\mathfrak{p}}))L((\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K,0)\end{aligned}\tag{10}$$

for all $j\geq 1$, where $\mathrm{Local}_{\mathfrak{p}}(\chi)=\mathrm{Local}_{\mathfrak{p}}(\chi,\Sigma,\delta)$ is defined as in [Kat78, 5.2.26] with $\Sigma=\{\mathfrak{p}\}$ and $\delta=\sqrt{d_K}/2$ (or as denoted $W_p(\lambda)$ in [HT93, 0.10]). For any prime ℓ, let $\psi_\ell(-\sqrt{d_K})$ denote the value $\psi_\ell(b)$, where again $b\in\mathbb{Z}$ is any integer such that $b+\sqrt{d_K}\in\mathfrak{f}$. By directly plugging in $\chi=(\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K$ into the definition of $\mathrm{Local}_{\mathfrak{p}}$, we have

$$\mathrm{Local}_{\mathfrak{p}}((\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K)=\psi_p(-\sqrt{d_K})\frac{f(\psi)_p}{\mathfrak{g}_p(\psi)}.$$

Plugging (10) into the identity in Lemma 2.8, we have for all $j\geq 1$

$$\begin{aligned}&(1-\psi^{-1}(p)\chi_j^{-1}(\overline{\mathfrak{p}}))(1-\psi(p)(\chi_j^{-1}\mathbb{N}_K)(\overline{\mathfrak{p}}))\sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)}(\chi_j^{-1}\mathbb{N}_K^{h_Kj})(\mathfrak{a})\theta^{-1+h_Kj}E_{2,\psi}(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega_{\mathrm{can}}))\\&=\frac{f(\psi)^{(p)}\cdot f(\psi)\cdot(\chi_j^{-1}\mathbb{N}_K)(\bar{\mathfrak{f}})}{4(\prod_{\ell|f(\psi)^{(p)}}\psi_\ell^{-1}(-\sqrt{d_K})\mathfrak{g}_\ell(\psi))(2\pi i)^{2h_Kj}}L_p^{\mathrm{Katz}}((\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K,0).\end{aligned}$$

Taking the limit $j\to 0=(0,0)\in\mathbb{Z}/(p-1)\times\mathbb{Z}_p$, noting that $\chi_j^{-1}\mathbb{N}_K\to\mathbb{N}_K$ and $\mathbb{N}_K(\bar{\mathfrak{f}})=f(\psi)^{-1}$, and applying (8), we have

$$\sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)}\theta^{-1}E_{2,\psi}^{(1,1,p)}(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega_{\mathrm{can}}))=\frac{f(\psi)^{(p)}}{4(\prod_{\ell|f(\psi)^{(p)}}\psi_\ell^{-1}(-\sqrt{d_K})\mathfrak{g}_\ell(\psi))}L_p^{\mathrm{Katz}}((\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\mathbb{N}_K,0).\tag{11}$$

2.8. **Gross's factorization theorem.** We now evaluate the Katz p-adic L-value on the right-hand side of (11).

Lemma 2.9. *We have, for $\psi \neq 1$,*

$$\sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1}E_{2,\psi}^{(1,1,p)}(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega_{\mathrm{can}})) = \pm\frac{1}{4}(1-\psi^{-1}(p))(1-(\psi\omega^{-1})(p))B_{1,\psi_0^{-1}\varepsilon_K}B_{1,\psi_0\omega^{-1}} \pmod{p\mathcal{O}_{\mathbb{C}_p}}$$

and for $\psi = 1$,

$$\sum_{[\mathfrak{a}]\in\mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1}E_{2,1}^{(1,1,p)}(\mathfrak{a}\star(A_0,A_0[\mathfrak{N}],\omega_{\mathrm{can}})) \equiv \frac{p-1}{2p}\log_p\overline{\alpha} \pmod{p\mathcal{O}_{\mathbb{C}_p}}$$

where $\alpha\in\mathcal{O}_K$ such that $(\alpha)=\mathfrak{p}^{h_K}$.

Proof. Applying Gross's factorization theorem (see [Gro80], and [Kri16, Theorem 28] for the extension to the general auxiliary conductor case), we have

$$\frac{f(\psi)^{(p)}}{(\prod_{\ell|f(\psi)^{(p)}}\psi_\ell^{-1}(-\sqrt{d_K})\mathfrak{g}_\ell(\psi))}L_p^{\mathrm{Katz}}((\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\mathbb{N}_K,0) = \pm L_p(\psi_0^{-1}\varepsilon_K\omega,0)L_p(\psi_0,1) \tag{12}$$

where $L_p(\cdot,s)$ denotes the Kubota-Leopoldt p-adic L-function; here the sign of ±1 is uniquely determined, as in loc. cit., by the special value formula due to Katz used in Gross's proof (the term on the left-hand side of the statement in loc. cit. already incorporates this sign). We now evaluate each Kubota-Leopoldt factor in the above identity. Using the fact that $\varepsilon_K(p)=1$ since p splits in K, by the interpolation property of the Kubota-Leopoldt p-adic L-function we have

$$L_p(\psi_0^{-1}\varepsilon_K,0) = -(1-\psi^{-1}(p))B_{1,\psi_0^{-1}\varepsilon_K}. \tag{13}$$

Now if by condition (3) in the case $\psi\neq1$ of the statement of the theorem, we know that $L_p(\psi_0,m)\equiv L_p(\psi_0,n) \pmod{p\mathcal{O}_{\mathbb{C}_p}}$ for all $m,n\in\mathbb{Z}$ by [Was97, Corollary 5.13]. Thus

$$L_p(\psi_0,1)\equiv L_p(\psi_0,0) = -(1-(\psi\omega^{-1})(p))B_{1,\psi_0\omega^{-1}} \pmod{p\mathcal{O}_{\mathbb{C}_p}}. \tag{14}$$

Combining (12), (13), and (14), we get

$$\frac{f(\psi)^{(p)}}{\prod_{\ell|f(\psi)^{(p)}}\psi_\ell^{-1}(-\sqrt{d_K})\mathfrak{g}_\ell(\psi)}L_p^{\mathrm{Katz}}((\psi\circ\mathrm{Nm}_{K/\mathbb{Q}})\mathbb{N}_K,0) \equiv \pm(1-\psi^{-1}(p))(1-(\psi\omega^{-1})(p))B_{1,\psi_0^{-1}\varepsilon_K}B_{1,\psi_0\omega^{-1}} \pmod{p\mathcal{O}_{\mathbb{C}_p}} \tag{15}$$

when $\psi\neq1$.

Now suppose $\psi=1$. In particular $f(\psi)=f(\psi)^{(p)}=1$. By the functional equation for the Katz p-adic L-function (e.g. see [HT93, Theorem II]), since $\check{\mathbb{N}}_K=\mathbb{N}_K^{-1}\mathbb{N}_K=1$ is the dual Hecke character of $\mathbb{N}_K$, we have

$$L_p^{\mathrm{Katz}}(\mathbb{N}_K,0) = L_p^{\mathrm{Katz}}(1,0).$$

By a standard special value formula (e.g. see [Gro80, Section 5, Formulas 1]), we have

$$L_p^{\mathrm{Katz}}(1,0) = \frac{4}{|\mathcal{O}_K^\times|}\cdot\frac{p-1}{p}\log_p(\overline{\alpha})$$

and so

$$L_p^{\mathrm{Katz}}(\mathbb{N}_K, 0) = \frac{4}{|\mathcal{O}_K^\times|} \cdot \frac{p-1}{p} \log_p(\overline{\alpha}) = 2 \cdot \frac{p-1}{p} \log_p(\overline{\alpha}) \tag{16}$$

since we assume $d_K < -4$ and hence $|\mathcal{O}_K^\times| = 2$.

Now plugging in (15) into (11) when $\psi \neq 1$, and (16) into (11) when $\psi = 1$, we establish the lemma. □

2.9. **The proof of Theorem 2.1.** Putting together (7) and Lemma (2.9), we arrive at our main congruence identities. If $\psi \neq 1$ we have

(17)

$$\frac{1+p-a_p}{p} \cdot \log_{\omega_A} P \equiv \pm \prod_{\ell | N_+, \ell \neq p} \left(1 - \psi^{-1}(\ell)\right) \prod_{\ell | N_-, \ell \neq p} \left(1 - \frac{\psi(\ell)}{\ell}\right) \prod_{\ell | N_0, \ell \neq p} \left(1 - \psi^{-1}(\ell)\right) \left(1 - \frac{\psi(\ell)}{\ell}\right)$$
$$\cdot \frac{1}{4}(1 - \psi^{-1}(p))(1 - (\psi\omega^{-1})(p)) B_{1, \psi_0^{-1}\varepsilon_K} B_{1, \psi_0 \omega^{-1}} \pmod{\lambda \mathcal{O}_{\mathbb{C}_p}}.$$

Now the statement for $\psi \neq 1$ in theorem 2.1 immediately follows from studying when the right-hand side of the congruence vanishes mod p. If $\psi = 1$ we have

(18)

$$\frac{1+p-a_p}{p} \cdot \log_{\omega_A} P \equiv \begin{cases} \prod_{\ell | N_-, \ell \neq p} \left(1 - \frac{1}{\ell}\right) \cdot \frac{p-1}{2p} \log_p \overline{\alpha} \pmod{\lambda \mathcal{O}_{\mathbb{C}_p}}, & \text{if } \ell | N_+ N_0 \implies \ell = p, \\ 0 \pmod{\lambda \mathcal{O}_{\mathbb{C}_p}}, & \text{if } \exists \ell \neq p \text{ such that } \ell | N_+ N_0, \end{cases}$$

where $(\overline{\alpha}) = \overline{\mathfrak{p}}^{h_K}$ and $\log_p$ is the Iwasawa p-adic logarithm (i.e. the locally analytic function defined by the usual power series $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$, and then uniquely extended to all of $\mathbb{C}_p^\times$ by defining $\log_p p = 0$).

We now finish the proof of Theorem 2.1 with the following lemma.

Lemma 2.10. *The right-hand side of (18) does not vanish mod p if any only if*
(1) $\ell | N, \ell \neq p$ implies $\ell || N, \ell \equiv -1 \pmod{p}, \ell \not\equiv 1 \pmod{p}$,
(2) $\mathrm{ord}_\lambda \left(\frac{p-1}{2p} \log_p \overline{\alpha} \right) = 0$..
We also have that the non-vanishing of the right-hand side of (18) mod p implies $p | N$, and so the right-hand side of (18) does not vanish mod p if and only if $p | N$ and (1) and (2) hold.

Proof. We first study when

$$\prod_{\ell | N_-, \ell \neq p} \left(1 - \frac{1}{\ell}\right) \cdot \frac{p-1}{2p} \log_p \overline{\alpha} \tag{19}$$

vanishes mod λ. Clearly (19) does not vanish mod λ if and only if each of its factors does not vanish mod λ. Then $\prod_{\ell | N_-, \ell \neq p} \left(1 - \frac{1}{\ell}\right)$ does not vanish mod λ if and only if

$$\ell | N_-, \ell \neq p \implies \ell \not\equiv 1 \pmod{p}. \tag{20}$$

Hence (19) does not vanish mod p if and only if (20) and (2) in the statement of the lemma hold.

If the right-hand side of (18) does not vanish, then we have $\ell | N_+ N_0 \implies \ell = p$, the right-hand side of (18) equals (19) mod p, and (20) holds. Thus (1) and (2) in the statement of the lemma hold.

