



# GOLDFELD'S CONJECTURE AND CONGRUENCES BETWEEN HEEGNER POINTS

DANIEL KRIZ<sup>1</sup> and CHAO LI<sup>2</sup>

<sup>1</sup> Department of Mathematics, Massachusetts Institute of Technology, 77 Memorial Drive,  
Cambridge, MA 02139, USA;

email: dkriz@mit.edu

<sup>2</sup> Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027, USA;  
email: chaoli@math.columbia.edu

Received 8 June 2018; accepted 10 January 2019

## 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 (respectively 1). We show that 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. For a more general elliptic curve  $E$ , we show that the number of quadratic twists of  $E$  up to twisting discriminant  $X$  of analytic rank 0 (respectively 1) is  $\gg X/\log^{5/6} X$ , improving the current best general bound toward Goldfeld's conjecture due to Ono–Skinner (respectively Perelli–Pomykala). To prove these results, we establish a congruence formula between  $p$ -adic logarithms of Heegner points and apply it in the special cases  $p = 3$  and  $p = 2$  to construct the desired twists explicitly. As a by-product, we also prove the corresponding  $p$ -part of the Birch and Swinnerton–Dyer conjecture for these explicit twists.

2010 Mathematics Subject Classification: 11G05 (primary); 11G40 (secondary)

## 1. Introduction

**1.1. Goldfeld's conjecture.** Let  $E$  be an elliptic curve over  $\mathbb{Q}$ . We denote by  $r_{\text{an}}(E)$  its analytic rank. By the theorem of Gross–Zagier and Kolyvagin, the rank part of the Birch and Swinnerton–Dyer (BSD) conjecture holds whenever  $r_{\text{an}}(E) \in \{0, 1\}$ . One can ask the following natural question: how is  $r_{\text{an}}(E)$  distributed when  $E$  varies in families? The simplest (1-parameter) family is given by the quadratic twist 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

© The Author(s) 2019. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

of Goldfeld [21] asserts that  $r_{\text{an}}(E^{(d)})$  tends to be as low as possible (compatible with the sign of the function equation). Namely in the quadratic twist family  $\{E^{(d)}\}$ ,  $r_{\text{an}}$  should be 0 (respectively 1) for 50% of  $d$ 's. Although  $r_{\text{an}} \geq 2$  occurs infinitely often, its occurrence should be sparse and accounts for only 0% of  $d$ 's. More precisely,

CONJECTURE 1.1 (Goldfeld). *Let*

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

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

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

*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 weaker version (replacing 50% by any positive proportion):

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

REMARK 1.3. Heath-Brown [30, Theorem 4] proved Conjecture 1.2 *conditional* on the Generalized Riemann Hypothesis. Recently, Smith [76] 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 [29] and Kane [35].

REMARK 1.4. Katz–Sarnak [40] 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–Zhang [7]. However, their method does not directly apply to quadratic twists families.

In the next two subsections, we describe our unconditional theorems concerning Goldfeld's conjecture for both special and general elliptic curves.

**1.2. Goldfeld's conjecture for special  $E$ .** The curve  $E = X_0(19)$  is the first known example for which Conjecture 1.2 is valid (see James [32] for  $r = 0$  and Vatsal [82] for  $r = 1$ ). Later, many authors have verified Conjecture 1.2 for infinitely many curves  $E$  (see [11, 83] and [42]) using various methods. However, all these examples are a bit special as they are all covered by our first main result:

**THEOREM 1.5.** *The weak Goldfeld conjecture is true for any  $E$  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 [75] and Tian–Yuan–Zhang [80]).

**REMARK 1.7.** For explicit lower bounds for the proportion in Theorem 1.5, see the more precise statements in Theorems 9.4 and 9.5, Proposition 9.7 and Example 9.9.

For an elliptic curve  $E$  of  $j$ -invariant 0 (respectively 1728), one can also consider its cubic or sextic (respectively 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 twist 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 sixth-power-free integer  $d$ , we denote by

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

the  $d$ th sextic twist of  $E$ .

**THEOREM 1.8 (Corollary 10.8).** *The weak Goldfeld conjecture is true for the sextic twist family  $\{E_d\}$ . In fact,  $E_d$  has analytic rank 0 (respectively 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 (respectively 1). However, these cubic twists do not have positive density. See the more precise statement in Theorem 11.1 and Example 11.3.

**REMARK 1.10.** In a recent work, Bhargava–Elkies–Shnidman [6] 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 [20]). The same method also works for quadratic twist family of any elliptic curve with

a 3-isogeny [8]. 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 [9] has used Theorem 1.8 as a 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. This result drastically increases the set of known cases of cubic surfaces which have a  $\mathbb{Q}$ -rational point and gives a very uniform family of such examples.

**1.3. Goldfeld’s conjecture for general  $E$ .** When  $r = 0$ , the best general result toward Goldfeld’s conjecture is due to Ono–Skinner [59]: they showed that for any elliptic curve  $E/\mathbb{Q}$ ,

$$N_0(E, X) \gg \frac{X}{\log X}.$$

When  $E(\mathbb{Q})[2] = 0$ , Ono [58] improved this result to

$$N_0(E, X) \gg \frac{X}{\log^{1-\alpha} X}$$

for some  $0 < \alpha < 1$  depending on  $E$ . When  $r = 1$ , even less is known. The best general result is due to Perelli–Pomykala [60] using analytic methods: they showed that for any  $\varepsilon > 0$ ,

$$N_1(E, X) \gg X^{1-\varepsilon}.$$

Our third main result improves both bounds under a technical assumption on the 2-adic logarithm of the associated Heegner point on  $E$ .

Let us be more precise. Let  $E/\mathbb{Q}$  be an elliptic curve of conductor  $N$ . Throughout this article, we will use  $K = \mathbb{Q}(\sqrt{d_K})$  to denote an imaginary quadratic field of fundamental discriminant  $d_K$  satisfying the *Heegner hypothesis* for  $N$ :

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

We denote by  $P \in E(K)$  the corresponding Heegner point, defined up to sign and torsion with respect to a fixed modular parametrization  $\pi_E : X_0(N) \rightarrow E$  (see [25]). Let

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

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

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

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

Now we are ready to state our third main result.

**THEOREM 1.12.** *Suppose  $E/\mathbb{Q}$  is an elliptic curve with  $E(\mathbb{Q})[2] = 0$ . Suppose there exists an imaginary quadratic field  $K$  by satisfying the Heegner hypothesis for  $N$  such that*

$$2 \text{ splits in } K \quad \text{and} \quad \frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_2)| \cdot \log_{\omega_E}(P)}{2} \not\equiv 0 \pmod{2}. \quad (\star)$$

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

$$N_r(E, X) \gg \begin{cases} \frac{X}{\log^{5/6} X}, & \text{if } \text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3, \\ \frac{X}{\log^{2/3} X}, & \text{if } \text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}. \end{cases}$$

**REMARK 1.13.** Assumption  $(\star)$  imposes certain constraints on  $E/\mathbb{Q}$  (for example, its local Tamagawa numbers at odd primes are odd; see Section 5.1), but it is satisfied for a wide class of elliptic curves. See Section 6 for examples and also Remark 6.6 on the wide applicability of Theorem 1.12.

**REMARK 1.14.** Mazur–Rubin [48] proved similar results for the number of twists of 2-Selmer rank 0, 1. Again we remark that it 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 Kolyagin for  $p = 2$  is not known.

**REMARK 1.15.** For certain elliptic curves with  $E(\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z}$ , the work of Coates–Li–Tian–Zhai [15] also improves the current bounds using a generalization of the classical method of Heegner and Birch for prime twists.

**1.4. Congruences between  $p$ -adic logarithms of Heegner points.** The starting point of the proof of Theorem 1.12 is the simple observation that quadratic twists do not change the mod 2 Galois representations:  $E[2] \cong E^{(d)}[2]$ . More generally, suppose  $p$  is a prime and  $E, E'$  are two elliptic curves with

isomorphic semisimplified Galois representations  $E[p^m]^{ss} \cong E'[p^m]^{ss}$  for some  $m \geq 1$ , one expects that there should be a congruence mod  $p^m$  between the special values (or derivatives) of the associated  $L$ -functions of  $E$  and  $E'$ . It is usually rather subtle to formulate such congruence precisely. Instead, we work directly with the  $p$ -adic incarnation of the  $L$ -values – the  $p$ -adic logarithm of Heegner points – and we prove the following key congruence formula.

**THEOREM 1.16.** *Let  $E$  and  $E'$  be two elliptic curves over  $\mathbb{Q}$  of conductors  $N$  and  $N'$ , respectively. Suppose  $p$  is a prime such that there is an isomorphism of semisimplified  $G_{\mathbb{Q}} := \text{Gal}(\mathbb{Q}/\mathbb{Q})$ -representations*

$$E[p^m]^{ss} \cong E'[p^m]^{ss}$$

for some  $m \geq 1$ . Let  $K$  be an imaginary quadratic field satisfying the Heegner hypothesis for both  $N$  and  $N'$ . Let  $P \in E(K)$  and  $P' \in E'(K)$  be the Heegner points. Assume that  $p$  is split in  $K$ . Then we have

$$\begin{aligned} & \left( \prod_{\ell|pNN'/M} \frac{|\tilde{E}^{ns}(\mathbb{F}_{\ell})|}{\ell} \right) \cdot \log_{\omega_E} P \\ & \equiv \pm \left( \prod_{\ell|pNN'/M} \frac{|\tilde{E}'^{ns}(\mathbb{F}_{\ell})|}{\ell} \right) \cdot \log_{\omega_{E'}} P' \pmod{p^m \mathcal{O}_{K_p}}. \end{aligned}$$

Here,

$$M = \prod_{\substack{\ell|(N, N') \\ a_{\ell}(E) \equiv a_{\ell}(E') \pmod{p^m}}} \ell^{\text{ord}_{\ell}(NN')}.$$

**REMARK 1.17.** Recall that  $\tilde{E}^{ns}(\mathbb{F}_{\ell})$  denotes the number of  $\mathbb{F}_{\ell}$ -points of the nonsingular part of the mod  $\ell$  reduction of  $E$ , which is  $\ell + 1 - a_{\ell}(E)$  if  $\ell \nmid N$ ,  $\ell \pm 1$  if  $\ell || N$  and  $\ell$  if  $\ell^2 | N$ . The factors in the above congruence can be understood as the result of removing the Euler factors of  $L(E, 1)$  and  $L(E', 1)$  at bad primes.

**REMARK 1.18.** The link between the  $p$ -adic logarithm of Heegner points and  $p$ -adic  $L$ -functions dates back to Rubin [66] in the Complex Multiplication case and was recently established in great generality by Bertolini–Darmon–Prasanna (BDP) [5] and Liu–Zhang–Zhang [45]. However, our congruence formula is based on direct  $p$ -adic integration and does not use this deep link with  $p$ -adic  $L$ -functions.

**REMARK 1.19.** Since there is no extra difficulty, we prove a slightly more general version (Theorem 3.9) for Heegner points on abelian varieties of  $GL_2$ -type. The

same type of congruence should hold for modular forms of weight  $k \geq 2$  (in a future work), where the  $p$ -adic logarithm of Heegner points is replaced by the  $p$ -adic Abel–Jacobi image of generalized Heegner cycles defined in [5].

Note that Theorem 1.16 allows us to propagate the nonvanishing (mod  $p$ ) of the  $p$ -adic logarithm of Heegner points through congruences as long as the extra Euler factors are  $p$ -adic units. As a first application, we apply to the case  $p = 2$  and  $E' = E^{(d)}$  and construct an explicit set of  $d$ 's such that the  $p$ -adic logarithm of  $P^{(d)} \in E^{(d)}(K)$  is nonzero. Combining with the Gross–Zagier formula ( $P^{(d)}$  is nontorsion if and only if  $r_{\text{an}}(E^{(d)}/K) = 1$ ), we can then deduce Theorem 1.12. Further applications of Theorem 1.16 will be given in a future work.

**1.5. Heegner points at Eisenstein primes.** The proof of Theorems 1.5 and 1.8 also relies on a congruence formula involving the  $p$ -adic logarithm of Heegner points. Now suppose  $p$  is an *Eisenstein prime* for  $E$  (that is,  $E[p]$  is a reducible  $G_{\mathbb{Q}}$ -representation, or equivalently,  $E$  admits a rational  $p$ -isogeny). In this case, we have congruence between the modular form  $f$  and an Eisenstein series. The Eisenstein series side of the congruence formula can be evaluated explicitly and gives rise to a product of two Bernoulli numbers.

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

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

Let  $\varepsilon_K$  be the quadratic character associated with  $K$ . We consider the even Dirichlet character

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

**THEOREM 1.20** (Theorem 7.1). *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  $E[p]^{\text{ss}} \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi^{-1}\omega)$  for some character  $\psi : G_{\mathbb{Q}} \rightarrow \text{Aut}(\mathbb{F}_p) \cong \mu_{p-1}$  and the mod  $p$  cyclotomic character  $\omega$ . 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

$$B_{1, \psi_0^{-1} \varepsilon_K} \cdot B_{1, \psi_0 \omega^{-1}} \not\equiv 0 \pmod{p}.$$

Then

$$\frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_p)|}{p} \cdot \log_{\omega_E} P \not\equiv 0 \pmod{p}.$$

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

REMARK 1.21. When  $E/\mathbb{Q}$  has CM by  $\mathbb{Q}(\sqrt{-p})$  (of class number 1), Rubin [64] proved a mod  $p$  congruence formula between the algebraic part of  $L(E, 1)$  and certain Bernoulli numbers. Note that  $E$  admits a  $p$ -isogeny (multiplication by  $\sqrt{-p}$ ), and Theorem 1.20 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.

Note 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 1.20 are nonzero mod  $p$  (see Section 8); hence, we conclude that  $r_{\text{an}}(E/K) = 1$ . 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 1.20 is Davenport–Heilbronn's theorem [18] (enhanced by Nakagawa–Horie [55] with congruence conditions), which allows one to find a positive proportion of twists such that both 3-class numbers in question are trivial.

**1.6. A by-product: the  $p$ -part of the BSD conjecture.** The BSD conjecture predicts the precise formula

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

for the leading coefficient of the Taylor expansion of  $L(E/\mathbb{Q}, s)$  at  $s = 1$  (here  $r = r_{\text{an}}(E)$ ) in terms of various important arithmetic invariants of  $E$  (see [26] 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).

REMARK 1.22. Much progress for  $\text{BSD}(p)$  has been made recently, but only in the case  $p \geq 3$  is *semistable* and *non-Eisenstein* (for  $r = 0$ : [36, 74, 77, 84]; for  $r = 1$ : [4, 13, 34, 73, 77, 90]). For the case  $p = 2$ , very little (beyond numerical verification) is known. Gonzalez-Avilés [22] establishes  $\text{BSD}(2)$  for the quadratic twists of  $X_0(49)$  when  $r = 0$ . Tian's breakthrough [81] on the congruent number problem establishes  $\text{BSD}(2)$  for many quadratic twists of  $X_0(32)$  when  $r \leq 1$ . Coates outlined a program [14, page 35] generalizing Tian's method for establishing  $\text{BSD}(2)$  for many quadratic twists of a general elliptic curve when  $r \leq 1$ , which has succeeded for two more examples  $X_0(49)$  [15] and  $X_0(36)$  [12]. All these three examples are CM with rational 2-torsion.

As a by-product of our congruence formulas for Heegner points, we establish new results on  $\text{BSD}(2)$  for the explicit twists of a general  $E$  constructed in Theorem 1.12 (see Theorem 5.1). We also establish the following new results on  $\text{BSD}(3)$  for many sextic twists  $E_d : y^2 = x^3 - 432d$ , in the case  $p = 3$  is *additive* and *Eisenstein*.

THEOREM 1.23 (Theorem 10.10). *Suppose  $K$  is an imaginary quadratic field that 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  $r_{\text{an}}(E_d/K) = 1$  and  $\text{BSD}(3)$  holds for  $E_d/K$ . (Here,  $h_3(D)$  denotes the 3-class number of  $\mathbb{Q}(\sqrt{D})$ .)

REMARK 1.24. Since the curve  $E_d$  has complex multiplication by  $\mathbb{Q}(\sqrt{-3})$ , we already know that  $\text{BSD}(p)$  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 [41, 44, 61, 62, 65]. When  $r = 0$ , we also know  $\text{BSD}(3)$  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 [33, 56, 57]).

## 1.7. Comparison with previous methods establishing the weak Goldfeld conjecture.

- (1) The work of James [32] on weak Goldfeld for  $r = 0$  uses Waldspurger's formula relating coefficients of weight  $3/2$  modular forms and quadratic

twist  $L$ -values (see also [56, 59]). 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 [47], 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  $\chi$ , for certain odd Dirichlet characters  $\chi$ . This was later generalized by Vatsal [83] 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 [47] 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 [25, II] to more general  $N$  and became the starting point of the work of Vatsal [82] and Byeon–Jeon–Kim [11] on weak Goldfeld for  $r = 1$ .
- (4) Our main congruence at Eisenstein primes (see Section 7.5) through which Theorem 1.20 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 cases. 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 [42] 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 [5]. This is the key observation to remove *all* technical hypotheses that appeared in previous works, which in particular makes the application to the sextic twist family possible.
- (6) Although the methods are completely different, the final appearance of the Davenport–Heilbronn-type theorem is a common feature in all previous works [11, 32, 42, 82, 83] and also ours.

**1.8. Structure of the paper.** The main congruence (Theorem 1.16) is proved in Section 3. We explain the ideal of the proof in Section 3.1. In Section 4, we prove the application to Goldfeld’s conjecture for general  $E$  (Theorem 1.12). In Section 5, we prove the application to BSD(2) (Theorem 5.1). In Section 6, we include numerical examples illustrating the wide applicability of Theorems 1.12 and 5.1. In Section 7, we establish the nontriviality criterion for Heegner points at Eisenstein primes in terms of  $p$ -indivisibility of Bernoulli numbers (Theorem 1.20). In Section 8, we recall the relation between the Bernoulli

numbers and relative class numbers. In Section 9, we combine our criterion and the Nakagawa–Horie theorem to prove the weak Goldfeld conjecture for curves with a 3-isogeny (Theorem 1.5). In Section 10, we give applications to Goldfeld's conjecture and BSD(3) for the sextic twist family (Theorems 1.8 and 1.23). Finally, in Section 11, we give an application to cubic twist families (Theorem 11.1).

## 2. Notations and conventions

In this section, we define some notation and fix some conventions that will be used throughout the paper.

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

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

where  $\psi_{\ell} : \mathbb{Q}_{\ell}^{\times} \rightarrow \overline{\mathbb{Q}}^{\times}$  is the local character at  $\ell$ . Following convention, we extend  $\psi$  to  $\overline{\mathbb{Z}}/f(\psi) \rightarrow \overline{\mathbb{Q}}$ , defining  $\psi(a) = 0$  if  $(a, f(\psi)) \neq 1$ . Given Dirichlet characters  $\psi_1$  and  $\psi_2$ , 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  $f(\psi)_p$  denote 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  $g(\psi)$  of  $\psi$  and local Gauss sums  $g_{\ell}(\psi)$  as in [42, Section 1]. We will often identify a Dirichlet character  $\psi : \mathbb{A}_{\mathbb{Q}}^{\times} \rightarrow \overline{\mathbb{Q}}^{\times}$  with its associated Galois character  $\psi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \overline{\mathbb{Q}}^{\times}$  via the (inverse of the) Artin reciprocity map  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\text{ab}} \xrightarrow{\sim} \hat{\mathbb{Z}}^{\times}$ , using the arithmetic normalization (that is the normalization where  $\text{Frob}_{\ell}$ , the Frobenius conjugacy class at  $\ell$ , gets sent to the idèle which is  $\ell$  at the place of  $\mathbb{Z}$  corresponding to  $\ell$  and 1 at all other places). Throughout, for a given  $p$ , let  $\omega : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mu_{p-1}$  denote the mod  $p$  cyclotomic character. Let  $\mathbb{N}_{\mathbb{Q}} : \mathbb{A}_{\mathbb{Q}}^{\times} \rightarrow \mathbb{C}^{\times}$  denote the norm character,

normalized to have infinity type  $-1$ . For a number field  $K$ , let  $\text{Nm}_{K/\mathbb{Q}} : \mathbb{A}_K^\times \rightarrow \mathbb{A}_\mathbb{Q}^\times$  denote the idèlic norm and let  $\mathbb{N}_K := \mathbb{N}_\mathbb{Q} \circ \text{Nm}_{K/\mathbb{Q}} : \mathbb{A}_K^\times \rightarrow \mathbb{C}^\times$ . Suppose we are given an imaginary quadratic field  $K$  with fundamental discriminant  $d_K$ . Let  $\varepsilon_K : (\mathbb{Z}/d_K)^\times \rightarrow \mu_2$  be the quadratic character associated with  $K$ . For any Dirichlet character  $\psi$  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  $N = N_{\text{split}} N_{\text{nonsplit}} N_{\text{add}}$ , where  $N_{\text{split}}$  is only divisible by primes of split multiplicative reduction,  $N_{\text{nonsplit}}$  is only divisible by primes of nonsplit multiplicative reduction and  $N_{\text{add}}$  is only divisible by primes of additive reduction.

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

### 3. Proof of the main congruence

**3.1. The strategy of the proof.** We first give the idea of the proof of Theorem 1.16. From the congruent Galois representations, we deduce that the coefficients of the associated modular forms are congruent away from the bad primes in  $pNN'/M$ . After applying suitable stabilization operators (Section 3.3) at primes in  $NN'/M$ , we obtain  $p$ -adic modular forms whose coefficients are all congruent. This congruence is preserved when applying a power  $\theta^j$  of the Atkin–Serre operator  $\theta$ . Letting  $j \rightarrow -1$  ( $p$ -adically) and using Coleman’s theorem on  $p$ -adic integration (generalized in [45], see Section 3.5), we can identify the values of  $\theta^{-1}f$  and  $\log_{\omega_f}$  at CM points. The action of stabilization operators at CM points (Section 3.4) gives rise to the extra Euler factors. Summing over the CM points finally proves the main congruence between  $p$ -adic logarithms of Heegner points (Section 3.6). This procedure is entirely parallel to the construction of anticyclotomic  $p$ -adic  $L$ -functions of [5], but we stress that the congruence itself (without linking to the  $p$ -adic  $L$ -function) is more direct and does *not* require the main result of [5]. In particular, we work on  $X_0(N)$  directly (as opposed to working on the finite cover  $X_1(N)$ ) and we do not require  $E$  to have good reduction at  $p$ .

The proof of Theorem 1.20 (and the more general version, Theorem 7.1) relies on a similar congruence identity (Section 7.5) 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. The rest of the argument is similar, applying stabilization operators to get an exact congruence and moving the congruence through a  $p$ -adic family in order to arrive at a congruence involving a  $p$ -adic logarithm of a Heegner point times Euler factors corresponding to the stabilization operators and a special value of a stabilized Katz  $p$ -adic  $L$ -function. The latter Katz  $L$ -value involves a product of two Bernoulli numbers by Gross's factorization. We finally arrive at the congruence identity in Section 7.5.

**3.2.  $p$ -adic modular forms.** Henceforth, it will be useful to adopt Katz's viewpoint of  $p$ -adic modular forms as rules on the moduli space of isomorphism classes of 'ordinary test triples'. (For a detailed reference, see for example [38, Ch. V].)

**DEFINITION 3.1 (Ordinary test triple).** Let  $R$  be a  $p$ -adic ring (that is, the natural map  $R \rightarrow \varprojlim R/p^n R$  is an isomorphism). An *ordinary test triple*  $(A, C, \omega)$  over  $R$  means the following:

- (1)  $A/R$  is an elliptic curve which is ordinary (that is,  $A$  is ordinary over  $R/pR$ ),
- (2) (level  $N$  structure)  $C \subset A[N]$  is a cyclic subgroup of order  $N$  over  $R$  such that the  $p$ -primary part  $C[p^\infty]$  is the *canonical subgroup* of that order (that is, letting  $\hat{A}$  be the formal group of  $A$ , we have  $C[p^\infty] = \hat{A}[p^\infty] \cap C$ ),
- (3)  $\omega \in \Omega_{A/R}^1 := H^0(A/R, \Omega^1)$  is a differential.

Given two ordinary test triples  $(A, C, \omega)$  and  $(A', C', \omega')$  over  $R$ , we say there is an *isomorphism*  $(A, C, \omega) \xrightarrow{\sim} (A', C', \omega')$  if there is an isomorphism  $i : A \rightarrow A'$  of elliptic curves over  $R$  such that  $\phi(C) = C'$  and  $i^*\omega' = \omega$ . Henceforth, let  $[(A, C, \omega)]$  denote the isomorphism class of the test triple  $(A, C, \omega)$ .

**DEFINITION 3.2 (Katz's interpretation of  $p$ -adic modular forms).** Let  $S$  be a fixed  $p$ -adic ring. Suppose  $F$  is a rule which, for every  $p$ -adic  $S$ -algebra  $R$ , assigns values in  $R$  to *isomorphism classes* of test triples  $(A, C, \omega)$  of level  $N$  defined over  $R$ . As such a rule assigning values to isomorphism classes of ordinary test triples, consider the following conditions:

- (1) (Compatibility under base change) For all  $S$ -algebra homomorphisms  $i : R \rightarrow R'$ , we have

$$F((A, C, \omega) \otimes_i R') = i(F(A, C, \omega)).$$

(2) (Weight  $k$  condition) Fix  $k \in \mathbb{Z}$ . For all  $\lambda \in R^\times$ ,

$$F(A, C, \lambda \cdot \omega) = \lambda^{-k} \cdot F(A, C, \omega).$$

(3) (Regularity at cusps) For any positive integer  $d|N$ , letting  $\text{Tate}(q) = \mathbb{G}_m/q^{\mathbb{Z}}$  denote the Tate curve over the  $p$ -adic completion of  $R((q^{1/d}))$  and letting  $C \subset \text{Tate}(q)[N]$  be any level  $N$  structure, we have

$$F(\text{Tate}(q), C, du/u) \in R[[q^{1/d}]],$$

where  $u$  is the canonical parameter on  $\mathbb{G}_m$ .

If  $F$  satisfies conditions (1) and (2), we say it is a *weak  $p$ -adic modular form over  $S$  of level  $N$* . If  $F$  satisfies conditions (1)–(3), we say it is a  *$p$ -adic modular form over  $S$  of level  $N$* . Denote the space of weak  $p$ -adic modular forms over  $S$  of level  $N$  and the space of  $p$ -adic modular forms over  $S$  of level  $N$  by  $\tilde{M}_k^{p\text{-adic}}(\Gamma_0(N))$  and  $M_k^{p\text{-adic}}(\Gamma_0(N))$ , respectively. Note that  $M_k^{p\text{-adic}}(\Gamma_0(N)) \subset \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N))$ .

Let  $\text{Tate}(q)$  be the Tate curve over the  $p$ -adic completion of  $S((q))$ . If  $F \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N))$ , one defines the  $q$ -expansion (at infinity) of  $F$  as  $F(q) := F(\text{Tate}(q), \mu_N, du/u) \in S[[q]]$ , which defines a  *$q$ -expansion map*  $F \mapsto F(q)$ . The  *$q$ -expansion principle* (see [23, Theorem I.3.1] or [37]) says that the  $q$ -expansion map is injective for  $F \in M_k^{p\text{-adic}}(\Gamma_0(N))$ .

From now on, let  $N$  denote the minimal level of  $F$  (that is, the smallest  $N$  such that  $F \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N))$ ). For any positive integer  $N'$  such that  $N|N'$ , we can define

$$[N'/N]^*F(A, C, \omega) := F(A, C[N], \omega)$$

so that  $[N'/N]^*F \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N'))$ . When the larger level  $N'$  is clear from context, we will often abuse notation and simply view  $F \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N'))$  by identifying  $F$  and  $[N'/N]^*F$ .

We now fix  $N^\# \in \mathbb{Z}_{>0}$  such that  $N|N^\#$  so that we can view  $F \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N^\#))$  and further suppose  $\ell^2|N^\#$ , where  $\ell$  is a prime (not necessarily different from  $p$ ). Take the base ring  $S = \mathcal{O}_{\mathbb{C}_p}$ . Then the operator on  $\tilde{M}_k^{p\text{-adic}}(\Gamma_0(N^\#))$  given on  $q$ -expansions by

$$F(q) \mapsto F(q^\ell)$$

has a moduli-theoretic interpretation given by ‘dividing by  $\ell$ -level structure’. That is, we have an operation on test triples  $(A, C, \omega)$  defined over  $p$ -adic  $\mathcal{O}_{\mathbb{C}_p}$ -algebras  $R$  given by

$$V_\ell(A, C, \omega) = (A/C[\ell], \pi(C), \check{\pi}^*\omega),$$

where  $\pi : A \rightarrow A/C[\ell]$  is the canonical projection and  $\check{\pi} : A/C[\ell] \rightarrow A$  is its dual isogeny.

Thus,  $V_\ell$  induces a form  $V_\ell^* F \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N^\#))$  defined by

$$V_\ell^* F(A, C, \omega) := F(V_\ell(A, C, \omega)).$$

For the Tate curve test triple  $(\text{Tate}(q), \mu_{N^\#}, du/u)$ , one sees that  $(\mu_{N^\#})[\ell] = \mu_\ell$  and  $\pi : \text{Tate}(q) \rightarrow \text{Tate}(q^\ell)$ . Since  $\pi : \widehat{\mathbb{G}}_m = \widehat{\text{Tate}(q)} \rightarrow \widehat{\text{Tate}(q^\ell)} = \widehat{\mathbb{G}}_m$  is multiplication by  $\ell$ , we have  $\pi^* du/u = \ell \cdot du/u$ , and so  $\tilde{\pi}^* du/u = du/u$ . Thus, one sees that  $V_\ell$  acts on  $q$ -expansions by

$$V_\ell^* F(q) = V_\ell^* F(\text{Tate}(q), \mu_{N^\#}, du/u) = F(\text{Tate}(q^\ell), \mu_{N^\#/\ell}, du/u) = F(q^\ell).$$

If  $F \in M_k^{p\text{-adic}}(\Gamma_0(N^\#))$ , then  $V_\ell^* F \in M_k^{p\text{-adic}}(\Gamma_0(N^\#))$ , and the  $q$ -expansion principle then implies that  $V_\ell^* F$  is the unique  $p$ -adic modular form of level  $N^\#$  with  $q$ -expansion  $F(q^\ell)$ .

**3.3. Stabilization operators.** In this section, we define the ‘stabilization operators’ alluded to in Section 3.1 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  $q^\ell$  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  $(\alpha_\ell(F), \beta_\ell(F))$ .

DEFINITION 3.3. 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  $\{+, -, 0\}$ . Observe that on  $q$ -expansions, we have

$$\begin{aligned} F^{(\ell)^+}(q) &:= F(q) - \beta_\ell(F)F(q^\ell), \\ F^{(\ell)^-}(q) &:= F(q) - \alpha_\ell(F)F(q^\ell), \\ F^{(\ell)^0}(q) &:= F(q) - a_\ell(F)F(q^\ell) + \ell^{k-1}F(q^{\ell^2}). \end{aligned}$$

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  $T_\ell$ -eigenform, one verifies by direct computation that  $a_\ell(F^{(\ell)^+}) = a_\ell(F)$ ,  $a_\ell(F^{(\ell)^-}) = \beta_\ell(F)$  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  $U_\ell$ -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  $N_+ = \prod_i \ell_i^{e_i}$ ,  $N_- = \prod_j \ell_j^{e_j}$ ,  $N_0 = \prod_m \ell_m^{e_m}$ , we define the  $(N_+, N_-, N_0)$ -stabilization of  $F$  as

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

**3.4. 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  $\mathcal{O}_{\mathbb{C}_p}$ .

A crucial observation is that at an ordinary CM test triple  $(A, A[\mathfrak{N}^\#], \omega)$ , one can express  $V_\ell(A, A[\mathfrak{N}^\#], \omega)$  and thus  $(\ell)$ -stabilization operators in terms of the action of  $\mathcal{C}\ell(\mathcal{O}_K)$  on  $A$  coming from Shimura’s reciprocity law. First, we recall the Shimura action: 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  $\mathcal{O}_K$ , whose isomorphism class depends only on the ideal class of  $\mathfrak{a}$ . Let  $\phi_\mathfrak{a} : A \rightarrow A_\mathfrak{a}$  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

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

where  $\omega_\mathfrak{a} \in \Omega_{A_\mathfrak{a}/\mathbb{C}_p}^1$  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 calculation relates the values of  $V_\ell$ ,  $F^{(\ell)}$  and  $F$  at CM test triples.

LEMMA 3.4. *For a prime  $\ell$ , let  $v|\mathfrak{N}^\#$  be the corresponding prime ideal of  $\mathcal{O}_K$  above it, let  $\bar{v}$  denote the prime ideal which is the complex conjugate of  $v$  and let  $\mathfrak{a} \subset \mathcal{O}_K$  be an ideal prime to  $\mathfrak{N}^\#$ . Then for any  $\omega \in \Omega_{A/\mathcal{O}_{C_p}}^1$ , we have*

$$[V_\ell(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega))] = [\bar{v}^{-1}\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#v^{-1}], \omega)] \quad (7)$$

and

$$[V_\ell(V_\ell(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)))] = [\bar{v}^{-2}\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#v^{-2}], \omega)]. \quad (8)$$

As a consequence, if  $F \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N^\#))$ , when  $\ell \nmid N$ , we have

$$\begin{aligned} &F^{(\ell)^+}(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)) \\ &= F(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)) - \beta_\ell(F)F(\bar{v}^{-1}\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)), \end{aligned} \quad (9)$$

$$\begin{aligned} &F^{(\ell)^-}(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)) \\ &= F(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)) - \alpha_\ell(F)F(\bar{v}^{-1}\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)), \end{aligned} \quad (10)$$

$$\begin{aligned} &F^{(\ell)^0}(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)) \\ &= F(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)) - a_\ell(F)F(\bar{v}^{-1}\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)) \\ &\quad + \ell^{k-1}F(\bar{v}^{-2}\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)), \end{aligned} \quad (11)$$

and when  $\ell|N$ ,

$$\begin{aligned} &F^{(\ell)^0}(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)) \\ &= F(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)) - a_\ell(F)F(\bar{v}^{-1}\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega)). \end{aligned} \quad (12)$$

*Proof.* Note that  $(A_{\mathfrak{a}\overline{\mathfrak{N}^\#}[\mathfrak{N}^\#]})[\ell] = A_{\mathfrak{a}\overline{\mathfrak{N}^\#}}[v]$ . Hence,

$$\begin{aligned} [V_\ell(\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#], \omega))] &= [\mathfrak{a}\overline{\mathfrak{N}^\#} \star V_\ell(A, A[\mathfrak{N}^\#], \omega)] \\ &= [\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A_v, A_v[\mathfrak{N}^\#v^{-1}], \check{\phi}_v^*\omega)] \\ &= [\bar{v}^{-1}\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A_{v\bar{v}}, A_{v\bar{v}}[\mathfrak{N}^\#v^{-1}], (\check{\phi}_v^*\omega)_{\bar{v}})] \\ &= [\bar{v}^{-1}\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A_{(\ell)}, A_{(\ell)}[\mathfrak{N}^\#v^{-1}], (\check{\phi}_v^*\omega)_{\bar{v}})] \\ &= [\bar{v}^{-1}\mathfrak{a}\overline{\mathfrak{N}^\#} \star (A, A[\mathfrak{N}^\#v^{-1}], \omega)], \end{aligned}$$

where the last equality and, hence, (7) follows, once we prove the following.