If (1) and (2) in the statement of the lemma hold, then since by definition $\ell | N_- \implies \ell \equiv \pm 1 \pmod{p}$, we have that (20) holds. So (19) does not vanish mod p. Now if $\ell | N_+ N_0$ and $\ell \neq p$,

then by (1) in the statement of the lemma, we have $\ell || N, \ell \not\equiv 1 \pmod{p}$. Hence $\ell \nmid N_0, \ell \nmid N_+$, a contradiction. So we have $\ell | N_+ N_0 \implies \ell = p$, and so the right-hand side of (18) equals (19) mod p, which does not vanish mod p.

Thus we have shown that the non-vanishing of the right-hand side of (18) mod p is equivalent to (1) and (2) in the statement of the lemma.

Now we show the second part of the theorem. Suppose that the right-hand side of (18) does not vanish. In particular, we have $\ell | N_+ N_0 \implies \ell = p$ and that the right-hand side of (18) equals (19) mod p. If $p \nmid N$, then we thus have $N_+ N_0 = 1$. We now show a contradiction, considering the cases $p = 2$ and $p \geq 3$ separately.

Suppose $p = 2$. Then since $2 \nmid N_- = N \neq 1$ (where $N \neq 1$ follows because E is an elliptic curve over $\mathbb{Q}$), we have that there exists $\ell | N_-$ with $\ell \equiv 1 \pmod{2}$. Hence

$$\prod_{\ell | N_-, \ell \neq p} \left(1 - \frac{1}{\ell}\right) \equiv 0 \pmod{p} \tag{21}$$

and the right-hand side of (18) vanishes mod p, a contradiction.

Suppose $p > 2$. Note that

$$(N_{\mathrm{split}}, N_-) = \prod_{\ell | N_-, \ell \equiv 1 \pmod{p}} \ell. \tag{22}$$

Since $N_0 = N_{\mathrm{add}}$ (because they are both the squarefull parts of N), we have $N_{\mathrm{add}} = N_0 = 1$. By [Yoo15, Theorem 2.2], we know that $N_{\mathrm{split}} N_{\mathrm{add}} \neq 1$, and hence $N_{\mathrm{split}} \neq 1$. Since $N_+ = 1$, we therefore have that $1 \neq N_{\mathrm{split}} | N_-$. By (22), we thus have that there is some $\ell | N_-$ such that $\ell \equiv 1 \pmod{p}$. In particular we have (21) once again, and so the right-hand side of (18) vanishes mod p, a contradiction. □

Remark 2.11. Note that our proof uses a direct method of p-adic integration, and does not go through the construction of the Bertolini–Darmon–Prasanna (BDP) p-adic L-function as in the proof of the main theorem of loc. cit. In particular, it does not recover the more general congruence of the BDP and Katz p-adic L-functions established when p is of good reduction established in [Kri16] (also for higher weight newforms). We expect that our method should extend to higher weight newforms, in particular establishing congruences between images of generalized Heegner cycles under appropriate p-adic Abel-Jacobi images and quantities involving higher Bernoulli numbers and Euler factors, without using the deep BDP formula.

3. Bernoulli numbers and relative class numbers

When $p = 3$ and A has a 3-isogeny defined over $\mathbb{Q}$, all Dirichlet characters in Theorem 2.1 are quadratic. Note that for an odd quadratic character ψ over $\mathbb{Q}$, by the analytic class number formula we have

$$B_{1,\psi} = -2 \frac{h_{K_\psi}}{|\mathcal{O}_{K_\psi}^\times|} \tag{23}$$

where K_ψ is the imaginary quadratic field associated with ψ. So the 3-indivisibility criteria of the theorem becomes a question of 3-indivisibility of quadratic class numbers. This fact will be employed in our applications to Goldfeld's conjecture.

More generally, for $p \geq 3$, we can find a sufficient condition for non-vanishing mod p of the Bernoulli numbers $B_{1,\psi_0^{-1}\varepsilon_K} B_{1,\psi_0\omega^{-1}}$ in terms of non-vanishing mod p of the relative class numbers

of the abelian CM fields of degrees dividing $p-1$ cut out by $\psi_0^{-1}\varepsilon_K$ and $\psi_0\omega^{-1}$. Let us first observe the following simple lemma.

Lemma 3.1. *Suppose $\psi : (\mathbb{Z}/f)^\times \to \mu_{p-1}$ is a Dirichlet character, and assume $\psi^{-1} \neq \omega$, or equivalently, assume there exists some $a \in (\mathbb{Z}/f)^\times$ such that $\psi(a)a \not\equiv 1 \pmod{p\mathbb{Z}[\mu_{p-1}]}$. Then*

$$\mathrm{ord}_p(B_{1,\psi}) \geq 0.$$

Proof. By our assumption, there exists some $a \in (\mathbb{Z}/f)^\times$ such that $\psi(a)a \not\equiv 1 \pmod{p\mathbb{Z}[\mu_{p-1}]}$. Then we have

$$\sum_{m=1}^{f} \psi(m)m \equiv \sum_{m=1}^{f} \psi(am)am = \psi(a)a \sum_{m=1}^{f} \psi(m)m \pmod{p\mathbb{Z}[\mu_{p-1}]}$$

$$\implies (1-\psi(a)a) \cdot \sum_{m=1}^{f} \psi(m)m \equiv 0 \pmod{p\overline{\mathbb{Z}}} \implies \sum_{m=1}^{f} \psi(m)m \equiv 0 \pmod{p\mathbb{Z}[\mu_{p-1}]}.$$

Now our conclusion follows from the formula for the Bernoulli numbers (1). □

For an odd Dirichlet character ψ, let K_ψ denote the abelian CM field cut out by ψ. Consider the relative class number $h^-_{K_\psi} = h_{K_\psi}/h_{K_\psi^+}$, where K_ψ^+ is the maximal totally real subfield of K_ψ. The relative class number formula ([Was97, 4.17]) gives

$$h^-_{K_\psi} = Q \cdot w \cdot \prod_{\chi \text{odd}} \left(-\frac{1}{2}B_{1,\chi}\right) \tag{24}$$

where χ runs over all odd characters of $\mathrm{Gal}(K_\psi/\mathbb{Q})$, w is the number of roots of unity in K_ψ and $Q = 1$ or 2 (see [Was97, 4.12]). By Lemma 3.1, assuming that $\psi^{-1} \not\equiv \omega$, we see that we have the following divisibility of numbers in $\mathbb{Z}_p[\psi]$:

$$p \nmid h^-_{K_\psi} \implies p \nmid B_{1,\psi}. \tag{25}$$

Lemma 3.2. *Suppose $\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mu_{p-1}$ is a Dirichlet character and K is an imaginary quadratic field such that $f(\psi)$ is prime to d_K and $p \nmid d_K$. As long as $\psi \neq 1$ or ω, we have*

$$p \nmid h^-_{K_{\psi_0\varepsilon_K}} \cdot h^-_{K_{\psi_0^{-1}\omega}} \implies p \nmid B_{1,\psi_0\varepsilon_K} \cdot B_{1,\psi_0^{-1}\omega}.$$

Proof. If ψ is even, then $\psi_0\varepsilon_K = \psi\varepsilon_K$ is ramified at some place outside p and so is not equal to ω, and $\psi_0^{-1}\omega = \psi^{-1}\omega$ is not equal to ω if and only if $\psi \neq 1$. Hence $(\psi_0^{-1}\varepsilon_K)^{-1} \pmod p = \psi_0\varepsilon_K \neq \omega$, and $(\psi_0\omega^{-1})^{-1} = \psi^{-1}\omega \neq \omega$ if and only if $\psi \neq 1$. If ψ is odd, then $\psi_0\varepsilon_K = \psi$ is not equal to ω if and only if $\psi \neq \omega$, and $\psi_0^{-1}\omega = \psi^{-1}\varepsilon_K\omega$ is ramified at some place outside p and so is not equal to ω. Hence $(\psi_0^{-1}\varepsilon_K)^{-1} = \psi_0\varepsilon_K \neq \omega$ unless $\psi = \omega$, and $(\psi_0\omega^{-1})^{-1} = \psi^{-1}\varepsilon_K\omega \neq \omega$.

Now the lemma follows from (25). □

Corollary 3.3. *Suppose we are in the setting of Theorem 2.1. Then $p \nmid h^-_{K_{\psi_0\varepsilon_K}} \cdot h^-_{K_{\psi_0^{-1}\omega}}$ implies condition (4) of the theorem.*

Proof. Condition (1) in the statement of Theorem 2.1 in particular implies $\psi \neq 1$ or ω. Now the statement follows from Lemma (3.2). □

4. Goldfeld's conjecture for abelian varieties over $\mathbb{Q}$ of GL_2-type with a rational 3-isogeny

The goal in this section is to prove Theorem 1.5. We will need some Davenport-Heilbronn type class number divisibility results due to Nakagawa–Horie and Taya. For any $x \geq 0$, let $K^+(x)$ denote the set of real quadratic fields k with fundamental discriminant $d_k < x$ and $K^-(x)$ the set of imaginary quadratic fields k with fundamental discriminant $|d_k| < x$. Let m and M be positive integers, and let

$$K^+(x, m, M) := \{k \in K^+(x) : d_k \equiv m \pmod{M}\},$$
$$K^-(x, m, M) := \{k \in K^-(x) : d_k \equiv m \pmod{M}\}.$$

Recall that we let $h_3(d)$ denote the 3-primary part of the class number of $\mathbb{Q}(\sqrt{d})$, and let $\Phi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ denote the Euler totient function. We introduce the following terminology for convenience.

Definition 4.1. We say that positive integers m and M comprise a *valid pair* (m, M) if both of the following properties hold:

(1) if ℓ is an odd prime number dividing (m, M), then ℓ^2 divides M but not m, and
(2) if M is even, then
   (a) $4|M$ and $m \equiv 1 \pmod 4$, or
   (b) $16|M$ and $m \equiv 8$ or $12 \pmod{16}$.

Horie and Nakagawa proved the following.

Theorem 4.2 ([NH88])**.** *We have*

$$|K^+(x, m, M)| \sim |K^-(x, m, M)| \sim \frac{3x}{\pi^2 \Phi(M)} \prod_{\ell | M} \frac{q}{\ell + 1} \quad (x \to \infty).$$

Suppose furthermore that (m, M) is a valid pair. Then

$$\sum_{k \in K^+(x,m,M)} h_3(d_k) \sim \frac{4}{3} |K^+(x, m, M)| \quad (x \to \infty),$$
$$\sum_{k \in K^-(x,m,M)} h_3(d_k) \sim 2|K^-(x, m, M)| \quad (x \to \infty).$$

Here $f(x) \sim g(x) \quad (x \to \infty)$ means that $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$, ℓ ranges over primes dividing M, $q = 4$ if $\ell = 2$, and $q = \ell$ otherwise.

Now put

$$K^+_*(x, m, M) := \{k \in K^+(x, m, M) : h_3(d_k) = 1\},$$
$$K^-_*(x, m, M) := \{k \in K^-(x, m, M) : h_3(d_k) = 1\}.$$

Taya [Tay00] proves the following bound using Theorem 4.2.

Proposition 4.3. *Suppose (m, M) is a valid pair. Then*

$$\lim_{x\to\infty} \frac{|K_*^+(x,m,M)|}{|K^+(x,1,1)|} \geq \frac{5}{6\Phi(M)} \prod_{\ell|M} \frac{q}{\ell+1},$$

$$\lim_{x\to\infty} \frac{|K_*^-(x,m,M)|}{|K^-(x,1,1)|} \geq \frac{1}{2\Phi(M)} \prod_{\ell|M} \frac{q}{\ell+1}.$$

In particular, the of real (resp. imaginary) quadratic fields k such that $d_k \equiv m \pmod M$ and $h_3(d_k) = 1$ has positive density in the set of all real (resp. imaginary) quadratic fields.