LEMMA 3.5. Under the canonical isomorphism  $i : A_{(\ell)} \xrightarrow{\sim} A$  sending an equivalence class  $x + A[\ell] \in A_{(\ell)}$  to  $[\ell]x$ , where  $[\ell] : A \rightarrow A$  denotes multiplication by  $\ell$  in the group law, we have

$$(\check{\phi}_v^* \omega)_{\bar{v}} = i^* \omega. \tag{13}$$

*Proof.* By definition of  $\omega_{\bar{v}}$  for a given differential  $\omega$ , (13) is equivalent to the identity

$$\check{\phi}_v^* \omega = \phi_{\bar{v}}^*(i^* \omega) = (i \circ \phi_{\bar{v}})^* \omega.$$

To show this, it suffices to establish the equality

$$\check{\phi}_v = i \circ \phi_{\bar{v}}$$

of isogenies  $A_v \rightarrow A$ . Since  $\phi_{\bar{v}} \circ \phi_v = \phi_{(\ell)} = A \rightarrow A_{(\ell)}$ , we have

$$i \circ \phi_{\bar{v}} \circ \phi_v = i \circ \phi_{(\ell)} : A \xrightarrow{\phi_{(\ell)}} A_{(\ell)} \xrightarrow[\sim]{i} A,$$

where the first arrow maps  $x \mapsto x + A[\ell]$  and the second arrow maps  $x + A[\ell] \mapsto [\ell]x$ . Hence, this composition is, in fact, just the multiplication by  $\ell$  map  $[\ell]$ . Hence,  $i \circ \phi_{\bar{v}}$  is the dual isogeny of  $\phi_v$ , that is  $\check{\phi}_v = i \circ \phi_{\bar{v}}$ , and the lemma follows.  $\square$

The identity (8) follows by the same argument as above, replacing  $\mathfrak{N}^\#$  with  $\mathfrak{N}^\# v^{-1}$ . Viewing  $F$  as a form of level  $N^\#$  and using (7) and (8), then (9), (10), (11) and (12) follow from (3), (4), (5) and (6), respectively.  $\square$

Finally, we relate the CM period sum of  $F^{(\ell)^*}$  for  $\ell \in \{+, -, 0\}$  to that of  $F$  by showing that they differ by an Euler factor at  $\ell$  associated with  $F \otimes \chi^{-1}$ . This calculation will be used in the proof of Theorem 3.9 to relate the values at Heegner points of the formal logarithms  $\log_{\omega_{F(\ell)}}$  and  $\log_{\omega_F}$  associated with  $F^{(\ell)^*}$  and  $F$ .

LEMMA 3.6. Suppose  $F \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N^\#))$ , and let  $\chi : \mathbb{A}_K^\times \rightarrow \mathbb{C}_p^\times$  be a  $p$ -adic Hecke character such that  $\chi$  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

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

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

and if  $\ell|N$ , we have

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

*Proof.* First, note that by our assumptions on  $\chi$ , for any  $G \in \tilde{M}_k^{p\text{-adic}}(\Gamma_0(N^\#))$ , the quantity

$$\chi^{-1}(\mathfrak{a}) G(\mathfrak{a} \star (A, A[\mathfrak{N}^\#], \omega))$$

depends only on the ideal class  $[\mathfrak{a}]$  of  $\mathfrak{a}$ . Since  $\{\mathfrak{a}\}$  is a full set of integral representatives. of  $\mathcal{C}\ell(\mathcal{O}_K)$ ,  $\{\mathfrak{a}\mathfrak{N}^\#\}$  is also a full set of integral representatives of  $\mathcal{C}\ell(\mathcal{O}_K)$ . By summing over  $\mathcal{C}\ell(\mathcal{O}_K)$ , the lemma follows from Lemma 3.4.  $\square$

**3.5. Coleman integration.** In this section, we recall Liu–Zhang–Zhang’s extension of Coleman’s theorem on  $p$ -adic integration. We will use this theorem later in order to directly realize (a pullback of) the formal logarithm along the weight 2 newform  $f \in S_2^{\text{new}}(\Gamma_0(N))$  as a rigid analytic function  $F$  on the ordinary locus of  $X_0(N)(\mathbb{C}_p)$  (viewed as a rigid analytic space) satisfying  $\theta F = f$ .

First, we recall the theorem of Liu–Zhang–Zhang, closely following the discussion preceding in [45, Appendix A, Proposition A.1]. Let  $R \subset \mathbb{C}_p$  be a local field. Suppose  $X$  is a quasiprojective scheme over  $R$ ,  $X^{\text{rig}} = X(\mathbb{C}_p)^{\text{rig}}$  is its rigid analytification and  $U \subset X^{\text{rig}}$  an affinoid domain with good reduction.

**DEFINITION 3.7.** Let  $X$  and  $U$  be as above and let  $\omega$  be a closed rigid analytic 1-form on  $U$ . Suppose there exists a locally analytic function  $F_\omega$  on  $U$  as well as a Frobenius endomorphism  $\phi$  of  $U$  (that is, an endomorphism reducing to an endomorphism induced by a power of Frobenius on the reduction of  $U$ ) and a polynomial  $P(X) \in \mathbb{C}_p[X]$  such that no root of  $P(T)$  is a root of unity, satisfying:

- $dF_\omega = \omega$ ;
- $P(\phi^*)F_\omega$  is rigid analytic;

and  $F_\omega$  is uniquely determined by these conditions up to additive constant. We then call  $F_\omega$  the *Coleman primitive of  $\omega$  on  $U$* . It turns out that  $F_\omega$ , if it exists, is independent of the choice of  $P(X)$  [16, Corollary 2.1(b)].

Given an abelian variety  $A$  over  $R$  of dimension  $d$ , recall the formal logarithm defined as follows. Choosing a  $\omega \in \Omega_{A/\mathbb{C}_p}^1$ , the  *$p$ -adic formal logarithm along  $\omega$*  is defined by formal integration

$$\log_\omega(T) := \int_0^T \omega$$

in a formal neighborhood  $\hat{A}$  of the origin. Since  $A(\mathbb{C}_p)$  is compact, we may extend by linearity to a map  $\log_\omega : A(\mathbb{C}_p) \rightarrow \mathbb{C}_p$  (that is,  $\log_\omega(x) := (1/n) \log_\omega(nx)$  if  $nx \in \hat{A}$ ).

Liu–Zhang–Zhang prove the following extension of Coleman’s theorem.

**THEOREM 3.8** (See [45, Proposition A.1]). *Let  $X$  and  $U$  be as above. Let  $A$  be an abelian variety over  $R$  which has either totally degenerate reduction (that is, after base changing to a finite extension of  $R$ , the connected component of the special fiber of the Néron model of  $A$  is isomorphic to  $\mathbb{G}_m^d$ ) or potentially good reduction. For a morphism  $\iota : X \rightarrow A$  and a differential form  $\omega \in \Omega_{A/F}^1$ , we have*

- (1)  $\iota^*\omega|_U$  admits a Coleman primitive on  $U$ , and in fact
- (2)  $\iota^*\log_{\omega|_U}$  is a Coleman primitive of  $\iota^*\omega|_U$  on  $U$ , where  $\log_\omega : A(\mathbb{C}_p) \rightarrow \mathbb{C}_p$  is the  $p$ -adic formal logarithm along  $\omega$ .

**3.6. The main congruence.** Let  $f \in M_2(\Gamma_0(N))$  and  $g \in M_2(\Gamma_0(N'))$  be normalized eigenforms defined over the ring of integers of a number field with minimal levels  $N$  and  $N'$ , respectively. Let  $K$  be an imaginary quadratic field with Hilbert class field  $H$  and suppose  $K$  satisfies the Heegner hypothesis with respect to both  $N$  and  $N'$ , with corresponding fixed choices of ideals  $\mathfrak{N}, \mathfrak{N}' \subset \mathcal{O}_K$  such that  $\mathcal{O}_K/\mathfrak{N} = \mathbb{Z}/N$ ,  $\mathcal{O}_K/\mathfrak{N}' = \mathbb{Z}/N'$  and such that  $\ell|(N, N')$  implies  $(\ell, \mathfrak{N}) = (\ell, \mathfrak{N}')$ ; hence,  $\mathcal{O}_K/\text{lcm}(\mathfrak{N}, \mathfrak{N}') = \mathbb{Z}/\text{lcm}(N, N')$ .

Recall the moduli-theoretic interpretation of  $X_0(N)$ , in which points on  $X_0(N)$  are identified with isomorphism classes  $[(A, C)]$  of pairs  $(A, C)$  consisting of an elliptic curve  $A$  and a cyclic subgroup  $C \subset A[N]$  of order  $N$ . Throughout this section, let  $A/\mathcal{O}_{\mathbb{C}_p}$  be a fixed elliptic curve with CM by  $\mathcal{O}_K$ , and note that

as in Section 3.4, the Shimura reciprocity law induces an action of integral ideals prime to  $\mathfrak{N}$  on  $(A, A[\mathfrak{N}])$ , which descends to an action of  $\mathcal{C}\ell(\mathcal{O}_K)$  on  $[(A, A[\mathfrak{N}])]$ . Let  $\chi : \text{Gal}(H/K) \rightarrow \overline{\mathbb{Q}}^\times$  be a character and let  $L$  be a finite extension of  $K$  containing the Hecke eigenvalues of  $f, g$ , the values of  $\chi$  and the field cut out by the kernel of  $\chi$ . For any full set of prime-to- $\mathfrak{N}$  integral representatives  $\{\mathfrak{a}\}$  of  $\mathcal{C}\ell(\mathcal{O}_K)$ , define the Heegner point on  $J_0(N)$  attached to  $\chi$  by

$$P(\chi) := \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) ([\mathfrak{a} \star (A, A[\mathfrak{N}])] - [\infty]) \in J_0(N)(H) \otimes_{\mathbb{Z}} L,$$

where  $[\infty] \in X_0(N)(\mathbb{C}_p)$  denotes the cusp at infinity. Similarly, for any full set of prime-to- $\mathfrak{N}'$  integral representatives  $\{\mathfrak{a}\}$  of  $\mathcal{C}\ell(\mathcal{O}_K)$ , define the Heegner point on  $J_0(N')$  attached to  $\chi$  by

$$P'(\chi) := \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) ([\mathfrak{a} \star (A, A[\mathfrak{N}'])] - [\infty']) \in J_0(N')(H) \otimes_{\mathbb{Z}} L,$$

where  $[\infty'] \in X_0(N')(\mathbb{C}_p)$  denotes the cusp at infinity.

Let  $\iota : X_0(N) \rightarrow J_0(N)$  denote the Abel–Jacobi map sending  $[\infty] \mapsto 0$  and let  $\iota' : X_0(N') \rightarrow J_0(N')$  denote the Abel–Jacobi map sending  $[\infty'] \mapsto 0$ . Let  $A_f$  and  $A_g$  be the abelian varieties over  $\mathbb{Q}$  of  $GL(2)$ -type associated with  $f$  and  $g$ . Fix modular parametrizations  $\pi_f : J_0(N) \rightarrow A_f$  and  $\pi_g : J_0(N') \rightarrow A_g$ . Let  $P_f(\chi) := \pi_f(P(\chi))$  and  $P_g(\chi) := \pi_g(P'(\chi))$ . Letting

$$\omega_f \in \Omega^1_{J_0(N)/\mathcal{O}_{\mathbb{C}_p}} \quad \text{such that } \iota^* \omega_f = f(q) \cdot dq/q$$

and

$$\omega_g \in \Omega^1_{J_0(N')/\mathcal{O}_{\mathbb{C}_p}} \quad \text{such that } \iota'^* \omega_g = g(q) \cdot dq/q,$$

we choose  $\omega_{A_f} \in \Omega^1_{A_f/\mathbb{Q}}$  and  $\omega_{A_g} \in \Omega^1_{A_g/\mathbb{Q}}$  such that  $\pi_f^* \omega_{A_f} = \omega_f$  and  $\pi_g^* \omega_{A_g} = \omega_g$ .

We define

$$\log_{\omega_f} P(\chi) := \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) \log_{\omega_f} ([\mathfrak{a} \star (A, A[\mathfrak{N}])] - [\infty]) \in L_p$$

and

$$\log_{\omega_g} P'(\chi) := \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) \log_{\omega_g} ([\mathfrak{a} \star (A, A[\mathfrak{N}'])] - [\infty']) \in L_p.$$

The fact that these are values in  $L_p$  follows from the fact  $P(\chi) \in J_0(N)(H) \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$  is in the  $\chi$ -isotypic component of  $\text{Gal}(\overline{\mathbb{Q}}/K)$ , and similarly for  $P'(\chi)$ . We similarly define  $\log_{\omega_{A_f}} P_f(\chi) \in L_p$  and  $\log_{\omega_{A_g}} P_g(\chi) \in L_p$ , and note

that by functoriality of the  $p$ -adic logarithm,  $\log_{\omega_f} P(\chi) = \log_{\omega_{A_f}} P_f(\chi)$  and  $\log_{\omega_g} P'(\chi) = \log_{\omega_{A_g}} P_g(\chi)$ .

Let  $\lambda$  be the prime of  $\mathcal{O}_L$  above  $p$  determined by the embedding  $L \hookrightarrow \overline{\mathbb{Q}}_p$ . We will now prove a generalization of Theorem 1.16 for general weight 2 forms.

**THEOREM 3.9.** *In the setting and notations described above, suppose that the associated semisimple mod  $\lambda^m$  representations  $\bar{\rho}_f, \bar{\rho}_g : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathcal{O}_{L_p}/\lambda^m)$  satisfy  $\bar{\rho}_f \cong \bar{\rho}_g$ . For each prime  $\ell|NN'$ , let  $v|\mathfrak{N}\mathfrak{N}'$  be the corresponding prime above it. Then we have*

$$\begin{aligned} & \left( \prod_{\ell|pNN'/M, \ell \nmid N} \frac{\ell - a_\ell(f)\chi^{-1}(\bar{v}) + \chi^{-2}(\bar{v})}{\ell} \right) \\ & \times \left( \prod_{\ell|pNN'/M, \ell|N} \frac{\ell - a_\ell(f)\chi^{-1}(\bar{v})}{\ell} \right) \log_{\omega_{A_f}} P_f(\chi) \\ & \equiv \left( \prod_{\ell|pNN'/M, \ell \nmid N'} \frac{\ell - a_\ell(g)\chi^{-1}(\bar{v}) + \chi^{-2}(\bar{v})}{\ell} \right) \\ & \times \left( \prod_{\ell|pNN'/M, \ell|N'} \frac{\ell - a_\ell(g)\chi^{-1}(\bar{v})}{\ell} \right) \log_{\omega_{A_g}} P_g(\chi) \pmod{\lambda^m \mathcal{O}_{L_p}}, \end{aligned}$$

where

$$M = \prod_{\ell|(N, N'), a_\ell(f) \equiv a_\ell(g) \pmod{\lambda^m}} \ell^{\text{ord}_\ell(NN')}.$$

*Proof of Theorem 3.9.* We first transfer all differentials and Heegner points on  $J_0(N)$  and  $J_0(N')$  to the Jacobian  $J_0(N^\#)$  of the modular curve  $X_0(N^\#)$ , where  $N^\# := \text{lcm}_{\ell|NN'}(N, N', p^2, \ell^2)$ . Note that for the newforms  $f$  and  $g$ , the minimal levels of the stabilizations  $f^{(\ell)}$  and  $g^{(\ell)}$  divide  $N^\#$  since if  $\ell^2|N$ , then  $a_\ell(f) = 0$  and  $f^{(\ell)} = f$  and, similarly, if  $\ell^2|N'$ , then  $g^{(\ell)} = g$ . By assumption,  $K$  satisfies the Heegner hypothesis with respect to  $N^\#$ , and let  $\mathfrak{N}^\# := \text{lcm}_{v|\mathfrak{N}\mathfrak{N}'}(\mathfrak{N}, \mathfrak{N}', p^2, v^2)$ . For any full set of prime-to- $\mathfrak{N}^\#$  integral representatives  $\{\mathfrak{a}\}$  of  $\mathcal{C}\ell(\mathcal{O}_K)$ , define

$$P^\#(\chi) := \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a})([\mathfrak{a} \star (A, A[\mathfrak{N}^\#])] - [\infty^\#]) \in J_0(N^\#)(H) \otimes_{\mathbb{Z}} L,$$

where  $[\infty^\#] \in X_0(N^\#)(\mathbb{C}_p)$  denotes the cusp at infinity. Letting  $\pi^b : J_0(N^\#) \rightarrow J_0(N)$  and  $\pi'^b : J_0(N^\#) \rightarrow J_0(N')$  denote the natural projections, one sees that  $\pi^b(P^\#(\chi)) = P(\chi)$  and that  $\pi'^b(P^\#(\chi)) = P'(\chi)$ . Let  $t^\# : X_0(N^\#) \rightarrow J_0(N^\#)$  denote the Abel–Jacobi map sending  $[\infty^\#] \mapsto 0$ . Viewing  $f$  and  $g$  as having level

$N^\#$ , we define their associated differential forms by

$$\omega_f^\# \in \Omega_{J_0(N^\#)/\mathcal{O}_{C_p}}^1 \quad \text{such that } \iota^{\#,*} \omega_f^\# = f(q) \cdot dq/q \in \Omega_{X_0(N^\#)/\mathcal{O}_{C_p}}^1$$

and similarly define  $\omega_g^\# \in \Omega_{J_0(N^\#)/\mathcal{O}_{C_p}}^1$ . One sees that  $\pi^{b,*} \omega_f = \omega_f^\#$  and  $\pi'^{b,*} \omega_g = \omega_g^\#$ . Finally, define

$$\log_{\omega_f^\#} P^\#(\chi) := \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a}) \log_{\omega_f^\#}([\mathfrak{a} \star (A, A[\mathfrak{N}^\#])] - [\infty^\#]) \in L_p$$

and similarly for  $\log_{\omega_g^\#} P^\#(\chi)$ .