Proof. This follows from the trivial bounds $K_*^+(x,m,M) + 3(K^+(x,m,M) - K_*^+(x,m,M)) \leq \sum_{k\in K^+(x,m,M)} h_3(d_k)$ and $K_*^-(x,m,M) + 3(K^-(x,m,M) - K_*^-(x,m,M)) \leq \sum_{k\in K^+(x,m,M)} h_3(d_k)$, and the asymptotic formulas from Theorem 4.2. □

We have the following positive density result.

Theorem 4.4. *Suppose $A/\mathbb{Q}$ is any GL_2-type abelian variety of conductor $N = N_+N_-N_0$ which has a rational 3-isogeny. Let d be the fundamental discriminant corresponding to the quadratic character ψ. Suppose that*

(1) $\psi(3) \neq 1$ and $(\psi^{-1}\omega)(3) \neq 1$;
(2) $\ell \neq 3, \ell | N_{\mathrm{split}}$ implies $\psi(\ell) = -1$;
(3) $\ell \neq 3, \ell | N_{\mathrm{nonsplit}}$ implies $\psi(\ell) = 1$;
(4) $\ell | N_{\mathrm{add}}, \ell \equiv 1 \pmod 3$ implies $\psi(\ell) = -1$ or 0;
(5) $\ell | N_{\mathrm{add}}, \ell \equiv 2 \pmod 3$ implies $\psi(\ell) = 0$.

Let

$$d_0 := \begin{cases} d, & d > 0, \\ -3d, & d < 0, d \not\equiv 0 \pmod 3, \\ -d/3, \pmod M & d < 0, d \equiv 0 \pmod 3, \end{cases} \tag{26}$$

let

$$r(A) := \begin{cases} 1, & 2 \nmid \mathrm{lcm}(N, d^2), \\ 2, & 2 || \mathrm{lcm}(N, d^2), \\ \mathrm{ord}_2(\mathrm{lcm}(N, d^2, 16)) - 1, & 4 | \mathrm{lcm}(N, d^2), \end{cases}$$

and let

$$s_3(d) := \begin{cases} 0, & d > 0, d \not\equiv 0 \pmod 3, \text{ or } d < 0, d \equiv 0 \pmod 3, \\ 1, & d > 0, d \equiv 0 \pmod 3, \text{ or } d < 0, d \not\equiv 0 \pmod 3. \end{cases}$$

Then a proportion of at least

$$\frac{d_0}{2^{r(A)+s_3(d)} \cdot 3} \prod_{\ell | N_{\mathrm{split}} N_{\mathrm{nonsplit}}, \ell \nmid d, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell | N_{\mathrm{add}}, \ell \nmid d, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell | d, \ell \text{ odd}, \ell \neq 3} \frac{1}{2\ell} \prod_{\ell | 3N} \frac{q}{\ell+1} \tag{27}$$

of all imaginary quadratic fields K have the following properties:

(1) d_K is odd,
(2) K satisfies the Heegner hypothesis with respect to $3N$,
(3) $h_3(d_0 d_K) = 1$.

If furthermore, we impose the assumption on A that

(6) $h_3(-3d) = 1$ *if* $\psi(-1) = 1$*, and* $h_3(d) = 1$ *if* $\psi(-1) = -1$

then at least the same proportion (27) of all imaginary quadratic fields K *have:*

(1) d_K *is odd,*
(2) K *satisfies the Heegner hypothesis with respect to* $3N$*, and*
(3) the Heegner point $P \in A(K)$ *is non-torsion.*

Proof. We will apply Proposition 4.3, as well as Theorem 2.1. Let N' denote the prime-to-3 part of N. We first divide into two cases (a) and (b) regarding d, corresponding to

(a) $d > 0$ and $d \not\equiv 0 \pmod 3$, or $d < 0$ and $d \equiv 0 \pmod 3$;
(b) $d > 0$ and $d \equiv 0 \pmod 3$, or $d < 0$ and $d \not\equiv 0 \pmod 3$.

We then define a positive integer M as follows:

(1) In case (a), let

$$M = \begin{cases} 3 \cdot \operatorname{lcm}(N', d^2, 4), & 2 \nmid \operatorname{lcm}(N', d^2), \\ 3 \cdot \operatorname{lcm}(N', d^2, 8), & 2 || \operatorname{lcm}(N', d^2), \\ 3 \cdot \operatorname{lcm}(N', d^2, 16), & 4 | \operatorname{lcm}(N', d^2). \end{cases}$$

(2) In case (b), let

$$M = \begin{cases} 9 \cdot \operatorname{lcm}(N', d^2, 4), & 2 \nmid \operatorname{lcm}(N', d^2), \\ 9 \cdot \operatorname{lcm}(N', d^2, 8), & 2 || \operatorname{lcm}(N', d^2), \\ 9 \cdot \operatorname{lcm}(N', d^2, 16), & 4 | \operatorname{lcm}(N', d^2). \end{cases}$$

Using the Chinese remainder theorem, choose a positive integer m such that

(1) $m \equiv 2 \pmod 3$ in case (a), or $m \equiv 3 \pmod 9$ in case (b),
(2) ℓ odd prime, $\ell \neq 3$, $\ell | N_{\text{split}} \implies \frac{m}{d_0} \equiv$ [quadratic residue unit] $\pmod \ell$, and $2 | N_{\text{split}} \implies \frac{m}{d_0} \equiv 1 \pmod 8$,
(3) ℓ odd prime, $\ell \neq 3$, $\ell | N_{\text{nonsplit}} \implies \frac{m}{d_0} \equiv$ [quadratic residue unit] $\pmod \ell$, and $2 | N_{\text{nonsplit}} \implies \frac{m}{d_0} \equiv 1 \pmod 8$,
(4) ℓ prime, $\ell \equiv 1 \pmod 3$, $\ell | N_{\text{add}}, \ell \nmid d \implies \frac{m}{d_0} \equiv$ [quadratic residue unit] $\pmod \ell$, and $\ell \equiv 1 \pmod 3, \ell | N_{\text{add}} \implies m \equiv \implies \frac{m}{d_0} \equiv$ [quadratic residue unit] $\pmod \ell$,
(5) ℓ prime, ℓ odd, $\ell \equiv 2 \pmod 3$, $\ell | N_{\text{add}}$ (which by our assumptions implies $\ell | d$) $\implies m \equiv 0 \pmod \ell$ where $\frac{m}{d_0} \equiv$ [quadratic residue unit] $\pmod \ell$, and $2 | N_{\text{add}} \implies m \equiv d \pmod{16}$,

and furthermore, if $2 \nmid N$, then suppose $m \equiv d \pmod 4$.

Suppose K is any imaginary quadratic field such that $d_0 d_K \equiv m \pmod M$. Then the congruence conditions corresponding to (1)-(5) above, along with assumptions (1)-(5) in the statement of the theorem, imply

(1) 3 splits in K,
(2) $\ell \neq 3, \ell | N_{\text{split}} \implies \ell$ splits in K,
(3) $\ell \neq 3, \ell | N_{\text{nonsplit}} \implies \ell$ splits in K,
(4) ℓ prime, $\ell \equiv 1 \pmod 3, \ell | N_{\text{add}} \implies \ell$ splits in K,
(5) ℓ prime, $\ell \equiv 2 \pmod 3, \ell | N_{\text{add}} \implies \ell$ splits in K,

and $d_K \equiv 1 \pmod 4$ (i.e. d_K is odd). Hence K satisfies the Heegner hypothesis with respect to $3N$.

Moreover, the congruence conditions above imply that (m, M) is a valid pair (see Definition 4.1), and the assumptions (4)-(5) in the statement of the theorem imply that (jd, d^2) is also a valid pair

whenever $(j,d)=1$. Thus, by Proposition 4.3, for any $d_0|M$,

$$\lim_{x\to\infty}\frac{|K_*^-(x,m,M)|}{|K^-(x/d_0,1,1)|}\geq\frac{d_0}{2\Phi(M)}\prod_{\ell|M}\frac{q}{\ell+1}. \tag{28}$$

The left-hand side of (28) is the proportion of imaginary quadratic K satisfying $d_0d_K\equiv m \pmod M$ and $h_3(d_0d_K)=1$. Moreover, notice that there are

$$\prod_{\ell|N_{\rm split}N_{\rm nonsplit},\ell\nmid d,\ell\text{ odd},\ell\neq 3}\frac{\ell-1}{2}\prod_{\ell|N_{\rm add},\ell\nmid d,\ell\text{ odd},\ell\neq 3}\frac{\ell(\ell-1)}{2}\prod_{\ell|d,\ell\text{ odd},\ell\neq 3}\frac{\ell-1}{2}$$

choices for residue classes of m mod M. Combining all the above and summing over each valid residue class m mod M, we immediately obtain our lower bound (33) for the proportion of imaginary quadratic fields K such that (1) d_K is odd, (2) K satisfies the Heegner hypothesis with respect to $3N$, and (3) $h_3(d_0d_K)=1$. This proves the part of the theorem before assumption (6) is introduced in the statement.

If we assume that A satisfies assumption (6) in the statement of the theorem, then for all K as above, we see that A, $p=3$ and K satisfy all the assumptions of Theorem 2.1 (see Remarks 2.4 and 2.5), thus implying that P is non-torsion. The final part of the theorem now follows.

□

Similarly, we have the following positive density result for producing A which satisfy the assumptions of Theorem 4.4.

Theorem 4.5. *Suppose (N_1,N_2,N_3) is a triple of pairwise coprime integers such that N_1N_2 is square-free, N_3 is square-full and $N_1N_2N_3=N$. Let*

$$r:=\begin{cases}0, & 2\nmid N,\\ 2, & 2|N.\end{cases}$$

Then a proportion of at least

$$\frac{1}{2^r\cdot 3}\prod_{\ell|N_1N_2,\ell\text{ odd},\ell\neq 3}\frac{1}{2}\prod_{\ell|N_3,\ell\text{ odd},\ell\neq 3}\frac{1}{\ell}\prod_{\ell|N,\ell\neq 3}\frac{q}{\ell+1}$$

of even (resp. odd) quadratic characters ψ corresponding to real (resp. imaginary) quadratic fields $\mathbb{Q}(\sqrt{d})$, where the $d>0$ (resp. $d<0$) are fundamental discriminants, satisfy

(1) $\psi(3)\neq 1$ and $(\psi^{-1}\omega)(3)\neq 1$;
(2) $\ell\neq 3,\ell|N_1$ implies $\psi(\ell)=-1$;
(3) $\ell\neq 3,\ell|N_2$ implies $\psi(\ell)=1$;
(4) $\ell\neq 3,\ell|N_3,\ell\equiv 1 \pmod 3$ implies $\psi(\ell)=0$;
(5) $\ell\neq 3,\ell|N_3,\ell\equiv 2 \pmod 3$ implies $\psi(\ell)=0$;
(6) $h_3(-3d)=1$ (resp. $h_3(d)=1$).

Moreover, we have that for any $i\in\{2,3,5,8\}$,

- *1/4 of the above fundamental discriminants $d>0$ (resp. $d<0$) satisfy $d\equiv i \pmod 9$.*

Proof. We will apply Proposition 4.3. Using the Chinese remainder theorem, choose a positive integer m which satisfies the following congruence conditions:

(1) $m\equiv 3 \pmod 9$ or $m\equiv 2 \pmod 3$,

(2) ℓ odd prime, $\ell \neq 3$, $\ell | N_1 \implies m \equiv -3$[quadratic non-residue] (mod ℓ), and $2|N_1 \implies m \equiv 1$ (mod 8),
(3) ℓ odd prime, $\ell \neq 3$, $\ell | N_2 \implies m \equiv -3$[quadratic residue unit] (mod ℓ), and $2|N_2 \implies m \equiv 5$ (mod 8),
(4) ℓ odd prime, $\ell \neq 3$, $\ell | N_3, \ell \equiv 1 \pmod 3 \implies m \equiv 0 \pmod \ell$ and $m \not\equiv 0 \pmod{\ell^2}$,
(5) ℓ odd prime, $\ell \neq 3$, $\ell | N_3, \ell \equiv 2 \pmod 3 \implies m \equiv 0 \pmod \ell$ and $m \not\equiv 0 \pmod{\ell^2}$, and $2|N_3 \implies m \equiv 8$ or $12 \pmod{16}$.