Let  $N_0^\#$  denote the prime-to- $p$  part of  $N^\#$ . Let  $\mathcal{X}$  denote the canonical smooth proper model of  $X_0(N_0^\#)$  over  $\mathbb{Z}_p$  and let  $\mathcal{X}_{\mathbb{F}_p}$  denote its special fiber. There is a natural reduction map  $\text{red} : X_0(N_0^\#)(\mathbb{C}_p) = \mathcal{X}(\mathcal{O}_{C_p}) \rightarrow \mathcal{X}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ . Viewing  $X_0(N_0^\#)(\mathbb{C}_p)$  as a rigid analytic space, the inverse image in  $X_0(N_0^\#)(\mathbb{C}_p)$  of an element of the finite set of supersingular points in  $\mathcal{X}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$  is conformal to an open unit disc and is referred to as a *supersingular disc*. Let  $\mathcal{D}_0$  denote the affinoid domain of good reduction obtained by removing the finite union of supersingular discs from the rigid space  $X_0(N_0^\#)(\mathbb{C}_p)$ . In the moduli-theoretic interpretation,  $\mathcal{D}_0$  consists of points  $[(A, C)]$  over  $\mathcal{O}_{C_p}$  of good reduction such that  $A \otimes_{\mathcal{O}_{C_p}} \overline{\mathbb{F}}_p$  is ordinary. The canonical projection  $X_0(N^\#) \rightarrow X_0(N_0^\#)$  has a *rigid analytic* section on  $\mathcal{D}_0$  given by ‘increasing level  $N_0^\#$  structure by the order  $N^\#/N_0^\#$  canonical subgroup’. Namely, given  $[(A, C)] \in \mathcal{D}_0$ , the section is defined by  $[(A, C)] \mapsto [(A, C \times \hat{A}[N^\#/N_0^\#])]$ . We identify  $\mathcal{D}_0$  with its lift  $\mathcal{D}$ , which is called the *ordinary locus* of  $X_0(N^\#)(\mathbb{C}_p)$ ; one sees from the above construction that  $\mathcal{D}$  is an affinoid domain of good reduction.

A  $p$ -adic modular form  $F$  of weight 2 (as defined in Section 3.2) can be equivalently viewed as a rigid analytic section of  $(\Omega_{X_0(N^\#)/\mathbb{C}_p}^1)_{|\mathcal{D}}$  (viewed as an analytic sheaf). Under this identification, the exterior differential is given on  $q$ -expansions by  $d = \theta(dq/q)$  where  $\theta$  is the Atkin–Serre operator on  $p$ -adic modular forms acting via  $q(d/dq)$  on  $q$ -expansions. Thus, for each  $j \in \mathbb{Z}_{\geq 0}$ ,  $\theta^j F$  is a rigid analytic section of  $(\Omega_{X_0(N^\#)/\mathbb{C}_p}^{1+j})_{|\mathcal{D}}$ . The collection of  $p$ -adic modular forms  $\theta^j(f^{(p)})$  varies  $p$ -adically continuously in  $j \in \mathbb{Z}/(p-1) \times \mathbb{Z}_p$  (as one verifies on  $q$ -expansions), and so

$$\theta^{-1}(f^{(p)}) := \lim_{j \rightarrow (-1,0)} \theta^j(f^{(p)})$$

is a rigid analytic function on  $\mathcal{D}$  and a Coleman primitive for  $\iota^{\#,*} \omega_{f^{(p)}}$  since

$$d\theta^{-1}(f^{(p)}) = f^{(p)}(q) \cdot dq/q = \iota^{\#,*} \omega_{f^{(p)}}.$$

Also note that  $t^{\#, *}\omega_f$  (restricted to  $\mathcal{D}$ ) has a Coleman primitive  $F_{t^{\#, *}\omega_f^{\#}}$  by part (1) of Theorem 3.8 (applied to  $R = \mathbb{Q}_p$ ,  $X = X_0(N^{\#})$ ,  $U = \mathcal{D}$  and  $A = J_0(N^{\#})$ ), which we can (and do) choose to take the value 0 at  $[\infty^{\#}]$ . As a locally analytic function on  $\mathcal{D}$ ,  $F_{t^{\#, *}\omega_f^{\#}}$  can be viewed as an element of  $\tilde{M}_0^{p\text{-adic}}(\Gamma_0(N^{\#}))$  (see Definition 3.2). By the moduli-theoretic definition of  $(p)$ -stabilization in terms of the operators  $V_p$  defined in Section 3.3, we have

$$d\theta^{-1}(f^{(p)}) = d(F_{t^{\#, *}\omega_f^{\#}})^{(p)},$$

and so

$$\theta^{-1}(f^{(p)}) = (F_{t^{\#, *}\omega_f^{\#}})^{(p)}$$

by uniqueness of Coleman primitives. The same argument shows that  $\theta^{-1}(g^{(p)}) = (F_{t^{\#, *}\omega_g^{\#}})^{(p)}$ .

Since  $\bar{\rho}_f \cong \bar{\rho}_g$ , we have

$$\theta^j(f^{(pNN'/M)})(q) \equiv \theta^j(g^{(pNN'/M)})(q) \pmod{\lambda^m \mathcal{O}_{\mathbb{C}_p}}$$

for all  $j \geq 0$ . Letting  $j \rightarrow (-1, 0) \in \mathbb{Z}/(p-1) \times \mathbb{Z}_p$ , we find that

$$\theta^{-1}(f^{(pNN'/M)})(q) \equiv \theta^{-1}(g^{(pNN'/M)})(q) \pmod{\lambda^m \mathcal{O}_{\mathbb{C}_p}}.$$

Let  $N_0$  denote the prime-to- $p$  part of  $NN'/M$ . One sees directly from the description of stabilization operators on  $q$ -expansions that  $\theta^{-1}(f^{(pNN'/M)})(q) = (\theta^{-1}(f^{(p)}))^{(N_0)}(q)$  and  $\theta^{-1}(g^{(pNN'/M)})(q) = (\theta^{-1}(g^{(p)}))^{(N_0)}(q)$ . Thus, the above congruence becomes

$$(\theta^{-1}(f^{(p)}))^{(N_0)}(q) \equiv (\theta^{-1}(g^{(p)}))^{(N_0)}(q) \pmod{\lambda^m \mathcal{O}_{\mathbb{C}_p}}.$$

Using the identities  $\theta^{-1}(f^{(p)}) = (F_{t^{\#, *}\omega_f^{\#}})^{(p)}$  and  $\theta^{-1}(g^{(p)}) = (F_{t^{\#, *}\omega_g^{\#}})^{(p)}$  and the equality of stabilization operators  $(pN_0) = (pNN'/M)$ , we have

$$(F_{t^{\#, *}\omega_f^{\#}})^{(pNN'/M)}(q) \equiv (F_{t^{\#, *}\omega_g^{\#}})^{(pNN'/M)}(q) \pmod{\lambda^m \mathcal{O}_{\mathbb{C}_p}}.$$

Thus, applying the  $q$ -expansion principle (that is, the fact that the  $q$ -expansion map is injective), we have that

$$(F_{t^{\#, *}\omega_f^{\#}})^{(pNN'/M)} \equiv (F_{t^{\#, *}\omega_g^{\#}})^{(pNN'/M)} \pmod{\lambda^m \mathcal{O}_{\mathbb{C}_p}} \quad (14)$$

as weight 0  $p$ -adic modular forms on  $\mathcal{D}$  over  $\mathcal{O}_{\mathbb{C}_p}$ . In particular, for an ordinary CM test triple  $(A, A[\mathfrak{N}^{\#}], \omega)$ , we have

$$\begin{aligned} & (F_{t^{\#, *}\omega_f^{\#}})^{(pNN'/M)}(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)) \\ & \equiv (F_{t^{\#, *}\omega_g^{\#}})^{(pNN'/M)}(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)) \pmod{\lambda^m \mathcal{O}_{\mathbb{C}_p}}. \end{aligned} \quad (15)$$

Applying Lemma 3.6 inductively to  $F_t = F_{i^{\#,*}\omega_f^{\#}}^{(\prod_{i=1}^{r-t} \ell_i)}$  for  $1 \leq t \leq r$ , where  $\prod_{i=1}^r \ell_i$  is the square-free part of  $pNN'/M$  (so that  $F_0 = F_{i^{\#,*}\omega_f^{\#}}^{(pNN'/M)}$ ,  $F_r = F_{i^{\#,*}\omega_f^{\#}}$  and  $F_t^{(\ell_t)} = F_{t-1}$ ), and noting that  $\theta F_{i^{\#,*}\omega_f^{\#}}(q) = f(q)$  implies  $a_{\ell_t}(F_t) = a_{\ell_t}(f)/\ell_t$ , we obtain, for any full set of prime-to- $\mathfrak{N}^{\#}$  integral representatives  $\{\mathfrak{a}\}$  of  $\mathcal{C}\ell(\mathcal{O}_K)$ ,

$$\begin{aligned} & \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a})(F_{i^{\#,*}\omega_f^{\#}})^{(pNN'/M)}(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)) \\ &= \left( \prod_{\ell | pNN'/M, \ell \nmid N} 1 - \frac{a_{\ell}(f)\chi^{-1}(\bar{v})}{\ell} + \frac{\chi^{-2}(\bar{v})}{\ell} \right) \\ & \quad \times \left( \prod_{\ell | pNN'/M, \ell | N} 1 - \frac{a_{\ell}(f)\chi^{-1}(\bar{v})}{\ell} \right) \\ & \quad \cdot \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a})F_{i^{\#,*}\omega_f^{\#}}(\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}], \omega)) \end{aligned}$$

and similarly for  $F_{i^{\#,*}\omega_g^{\#}}$ . Thus, by (15), we have

$$\begin{aligned} & \left( \prod_{\ell | pNN'/M, \ell \nmid N} 1 - \frac{a_{\ell}(f)\chi^{-1}(\bar{v})}{\ell} + \frac{\chi^{-2}(\bar{v})}{\ell} \right) \left( \prod_{\ell | pNN'/M, \ell | N} 1 - \frac{a_{\ell}(f)\chi^{-1}(\bar{v})}{\ell} \right) \\ & \quad \cdot \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a})F_{i^{\#,*}\omega_f^{\#}}([\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}])]) \\ & \equiv \left( \prod_{\ell | pNN'/M, \ell \nmid N} 1 - \frac{a_{\ell}(g)\chi^{-1}(\bar{v})}{\ell} + \frac{\chi^{-2}(\bar{v})}{\ell} \right) \\ & \quad \times \left( \prod_{\ell | pNN'/M, \ell | N} 1 - \frac{a_{\ell}(g)\chi^{-1}(\bar{v})}{\ell} \right) \\ & \quad \cdot \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \chi^{-1}(\mathfrak{a})F_{i^{\#,*}\omega_g^{\#}}([\mathfrak{a} \star (A, A[\mathfrak{N}^{\#}])]) \pmod{\lambda^m \mathcal{O}_{\mathbb{C}_p}}. \end{aligned}$$

By part (2) of Theorem 3.8, we have  $F_{i^{\#,*}\omega_f^{\#}} = i^{\#,*} \log_{\mathfrak{G}_{\omega_f^{\#}}}$  and  $F_{i^{\#,*}\omega_g^{\#}} = i^{\#,*} \log_{\mathfrak{G}_{\omega_g^{\#}}}$ . Thus, the above congruence becomes

$$\begin{aligned} & \left( \prod_{\ell | pNN'/M, \ell \nmid N} 1 - \frac{a_{\ell}(f)\chi^{-1}(\bar{v})}{\ell} + \frac{\chi^{-2}(\bar{v})}{\ell} \right) \\ & \quad \times \left( \prod_{\ell | pNN'/M, \ell | N} 1 - \frac{a_{\ell}(f)\chi^{-1}(\bar{v})}{\ell} \right) \log_{\omega_f^{\#}} P^{\#}(\chi) \end{aligned}$$

$$\begin{aligned} &\equiv \left( \prod_{\ell|pNN'/M, \ell \nmid N} 1 - \frac{a_\ell(g)\chi^{-1}(\bar{v})}{\ell} + \frac{\chi^{-2}(\bar{v})}{\ell} \right) \\ &\quad \times \left( \prod_{\ell|pNN'/M, \ell|N} 1 - \frac{a_\ell(g)\chi^{-1}(\bar{v})}{\ell} \right) \log_{\mathfrak{g}_g^\#} P^\#(\chi) \pmod{\lambda^m \mathcal{O}_{\mathbb{C}_p}}. \end{aligned}$$

Since both sides of this congruence belong to  $L_p$  and  $L_p \cap \mathcal{O}_{\mathbb{C}_p} = \mathcal{O}_{L_p}$ , this congruence, in fact, holds mod  $\lambda^m \mathcal{O}_{L_p}$ . The theorem now follows from the functoriality of the  $p$ -adic logarithm:

$$\log_{\omega_f^\#} P^\#(\chi) = \log_{\pi^{b,*}\omega_f} P^\#(\chi) = \log_{\omega_f} P(\chi) = \log_{\pi_f^* \omega_{A_f}} P(\chi) = \log_{\omega_{A_f}} P_f(\chi)$$

and similarly  $\log_{\mathfrak{g}_g^\#} P^\#(\chi) = \log_{\omega_{A_g}} P_g(\chi)$ . □

REMARK 3.10. The normalizations of  $\omega_E$  and  $\omega_{E'}$  in the statement of Theorem 1.16 *a priori* imply that both sides of Theorem 1.16 are  $p$ -integral. This is because CM points are integrally defined by the theory of CM and the above proof shows that the rigid analytic function  $\iota^{\#,*} \log_{\omega_f(pNN'/M)}$  has integral  $q$ -expansion.

Let  $\omega_E$  denote the canonical Néron differential of  $E$  (as we do in Section 5), and let  $c \in \mathbb{Z}$  such that  $\omega_E = c \cdot \omega_{E'}$ . Note that the normalization of the  $p$ -adic formal logarithm  $\log_{\omega_{E'}}$  above differs by a factor of  $c$  from that of the normalization  $\log_E := \log_{\omega_E}$ . So we know that

$$\frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_p)|}{p \cdot c} \cdot \log_E P = \frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_p)|}{p} \cdot \log_{\omega_{E'}} P$$

is  $p$ -integral. We remark that this is compatible with the  $p$ -part of the BSD conjecture. In fact, the  $p$ -part of the BSD conjecture predicts that  $P$  is divisible by  $p^{\text{ord}_p c} \cdot c_p(E)$  in  $E(K)$  (see the conjectured formula (59)) and so  $(|\tilde{E}^{\text{ns}}(\mathbb{F}_p)|)/c \cdot P$  lies in the formal group and, hence,  $(|\tilde{E}^{\text{ns}}(\mathbb{F}_p)|)/c \cdot \log_E P \in p\mathcal{O}_{K_p}$ .

REMARK 3.11. Note that both sides of the congruence in the statement of Theorem 3.9 depend on the choices of appropriate  $\mathfrak{N}, \mathfrak{N}'$  up to a sign  $\pm 1$ . In fact, for a rational prime  $\ell|N$  (respectively  $\ell|N'$ ), if we let  $v = (\mathfrak{N}, \ell)$  with complex conjugate prime ideal  $\bar{v}$  (respectively  $v' = (\mathfrak{N}', \ell)$  with complex conjugate prime ideal  $\bar{v}'$ ), replacing  $\mathfrak{N}$  with  $\mathfrak{N}v^{-1}\bar{v}$  (respectively  $\mathfrak{N}'$  with  $\mathfrak{N}'v'^{-1}\bar{v}'$ ) amounts to performing an Atkin–Lehner involution on the Heegner point  $P_f(\chi)$  (respectively  $P_g(\chi)$ ), which amounts to multiplying the Heegner point by the local root number  $w_\ell(A_f) \in \{\pm 1\}$  (respectively  $w_\ell(A_g) \in \{\pm 1\}$ ). Our proof, in fact, shows that for whatever change we make in choice of  $\mathfrak{N}$  (respectively  $\mathfrak{N}'$ ), both sides are multiplied by the same sign  $\pm 1$ .

**3.7. Proof of Theorem 1.16.** It follows immediately from Theorem 3.9 by taking  $\chi = \mathbf{1}$ ,  $L = K$ , and  $f$  and  $g$  to be associated with  $E$  and  $E'$ . The Heegner points  $P = P_f(\mathbf{1})$  and  $P' = P_g(\mathbf{1})$  are defined up to sign and torsion depending on the choices of  $\mathfrak{N}$  and  $\mathfrak{N}'$  (see [25]).

#### 4. Goldfeld's conjecture for a general class of elliptic curves

Our goal in this section is to prove Theorem 1.12. Throughout this section, we assume

$$E(\mathbb{Q})[2] = 0, \text{ or equivalently, } \text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3 \text{ or } \mathbb{Z}/3\mathbb{Z}.$$

Note that this assumption is mild and is satisfied by 100% of all elliptic curves (when ordered by naive height).