Let N' denote the prime-to-3 part of N. Given such an m, let a positive integer M be defined as follows:

- If $m \equiv 3 \pmod 9$, let
$$M = \begin{cases} 9N', & 2 \nmid N, \\ 9 \cdot \operatorname{lcm}(N', 8), & 2 || N, \\ 9 \cdot \operatorname{lcm}(N', 16), & 4 | N. \end{cases}$$
- If $m \equiv 2 \pmod 3$, let
$$M = \begin{cases} 3N', & 2 \nmid N, \\ 3 \cdot \operatorname{lcm}(N', 8), & 2 || N, \\ 3 \cdot \operatorname{lcm}(N', 16), & 4 | N. \end{cases}$$

If $m \equiv 2 \pmod 3$, suppose d is a fundamental discriminant with

- $d > 0, d \equiv 0 \pmod 3$, and $-d/3 \equiv m \pmod M$, or
- $d < 0, d \not\equiv 0 \pmod 3$, and $d \equiv m \pmod M$.

If $m \equiv 3 \pmod 9$, suppose d is a fundamental discriminant with

- $d > 0, d \not\equiv 0 \pmod 3$, and $-3d \equiv m \pmod M$, or
- $d < 0, d \equiv 0 \pmod 3$, and $d \equiv m \pmod M$.

Let ψ be the quadratic character associated with d. Then the congruence conditions on m corresponding to (1)-(5) above imply

(1) $\psi(3) \neq 1$ and $(\psi^{-1}\omega)(3) \neq 1$;
(2) $\ell \neq 3$ prime, $\ell | N_1 \implies \psi(\ell) = -1$;
(3) $\ell \neq 3$ prime, $\ell | N_2 \implies \psi(\ell) = 1$;
(4) $\ell \neq 3$ prime, $\ell | N_3, \ell \equiv 1 \pmod 3 \implies \psi(\ell) = 0$;
(5) $\ell \neq 3$ prime, $\ell | N_3, \ell \equiv 2 \pmod 3 \implies \psi(\ell) = 0$.

Thus ψ satisfies the desired congruence conditions (1)-(5) in the statement of the theorem. Now we address (6). The congruence conditions (1)-(5) above imply that (m, M) is a valid pair. Thus, by Proposition 4.3, if $m \equiv 2 \pmod 3$ with corresponding M as defined above, then

$$\lim_{x \to \infty} \frac{|K_*^-(x, m, M)|}{|K^+(3x, 3, 9)| + |K^+(3x, 6, 9)|} \geq \frac{1}{6\Phi(M)} \prod_{\ell | M, \ell \neq 3} \frac{q}{\ell + 1} \tag{29}$$

where the left-hand side of (29) is the proportion of $d > 0$ which satisfy $d \equiv 0 \pmod 3$ and $-d/3 \equiv m \pmod M$ and $h_3(-3d) = h_3(-d/3) = 1$, and

$$\lim_{x \to \infty} \frac{|K_*^-(x, m, M)|}{|K^-(x, 1, 3)| + |K^-(x, 2, 3)|} \geq \frac{1}{2\Phi(M)} \prod_{\ell | M, \ell \neq 3} \frac{q}{\ell + 1} \tag{30}$$

where the left-hand side of (30) is the proportion of $d < 0$ which satisfy $d \not\equiv 0 \pmod 3$, $d \equiv m \pmod M$ and $h_3(d) = 1$. Similarly by Proposition 4.3, if $m \equiv 3 \pmod 9$ with corresponding M as defined above, then

$$\lim_{x\to\infty} \frac{|K_*^-(x,m,M)|}{|K^+(x/3,1,3)| + |K^+(x/3,2,3)|} \geq \frac{3}{2\Phi(M)} \prod_{\ell|M,\ell\neq 3} \frac{q}{\ell+1} \tag{31}$$

where the left-hand side of (31) is the proportion of $d > 0$ which satisfy $d \not\equiv 0 \pmod 3$, $-3d \equiv m \pmod M$ and $h_3(-3d) = 1$, and

$$\lim_{x\to\infty} \frac{|K_*^-(x,m,M)|}{|K^-(x,1,3)| + |K^-(x,2,3)|} \geq \frac{1}{2\Phi(M)} \prod_{\ell|M,\ell\neq 3} \frac{q}{\ell+1} \tag{32}$$

where the left-hand side of (32) is the proportion of $d < 0$ which satisfy $d \equiv 0 \pmod 3$, $d \equiv m \pmod M$ and $h_3(d) = 1$.

Moreover, in each case, we have

$$\prod_{\ell|N_1,\ell \text{ odd},\ell\neq 3} \frac{\ell-1}{2} \prod_{\ell|N_2,\ell \text{ odd},\ell\neq 3} \frac{\ell-1}{2} \cdot \prod_{\ell|N_3,\ell \text{ odd},\ell\equiv 1 \pmod 3} (\ell-1) \prod_{\ell|N_3,\ell \text{ odd},\ell\equiv 2 \pmod 3} (\ell-1) \prod_{\text{if } 2|N_3} 2$$

choices of residue classes $m \bmod M$ which satisfy congruence conditions (1)-(5). Combining all the above and summing over each these residue class $m \bmod M$, we immediately obtain our lower bounds for the proportions of desired $d > 0$ from (30) and desired $d < 0$ from (31).

The final part of the theorem follows by directly counting the number of residue classes $m \bmod M$ which force $d \equiv i \pmod 9$ for $i \in \{2,3,5,8\}$. □

Remark 4.6. Let λ be the prime above $p = 3$ fixed in the beginning of §2.2. Suppose for A as above, $A[\lambda]^{\mathrm{ss}} \cong \mathbb{F}_\lambda \oplus \mathbb{F}_\lambda(\omega)$. For a fundamental discriminant d, let $A^{(d)}$ denote the quadratic twist of A by d. Note that for each d produced by Theorem 4.5, Theorem 4.4 shows that there is a positive proportion of imaginary quadratic K satisfying the Heegner hypothesis with respect to Nd^2 such that the corresponding Heegner point $P \in A^{(d)}(K)$ is non-torsion. In particular, for each such d there is *at least one* K such that $P \in A^{(d)}(K)$ is non-torsion. Thus $r_{\mathrm{an}}(A^{(d)}) = \dim A \cdot \frac{1-w(A^{(d)})}{2}$.

Theorem 4.7. *The weak Goldfeld Conjecture is true for any abelian variety $A/\mathbb{Q}$ of GL_2-type with a rational 3-isogeny. Namely, there is a positive proportion of quadratic twists of $A/\mathbb{Q}$ of analytic rank 0 (resp. analytic rank equal to $\dim A$).*

Proof. Suppose A has a 3-isogeny defined over $\mathbb{Q}$ and that (without loss of generality) A satisfies our assumptions stated before Theorem 2.1, i.e. $A[\lambda]^{\mathrm{ss}} \cong \mathbb{F}_\lambda(\psi) \oplus \mathbb{F}_\lambda(\psi^{-1}\omega)$ for some quadratic character $\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mu_2$. Twisting by the quadratic character ψ^{-1}, we may assume without loss of generality that $A[\lambda]^{\mathrm{ss}} \cong \mathbb{F}_\lambda \oplus \mathbb{F}_\lambda(\omega)$.

Let d be a fundamental discriminant corresponding to a quadratic character ψ in the family of d produced by Theorem 4.5 (with the integers $N_1 = N_+, N_2 = N_-$ and $N_3 = N_0$ as in our setting). In particular, $A^{(d)}[\lambda]^{\mathrm{ss}} \cong \mathbb{F}_\lambda(\psi) \oplus \mathbb{F}_\lambda(\psi^{-1}\omega)$ satisfies the assumptions of Theorem 4.4, including assumption (6). Hence, we can apply Theorem 4.4 to $A^{(d)}$ to conclude that a positive proportion of imaginary quadratic fields K satisfy the Heegner hypothesis with respect to $3Nd^2$ and have that

the associated Heegner point $P \in A^{(d)}(K)$ is non-torsion. Since $w(A^{(d)})w(A^{(dd_K)}) = w(A/K) = -1$ (the last equality following from the Heegner hypothesis), we have that each such K satisfies

$$r_{\mathrm{an}}(A^{(dd_K)}) = \dim A \cdot \frac{1 + w(A^{(d)})}{2}.$$

Hence there are a positive proportion of quadratic twists of A with rank $\dim A \cdot \frac{1+w(A^{(d)})}{2}$, and in fact by Theorem 4.4, a lower bound for this proportion is given by

$$\frac{d_0}{2^{r(A^{(d)})+s_3(d)} \cdot 3} \prod_{\substack{\ell | N_{\mathrm{split}} N_{\mathrm{nonsplit}}, \\ \ell \nmid d, \ell \text{ odd}, \ell \neq 3}} \frac{1}{2} \prod_{\substack{\ell | N_{\mathrm{add}} d^2, \\ \ell \nmid d, \ell \text{ odd}, \ell \neq 3}} \frac{1}{2} \prod_{\ell | d, \text{ odd}, \ell \neq 3} \frac{1}{2\ell} \prod_{\ell | 3Nd^2} \frac{q}{\ell + 1} \tag{33}$$

in the notation of the statement of the theorem.

Now choose any K as produced by Theorem 4.4 for $A^{(d)}$, so that $w(A^{(dd_K)}) = -w(A^{(d)})$. In particular, d_K is odd and prime to $3Nd$. Then by construction $h_3(dd_K) = 1$ if $d > 0$ and $h_3(-3dd_K) = 1$ if $d < 0$, and so $A^{(dd_K)}[\lambda]^{\mathrm{ss}} \cong \mathbb{F}_\lambda(\psi\varepsilon_K) \oplus \mathbb{F}_\lambda((\psi\varepsilon_K)^{-1}\omega)$ satisfies all of the assumptions (including (6)) of Theorem 4.4. Hence, we can apply Theorem 4.4 to $A^{(dd_K)}$ to conclude that a positive proportion of imaginary quadratic fields K' satisfy the Heegner hypothesis with respect to $3Nd^2d_K^2$ and have that the associated Heegner point $P \in A^{(dd_K)}(K')$ is non-torsion. Since $w(A^{(dd_K)})w(A^{(dd_Kd_{K'})}) = w(A^{(dd_K)}/K') = -1$, we have that each such K' satisfies

$$r_{\mathrm{an}}(A^{(dd_Kd_{K'})}) = \dim A \cdot \frac{1 + w(A^{(dd_K)})}{2} = \dim A \cdot \frac{1 - w(A^{(d)})}{2}. \tag{34}$$

Hence there are a positive proportion of quadratic twists of A with rank $\dim A \cdot \frac{1-w(A^{(d)})}{2}$, and in fact by Theorem 4.4, a lower bound for this proportion is given by

$$\frac{(dd_K)_0}{2^{r(A^{(dd_K)})+s_3(dd_K)} \cdot 3} \prod_{\substack{\ell | N_{\mathrm{split}} N_{\mathrm{nonsplit}}, \\ \ell \nmid dd_K, \ell \text{ odd}, \ell \neq 3}} \frac{1}{2} \prod_{\substack{\ell | N_{\mathrm{add}} (dd_K)^2, \\ \ell \nmid dd_K, \ell \text{ odd}, \ell \neq 3}} \frac{1}{2} \prod_{\ell | dd_K, \text{ odd}, \ell \neq 3} \frac{1}{2\ell} \prod_{\ell | 3N(dd_K)^2} \frac{q}{\ell + 1}$$

in the notation of the statement of the theorem. (Note that in fact $r(A^{(dd_K)}) = r(A^{(d)})$ since d_K is odd.) □

Suppose now $A = E$ is an elliptic curve over $\mathbb{Q}$, and so $\lambda = 3$. When E is semistable, we have $E[3]^{\mathrm{ss}} \cong \mathbb{F}_3 \oplus \mathbb{F}_3(\omega)$ for the following reason: Suppose $E[3]^{\mathrm{ss}} \cong \mathbb{F}_3(\psi) \oplus \mathbb{F}_3(\psi^{-1}\omega)$ for some quadratic character ψ. Then ψ cannot be ramified at any $\ell || N$ since the corresponding admissible $\mathrm{GL}_2(\mathbb{Q}_\ell)$ representation is Steinberg of conductor ℓ, but if ψ was ramified at ℓ it would force the conductor to be divisible by ℓ^2 by the above description of $E[3]^{\mathrm{ss}}$. Hence ψ is a quadratic character only possibly ramified at 3 and hence must be either 1 or ω.

Now we can use Theorem 4.5 to compute explicit lower bounds on the proportion of rank 0 and rank 1 quadratic twists.

Proposition 4.8. *Let $E/\mathbb{Q}$ be semistable and suppose that E has a rational 3-isogeny.*

If $3 \nmid N$, then in the notation of Theorem 4.5 (with $N_1 = N_{\mathrm{split}}, N_2 = N_{\mathrm{nonsplit}}$, and $N_3 = N_{\mathrm{add}} = 1$, at least

$$\frac{1}{2^r \cdot 3} \prod_{\ell | N, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell | N, \ell \neq 3} \frac{q}{\ell + 1} \tag{35}$$

of $d > 0$ (resp. $d < 0$) have $r_{\mathrm{an}}(E^{(d)}) = 1$ (resp. $r_{\mathrm{an}}(E^{(d)}) = 0$).

If $3|N$, then:

(1) If 3 is of split multiplicative reduction, then at least

$$\frac{1}{2^r \cdot 3} \prod_{\ell|N,\ell \text{ odd},\ell\neq 3} \frac{1}{2} \prod_{\ell|N,\ell\neq 3} \frac{q}{\ell+1} \tag{36}$$

of $d > 0$ (resp. $d < 0$) have $r_{\mathrm{an}}(E^{(d)}) = 1$ (resp. $r_{\mathrm{an}}(E^{(d)}) = 0$).

(2) If 3 is of nonsplit multiplicative reduction, then at least

$$\frac{1}{2^{r+2} \cdot 3} \prod_{\ell|N,\ell \text{ odd},\ell\neq 3} \frac{1}{2} \prod_{\ell|N,\ell\neq 3} \frac{q}{\ell+1} \tag{37}$$

of $d > 0$ (resp. $d < 0$) have $r_{\mathrm{an}}(E^{(d)}) = 0$ (resp. $r_{\mathrm{an}}(E^{(d)}) = 1$), and at least

$$\frac{1}{2^{r+2}} \prod_{\ell|N,\ell \text{ odd},\ell\neq 3} \frac{1}{2} \prod_{\ell|N,\ell\neq 3} \frac{q}{\ell+1} \tag{38}$$

of $d > 0$ (resp. $d < 0$) have $r_{\mathrm{an}}(E^{(d)}) = 1$ (resp. $r_{\mathrm{an}}(E^{(d)}) = 0$).

Proof. First we apply Theorem 4.5 to $N_1 = N_{\mathrm{split}}, N_2 = N_{\mathrm{nonsplit}}$, and $N_3 = N_{\mathrm{add}} = 1$. For any d produced by the theorem, Remark 4.6 implies that

$$r_{\mathrm{an}}(E^{(d)}) = \frac{1 - w(E^{(d)})}{2}. \tag{39}$$

Let d be any fundamental discriminant produced by Theorem 4.5. By the properties of the d produced in Theorem 4.5, the corresponding local characters ψ_ℓ for satisfy the implications

$$\ell|N, \ell \nmid d \implies \ell||N \implies \psi_\ell(\ell)w_\ell(E) = -\psi_\ell(\ell)a_\ell(E) = -\psi(\ell)a_\ell(E) = 1 \tag{40}$$

(where the last chain of equalities follows since for $\ell||N$, $w_\ell(E) = -a_\ell(E)$), and furthermore since $N = N_{\mathrm{split}}N_{\mathrm{nonsplit}}$ (since we assume that E is semistable),

$$\ell|(N, d) \implies \ell = 3. \tag{41}$$

We now calculate $w(E^{(d)})$ using (40) and (41). Since E is semistable, the global root number $w(E^{(d)})$ is computed via changes to local root numbers $w_\ell(E)$ under the quadratic twist by d as follows (see [Bal14, Table 1]):

(1) if $\ell \nmid Nd$, then $w_\ell(E^{(d)}) = w_\ell(E) = 1$;
(2) if $\ell|N, \ell \nmid d$, then $w_\ell(E^{(d)}) = \psi_\ell(\ell)w_\ell(E) = 1$;
(3) if $\ell \nmid N, \ell|d$ then $w_\ell(E^{(d)}) = \psi_\ell(-1)w_\ell(E) = \psi_\ell(-1)$;
(4) if $\ell|(N, d)$, then $\ell = 3$ and $w_3(E^{(d)}) = -\psi_3(-1)w_3(E)$;
(5) $w_\infty(E^{(d)}) = w_\infty(E) = -1$.

Hence

$$w(E^{(d)}) = -\psi(-1) \left(\prod_{\text{if } 3|(N,d)} -w_3(E) \right). \tag{42}$$

If $3 \nmid N$, then we have $3 \nmid (N, d)$, and so $w(E^{(d)}) = -\psi(-1)$. Thus, by (39) and the lower bound given in the statement of Theorem 4.5, in the notation of the theorem we have that at least

$$\frac{1}{2^r \cdot 3} \prod_{\ell|N,\ell \text{ odd},\ell\neq 3} \frac{1}{2} \prod_{\ell|N,\ell\neq 3} \frac{q}{\ell+1} \tag{43}$$

of $d>0$ have $r_{\mathrm{an}}(E^{(d)})=1$, and at least the same proportion of $d<0$ have $r_{\mathrm{an}}(E^{(d)})=0$.

If $3|N$, then

$$w(E^{(d)})=\begin{cases}-\psi(-1), & 3\nmid d,\\ -\psi(-1), & 3|d, 3 \text{ is of split multiplicative reduction (i.e. } w_3(E)=-1),\\ \psi(-1), & 3|d, 3 \text{ is of nonsplit multiplicative reduction (i.e. } w_3(E)=1).\end{cases}$$

The desired bounds in this case follow again from (39), the lower bound given in the statement of Theorem 4.5 and the final part of that theorem. □

Remark 4.9. It is most likely possible to refine the casework in the proofs of Theorems 4.5 and 4.4 in order to achieve better lower bounds of twists with ranks 0 or 1.

Example 4.10. Consider the elliptic curve

$$E=19a1: y^2+y=x^3+x^2-9x-15$$

in Cremona's labeling. Then $E(\mathbb{Q})\cong\mathbb{Z}/3\mathbb{Z}$, so we take $p=3$ and obtain $E[3]^{\mathrm{ss}}=\mathbb{F}_3\oplus\mathbb{F}_3(\omega)$. Notice that $N=N_{\mathrm{split}}=19$ and the root number $w(E)=+1$. Consider the set of fundamental discriminant $d>0$ (resp. $d<0$) such that

(1) $\psi_d(3)\neq 1$ and $(\psi_d\omega)(3)\neq 1$.
(2) $\psi_d(19)=-1$.
(3) $h_3(-3d)=1$ (resp. $h_3(d)=1$).

The first few such $d>0$ are

$$d=8,12,21,41,53,56,65,84,89,129,164,165,185,189,\cdots$$

and the first few such $d<0$ are

$$d=-4,-7,-24,-28,-43,-55,-63,-115,-123,-159,-163,-168,-172,-175,-187,-195,\cdots$$

Notice that the root number $w(E^{(d)})=\psi_d(-19)=-1$ (resp. $+1$), we know from Theorem 4.4 that

$$r_{\mathrm{an}}(E^{(d)})=\begin{cases}0, & d<0,\\ 1, & d>0.\end{cases}$$

The explicit lower bounds in Proposition 4.8 show that at least $\frac{19}{120}=15.833\%$ of real quadratic twists of E have rank 1, and at least $\frac{19}{120}=15.833\%$ of imaginary quadratic twists of E have rank 0 (compare the lower bound $\frac{19}{240}=7.917\%$ in [Jam98, p. 640]).

5. The sextic twists family

5.1. **The curves E_d.** In this section we consider the elliptic curve of j-invariant 0,

$$E=27a1=X_0(27): y^2=x^3-432.$$

We remind the reader that E has CM by the ring of integers $\mathbb{Z}[\zeta_3]$ of $\mathbb{Q}(\sqrt{-3})$ and is isomorphic to the Fermat cubic curve $X^3+Y^3=1$ via the transformation

$$X=\frac{36-y}{6x},\quad Y=\frac{36+y}{6x}.$$

Definition 5.1. For $d \in \mathbb{Z}$, we denote E_d the d-th sextic twist of E,

$$E_d : y^2 = x^3 - 432d.$$

Notice that the d-th quadratic twist $E^{(d)}$ of E is given by

$$E_{d^3} = E^{(d)} : y^2 = x^3 - 432d^3,$$

and the d-th cubic twist of E is given by

$$E_{d^2} : y^2 = x^3 - 432d^2.$$

Remark 5.2. The cubic twist E_{d^2} is isomorphic to the curve $X^3 + Y^3 = d$ and its rational points provide solutions to the classical *sum of two cubes* problem. These equations have a long history, see [ZK87, §1] or [Wat07, §1] for an overview.

Lemma 5.3. *We have an isomorphism of $G_{\mathbb{Q}}$-representations*

$$E_d[3]^{\mathrm{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega).$$

Here $\psi_d : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathbb{F}_3) = \{\pm 1\}$ is the quadratic character associated to the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ and $\omega = \psi_{-3} : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathbb{F}_3) = \{\pm 1\}$.

Proof. Notice that under cubic twisting the associated modular forms are congruent mod $(\zeta_3 - 1)$. Since the Hecke eigenvalues are integers, we know that the associated modular forms are indeed congruent mod 3. Hence cubic twisting does not change the semi-simplification of the mod 3 Galois representations. Notice that $E_d \cong E_{d^7}$ is the d^4-th sextic twist of the curve E_{d^3}, which is the same as the d^2-cubic twist of the quadratic twist $E^{(d)}$. Since $E(\mathbb{Q})[3] \cong \mathbb{Z}/3\mathbb{Z}$, we have an exact sequence of $G_{\mathbb{Q}}$-modules,

$$0 \to \mathbb{F}_3 \to E[3] \to \mathbb{F}_3(\omega) \to 0.$$

Hence we have an exact sequence of $G_{\mathbb{Q}}$-modules

$$0 \to \mathbb{F}_3(\psi_d) \to E^{(d)}[3] \to \mathbb{F}_3(\psi_d\omega) \to 0.$$

The result then follows. □

Lemma 5.4. *Assume that:*

(1) d is a fundamental discriminant.

(2) $d \equiv 0 \pmod 3$.