**4.1. Explicit twists.** Now we restrict our attention to the following well-chosen set of twisting discriminants.

**DEFINITION 4.1.** Given an imaginary quadratic field  $K$  satisfying the Heegner hypothesis for  $N$ , we define the set  $\mathcal{S}$  consisting of primes  $\ell \nmid 2N$  such that

- (1)  $\ell$  splits in  $K$ ;
- (2)  $\text{Frob}_\ell \in \text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$  has order 3.

We define  $\mathcal{N}$  to be the set of all integers  $d \equiv 1 \pmod{4}$  such that  $|d|$  is a square-free product of primes in  $\mathcal{S}$ .

**REMARK 4.2.** By Chebotarev's density theorem, the set of primes  $\mathcal{S}$  has Dirichlet density  $\frac{1}{6} = \frac{1}{2} \cdot \frac{1}{3}$  or  $\frac{1}{3} = \frac{1}{2} \cdot \frac{2}{3}$  depending on  $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$  or  $\mathbb{Z}/3\mathbb{Z}$ . In particular, there are infinitely many elements of  $\mathcal{N}$  with  $k$  prime factors for any fixed  $k \geq 1$ .

For  $d \in \mathcal{N}$ , we consider  $E^{(d)}/\mathbb{Q}$ , the quadratic twist of  $E/\mathbb{Q}$  by  $\mathbb{Q}(\sqrt{d})$ . Since  $d \equiv 1 \pmod{4}$ , we know that 2 is unramified in  $\mathbb{Q}(\sqrt{d})$  and  $E^{(d)}/\mathbb{Q}$  has conductor  $Nd^2$ . Hence,  $K$  also satisfies the Heegner hypothesis for  $Nd^2$ . Let  $P^{(d)} \in E^{(d)}(K)$  be the corresponding Heegner point. Since

$$E[2] \cong E^{(d)}[2],$$

we can apply Theorem 1.16 to  $E$  and  $E^{(d)}$ ,  $p = 2$  and obtain the following theorem.

**THEOREM 4.3.** *Suppose  $E/\mathbb{Q}$  is an elliptic curve with  $E(\mathbb{Q})[2] = 0$ . Let  $K$  be an imaginary quadratic field satisfying the Heegner hypothesis for  $N$ . Assume*

$$2 \text{ splits in } K \quad \text{and} \quad \frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_2)| \cdot \log_{\omega_E}(P)}{2} \not\equiv 0 \pmod{2}. \quad (\star)$$

Then for any  $d \in \mathcal{N}$ :

(1) *We have*

$$\frac{|\tilde{E}^{(d), \text{ns}}(\mathbb{F}_2)| \cdot \log_{\omega_{E^{(d)}}}(P^{(d)})}{2} \not\equiv 0 \pmod{2}.$$

*In particular,  $P^{(d)} \in E^{(d)}(K)$  is of infinite order and  $E^{(d)}/K$  has both algebraic and analytic rank one.*

(2) *The rank part of the BSD conjecture is true for  $E^{(d)}/\mathbb{Q}$  and  $E^{(d-d_K)}/\mathbb{Q}$ . One of them has both algebraic and analytic rank one and the other has both algebraic and analytic rank zero.*

(3)  *$E^{(d)}/\mathbb{Q}$  (respectively  $E^{(d-d_K)}/\mathbb{Q}$ ) has the same rank as  $E/\mathbb{Q}$  if and only if  $\psi_d(-N) = 1$  (respectively  $\psi_d(-N) = -1$ ), where  $\psi_d$  is the quadratic character associated with  $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ .*

#### 4.2. Proof of Theorem 4.3.

(1) We apply Theorem 1.16 to the two elliptic curves  $E/\mathbb{Q}$  and  $E^{(d)}/\mathbb{Q}$  and  $p = 2$ . Let  $\ell | Nd^2$  be a prime. Note

(a) if  $\ell | N$ ,

$$a_\ell(E), a_\ell(E^{(d)}) \in \{\pm 1\},$$

(b) if  $\ell^2 | N$ ,

$$a_\ell(E) = a_\ell(E^{(d)}) = 0,$$

(c) if  $\ell | d$ , we have  $\ell \in \mathcal{S}$ . Since  $\text{Frob}_\ell$  is order 3 on  $E[2]$ , we know that its trace

$$a_\ell(E) \equiv 1 \pmod{2}.$$

Since  $\ell^2 | Nd^2$ , we know that

$$a_\ell(E^{(d)}) = 0.$$

It follows that  $M = N^2$ . The congruence formula in Theorem 1.16 then reads

$$\begin{aligned} & \frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_2)|}{2} \cdot \prod_{\ell|d} \frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_\ell)|}{\ell} \cdot \log_{\omega_E} P \\ & \equiv \frac{|\tilde{E}^{(d),\text{ns}}(\mathbb{F}_2)|}{2} \cdot \prod_{\ell|d} \frac{|\tilde{E}^{(d),\text{ns}}(\mathbb{F}_\ell)|}{\ell} \cdot \log_{\omega_{E^{(d)}}} P^{(d)} \pmod{2}. \end{aligned}$$

Since  $E$  has good reduction at  $\ell \mid d$  and  $\ell$  is odd, we have

$$|\tilde{E}^{\text{ns}}(\mathbb{F}_\ell)| = |E(\mathbb{F}_\ell)| = \ell + 1 - a_\ell(E) \equiv a_\ell(E) \equiv 1 \pmod{2}.$$

Since  $E^{(d)}$  has additive reduction at  $\ell \mid d$  and  $\ell$  is odd, we have

$$|\tilde{E}^{(d),\text{ns}}(\mathbb{F}_\ell)| = \ell \equiv 1 \pmod{2}.$$

Therefore, we obtain the congruence

$$\frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_2)| \cdot \log_{\omega_E} P}{2} \equiv \frac{|\tilde{E}^{(d),\text{ns}}(\mathbb{F}_2)| \cdot \log_{\omega_{E^{(d)}}} P^{(d)}}{2} \pmod{2}.$$

Assumption (★) says that the left-hand side is nonzero; hence, the right-hand side is also nonzero. In particular, the Heegner point  $P^{(d)}$  is of infinite order. The last assertion follows from the celebrated work of Gross–Zagier and Kolyagin.

(2) Since

$$L(E^{(d)}/K, s) = L(E^{(d)}/\mathbb{Q}, s) \cdot L(E^{(d \cdot d_K)}/\mathbb{Q}, s),$$

the sum of the analytic rank of  $E^{(d)}/\mathbb{Q}$  and  $E^{(d \cdot d_K)}/\mathbb{Q}$  is equal to the analytic rank of  $E^{(d)}/K$ , which is one by the first part. Hence, one of them has analytic rank one and the other has analytic rank zero. The remaining claims follow from Gross–Zagier and Kolyagin.

(3) It is well known that the global root numbers of quadratic twists are related by

$$\varepsilon(E/\mathbb{Q}) \cdot \varepsilon(E^{(d)}/\mathbb{Q}) = \psi_d(-N).$$

It follows that  $E^{(d)}/\mathbb{Q}$  and  $E/\mathbb{Q}$  have the same global root number if and only if  $\psi_d(-N)=1$ . Since the analytic ranks of  $E^{(d)}/\mathbb{Q}$  and  $E/\mathbb{Q}$  are at most one, the equality of global root numbers implies the equality of the analytic ranks.

**4.3. Proof of Theorem 1.12.** This is a standard application of Ikehara's tauberian theorem (see, for example, [71, 2.4]). We include the argument for completeness. Since the set of primes  $\mathcal{S}$  has Dirichlet density  $\alpha = \frac{1}{6}$  or  $\frac{1}{3}$  depending on  $\text{Gal}(\mathbb{Q}(E[2]/\mathbb{Q})) \cong S_3$  or  $\mathbb{Z}/3\mathbb{Z}$ , we know that

$$\sum_{\ell \in \mathcal{S}} \ell^{-s} \sim \alpha \cdot \log \frac{1}{s-1}, \quad s \rightarrow 1^+.$$

Then,

$$\log \left( \sum_{d \in \mathcal{N}} |d|^{-s} \right) = \log \left( \prod_{\ell \in \mathcal{S}} (1 + \ell^{-s}) \right) \sim \sum_{\ell \in \mathcal{S}} \ell^{-s} \sim \alpha \cdot \log \frac{1}{s-1}, \quad s \rightarrow 1^+.$$

Hence,

$$\sum_{d \in \mathcal{N}} |d|^{-s} = \frac{1}{(s-1)^\alpha} \cdot f(s)$$

for some function  $f(s)$  holomorphic and nonzero when  $\Re(s) \geq 1$ . It follows from Ikehara's tauberian theorem that

$$\#\{d \in \mathcal{N} : |d| < X\} \sim c \cdot \frac{X}{\log^{1-\alpha} X}, \quad X \rightarrow \infty$$

for some constant  $c > 0$ . But by Theorem 4.3(2), we have for  $r = 0, 1$ ,

$$N_r(E, X) \geq \#\{d \in \mathcal{N} : |d| < X/|d_K|\}.$$

The results then follow.

## 5. The 2-part of the BSD conjecture

In this section, we aim to prove the following consequence on BSD(2) when  $r \leq 1$  for all the explicit quadratic twists under consideration, at least when the local Tamagawa number at 2 is odd.

**THEOREM 5.1.** *Let  $E/\mathbb{Q}$  be an elliptic curve with  $E(\mathbb{Q})[2] = 0$ . Assume that there is an imaginary quadratic field  $K$  satisfying the Heegner hypothesis for  $N$  and Assumption (★). Further assume that the local Tamagawa number  $c_2(E)$  is odd. If  $E$  has additive reduction at 2, further assume that its Manin constant is odd. Let  $\mathcal{N}$  be as in Definition 4.1.*

- (1) *If BSD(2) is true for  $E/K$ , then BSD(2) is true for  $E^{(d)}/K$ , for any  $d \in \mathcal{N}$ .*
- (2) *If BSD(2) is true for  $E/\mathbb{Q}$  and  $E^{(d_K)}/\mathbb{Q}$ , then BSD(2) is true for  $E^{(d)}/\mathbb{Q}$  and  $E^{(d \cdot d_K)}/\mathbb{Q}$ , for any  $d \in \mathcal{N}$  such that  $\psi_d(-N) = 1$ .*

REMARK 5.2. BSD(2) for a single elliptic curve (of small conductor) can be proved by numerical calculation when  $r \leq 1$  (see [51] for curves of conductor at most 5000). Theorem 5.1 then allows one to deduce BSD(2) for many of its quadratic twists (of arbitrarily large conductor). See Section 6 for examples.

REMARK 5.3. Manin's conjecture asserts that the Manin constant for any optimal curve is 1, which would imply that the Manin constant for  $E$  is odd since  $E$  is assumed to have no rational 2-torsion. Cremona has proved Manin's conjecture for all optimal curves of conductor at most 380 000 (see [2, Theorem 2.6] and the update at <http://johncremona.github.io/ecdata/#optimality>).

**5.1. The strategy of the proof.** Under Assumption (★) and the assumption that  $c_2(E)$  is odd, the Heegner point  $P \in E(K)$  is *indivisible by 2* (Lemma 5.4), equivalently, all the local Tamagawa numbers of  $E$  are odd, and the 2-Selmer group  $\text{Sel}_2(E/K)$  has rank one (Corollary 5.5). We are able to deduce that all the local Tamagawa numbers of  $E^{(d)}$  are also odd (Lemma 10.12), and  $\text{Sel}_2(E^{(d)}/K)$  also has rank one (Lemma 5.9). These are consequences of the primes in the well-chosen set  $\mathcal{S}$  being *silent* in the sense of Mazur–Rubin [49]. Note that  $\text{Sel}_2(E^{(d)}/K)$  having rank one predicts that  $E^{(d)}(K)$  has rank one and  $\text{III}(E^{(d)}/K)[2]$  is trivial, though it is not known in general how to show this directly (Remark 1.14). The advantage here is that we know *a priori* from the mod 2 congruence that the Heegner point  $P^{(d)} \in E^{(d)}(K)$  is also *indivisible by 2*. Hence, the prediction is indeed true and implies BSD(2) for  $E^{(d)}/K$  (Corollary 5.8).

Since the Iwasawa main conjecture is not known for  $p = 2$ , the only known way to prove BSD(2) over  $\mathbb{Q}$  is to compute the 2-part of both sides of (2) explicitly. We compute the 2-Selmer group  $\text{Sel}_2(E^{(d)}/\mathbb{Q})$  (Lemma 5.10) and compare this to a formula of Zhai [89] (based on modular symbols) for 2-part of algebraic  $L$ -values for rank-zero twists. This allows us to deduce BSD(2) for the rank-zero curve among  $E^{(d)}$  and  $E^{(d \cdot d_K)}$  (Lemma 5.12). Finally, BSD(2) for  $E^{(d)}/K$  and BSD(2) for the rank-zero curve together imply BSD(2) for the rank-one curve between  $E^{(d)}$  and  $E^{(d \cdot d_K)}$ .

**5.2. BSD(2) for  $E/K$ .** Let  $E$  and  $K$  be as in Theorem 5.1. By the Gross–Zagier formula, the BSD conjecture for  $E/K$  is equivalent to the equality [28, V.2.2]

$$u_K \cdot c_E \cdot \prod_{\ell|N} c_\ell(E) \cdot |\text{III}(E/K)|^{1/2} = [E(K) : \mathbb{Z}P], \quad (16)$$

where  $u_K = |\mathcal{O}_K^\times / \{\pm 1\}|$ ,  $c_E$  is the Manin constant of  $E/\mathbb{Q}$ ,  $c_\ell(E) = [E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell)]$  is the local Tamagawa number of  $E$  and  $[E(K) : \mathbb{Z}P]$  is the index of the Heegner point  $P \in E(K)$ . By Assumption (★) that 2 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  $E/K$  is equivalent to the equality

$$\prod_{\ell|N} c_\ell(E) \cdot |\text{III}(E/K)|^{1/2} = \frac{[E(K) : \mathbb{Z}P]}{c_E}. \tag{17}$$

LEMMA 5.4. *The right-hand side of (17) is a 2-adic unit.*

*Proof.* Since  $\mathbb{Q}(E[2])/\mathbb{Q}$  is an  $S_3$  or  $\mathbb{Z}/3\mathbb{Z}$  extension, we know that the Galois representation  $E[2]$  remains irreducible when restricted to any quadratic field; hence,  $E(K)[2] = 0$ .

Note that the Manin constant  $c_E$  is odd: it follows from [1, Theorem A] when  $E$  is good at 2, from [1, page 270(ii)] when  $E$  is multiplicative at 2 since  $c_2(E)$  is assumed to be odd and by our extra assumption when  $E$  is additive at 2.

Since  $c_E$  is odd, we know that the right-hand side of (17) is 2-adically integral. If it is not a 2-adic unit, then there exists some  $Q \in E(K)$  such that  $2Q$  is an odd multiple of  $P$ . Let  $\omega_E$  be the Néron differential of  $E$  and let  $\log_E := \log_{\omega_E}$ . By the very definition of the Manin constant, we have  $c_E \cdot \omega_E = \omega_E$  and  $c_E \cdot \log_{\omega_E} = \log_E$ . Hence, up to a 2-adic unit, we have

$$\frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_2)| \cdot \log_{\omega_E} P}{2} = \frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_2)| \cdot \log_E P}{2} = |\tilde{E}^{\text{ns}}(\mathbb{F}_2)| \cdot \log_E(Q).$$

On the other hand,  $c_2(E) \cdot |\tilde{E}^{\text{ns}}(\mathbb{F}_2)| \cdot Q$  lies in the formal group  $\hat{E}(2\mathcal{O}_{K_2})$  and  $c_2(E)$  is assumed to be odd; we know that

$$|\tilde{E}^{\text{ns}}(\mathbb{F}_2)| \cdot \log_E(Q) \in 2\mathcal{O}_{K_2},$$

which contradicts (★). So the right-hand side of (17) is a 2-adic unit. □

Since the left-hand side of (17) is a product of integers, Lemma 5.4 implies the following.

COROLLARY 5.5. *BSD(2) for  $E/K$  is equivalent to the following:*

*all the local Tamagawa numbers  $c_\ell(E)$  are odd and  $\text{III}(E/K)[2] = 0$ .*

**5.3. BSD(2) for  $E^{(d)}/K$ .** Let  $d \in \mathcal{N}$ . The BSD conjecture for  $E^{(d)}/K$  is equivalent to the equality

$$\prod_{\ell|Nd^2} c_\ell(E^{(d)}) \cdot |\text{III}(E^{(d)}/K)|^{1/2} = \frac{[E^{(d)}(K) : \mathbb{Z}P^{(d)}]}{c_{E^{(d)}}}. \tag{18}$$

LEMMA 5.6. Assume that BSD(2) is true for  $E/K$ . Then  $c_\ell(E^{(d)})$  is odd for any  $\ell \mid Nd^2$ .

*Proof.* First consider  $\ell \mid N$ . Let  $\mathcal{E}$  and  $\mathcal{E}^{(d)}$  be the Néron model over  $\mathbb{Z}_\ell$  of  $E$  and  $E^{(d)}$ , respectively. Note that  $E^{(d)}/\mathbb{Q}_p$  is the unramified quadratic twist of  $E^{(d)}$ . Since Néron models commute with unramified base change, we know that the component groups  $\Phi_{\mathcal{E}}$  and  $\Phi_{\mathcal{E}^{(d)}}$  are quadratic twists of each other as  $\text{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ -modules. In particular,  $\Phi_{\mathcal{E}}[2] \cong \Phi_{\mathcal{E}^{(d)}}[2]$  as  $\text{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ -modules and thus,

$$\Phi_{\mathcal{E}}(\mathbb{F}_\ell)[2] \cong \Phi_{\mathcal{E}^{(d)}}(\mathbb{F}_\ell)[2].$$

It follows that  $c_\ell(E)$  and  $c_\ell(E^{(d)})$  have the same parity.