Then the root number of E_d is given by

$$w(E_d) = \begin{cases} -\operatorname{sign}(d), & d \equiv 3 \pmod 9, \\ \operatorname{sign}(d), & d \equiv 6 \pmod 9. \end{cases}$$

Proof. We use the closed formula for the local root numbers $w_\ell(E_d)$ in [Liv95, §9].

(1) Since d is a fundamental discriminant, we have either $d \equiv 1 \pmod 4$, or $d = 4d'$ for some $d' \equiv 3 \pmod 4$, or $d = 8d'$ for some $d' \equiv 1 \pmod 4$. In the first case we have $-432d = 2^4 \cdot (-27d)$, with $2 \nmid (-27d)$. In the second case we have $-432d = 2^6 \cdot (-27d')$, and in the third case we have $-432d = 2^7 \cdot (-27d')$, with $2 \nmid (-27d')$. The local root number formula gives

$$w_2(E_d) = \begin{cases} +1, & 2 \nmid d \text{ or } 4 \| d, \\ -1, & 8 \| d. \end{cases} \tag{44}$$

(2) Let $d = 3d'$. Then $-432d = 3^4 \cdot (-16d')$, with $3 \nmid -16d'$. Since the exponent of 3 is 4, which is $\equiv 1 \pmod 3$, we know that $w_3(E_d) = +1$.

(3) Notice that if $2 \nmid d$ or $4||d$, then the number of prime factors $\ell|d$ such that $\ell \geq 5$ and $\ell \equiv 2 \pmod 3$ is odd if and only if $|d'| \equiv 2 \pmod 3$. Similarly, if $8||d$, then the number of prime factors $\ell|d$ such that $\ell \geq 5$ and $\ell \equiv 2 \pmod 3$ is odd if and only if $|d'| \equiv 1 \pmod 3$. It follows that if $d' \equiv 1 \pmod 3$, then

$$\prod_{\ell \geq 5} w_\ell(E_d) = \begin{cases} \operatorname{sign}(d), & 2 \nmid d \text{ or } 4||d, \\ -\operatorname{sign}(d), & 8||d. \end{cases}$$

If $d' \equiv 2 \pmod 3$, then the product of the local root numbers

$$\prod_{\ell \geq 5} w_\ell(E_d) = \begin{cases} -\operatorname{sign}(d), & 2 \nmid d \text{ or } 4||d, \\ \operatorname{sign}(d), & 8||d. \end{cases} \tag{45}$$

Now the result follows from the product formula $w(E_d) = -w_2(E_d)w_3(E_d)\prod_{\ell \geq 5} w_\ell(E_d)$. □

Lemma 5.5. *Assume that:*

(1) d is a fundamental discriminant.

(2) $d \equiv 2 \pmod 3$.

Then the root number of E_d is given by

$$w(E_d) = \begin{cases} \operatorname{sign}(d), & d \equiv 2 \pmod 9, \\ -\operatorname{sign}(d), & d \equiv 5, 8 \pmod 9. \end{cases}$$

Proof. The proof is similar to Lemma 5.4 using [Liv95, §9].

(1) Since d is a fundamental discriminant, we again have the formula (44).

(2) Notice that $-432d = 3^3 \cdot (-16d)$. Its prime-to-3 part $-16d$ satisfies $-16d \equiv \pm 2, 1 \pmod 9$ if and only if $d \equiv \pm 1, 5 \pmod 9$. It follows that the local root number

$$w_3(E_d) = \begin{cases} +1, & d \equiv 2 \pmod 9, \\ -1, & d \equiv 5, 8 \pmod 9. \end{cases}$$

(3) Since $d \equiv 2 \pmod 3$, we again have the formula (45).

Now the result again follows from the product formula. □

5.2. **Weak Goldfeld conjecture for $\{E_d\}$.** Since E_d is CM, we know that its conductor $N(E_d) = N_{\mathrm{add}}(E_d)$. When d is a fundamental discriminant, the curve E_d has additive reduction exactly at the prime factors of $3d$.

Theorem 5.6. *Let $K = \mathbb{Q}(\sqrt{d_K})$ be an imaginary quadratic field satisfying the Heegner hypothesis with respect to $3d$. Let $P_d \in E_d(K)$ be the associated Heegner point. Assume that:*

(1) d is a fundamental discriminant.

(2) $d \equiv 2 \pmod 3$ or $d \equiv 3 \pmod 9$.

(3) If $d > 0$, then $h_3(-3d) = h_3(d_K d) = 1$. If $d < 0$, then $h_3(d) = h_3(-3d_K d) = 1$.

Then

$$\log_{\omega_{E_d}} P_d \not\equiv 0 \pmod 3. \tag{46}$$

In particular, P_d is of infinite order and E_d/K has both analytic and algebraic rank one.

Proof. It follows by applying Theorem 2.1 for $p = 3$ and noticing that $|\tilde{E}_d^{\mathrm{ns}}(\mathbb{F}_3)| = 3$ since E_d has additive reduction at 3. It remains to check that all the assumptions of Theorem 2.1 are satisfied. By Lemma 5.3, we have $E[3]$ is reducible with $\psi = \psi_d$. The condition that $\psi(3) \neq 1$ and $(\psi^{-1}\omega)(3) \neq 1$ is equivalent to that $d \equiv 2 \pmod 3$ or $d \equiv 3 \pmod 9$. For $\ell \neq 3$ and $\ell | N_{\mathrm{add}}(E_d)$, we have $\ell | d$, so $\psi_d(\ell) = 0$. Finally, the requirement on the trivial 3-class numbers is exactly the assumption that $3 \nmid B_{1,\psi_0^{-1}\varepsilon_K} B_{1,\psi_0\omega^{-1}}$ by noticing that

$$(\psi_d)_0 = \begin{cases} \psi_d, & d > 0, \\ \psi_{d_K d}, & d < 0, \end{cases}$$

and using the formula for the Bernoulli numbers (23) (see also Corollary 3.3). □

Corollary 5.7. *Assume we are in the situation of Theorem 5.6.*
(1) If $d > 0$ and $d \equiv 2 \pmod 9$, or $d < 0$ and $d \equiv 3, 5, 8 \pmod 9$, then

$$r_{\mathrm{an}}(E_d/\mathbb{Q}) = 0, \quad r_{\mathrm{an}}(E_d^{(d_K)}/\mathbb{Q}) = 1.$$

(2) If $d < 0$ and $d \equiv 2 \pmod 9$, or $d > 0$ and $d \equiv 3, 5, 8 \pmod 9$, then

$$r_{\mathrm{an}}(E_d/\mathbb{Q}) = 1, \quad r_{\mathrm{an}}(E_d^{(d_K)}/\mathbb{Q}) = 0.$$

Proof. It follows immediately from Theorem 5.6 using the root number calculation in Lemmas 5.4 and 5.5. □

Corollary 5.8. *The weak Goldfeld's conjecture holds for the sextic twists family $\{E_d\}$. In fact, E_d has analytic rank 0 (resp. 1) for at least 1/6 of fundamental discriminants d.*

Proof. By Theorem 4.5, at least $1/3$ of all (positive or negative) fundamental discriminants d satisfy the assumptions of Theorem 5.6, and by Remark 4.6, for each of these d there is at least one imaginary quadratic field K satisfying the Heegner hypothesis with respect to $3d$ and such that $h_3(d_K d) = 1$ if $d > 0$ and $h_3(-3d_K d) = 1$ if $d < 0$. Thus d and K satisfy all of the assumptions of Theorem 5.6. The final part of Theorem 4.5 implies that $1/4$ of the fundamental discriminants d considered above (which in turn comprise $1/3$ of all fundamental discriminants) satisfy $d \equiv i \pmod 9$, for each $i \in \{2, 3, 5, 8\}$. Moreover $1/2$ of these d give $r_{\mathrm{an}}(E_d) = 0$ (resp. 1) by Corollary 5.7. The desired density $1/6$ then follows. □

Remark 5.9. One can also obtain $r_{\mathrm{an}}(E_d) \in \{0, 1\}$ for many d's which are not fundamental discriminants. From the proof of Theorem 5.6 one sees that the fundamental discriminant assumption can be relaxed by allowing the exponent of prime factors of d to be 3 or 5 (all we use is that $\mathbb{Q}(\sqrt{d})$ is ramified exactly at the prime factors of d). We assume d is a fundamental discriminant only to simplify the root number computation in Lemmas 5.4 and 5.5.

5.3. **The 3-part of the BSD conjecture over K.** The goal of this subsection is to prove the following theorem.

Theorem 5.10. *Assume we are in the situation of Theorem 5.6. Assume the Manin constant of E_d is coprime to 3. Then BSD(3) is true for E_d/K.*

By the Gross–Zagier formula, the BSD conjecture for E_d/K is equivalent to the equality ([GZ86, V.2.2])

$$u_K \cdot c_{E_d} \cdot \prod_{\ell | N(E_d)} c_\ell(E_d) \cdot |Ш(E_d/K)|^{1/2} = [E_d(K) : \mathbb{Z}P_d], \tag{47}$$

where $u_K = |\mathcal{O}_K^\times/\{\pm 1\}|$, c_{E_d} is the Manin constant of $E_d/\mathbb{Q}$, $c_\ell(E_d) = [E_d(\mathbb{Q}_\ell) : E_d^0(\mathbb{Q}_\ell)]$ is the local Tamagawa number of E_d and $[E_d(K) : \mathbb{Z}P_d]$ is the index of the Heegner point $P_d \in E_d(K)$.

From now on assume we are in the situation of Theorem 5.6. Since 3 splits in K, we know $K \neq \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, so $u_K = 1$. Therefore the BSD conjecture for E_d/K is equivalent to the equality

$$\prod_{\ell | N(E_d)} c_\ell(E_d) \cdot |Ш(E_d/K)|^{1/2} = \frac{[E_d(K) : \mathbb{Z}P_d]}{c_{E_d}}. \tag{48}$$

We will prove BSD(3) by computing the 3-part of both sides of (48) explicitly.

Lemma 5.11. *We have $E_d(K)[3] = 0$.*

Proof. By Lemma 5.3, we have $E_d[3]^{\mathrm{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega)$. Since neither ψ_d nor $\psi_d\omega$ becomes trivial when restricted to G_K, we know that $E_d(K)[3] = 0$. □

Lemma 5.12. *If $\ell | N(E_d)$ and $\ell \neq 3$ (equivalently, $\ell | d$), then $3 \nmid c_\ell(E_d)$.*

Proof. By Lemma 5.3, we have $E_d[3]^{\mathrm{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega)$. Because ψ_d and $\psi_d\omega$ are both nontrivial at ℓ (in fact, ramified at ℓ), we know that $E_d(\mathbb{Q}_\ell)[3] = 0$. Since $E_d(\mathbb{Q}_\ell)$ has a pro-ℓ-subgroup ($\ell \neq 3$) of finite index and $E_d(\mathbb{Q}_\ell)$ has trivial 3-torsion, we know that $3 \nmid c_\ell(E_d)$. □

Definition 5.13. Let F be any number field. Let $\mathcal{L} = \{\mathcal{L}_v\}$ be a collection of subspaces $L_v \subseteq H^1(F_v, E_d[3])$, where v runs over all places of L. We say $\mathcal{L}$ is a collection of *local conditions* if for almost all v, we have $\mathcal{L}_v = H^1_{\mathrm{ur}}(F_v, E_d[3])$ is the unramified subspace. Notice that $H^1(F_v, E_d[3]) = 0$, if $v \mid \infty$. We define the *Selmer group cut out by the local conditions* $\mathcal{L}$ to be

$$H^1_{\mathcal{L}}(F, E_d[3]) := \{x \in H^1(F, E_d[3]) : \mathrm{res}_v(x) \in \mathcal{L}_v, \text{for all } v\}.$$

We will consider the following four types of local conditions:

(1) The *Kummer* conditions $\mathcal{L}$ given by $\mathcal{L}_v = \mathrm{im}\left(E(F_v)/3E(F_v) \to H^1(F_v, E_d[3])\right)$. The 3-Selmer group $\mathrm{Sel}_3(E_d/F) = H^1_{\mathcal{L}}(F, E_d[3])$ is cut out by the Kummer conditions.
(2) The *unramified* conditions $\mathcal{U}$ given by $\mathcal{U}_v = H^1_{\mathrm{ur}}(F_v, E_d[3])$.
(3) The *strict* conditions $\mathcal{S}$ given by $\mathcal{S}_v = \mathcal{U}_v$ for $v \nmid 3$ and $\mathcal{S}_v = 0$ for $v|3$.
(4) The *relaxed* conditions $\mathcal{R}$ given by $\mathcal{R}_v = \mathcal{U}_v$ for $v \nmid 3$ and $\mathcal{R}_v = H^1(F_v, E_d[3])$ for $v|3$.

Lemma 5.14. $H^1_{\mathcal{U}}(K, E_d[3]) = H^1_{\mathcal{S}}(K, E_d[3]) = 0$.

Proof. By Shapiro's lemma, we have

$$H^1_{\mathcal{U}}(K, E_d[3]) \cong H^1_{\mathcal{U}}(\mathbb{Q}, E_d[3]) \oplus H^1_{\mathcal{U}}(\mathbb{Q}, E_d^{(d_K)}[3]).$$

By Lemma 5.3, we have an exact sequence

$$\cdots \to H^1(\mathbb{Q}, \mathbb{F}_3(\psi_d)) \to H^1(\mathbb{Q}, E_d[3]) \to H^1(\mathbb{Q}, \mathbb{F}_3(\psi_d\omega)) \to \cdots.$$

Restricting to the unramfied Selmer group we obtain a map

$$H^1_{\mathcal{U}}(\mathbb{Q}, E_d[3]) \to H^1(\mathbb{Q}, \mathbb{F}_3(\psi_d\omega))$$

whose kernel and image consist of everywhere unramfied classes. It follows from class field theory that

$$|H^1_{\mathcal{U}}(\mathbb{Q}, E_d[3])| \leq h_3(d) \cdot h_3(-3d).$$

Similarly, we have

$$|H^1_{\mathcal{U}}(\mathbb{Q}, E_d^{(d_K)}[3])| \leq h_3(d_K d) \cdot h_3(-3d_K d).$$

By the assumptions on the 3-class numbers in Theorem 5.6 and Scholz's reflection theorem ([Sch32], see also [Was97, 10.2]), we know that the four 3-class numbers appearing above are all trivial. Hence $H^1_{\mathcal{U}}(K, E_d[3]) = 0$. Since by definition we have

$$H^1_{\mathcal{S}}(K, E_d[3]) \subseteq H^1_{\mathcal{U}}(K, E_d[3]),$$

we also know that $H^1_{\mathcal{S}}(K, E_d[3]) = 0$. □

Lemma 5.15. $\dim H^1_{\mathcal{R}}(K, E_d[3]) = 2$.

Proof. It follows from [DDT97, Theorem 2.18] that

$$\dim H^1_{\mathcal{R}}(K, E_d[3]) - \dim H^1_{\mathcal{S}}(K, E_d[3]) = \frac{1}{2} \sum_{v|3} \dim \mathcal{R}_v. \tag{49}$$

Consider $v|3$. Since 3 is split in K, we know that $H^1(K_v, E_d[3]) \cong H^1(\mathbb{Q}_3, E_d[3])$. By Lemma 5.3 that $E_d[3]^{\mathrm{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega)$. Since $\psi_d(3) \neq 1$ and $\psi_d\omega(3) \neq 1$, we know that

$$H^0(\mathbb{Q}_3, E_d[3]) = H^2(\mathbb{Q}_3, E_d[3]) = 0.$$

It follows from the Euler characteristic formula that

$$\dim H^1(\mathbb{Q}_3, E_d[3]) = 2.$$

Namely, $\dim \mathcal{R}_v = 2$. The result then follows from Lemma 5.14 and the formula (49). □

Lemma 5.16. $\mathrm{Sel}_3(E_d/K) \cong \mathbb{Z}/3\mathbb{Z}$. *In particular,* $Ш(E_d/K)[3] = 0$.

Proof. We claim that $\mathcal{L}_v = \mathcal{U}_v$ for any $v \nmid 3$. In fact:

(1) If $v \nmid 3d\infty$, then E_d has good reduction at v and so $\mathcal{L}_v = H^1_{\mathrm{ur}}(K_v, E_d[3])$ by [GP12, Lemma 6].
(2) If $v|\infty$, then v is complex and $H^1(K_v, E_d[3]) = 0$. So $\mathcal{L}_v = H^1_{\mathrm{ur}}(K_v, E_d[3]) = 0$.
(3) If $v|d$, then v is split in K and thus $K_v \cong \mathbb{Q}_\ell$. By Lemma 5.12, $c_\ell(E)$ is coprime to 3. It follows that $\mathcal{L}_v = H^1_{\mathrm{ur}}(K_v, E_d[3])$ by [GP12, Lemma 6].

It follows from the claim that

$$\mathrm{Sel}_3(E_d/K) \subseteq H^1_{\mathcal{R}}(K, E_d[3]).$$

So $\dim \mathrm{Sel}_3(E_d/K) \leq 2$ by Lemma 5.15.

By the Heegner hypothesis, the root number of E_d/K is -1. Since the 3-parity conjecture is known for elliptic curves with a 3-isogeny ([DD11, Theorem 1.8]), we know that $\dim \mathrm{Sel}_3(E_d/K)$ is odd and thus must be 1. Hence $\mathrm{Sel}_3(E_d/K) \cong \mathbb{Z}/3\mathbb{Z}$ as desired. □

Lemma 5.17. *We have*

$$c_3(E_d) = \begin{cases} 3, & d \equiv 2 \pmod 9, \\ 1, & d \equiv 3, 5, 8 \pmod 9. \end{cases}$$

In either case we have $\mathrm{ord}_3(c_3(E_d)) = \mathrm{ord}_3\left(\frac{[E_d(K):\mathbb{Z}P_d]}{c_{E_d}}\right)$.

Proof. The first part follows directly from Tate's algorithm [Sil94, IV.9] (see also the formula in [Sat86, 0.5]).

Suppose $\mathrm{ord}_3(c_3(E_d)) = 0$. We need to show that $\mathrm{ord}_3([E_d(K) : \mathbb{Z}P_d]) = 0$. If not, then since $E_d(K)[3] = 0$ (Lemma 5.11), we know that there exists some $Q \in E_d(K)$ such that $3Q = nP_d$ for some n coprime to 3. Let $\omega_{\mathcal{E}_d}$ be the Néron differential of E_d and let $\log_{E_d} := \log_{\omega_{\mathcal{E}_d}}$. By the very definition of the Manin constant we have $c_{E_d} \cdot \omega_{E_d} = \omega_{\mathcal{E}_d}$ and $c_{E_d} \cdot \log_{\omega_{E_d}} = \log_{E_d}$. Since c_{E_d} is assumed to be coprime to 3, we have up to a 3-adic unit,

$$\frac{|\tilde{E}_d^{\mathrm{ns}}(\mathbb{F}_3)| \cdot \log_{\omega_{E_d}} P_d}{3} = \frac{|\tilde{E}_d^{\mathrm{ns}}(\mathbb{F}_3)| \cdot \log_{E_d} P_d}{3} = |\tilde{E}_d^{\mathrm{ns}}(\mathbb{F}_3)| \cdot \log_{E_d}(Q).$$

On the other hand, $c_3(E_d) \cdot |\tilde{E}_d^{\mathrm{ns}}(\mathbb{F}_3)| \cdot Q$ lies in the formal group $\hat{E}_d(3\mathcal{O}_{K_3})$ and $\mathrm{ord}_3(c_3(E_d)) = 0$, we know that

$$|\tilde{E}_d^{\mathrm{ns}}(\mathbb{F}_3)| \cdot \log_{E_d}(Q) \in 3\mathcal{O}_{K_3},$$

which contradicts the formula (46).

Now suppose $\mathrm{ord}_3(c_3(E_d)) = 1$. The same argument as the previous case shows that we have $\mathrm{ord}_3([E_d(K) : \mathbb{Z}P_d]) \leq 1$. It remains to show that

$$\mathrm{ord}_3([E_d(K) : \mathbb{Z}P_d]) \neq 0.$$

Assume otherwise, then the image of P_d in $E_d(K)/3E_d(K)$ is *nontrivial*, and hence its image in $\mathrm{Sel}_3(E_d/K) \cong \mathbb{Z}/3\mathbb{Z}$ is nontrivial. We now analyze its local Kummer image at 3 and derive a contradiction.

Since $c_3(E_d) = 3$ and $\tilde{E}_d^{\mathrm{ns}}(\mathbb{F}_3) = \mathbb{Z}/3\mathbb{Z}$, we know that $E_d(\mathbb{Q}_3)/\hat{E}_d(3\mathbb{Z}_3)$ is a group of order 9, so

$$E_d(\mathbb{Q}_3)/\hat{E}_d(3\mathbb{Z}_3) \cong \mathbb{Z}/9\mathbb{Z} \text{ or } \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Since $\dim H^1(\mathbb{Q}_3, E_d[3]) = 2$ and the local Kummer condition is a maximal isotropic subspace of $H^1(\mathbb{Q}_3, E_d[3])$ under the local Tate pairing, we know that $E_d(\mathbb{Q}_3)/3E_d(\mathbb{Q}_3) = \mathbb{Z}/3\mathbb{Z}$. So the only possibility is that

$$E_d(\mathbb{Q}_3)/\hat{E}_d(3\mathbb{Z}_3) \cong \mathbb{Z}/9\mathbb{Z}. \tag{50}$$

Now by the formula (46), we know that $P_d \notin \hat{E}_d(3\mathcal{O}_{K_3})$, but $3P_d \in \hat{E}_d(3\mathcal{O}_{K_3})$. Using $K_3 \cong \mathbb{Q}_3$ and (50), we deduce that $P_d \in 3E_d(K_3)$. So the local image of P_d in $E_d(K_3)/3E_d(K_3)$ is *trivial*.

Therefore $\mathrm{Sel}_3(E_d/K)$ is equal to the strict Selmer group $H^1_{\mathcal{S}}(K, E_d[3])$, a contradiction to Lemmas 5.14 and 5.16. □

Proof of Theorem 5.10. Theorem 5.10 follows immediately from the equivalent formula (48) and Lemmas 5.12, 5.16 and 5.17. □

6. Cubic twists families

In this section we consider the elliptic curve $E_d/\mathbb{Q} : y^2 = x^3 - 432d$ of j-invariant 0, where d is any 6th-power-free integer. Recall that for a cube-free positive integer D, the D-th cubic twist E_d is the curve E_{dD^2} (cf. Definition 5.1). For $r \geq 0$, we define

$$C_r(E_d, X) = \{D < X : D > 0 \text{ cube-free}, r_{\mathrm{an}}(E_{dD^2}) = r\}$$

to be the counting function for the number of cubic twists of E_d of analytic rank r. Recall that by Lemma 5.3, $E_d[3]^{\mathrm{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega)$.