Next consider  $\ell \mid d$ . Since  $E^{(d)}$  has additive reduction and  $\ell$  is odd, we know that

$$E^{(d)}(\mathbb{Q}_\ell)[2] \cong \Phi_{\mathcal{E}^{(d)}}(\mathbb{F}_\ell)[2].$$

Since  $\ell \in \mathcal{S}$ ,  $\text{Frob}_\ell$  is assumed to have order 3 acting on  $E^{(d)}[2] \cong E[2]$ , we know that  $E^{(d)}(\mathbb{Q}_\ell)[2] = 0$ . Hence,  $c_\ell(E^{(d)})$  is odd. □

LEMMA 5.7. Assume that BSD(2) is true for  $E/K$ . The right-hand side of (18) is a 2-adic unit.

*Proof.* Since  $E$  has no rational 2-torsion, we know that the Manin constants (with respect to both  $X_0(N)$ -parametrization and  $X_1(N)$ -parametrization) for all curves in the isogeny of  $E$  have the same 2-adic valuation. The twisting argument of Stevens [78, Section 5] shows that if the Manin constant  $c_1$  for the  $X_1(N)$ -optimal curve in the isogeny class of  $E$  is 1, then the Manin constant  $c_1^{(d)}$  for the  $X_1(N)$ -optimal curve in the isogeny class of  $E^{(d)}$  is also 1. The same twisting argument in fact shows that if  $c_1$  is a 2-adic unit, then  $c_1^{(d)}$  is also a 2-adic unit. Since  $c_E$  is odd, we know that  $c_1$  is odd; therefore,  $c_1^{(d)}$  is also odd. Since  $E^{(d)}$  has no rational 2-torsion, it follows that the Manin constant  $c_{E^{(d)}}$  is also odd.

Now using  $c_2(E^{(d)})$  is odd (by Lemma 10.12) and  $c_{E^{(d)}}$  is odd, and replacing  $E$  by  $E^{(d)}$  and replacing (★) by the conclusion of Theorem 4.3(1), the same argument as in the proof of Lemma 5.4 shows that the right-hand side of (18) is also a 2-adic unit. □

Again, since the left-hand side of (18) is a product of integers, Lemma 5.7 implies the following.

**COROLLARY 5.8.** *BSD(2) for  $E^{(d)}/K$  is equivalent to the following:*

*all the local Tamagawa numbers  $c_\ell(E^{(d)})$  are odd and  $\text{III}(E^{(d)}/K)[2] = 0$ .*

**5.4. 2-Selmer groups over  $K$ .** Now let us compare the 2-Selmer groups of  $E/K$  and  $E^{(d)}/K$ .

**LEMMA 5.9.** *Assume that BSD(2) is true for  $E/K$ . The isomorphism of Galois representations  $E[2] \cong E^{(d)}[2]$  induces an isomorphism of 2-Selmer groups*

$$\text{Sel}_2(E/K) \cong \text{Sel}_2(E^{(d)}/K).$$

*In particular,*

$$\text{III}(E^{(d)}/K)[2] = 0.$$

*Proof.* The 2-Selmer group  $\text{Sel}_2(E/K)$  is defined by the local Kummer conditions

$$\mathcal{L}_v(E/K) = \text{im}(E(K_v)/2E(K_v) \rightarrow H^1(K_v, E[2])).$$

Denote by  $\mathcal{L}_v(E^{(d)}/K)$  the local Kummer conditions for  $E^{(d)}/K$ . It suffices to show that  $\mathcal{L}_v(E/K) = \mathcal{L}_v(E^{(d)}/K)$  are the same at all places  $v$  of  $K$ :

- (1)  $v \mid \infty$ : Since  $v$  is complex,  $H^1(K_v, E[2]) = 0$ . So  $\mathcal{L}_v(E/K) = \mathcal{L}_v(E^{(d)}/K) = 0$ .
- (2)  $v \mid d$ : Suppose  $v$  lies above  $\ell \in \mathcal{S}$ . Since  $\text{Frob}_\ell$  acts by order 3 on  $E[2]$ , we know that the unramified cohomology

$$H_{\text{ur}}^1(\mathbb{Q}_\ell, E[2]) \cong E[2]/(\text{Frob}_\ell - 1)E[2] = 0$$

(such  $\ell$  is called *silent* by Mazur–Rubin), and thus  $\dim H^1(\mathbb{Q}_\ell, E[2]) = 2 \dim H_{\text{ur}}^1(\mathbb{Q}_\ell, E[2]) = 0$  ([52, I.2.6]). Since  $\ell$  is split in  $K$ , it follows that

$$H^1(K_v, E[2]) \cong H^1(\mathbb{Q}_\ell, E[2]) = 0.$$

So  $\mathcal{L}_v(E/K) = \mathcal{L}_v(E^{(d)}/K) = 0$ .

- (3)  $v \nmid d\infty$ : By [48, Lemma 2.9], we have

$$\mathcal{L}_v(E/K) \cap \mathcal{L}_v(E^{(d)}/K) = E_{\mathbb{N}}(K_v)/2E(K_v),$$

where

$$E_{\mathbb{N}}(K_v) = \text{im}(\mathbb{N} : E(L_v) \rightarrow E(K_v))$$

is the image of the norm map induced from the quadratic extension  $L_v = K_v(\sqrt{d})$  over  $K_v$ . To show that  $\mathcal{L}_v(E/K) = \mathcal{L}_v(E^{(d)}/K)$ , it suffices to show that

$$E(K_v)/\mathbb{N}E(L_v) = 0.$$

By local Tate duality, it suffices to show that

$$H^1(\text{Gal}(L_v/K_v), E(L_v)) = 0.$$

Note that  $K_v \cong \mathbb{Q}_\ell$  and  $L_v/K_v$  is the unramified quadratic extension; we know that

$$E(L_v)/E^0(L_v) \cong \Phi_{\mathcal{E}}(\mathbb{F}_{\ell^2}),$$

where  $\Phi_{\mathcal{E}}$  is the component group of the Néron model of  $E$  over  $\mathbb{Z}_\ell$ . Let  $c \in \text{Gal}(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell)$  be the order 2 automorphism, then  $\Phi_{\mathcal{E}}(\mathbb{F}_{\ell^2})[2]^c = \Phi_{\mathcal{E}}(\mathbb{F}_\ell)[2]$ . Since  $c_\ell(E)$  is odd, it follows that  $\Phi_{\mathcal{E}}(\mathbb{F}_{\ell^2})[2]^c = \Phi_{\mathcal{E}}(\mathbb{F}_\ell)[2] = 0$ . Since an order 2 automorphism on a nonzero  $\mathbb{F}_2$ -vector space must have a nonzero fixed vector, we know that  $\Phi_{\mathcal{E}}(\mathbb{F}_{\ell^2})[2] = 0$ . Therefore,  $E(L_v)/E^0(L_v)$  has odd order. It remains to show that

$$H^1(\text{Gal}(L_v/K_v), E^0(L_v)) = 0,$$

which is true by Lang's theorem since  $L_v/K_v$  is unramified (see [50, Proposition 4.3]).  $\square$

**5.5. Proof of Theorem 5.1(1).** It follows immediately from Corollary 5.8 and Lemmas 10.12 and 5.9.

**5.6. 2-Selmer groups over  $\mathbb{Q}$ .** Let us compare the 2-Selmer groups of  $E/\mathbb{Q}$  and  $E^{(d)}/\mathbb{Q}$ .

LEMMA 5.10. *Let  $\Delta(E)$  be the discriminant of a Weierstrass equation of  $E/\mathbb{Q}$ .*

- (1) *If  $\Delta(E) < 0$ , then  $\text{Sel}_2(E/\mathbb{Q}) \cong \text{Sel}_2(E^{(d)}/\mathbb{Q})$ .*
- (2) *If  $\Delta(E) > 0$  and  $d > 0$ , then  $\text{Sel}_2(E/\mathbb{Q}) \cong \text{Sel}_2(E^{(d)}/\mathbb{Q})$ .*
- (3) *If  $\Delta(E) > 0$  and  $d < 0$ , then  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/\mathbb{Q})$  and  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^{(d)}/\mathbb{Q})$  differ by 1.*

*Proof.* By the same proof as Lemma 5.9, we know that  $\mathcal{L}_v(E/\mathbb{Q}) = \mathcal{L}_v(E^{(d)}/\mathbb{Q})$  for any place  $v \nmid \infty$  of  $\mathbb{Q}$ . The only issue is that the local condition at  $\infty$  may

differ for  $E/\mathbb{Q}$  and  $E^{(d)}/\mathbb{Q}$ . By [70, page 305], we have  $\mathbb{Q}(\sqrt{\Delta(E)}) \subseteq \mathbb{Q}(E[2])$ . So complex conjugation acts nontrivially on  $E[2]$  if and only if  $\Delta(E) < 0$ . Hence,

$$\dim_{\mathbb{R}_2} H^1(\text{Gal}(\mathbb{C}/\mathbb{R}), E[2]) = \begin{cases} 0, & \Delta(E) < 0, \\ 2, & \Delta(E) > 0. \end{cases}$$

Item (3) follows immediately. When  $\Delta(E) > 0$ ,  $\mathcal{L}_\infty(E/\mathbb{Q}) = E(\mathbb{R})/2E(\mathbb{R})$  and  $\mathcal{L}_\infty(E^{(d)}/\mathbb{R}) = E^{(d)}(\mathbb{R})/2E^{(d)}(\mathbb{R})$  define the same line in  $H^1(\text{Gal}(\mathbb{C}/\mathbb{R}), E[2])$  if and only if  $d > 0$ . Item (2) follows immediately and item (3) follows from a standard application of global duality (for example, by [43, Lemma 8.5]).  $\square$

We immediately obtain a more explicit description of the condition  $\psi_d(-N) = 1$  in Theorem 4.3(3) under our extra assumption that  $c_2(E)$  is odd.

**COROLLARY 5.11.** *The following conditions are equivalent:*

- (1)  $E^{(d)}/\mathbb{Q}$  has the same rank as  $E/\mathbb{Q}$ .
- (2)  $\psi_d(-N) = 1$ , where  $\psi_d$  is the quadratic character associated with  $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ .
- (3)  $\Delta(E) < 0$ , or  $\Delta(E) > 0$  and  $d > 0$ .

*Proof.* Since the parity conjecture for 2-Selmer groups of elliptic curves is known [54, Theorem 1.5], we know that  $E/\mathbb{Q}$  and  $E^{(d)}/\mathbb{Q}$  have the same root number if and only if they have the same 2-Selmer rank. The result then follows from Lemma 5.10 and Theorem 4.3(3).  $\square$

**5.7. Rank-zero twists.** Let  $K$  be as in Theorem 5.1. We now verify BSD(2) for the rank-zero twists.

**LEMMA 5.12.** *If BSD(2) is true for  $E/\mathbb{Q}$  and  $E^{(d_K)}/\mathbb{Q}$ , then BSD(2) is true for all twists  $E^{(d)}/\mathbb{Q}$  and  $E^{(d-d_K)}/\mathbb{Q}$  of rank zero, where  $d \in \mathcal{N}$  with  $\psi_d(-N) = 1$ .*

*Proof.* Note exactly that one of  $E/\mathbb{Q}$  and  $E^{(d_K)}/\mathbb{Q}$  has rank zero. Consider the case that  $E/\mathbb{Q}$  has rank zero. Since all the local Tamagawa numbers  $c_\ell(E)$  are odd and  $\text{III}(E/\mathbb{Q})[2] = 0$ , BSD(2) for  $E/\mathbb{Q}$  implies that

$$\frac{L(E/\mathbb{Q}, 1)}{\Omega(E/\mathbb{Q})}$$

is a 2-adic unit. Assume that  $\psi_d(-N) = 1$ . We know from Corollary 5.11 that  $\Delta(E) < 0$ , or  $\Delta(E) > 0$  and  $d > 0$ . Under these conditions, it follows from [89, Theorems 1.1 and 1.3] that

$$\frac{L(E^{(d)}/\mathbb{Q}, 1)}{\Omega(E^{(d)}/\mathbb{Q})}$$

is also a 2-adic unit (note that the Néron period  $\Omega(E/\mathbb{Q})$  is twice the real period when  $\Delta(E) > 0$ ). Since all the local Tamagawa numbers  $c_\ell(E^{(d)})$  are odd (Lemma 10.12) and  $\text{III}(E^{(d)}/\mathbb{Q})[2] = 0$  (Lemma 5.11, (3, 2)), we know that BSD(2) is true for  $E^{(d)}/\mathbb{Q}$ . By the same argument, if  $E^{(d_K)}/\mathbb{Q}$  has rank zero and  $\psi_d(-N) = 1$ , we know that BSD(2) is true for  $E^{(d_K)}/\mathbb{Q}$ .  $\square$

**5.8. Proof of Theorem 5.1(2).** Now we can finish the proof of Theorem 5.1(2). Because the abelian surface  $E \times E^{(d_K)}/\mathbb{Q}$  is isogenous to the Weil restriction  $\text{Res}_{K/\mathbb{Q}} E$  and the validity of the BSD conjecture for abelian varieties is invariant under isogeny [53, I.7.3], we know that BSD(2) for  $E/\mathbb{Q}$  and  $E^{(d_K)}/\mathbb{Q}$  implies that BSD(2) is true for  $E/K$ . Hence, by Theorem 5.1(2), BSD(2) is true for  $E^{(d)}/\mathbb{Q}$ . By Lemma 5.12, BSD(2) is true for the rank-zero curve between  $E^{(d)}/\mathbb{Q}$  and  $E^{(d_K)}/\mathbb{Q}$  for  $d \in \mathcal{N}$  such that  $\psi_d(-N) = 1$ . Then again by the invariance of BSD(2) under isogeny, we know that BSD(2) is also true for the other rank-one curve between  $E^{(d)}/\mathbb{Q}$  and  $E^{(d_K)}/\mathbb{Q}$ .

## 6. Examples

In this section, we illustrate our application to Goldfeld's conjecture and the 2-part of the BSD conjecture in Sections 4 and 5 by providing examples of  $E/\mathbb{Q}$  and  $K$  which satisfy Assumption (★).

Let us first consider curves  $E/\mathbb{Q}$  of rank one.

EXAMPLE 6.1. Consider the curve 37a1 in Cremona's table,

$$E = 37a1 : y^2 + y = x^3 - x.$$

It is the rank-one optimal curve over  $\mathbb{Q}$  of smallest conductor ( $N = 37$ ). Take

$$K = \mathbb{Q}(\sqrt{-7}),$$

the imaginary quadratic field with smallest  $|d_K|$  satisfying the Heegner hypothesis for  $N$  such that 2 is split in  $K$ . The Heegner point

$$P = (0, 0) \in E(K)$$

generates  $E(\mathbb{Q}) = E(K) \cong \mathbb{Z}$ . Since  $E$  is optimal with Manin constant 1, we know that  $\omega_E$  is equal to the Néron differential. The formal logarithm associated with  $\omega_E$  is

$$\log_{\omega_E}(t) = t + 1/2 \cdot t^4 - 2/5 \cdot t^5 + 6/7 \cdot t^7 - 3/2 \cdot t^8 + 2/3 \cdot t^9 + \dots$$

We have  $|\tilde{E}(\mathbb{F}_2)| = 5$ , and the point  $5P = (1/4, -5/8)$  reduces to  $\infty \in \tilde{E}(\mathbb{F}_2)$ . Plugging in the parameter  $t = -x(5P)/y(5P) = 2/5$ , we know that up to a 2-adic unit,

$$\log_{\omega_E} P = \log_{\omega_E} 5P = 2 + 2^5 + 2^6 + 2^8 + 2^9 + \dots \in 2\mathbb{Z}_2^\times.$$

Hence,

$$\frac{|\tilde{E}(\mathbb{F}_2)| \cdot \log_{\omega_E} P}{2} \in \mathbb{Z}_2^\times$$

and (★) is satisfied. The set  $\mathcal{N}$  consists of square-free products of the signed primes

$$-11, 53, -71, -127, 149, 197, -211, -263, 337, -359, 373, -379, -443, \\ -571, -599, 613, \dots$$

For any  $d \in \mathcal{N}$ , we deduce the following:

- (1) The rank part of BSD conjecture is true for  $E^{(d)}$  and  $E^{(-7d)}$  by Theorem 4.3.
- (2) Since  $\Delta(E) > 0$ , we know from Corollary 5.11 that

$$\begin{cases} \text{rank } E^{(d)}(\mathbb{Q}) = 1, & \text{rank } E^{(-7d)}(\mathbb{Q}) = 0, & d > 0, \\ \text{rank } E^{(d)}(\mathbb{Q}) = 0, & \text{rank } E^{(-7d)}(\mathbb{Q}) = 1, & d < 0. \end{cases}$$

- (3) Since  $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$ , it follows from Theorem 1.12 that

$$N_r(E, X) \gg \frac{X}{\log^{5/6} X}, \quad r = 0, 1.$$

- (4) Since BSD(2) is true for  $E/\mathbb{Q}$  and  $E^{(-7)}/\mathbb{Q}$  by numerical verification, it follows from Theorem 5.1 that the BSD(2) is true for  $E^{(d)}$  and  $E^{(-7d)}$  when  $d > 0$ .

EXAMPLE 6.2. As we saw in Section 5, a necessary condition for (★) is that the local Tamagawa numbers  $c_p(E)$  are all odd for  $p \neq 2$ . Another necessary condition is that the formal group of  $E$  at 2 cannot be isomorphic to  $\mathbb{G}_m$ ; this is due to the usual subtlety that the logarithm on  $\mathbb{G}_m$  sends  $1 + 2\mathbb{Z}_2$  into  $4\mathbb{Z}_2$

(rather than  $2\mathbb{Z}_2$ ). We search for rank-one optimal elliptic curves with  $E(\mathbb{Q})[2] = 0$  satisfying these two necessary conditions. There are 38 such curves of conductor  $\leq 300$ . For each curve, we choose  $K$  with smallest  $|d_K|$  satisfying the Heegner hypothesis for  $N$  and such that 2 is split in  $K$ . Then 31 out of 38 curves satisfy (★); see Table 1. The first three columns list  $E$ ,  $d_K$  and the local Tamagawa number  $c_2(E)$  at 2, respectively. A check mark in the last column means that (★) holds, in which case Theorems 4.3 and 1.12 apply and the improved bound toward Goldfeld's conjecture holds. If  $c_2(E)$  is further odd (true for 23 out of 31), then the application to BSD(2) (Theorem 5.1) also applies.

REMARK 6.3. There is one CM elliptic curve in Table 1: namely  $E = 243a1$  with  $j$ -invariant 0, which seems to be only  $j$ -invariant of CM elliptic curves over  $\mathbb{Q}$  for which (★) holds.

Next let us consider curves  $E/\mathbb{Q}$  of rank zero.

EXAMPLE 6.4. Consider

$$E = X_0(11) = 11a1 : y^2 + y = x^3 - x^2 - 10x - 20,$$

the optimal elliptic curve over  $\mathbb{Q}$  of smallest conductor ( $N = 11$ ). Take

$$K = \mathbb{Q}(\sqrt{-7}),$$

the imaginary quadratic field with smallest  $|d_K|$  satisfying the Heegner hypothesis for  $N$  such that 2 is split in  $K$ . The Heegner point

$$P = \left(-\frac{1}{2}\sqrt{-7} + \frac{1}{2}, -2\sqrt{-7} - 2\right) \in E(K)$$

generates the free part of  $E(K)$ . Since  $E$  is optimal with Manin constant 1, we know that  $\omega_E$  is equal to the Néron differential. The formal logarithm associated with  $\omega_E$  is

$$\log_{\omega_E}(t) = t - 1/3 \cdot t^3 + 1/2 \cdot t^4 - 19/5 \cdot t^5 - t^6 + 5/7 \cdot t^7 - 27/2 \cdot t^8 + 691/9 \cdot t^9 + \dots$$

We have  $|\tilde{E}(\mathbb{F}_2)| = 5$  and the point  $5P = (-\frac{3}{4}, -\frac{11}{8}\sqrt{-7} - \frac{1}{2})$  reduces to  $\infty \in \tilde{E}(\mathbb{F}_2)$ . The prime 2 splits in  $K$  as

$$(2) = \left(-\frac{1}{2}\sqrt{-7} + \frac{1}{2}\right) \cdot \left(\frac{1}{2}\sqrt{-7} + \frac{1}{2}\right)$$

and the parameter  $t = -x(5P)/y(5P)$  has valuation 1 for both primes above 2. Plugging in  $t$ , we find that

$$\log_{\omega_E} P \in 2\mathcal{O}_{K_2}^\times.$$

Table 1. Assumption (★) for rank-one curves.

$E$	$d_K$	$c_2(E)$	★	$E$	$d_K$	$c_2(E)$	★
37a1	-7	1	✓	148a1	-7	3	✓
43a1	-7	1	✓	152a1	-15	4	✓
88a1	-7	4	✓	155a1	-79	1	✓
91a1	-55	1	✓	155c1	-79	1	✓
91b1	-55	1	✓	163a1	-7	1	✓
92b1	-7	3	✓	172a1	-7	3	✓
101a1	-23	1	✓	176c1	-7	2	✓
123a1	-23	1	✓	184a1	-7	2	✓
123b1	-23	1	✓	184b1	-7	2	✓
124a1	-15	3	✓	189a1	-47	1	✓
131a1	-23	1	✓	189b1	-47	1	✓
141a1	-23	1	✓	196a1	-31	3	✓
141d1	-23	1	✓	197a1	-7	1	
		$E$	$d_K$	$c_2(E)$	★		
		208a1	-23	4			
		208b1	-23	4			
		212a1	-7	3			
		216a1	-23	4	✓		
		219a1	-23	1	✓		
		219b1	-23	1	✓		
		232a1	-7	2			
		236a1	-23	3			
		243a1	-23	1	✓		
		244a1	-15	3			
		248a1	-15	2	✓		
		248c1	-15	2	✓		

Hence,

$$\frac{|\tilde{E}(\mathbb{F}_2)| \cdot \log_{\omega_E} P}{2} \in \mathcal{O}_{K_2}^\times$$

and (★) is satisfied. The set  $\mathcal{N}$  consists of square-free products of the signed primes

$$-23, 37, -67, -71, 113, 137, -179, -191, 317, -331, -379, 389, -443, 449, -463, -487, -631, \dots$$

For any  $d \in \mathcal{N}$ , we deduce the following:

- (1) The rank part of BSD conjecture is true for  $E^{(d)}$  and  $E^{(-7d)}$  by Theorem 4.3.

(2) Since  $\Delta(E) < 0$ , we know from Corollary 5.11 that

$$\text{rank } E^{(d)}(\mathbb{Q}) = 0, \quad \text{rank } E^{(-7d)}(\mathbb{Q}) = 1.$$

(3) Since  $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$ , it follows from Theorem 1.12 that

$$N_r(E, X) \gg \frac{X}{\log^{5/6} X}, \quad r = 0, 1.$$

(4) Since BSD(2) is true for  $E/\mathbb{Q}$  and  $E^{(-7)}/\mathbb{Q}$  by numerical verification, it follows from Theorem 5.1 that the BSD(2) is true for  $E^{(d)}$  and  $E^{(-7d)}$ .

EXAMPLE 6.5. For rank-zero curves, the computation of Heegner points is most feasible when  $|d_K|$  is small. Thus, we fix  $d_K = -7$  and search for rank-zero optimal curves with  $E(\mathbb{Q})[2] = 0$  satisfying the two necessary conditions in Example 6.2 and such that  $K = \mathbb{Q}(\sqrt{-7})$  satisfies the Heegner hypothesis. There are 39 such curves of conductor  $\leq 750$ ; see Table 2. Then 28 out of 39 curves satisfy  $(\star)$ , in which case Theorems 4.3 and 1.12 apply and the improved bound toward Goldfeld's conjecture holds. If  $c_2(E)$  is further odd (true for 24 out of 28), then the application to BSD(2) (Theorem 5.1) also applies.

REMARK 6.6. Even when  $E$  does not satisfy  $(\star)$  for any  $K$  (for example, when  $E(\mathbb{Q})$  has rank  $\geq 2$  or  $\text{III}(E/\mathbb{Q})[2]$  is nontrivial), one can still prove the same bound in Theorem 1.12 by exhibiting *one* quadratic twist  $E^*$  of  $E$  such that  $E^*$  satisfies  $(\star)$  (as quadratic twisting can *lower* the 2-Selmer rank). We expect that one can always find such  $E^*$  when the two necessary conditions ( $c_p(E)$ 's are odd for  $p \neq 2$  and  $a_2(E)$  is even) are satisfied, and so we expect that Theorem 1.12 applies to a large positive proportion of elliptic curves  $E$ . Showing the existence of such  $E^*$  amounts to showing that the value of the anticyclotomic  $p$ -adic  $L$ -function at the trivial character is nonvanishing mod  $p$  among quadratic twist families for  $p = 2$ . This nonvanishing mod  $p$  result seems to be more difficult and we do not address it here (but when  $p \geq 5$ , see Prasanna [63] and the recent work of Burungale–Hida–Tian [10]).

## 7. Heegner points at Eisenstein primes

In this section, we carry out the  $p$ -adic integration which makes up the heart of Theorem 1.20 (see the strategy sketched in Section 3.1). We will show, by direct  $p$ -adic integration, the following generalization of [42, Theorem 13]. (Here, our generalization also corrects a self-contained typo in the statement of [42, Theorem 13], where part of condition (3) was mistranscribed from [42, Theorem 7]:

Table 2. Assumption (★) for rank-zero curves.

$E$	$d_K$	$c_2(E)$	★	$E$	$d_K$	$c_2(E)$	★
11a1	-7	1	✓	316a1	-7	1	
37b1	-7	1	✓	352a1	-7	2	✓
44a1	-7	3	✓	352e1	-7	2	✓
67a1	-7	1	✓	368c1	-7	1	✓
92a1	-7	3	✓	368f1	-7	1	✓
116a1	-7	3		428a1	-7	3	
116b1	-7	3		464c1	-7	2	
176a1	-7	1	✓	464d1	-7	1	
176b1	-7	1	✓	464f1	-7	1	
179a1	-7	1	✓	464g1	-7	2	
184d1	-7	2	✓	557b1	-7	1	✓
232b1	-7	2		568a1	-7	1	
268a1	-7	1	✓	571a1	-7	1	
		$E$	$d_K$	$c_2(E)$	★		
		592b1	-7	1	✓		
		592c1	-7	1	✓		
		659b1	-7	1	✓		
		688b1	-7	2	✓		
		701a1	-7	1	✓		
		704c1	-7	1	✓		
		704d1	-7	1	✓		
		704e1	-7	1	✓		
		704f1	-7	1	✓		
		704g1	-7	1	✓		
		704h1	-7	1	✓		
		704i1	-7	1	✓		
		739a1	-7	1	✓		

‘ $\ell \not\equiv -1 \pmod p$ ’ should be ‘ $\ell \not\equiv \psi(\ell) \pmod p$ .’) Our generalization, in particular, does not require  $p \nmid N$ .

**THEOREM 7.1.** *Let  $E/\mathbb{Q}$  be an elliptic curve. Let  $p$  be a prime such that  $E[p]$  is a reducible  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -representation, or equivalently,  $E[p]^{\text{ss}} \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi^{-1}\omega)$ , for some character  $\psi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mu_{p-1}$ . Let  $K$  be an imaginary quadratic field satisfying the Heegner hypothesis for  $N$ . Suppose  $p$  splits in  $K$ . Suppose further that either the following four conditions hold:*

- (1)  $\psi(p) \neq 1$  and  $(\psi^{-1}\omega)(p) \neq 1$ ,
- (2)  $N_{\text{split}} = 1$ ,

(3)  $\ell \neq p$ ,  $\ell | N_{\text{add}}$  implies either  $\psi(\ell) \neq 1$  and  $\ell \not\equiv \psi(\ell) \pmod{p}$ , or  $\psi(\ell) = 0$ ,

(4)  $p \nmid B_{1, \psi_0^{-1} \varepsilon_K} \cdot B_{1, \psi_0 \omega^{-1}}$ ,

or the following four 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)  $\text{ord}_p((p - 1/2p) \log_p \bar{\alpha}) = 0$ ,

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

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

$$\frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_p)|}{p} \cdot \log_{\omega_E} P \not\equiv 0 \pmod{p}.$$

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

REMARK 7.2. When  $p = 2$ , we must have  $\psi = 1$  (since  $\psi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mu_{p-1} = \{1\}$ ). Note also that by (3) of the second part of Theorem 7.1, in this case,  $N$  must be a power of 2.

REMARK 7.3. Note that when  $p = 3$  and  $\psi$  is quadratic, condition (3) in the first part of the statement of Theorem 7.1 is equivalent to

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

**7.1. The Eisenstein congruence.** We may assume without loss of generality that  $\psi \neq \omega$  (otherwise, interchange  $\psi$  and  $\psi^{-1}\omega$ ). As in the proof of [42, Theorem 13], the argument relies on establishing an Eisenstein congruence. More precisely, let  $f$  be the normalized weight 2  $\Gamma_0(N)$ -level newform associated with  $E$ . Recall the weight 2 Eisenstein series  $E_{2, \psi}$  defined by the  $q$ -expansion (at  $\infty$ )

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

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 [38, Ch. II]). The assumption that  $E[p]$  is reducible and  $E[p]^{ss} \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi^{-1}\omega)$  implies the following lemma (see [42, Theorem 34(2)]).

LEMMA 7.4. *N has a decomposition  $N = N_+N_-N_0$  into pairwise coprime integers  $N_+, N_-, N_0$  such that  $N_+N_-$  is the square-free part of  $N$ ,  $N_0$  is the square-full part of  $N$ , and*

- (1) *if  $\ell|N_+$ , then  $a_\ell(f) \equiv \psi(\ell) \pmod{p}$ ,*
- (2) *if  $\ell|N_-$ , then  $a_\ell(f) \equiv \psi^{-1}(\ell)\ell \pmod{p}$ ,*
- (3) *if  $\ell|N_0$ , then  $a_\ell(f) = 0$ .*

Note that the minimal level of  $E_{2,\psi}$  is  $f(\psi)^2$ . With respect to this level, take  $N^\#$  as in Section 3.3 to be  $N^\# = \text{lcm}_{\ell|N}(\ell^2, f(\psi))$ . 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 3.3. 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

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

for all  $j \geq 1$ .

Let  $A$  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  $\mathcal{O}_K$ . As is explained in Section 3, by Theorem 3.8, this implies that (for any generator  $\omega \in \Omega_{A/\mathcal{O}_{\mathbb{C}_p}}^1$ )

$$\begin{aligned} & \frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_p)|}{p} \cdot \log_{\omega_E} P \\ &= \sum_{[\alpha] \in \mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1} f^{(1,1,p)}(\mathfrak{a} \star (A, A[\mathfrak{N}], \omega)) \\ &\equiv \sum_{[\alpha] \in \mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1} E_{2,\psi}^{(N_+, N_-, pN_0)}(\mathfrak{a} \star (A, A[\mathfrak{N}], \omega)) \end{aligned}$$

$$\begin{aligned}
 &= \prod_{\ell|N_+, \ell \neq p} (1 - \psi^{-1}(\ell)) \prod_{\ell|N_-, \ell \neq p} \left(1 - \frac{\psi(\ell)}{\ell}\right) \prod_{\ell|N_0, \ell \neq p} (1 - \psi^{-1}(\ell)) \left(1 - \frac{\psi(\ell)}{\ell}\right) \\
 &\cdot \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1} E_{2,\psi}^{(1,1,p)}(\mathfrak{a} \star (A, A[\mathfrak{N}], \omega)) \pmod{p\mathcal{O}_{\mathbb{C}_p}}, \tag{19}
 \end{aligned}$$

where the final equality follows from Lemma 3.6, applied to successive stabilizations of  $E_{2,\psi}$ .

**7.2. CM period of Eisenstein series.** To evaluate (19) further, we need to study the period

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

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

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

where  $(\alpha) = \mathfrak{a}^{h_K}$  and  $h_K$  is the class number of  $K$ . Let  $\bar{\mathfrak{p}}$  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  $\mathbb{N}_K : K^\times \backslash \mathbb{A}_K^\times \rightarrow \mathbb{C}^\times$ . Then by looking at  $q$ -expansions and invoking the  $q$ -expansion principle, it is apparent that the above sum is given by

$$\begin{aligned}
 &\sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1} E_{2,\psi}^{(1,1,p)}(\mathfrak{a} \star (A, A[\mathfrak{N}], \omega)) \\
 &= \lim_{j \rightarrow 0} \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} (\chi_j^{-1} \mathbb{N}_K^{h_K j})(\mathfrak{a}) \theta^{-1+h_K j} E_{2,\psi}^{(1,1,p)}(\mathfrak{a} \star (A, A[\mathfrak{N}], \omega)) \\
 &= \lim_{j \rightarrow 0} (1 - \psi^{-1}(p) \chi_j^{-1}(\bar{\mathfrak{p}}))(1 - \psi(p) (\chi_j^{-1} \mathbb{N}_K)(\bar{\mathfrak{p}})) \\
 &\cdot \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} (\chi_j^{-1} \mathbb{N}_K^{h_K j})(\mathfrak{a}) \theta^{-1+h_K j} E_{2,\psi}(\mathfrak{a} \star (A, A[\mathfrak{N}], \omega)) \tag{20}
 \end{aligned}$$

since  $\chi_j^{-1} \mathbb{N}_K^{h_K j} \rightarrow 1$  as  $j \rightarrow 0 = (0, 0) \in \mathbb{Z}/(p-1) \times \mathbb{Z}_p$ ; here, the last equality again follows from Lemma 3.6 applied to  $F = E_{2,\psi}$ .

**7.3. 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  $\mathcal{A}$  of  $A$  at  $p$ , choose an identification  $\iota : \hat{A} \xrightarrow{\sim} \hat{\mathbb{G}}_m$  (unique up to  $\mathbb{Z}_p^\times$ ) and let  $\omega_{\text{can}} := \iota^*(du/u)$  where  $u$  is the coordinate on  $\hat{\mathbb{G}}_m$ . This choice of  $\omega_{\text{can}}$  determines  $p$ -adic and complex periods  $\Omega_p$  and  $\Omega_\infty$  as in [42, Section 3]. As an intermediate step to establishing the  $p$ -adic interpolation, we have the following identity of algebraic values.