Theorem 6.1. *Assume for any prime $\ell | N(E_d)$, we have $\psi_d(\ell) \neq 1$ and $\psi_d\omega(\ell) \neq 1$. Assume there exists an imaginary quadratic field K satisfying the Heegner hypothesis for $N(E_d)$ such that*
(1) 3 is split in K.
(2) If $d > 0$, then $h_3(-3d) = h_3(d_K d) = 1$. If $d < 0$, then $h_3(d) = h_3(-3d_K d) = 1$.
Then for $r \in \{0, 1\}$, we have

$$C_r(E_d, X) \gg \frac{X}{\log^{7/8}(X)}.$$

Remark 6.2. Notice that when $3 \nmid d$ is a fundamental discriminant, the conditions $\psi_d(\ell) \neq 1$ and $\psi_d\omega(\ell) \neq 1$ for $\ell | N(E_d)$ are automatically satisfied.

Proof. We consider the following set $\mathcal{S}$ consisting of primes $\ell \nmid 6N(E_d)$ such that
(1) ℓ is split in K.
(2) $\psi_d(\ell) = -1$ (ℓ is inert in $\mathbb{Q}(\sqrt{d})$).
(3) $\omega(\ell) = 1$ (ℓ is split in $\mathbb{Q}(\sqrt{-3})$).
Since our assumption implies that the three quadratic fields K, $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-3})$ are linearly disjoint, we know that the set of primes $\mathcal{S}$ has density $\alpha = (\frac{1}{2})^3 = \frac{1}{8}$ by Chebotarev's density theorem.

Let $\mathcal{N}$ be the set of integers consisting of square-free products of primes in $\mathcal{S}$. Then for any $D \in \mathcal{N}$. We have $E_{dD^2}[3]^{\mathrm{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega)$. For any $\ell | N(E_{dD^2})$, we have $\psi_d(\ell) \neq 1$ and $\psi_d\omega(\ell) \neq 1$ by construction. The imaginary quadratic field K also satisfies the Heegner hypothesis for $N(E_{dD^2})$. Since the relevant 3-class numbers are trivial, we can apply Theorem 2.1 ($p = 3$) to E_{dD^2} and conclude that

$$r_{\mathrm{an}}(E_{dD^2}/K) = 1.$$

The root number $w(E_{dD^2})$ is $+1$ (resp. -1) for a positive proportion of $D \in \mathcal{N}$, so we have for $r \in \{0, 1\}$,

$$C_r(E_d, X) \gg \#\{D \in \mathcal{N} : D < X\}.$$

By a standard application of Ikehara's tauberian theorem (see [KL16, 3.3]), we know that

$$\#\{D \in N : D < X\} \sim c \cdot \frac{X}{\log^{1-\alpha} X},$$

for some $c > 0$. Here $\alpha = \frac{1}{8}$ is the density of the set of primes $\mathcal{S}$. The results then follow. □

Example 6.3. Consider $d = 2^2 \cdot 3^3 = 108$. Then $E_d = 144a1 : y^2 = x^3 - 1$. The field $K = \mathbb{Q}(\sqrt{-23})$ satisfies the Heegner hypothesis for $N = 144$ and 3 is split in K. We compute the 3-class numbers $h_3(-3d) = h_3(-1) = 1$ and $h_3(d_K d) = h_3(-69) = 1$. So the assumptions of Theorem 6.1 are satisfied. The set $\mathcal{N}$ in the proof of Theorem 6.1 consists of square-free products of the primes

$$31, 127, 139, 151, 163, 211, 223, 271, 307, 331, 439, 463, 487, 499, \cdots$$

Notice that $D \in \mathcal{N}$ implies that $D \equiv 1 \pmod 3$. One can then compute the root number of the cubic twist

$$E_{dD^2} : y^2 = x^3 - D^2$$

to be

$$w(E_{dD^2}) = \begin{cases} +1, & D \equiv 1, 4 \pmod 9, \\ -1, & D \equiv 7 \pmod 9. \end{cases}$$

We conclude that for $D \in \mathcal{N}$,

$$r_{\mathrm{an}}(E_{dD^2}) = \begin{cases} 0, & D \equiv 1, 4 \pmod 9, \\ 1, & D \equiv 7 \pmod 9. \end{cases}$$

References

[Bal14] Nava Balsam. The parity of analytic ranks among quadratic twists of elliptic curves over number fields, 2014.

[BDP13] Massimo Bertolini, Henri Darmon, and Kartik Prasanna. Generalized Heegner cycles and p-adic Rankin L-series. *Duke Math. J.*, 162(6):1033–1148, 2013. With an appendix by Brian Conrad.

[BES16] M. Bhargava, N. Elkies, and A. Shnidman. The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$. *ArXiv e-prints*, October 2016.

[BJK09] Dongho Byeon, Daeyeol Jeon, and Chang Heon Kim. Rank-one quadratic twists of an infinite family of elliptic curves. *J. Reine Angew. Math.*, 633:67–76, 2009.

[BKLS17] M. Bhargava, Z. Klagsbrun, R. J. Lemke Oliver, and A. Shnidman. Three-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field. *ArXiv e-prints*, September 2017.

[Bro17] T. D. Browning. Many cubic surfaces contain rational points. *ArXiv e-prints*, January 2017.

[BSZ14] M. Bhargava, C. Skinner, and W. Zhang. A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture. *ArXiv e-prints*, July 2014.

[DD11] Tim Dokchitser and Vladimir Dokchitser. Root numbers and parity of ranks of elliptic curves. *J. Reine Angew. Math.*, 658:39–64, 2011.

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[Fou93] É. Fouvry. Sur le comportement en moyenne du rang des courbes $y^2 = x^3 + k$. In *Séminaire de Théorie des Nombres, Paris, 1990–91*, volume 108 of *Progr. Math.*, pages 61–84. Birkhäuser Boston, Boston, MA, 1993.

[Gol79] Dorian Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, volume 751 of *Lecture Notes in Math.*, pages 108–118. Springer, Berlin, 1979.

[GP12] Benedict H. Gross and James A. Parson. On the local divisibility of Heegner points. In *Number theory, analysis and geometry*, pages 215–241. Springer, New York, 2012.

[Gro80] Benedict H. Gross. On the factorization of p-adic L-series. *Invent. Math.*, (1):83–95, 1980.

[Gro84] Benedict H. Gross. Heegner points on $X_0(N)$. In *Modular forms (Durham, 1983)*, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., pages 87–105. Horwood, Chichester, 1984.

[Gro11] Benedict H. Gross. Lectures on the conjecture of Birch and Swinnerton-Dyer. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 169–209. Amer. Math. Soc., Providence, RI, 2011.

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[HB94] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. *Invent. Math.*, 118(2):331–370, 1994. With an appendix by P. Monsky.

[HB04] D. R. Heath-Brown. The average analytic rank of elliptic curves. *Duke Math. J.*, 122(3):591–623, 2004.

[HT93] H. Hida and J. Tilouine. Anti-cyclotomic Katz p-adic L-functions and congruence modules. *Ann. Sci. École Norm. Sup. (4)*, 26(2):189–259, 1993.

[Jam98] Kevin James. L-series with nonzero central critical value. *J. Amer. Math. Soc.*, 11(3):635–641, 1998.

[Jam99] Kevin James. Elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture mod 3. *J. Number Theory*, 76(1):16–21, 1999.

[Kan13] Daniel Kane. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. *Algebra Number Theory*, 7(5):1253–1279, 2013.

[Kat76] Nicholas M. Katz. p-adic Interpolation of Real Analytic Eisenstein Series. *Ann. of Math.*, 104(3):459–571, 1976.

[Kat78] Nicholas M. Katz. p-adic L-functions for CM fields. *Invent. Math.*, 49(3):199–297, 1978.

[KL16] D. Kriz and C. Li. Congruences between Heegner points and quadratic twists of elliptic curves. *ArXiv e-prints*, June 2016.

[Kob13] Shinichi Kobayashi. The p-adic Gross-Zagier formula for elliptic curves at supersingular primes. *Invent. Math.*, 191(3):527–629, 2013.

[Kri16] Daniel Kriz. Generalized Heegner cycles at Eisenstein primes and the Katz p-adic L-function. *Algebra Number Theory*, 10(2):309–374, 2016.

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.

[Liv95] Eric Liverance. A formula for the root number of a family of elliptic curves. *J. Number Theory*, 51(2):288–305, 1995.

[LLT16] Y. Li, Y. Liu, and Y. Tian. On The Birch and Swinnerton-Dyer Conjecture for CM Elliptic Curves over $\mathbb{Q}$. *ArXiv e-prints*, May 2016.

[LZZ15] Y. Liu, S. Zhang, and W. Zhang. On p-adic Waldspurger formula. *ArXiv e-prints*, November 2015.

[Maz79] B. Mazur. On the arithmetic of special values of L functions. *Invent. Math.*, 55(3):207–240, 1979.

[Nek90] Jan Nekovář. Class numbers of quadratic fields and Shimura's correspondence. *Math. Ann.*, 287(4):577–594, 1990.

[NH88] Jin Nakagawa and Kuniaki Horie. Elliptic curves with no rational points. *Proc. Amer. Math. Soc.*, 104(1):20–24, 1988.

[Ono98] Ken Ono. A note on a question of J. Nekovář and the Birch and Swinnerton-Dyer conjecture. *Proc. Amer. Math. Soc.*, 126(10):2849–2853, 1998.

[OS98] Ken Ono and Christopher Skinner. Non-vanishing of quadratic twists of modular L-functions. *Invent. Math.*, 134(3):651–660, 1998.

[PR87] Bernadette Perrin-Riou. Points de Heegner et dérivées de fonctions L p-adiques. *Invent. Math.*, 89(3):455–510, 1987.

[PR04] Robert Pollack and Karl Rubin. The main conjecture for CM elliptic curves at supersingular primes. *Ann. of Math. (2)*, 159(1):447–464, 2004.

[Rub83] Karl Rubin. Congruences for special values of L-functions of elliptic curves with complex multiplication. *Invent. Math.*, 71(2):339–364, 1983.

[Rub91] Karl Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[Sag16] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.2)*, 2016. `http://www.sagemath.org`.

[Sat86] Philippe Satgé. Groupes de Selmer et corps cubiques. *J. Number Theory*, 23(3):294–317, 1986.

[Sch32] Arnold Scholz. Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. *J. Reine Angew. Math.*, 166:201–203, 1932.

[Shn17] A. Shnidman. Quadratic twists of abelian varieties with real multiplication. *ArXiv e-prints*, October 2017.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Smi16] A. Smith. The congruent numbers have positive natural density. *ArXiv e-prints*, March 2016.

[Smi17] A. Smith. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. *ArXiv e-prints*, February 2017.

[Tay00] Hisao Taya. Iwasawa invariants and class numbers of quadratic fields for the prime 3. *Proc. Amer. Math. Soc.*, 128(5):1285–1292, 2000.

[TYZ14] Y. Tian, X. Yuan, and S. Zhang. Genus Periods, Genus Points and Congruent Number Problem. *ArXiv e-prints*, November 2014.

[Vat98] V. Vatsal. Rank-one twists of a certain elliptic curve. *Math. Ann.*, 311(4):791–794, 1998.

[Vat99] V. Vatsal. Canonical periods and congruence formulae. *Duke Math. J.*, 98(2):397–419, 1999.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wat07] Mark Watkins. Rank distribution in a family of cubic twists. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 237–246. Cambridge Univ. Press, Cambridge, 2007.

[Yoo15] Hwajong Yoo. Non-optimal levels of a reducible mod l modular representation, 2015.

[ZK87] D. Zagier and G. Kramarz. Numerical investigations related to the L-series of certain elliptic curves. *J. Indian Math. Soc. (N.S.)*, 52:51–69 (1988), 1987.

E-mail address: dkriz@princeton.edu

Department of Mathematics, Princeton University, Fine Hall, Washington Rd, Princeton, NJ 08544

E-mail address: chaoli@math.columbia.edu

Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027