LEMMA 7.5. *We have the following identity of values in  $\overline{\mathbb{Q}}$  for  $j \geq 1$ :*

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

where  $\psi^{-1}(-\sqrt{d_K})$  denotes the Dirichlet character  $\psi^{-1}$  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  $(A, A[\mathfrak{N}], 2\pi i dz)$  as a triple over  $\mathbb{C}$  by considering the uniquely determined complex uniformization  $\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}) \cong A$  for some  $\tau$  in the complex upper half-plane, and identifying  $A[\mathfrak{N}]$  with  $(1/N)\mathbb{Z} \subset \mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$ . By plugging  $\psi_1 = \psi_2^{-1} = \psi$  and  $u = t = \mathfrak{f}$ ,  $\mathfrak{N}' = \mathfrak{f}^2$  into [42, Proposition 36], we have the complex identity

$$\begin{aligned} & \sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} (\chi_j^{-1} \mathbb{N}_K^{h_k j})(\mathfrak{a}) \partial^{-1+h_k j} E_{2,\psi}(\mathfrak{a} \star (A, A[\mathfrak{N}], 2\pi i dz)) \\ &= \frac{f(\psi)^2 \Gamma(1 + h_k j) \psi^{-1}(-\sqrt{d_K}) (\chi_j^{-1} \mathbb{N}_K)(\bar{\mathfrak{f}})}{(2\pi i)^{1+h_k j} \mathfrak{g}(\psi^{-1})(\sqrt{d_K})^{-1+h_k j}} L((\psi \circ \text{Nm}_{K/\mathbb{Q}}) \chi_j^{-1} \mathbb{N}_K, 0), \end{aligned} \tag{21}$$

where  $\partial$  is the complex Maass–Shimura operator and  $\mathbb{N}_K : K^\times \backslash \mathbb{A}_K^\times \rightarrow \mathbb{C}^\times$  is the complex norm character over  $K$ . By definition of  $\Omega_p$  and  $\Omega_\infty$ , we have

$$2\pi i dz = \frac{\Omega_p}{\Omega_\infty} \cdot \omega_{\text{can}}.$$

By [42, Proposition 21], we have the equality of algebraic values

$$\partial^{-1+h_k j} E_2(\mathfrak{a} \star (A, A[\mathfrak{N}], \omega_{\text{can}})) = \theta^{-1+h_k j} E_2(\mathfrak{a} \star (A, A[\mathfrak{N}], \omega_{\text{can}}))$$

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 is denoted by  $\mathbb{N}_K$ , at  $\mathfrak{a}$ . Applying these identities to the identity of complex numbers (21), we get the desired identity of algebraic numbers.  $\square$

We now apply the interpolation property of the Katz  $p$ -adic  $L$ -function (see [31, Theorem II]) to our situation, taking the normalization as in [24], thus arriving at the identity

$$\begin{aligned} L_p^{\text{Katz}}((\psi \circ \text{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K, 0) &= 4 \cdot \text{Local}_p((\psi \circ \text{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K) \left(\frac{\Omega_p}{\Omega_\infty}\right)^{2h_k j} \\ &\cdot \left(\frac{2\pi i}{\sqrt{d_K}}\right)^{-1+h_k j} \Gamma(1+h_k j)(1-\psi(p)(\chi_j^{-1}\mathbb{N}_K)(\bar{\mathfrak{p}}))(1-\psi(p)\chi_j^{-1}(\bar{\mathfrak{p}})) \\ &\times L((\psi \circ \text{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K, 0) \end{aligned} \tag{22}$$

for all  $j \geq 1$ , where  $\text{Local}_p(\chi) = \text{Local}_p(\chi, \Sigma, \delta)$  is defined as in [39, 5.2.26] with  $\Sigma = \{\mathfrak{p}\}$  and  $\delta = \sqrt{d_K}/2$  (or as denoted by  $W_p(\lambda)$  in [31, 0.10]). For any prime  $\ell$ , let  $\psi_\ell(-\sqrt{d_K})$  denote the value  $\psi_\ell(b)$ , where again  $b$  is any integer such that  $b + \sqrt{d_K} \in \mathfrak{f}$ . By directly plugging in  $\chi = (\psi \circ \text{Nm}_{K/\mathbb{Q}})\chi_j^{-1}\mathbb{N}_K$  into the definition of  $\text{Local}_p$ , we have

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

Plugging (22) into the identity in Lemma 7.5, we have for all  $j \geq 1$

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

Taking the limit  $j \rightarrow 0 = (0, 0) \in \mathbb{Z}/(p-1) \times \mathbb{Z}_p$ , noting that  $\chi_j^{-1}\mathbb{N}_K \rightarrow \mathbb{N}_K$  and  $\mathbb{N}_K(\bar{\mathfrak{f}}) = f(\psi)^{-1}$  and applying (20), we have

$$\begin{aligned} &\sum_{[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O}_K)} \theta^{-1} E_{2,\psi}^{(1,1,p)}(\mathfrak{a} \star (A, A[\mathfrak{N}], \omega_{\text{can}})) \\ &= \frac{f(\psi)^{(p)}}{4(\prod_{\ell|f(\psi)^{(p)}} \psi_\ell^{-1}(-\sqrt{d_K})\mathfrak{g}_\ell(\psi))} L_p^{\text{Katz}}((\psi \circ \text{Nm}_{K/\mathbb{Q}})\mathbb{N}_K, 0). \end{aligned} \tag{23}$$

**7.4. Gross’s factorization theorem.** We now evaluate the Katz  $p$ -adic  $L$ -value on the right-hand side of (23).

LEMMA 7.6. We have, for  $\psi \neq 1$ ,

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

and for  $\psi = 1$ ,

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

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

*Proof.* Applying Gross’s factorization theorem (see [24] and [42, Theorem 28] for the extension to the general auxiliary conductor case), we have

$$\begin{aligned} & \frac{f(\psi)^{(p)}}{(\prod_{\ell|f(\psi)^{(p)}} \psi_\ell^{-1}(-\sqrt{d_K}) \mathfrak{g}_\ell(\psi))} L_p^{\text{Katz}}((\psi \circ \text{Nm}_{K/\mathbb{Q}})\mathbb{N}_K, 0) \\ &= \pm L_p(\psi_0^{-1}\varepsilon_K\omega, 0) L_p(\psi_0, 1), \end{aligned} \tag{24}$$

where  $L_p(\cdot, s)$  denotes the Kubota–Leopoldt  $p$ -adic  $L$ -function; here, the sign of  $\pm 1$  is uniquely determined by the suitably normalized  $p$ -adic Kronecker limit formula due to Katz used in Gross’s proof to compare elliptic and cyclotomic units (the normalization factor in [42, Theorem 28] 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

$$L_p(\psi_0^{-1}\varepsilon_K, 0) = -(1 - \psi^{-1}(p)) B_{1,\psi_0^{-1}\varepsilon_K}. \tag{25}$$

Now suppose  $\psi \neq 1$ . We claim that

- (1)  $8 \nmid f(\psi_0)$  if  $p = 2$ , and
- (2)  $p^2 \nmid f(\psi_0)$  if  $p > 2$ .

If  $p = 2$ , then  $\psi_0 = 1$  and  $f(\psi_0) = 1$ . If  $p = 3$ , then  $\psi_0 : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mu_2$  is quadratic, and so  $9 \nmid f(\psi_0)$  (since  $f(\psi_0)$  is square-free outside of 2). If  $p \geq 5$ , then since  $E[p]^{\text{ss}} \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi^{-1}\omega)$ , 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  $\text{ord}_p(N) \leq 2$ , a contradiction.

Having justified this claim, we know that  $L_p(\psi_0, m) \equiv L_p(\psi_0, n) \pmod{p\mathcal{O}_{C_p}}$  for all  $m, n \in \mathbb{Z}$  (for example, see [85, Corollary 5.13]). Thus,

$$L_p(\psi_0, 1) \equiv L_p(\psi_0, 0) = -(1 - (\psi\omega^{-1})(p))B_{1, \psi_0\omega^{-1}} \pmod{p\mathcal{O}_{C_p}}. \tag{26}$$

Combining (24)–(26), we get

$$\begin{aligned} & \frac{f(\psi)^{(p)}}{\prod_{\ell|f(\psi)^{(p)}} \psi_\ell^{-1}(-\sqrt{d_K})g_\ell(\psi)} L_p^{\text{Katz}}((\psi \circ \text{Nm}_{K/\mathbb{Q}})\mathbb{N}_K, 0) \\ & \equiv \pm(1 - \psi^{-1}(p))(1 - (\psi\omega^{-1})(p))B_{1, \psi_0^{-1}\varepsilon_K} B_{1, \psi_0\omega^{-1}} \pmod{p\mathcal{O}_{C_p}} \end{aligned} \tag{27}$$

when  $\psi \neq 1$ .

Now suppose  $\psi = 1$ . In particular,  $f(\psi) = f(\psi)^{(p)} = 1$ . By the functional equation for the Katz  $p$ -adic  $L$ -function (for example, see [31, 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

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

By a standard special value formula (for example, see [24, Section 5, Formulas 1]), we have

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

and so

$$L_p^{\text{Katz}}(\mathbb{N}_K, 0) = \frac{4}{|\mathcal{O}_K^\times|} \cdot \frac{p-1}{p} \log_p(\bar{\alpha}) = 2 \cdot \frac{p-1}{p} \log_p(\bar{\alpha}) \tag{28}$$

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

Now plugging in (27) into (23) when  $\psi \neq 1$ , and (28) into (23) when  $\psi = 1$ , we establish the lemma.  $\square$

**7.5. Proof of Theorem 7.1.** Putting together (19) and Lemma (7.6), we arrive at our main congruence identities. If  $\psi \neq 1$ , we have

$$\begin{aligned} & \frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_p)|}{p} \cdot \log_{\omega_E} P \\ & \equiv \pm \prod_{\ell|N_+, \ell \neq p} (1 - \psi^{-1}(\ell)) \prod_{\ell|N_-, \ell \neq p} \left(1 - \frac{\psi(\ell)}{\ell}\right) \end{aligned}$$

$$\begin{aligned} &\times \prod_{\ell|N_0, \ell \neq p} (1 - \psi^{-1}(\ell)) \left(1 - \frac{\psi(\ell)}{\ell}\right) \\ &\cdot \frac{1}{4} (1 - \psi^{-1}(p))(1 - (\psi\omega^{-1})(p)) B_{1, \psi_0^{-1}\varepsilon_K} B_{1, \psi_0\omega^{-1}} \pmod{p\mathcal{O}_{\mathbb{C}_p}}. \end{aligned} \tag{29}$$

Now the statement for  $\psi \neq 1$  in Theorem 7.1 immediately follows from studying when the right-hand side of the congruence vanishes mod  $p$ . If  $\psi = 1$ , we have

$$\begin{aligned} &\frac{|\tilde{E}^{\text{ns}}(\mathbb{F}_p)|}{p} \cdot \log_{\omega_E} P \\ &\equiv \begin{cases} \prod_{\ell|N_-, \ell \neq p} \left(1 - \frac{1}{\ell}\right) \cdot \frac{p-1}{2p} \log_p \bar{\alpha} \pmod{p\mathcal{O}_{\mathbb{C}_p}}, & \text{if } \ell|N_+N_0 \implies \ell = p, \\ 0 \pmod{p\mathcal{O}_{\mathbb{C}_p}}, & \text{if } \exists \ell \neq p \text{ such that } \ell|N_+N_0, \end{cases} \end{aligned} \tag{30}$$

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

We now finish the proof of Theorem 7.1 with the following lemma.

LEMMA 7.7. *The right-hand side of (30) does not vanish mod  $p$  if and only if*

- (1)  $\ell|N, \ell \neq p$  implies  $\ell|N, \ell \equiv -1 \pmod{p}, \ell \not\equiv 1 \pmod{p}$ ,
- (2)  $\text{ord}_p((p-1/2p) \log_p \bar{\alpha}) = 0$ .

We also have that the nonvanishing of the right-hand side of (30) mod  $p$  implies  $p|N$ , and so the right-hand side of (30) does not vanish mod  $p$  if and only if  $p|N$  and (1) and (2) hold.

*Proof.* We first study when

$$\prod_{\ell|N_-, \ell \neq p} \left(1 - \frac{1}{\ell}\right) \cdot \frac{p-1}{2p} \log_p \bar{\alpha} \tag{31}$$

vanishes mod  $p$ . Clearly (31) does not vanish mod  $p$  if and only if each of its factors does not vanish mod  $p$ . Then  $\prod_{\ell|N_-, \ell \neq p} (1 - 1/\ell)$  does not vanish if and only if

$$\ell|N_-, \ell \neq p \implies \ell \not\equiv 1 \pmod{p}. \tag{32}$$

Hence, (31) does not vanish mod  $p$  if and only if (32) and (2) in the statement of the lemma hold.

If the right-hand side of (30) does not vanish, then we have  $\ell|N_+N_0 \implies \ell = p$ , the right-hand side of (30) equals (31) mod  $p$  and (32) 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 (32) holds. So (31) 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 (30) equals (31) mod  $p$ , which does not vanish mod  $p$ .

Thus, we have shown that the nonvanishing of the right-hand side of (30) 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 (30) does not vanish. In particular, we have  $\ell|N_+N_0 \implies \ell = p$  and that the right-hand side of (30) equals (31) 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,

$$\prod_{\ell|N_-, \ell \neq p} \left(1 - \frac{1}{\ell}\right) \equiv 0 \pmod{p} \tag{33}$$

and the right-hand side of (30) vanishes mod  $p$ , a contradiction.

Suppose  $p > 2$ . Note that

$$(N_{\text{split}}, N_-) = \prod_{\ell|N_-, \ell \equiv 1 \pmod{p}} \ell. \tag{34}$$

Since  $N_0 = N_{\text{add}}$  (because they are both the square-full parts of  $N$ ), we have  $N_{\text{add}} = N_0 = 1$ . By [87, Theorem 2.2], we know that  $N_{\text{split}}N_{\text{add}} \neq 1$ , and hence  $N_{\text{split}} \neq 1$ . Since  $N_+ = 1$ , we therefore have that  $1 \neq N_{\text{split}}|N_-$ . By (34), we thus have that there is some  $\ell|N_-$  such that  $\ell \equiv 1 \pmod{p}$ . In particular, we have (33) once again, and so the right-hand side of (30) vanishes mod  $p$ , a contradiction.  $\square$

REMARK 7.8. Note that our proof uses a direct method of  $p$ -adic integration and does not go through the construction of the BDP  $p$ -adic  $L$ -function as in the proof of the main theorem of [42]. 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 [42] (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.

### 8. Bernoulli numbers and relative class numbers

When  $p = 3$ , all Dirichlet characters in Theorem 7.1 are quadratic. Note that for an odd quadratic character  $\psi$  over  $\mathbb{Q}$ , by the analytic class number formula, we have

$$B_{1,\psi} = -2 \frac{h_{K_\psi}}{|\mathcal{O}_{K_\psi}^\times|}, \tag{35}$$

where  $K_\psi$  is the imaginary quadratic field associated with  $\psi$ . 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 nonvanishing mod  $p$  of the Bernoulli numbers  $B_{1,\psi_0^{-1}\varepsilon_K} B_{1,\psi_0\omega^{-1}}$  in terms of nonvanishing 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 8.1.** *Suppose  $\psi : (\mathbb{Z}/f)^\times \rightarrow \mu_{p-1}$  is a Dirichlet character and assume that  $\psi^{-1} \pmod{p} \neq \omega$  or, equivalently, assume that 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*

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

*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

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

Now our conclusion follows from the formula for the Bernoulli numbers (1).  $\square$

For an odd Dirichlet character  $\psi$ , let  $K_\psi$  denote the abelian CM field cut out by  $\psi$ . Consider the relative class number  $h_{K_\psi}^- = h_{K_\psi} / h_{K_\psi^+}$ , where  $K_\psi^+$  is the maximal

totally real subfield of  $K_\psi$ . The relative class number formula [85, 4.17] gives

$$h_{K_\psi}^- = Q \cdot w \cdot \prod_{\chi \text{ odd}} \left( -\frac{1}{2} B_{1,\chi} \right), \tag{36}$$

where  $\chi$  runs over all odd characters of  $\text{Gal}(K_\psi/\mathbb{Q})$ ,  $w$  is the number of roots of unity in  $K_\psi$  and  $Q = 1$  or  $2$  (see [85, 4.12]). By Lemma 8.1, assuming that  $\psi^{-1} \not\equiv \omega$ , we see that we have the following divisibility of numbers in  $\mathbb{Z}_p[\psi]$ :

$$p \nmid h_{K_\psi}^- \implies p \nmid B_{1,\psi}. \tag{37}$$

LEMMA 8.2. *Suppose  $\psi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mu_{p-1}$  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  $\omega$ , 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  $\psi$  is even, then  $\psi_0 \varepsilon_K = \psi \varepsilon_K$  is ramified at some place outside  $p$  and so is not equal to  $\omega$ , and  $\psi_0^{-1} \omega = \psi^{-1} \omega$  is not equal to  $\omega$  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  $\psi$  is odd, then  $\psi_0 \varepsilon_K = \psi$  is not equal to  $\omega$  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  $\omega$ . 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 (37). □

COROLLARY 8.3. *Suppose we are in the setting of Theorem 7.1. 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 7.1, in particular, implies  $\psi \neq 1$  or  $\omega$ . Now the statement follows from Lemma (8.2). □

### 9. Goldfeld's conjecture for elliptic curves with a 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  $K^-(x)$  denote the set of imaginary quadratic fields  $k$  with fundamental discriminant  $|d_k| < x$ . Let  $m$  and  $M$  be positive integers, and let

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

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

DEFINITION 9.1. We say that positive integers  $m$  and  $M$  comprise a *valid pair*  $(m, M)$  if both of the following properties hold:

- (1) if  $\ell$  is an odd prime number dividing  $(m, M)$ , then  $\ell^2$  divides  $M$  but not  $m$ ;
- (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 9.2 [55]. *We have*

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

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

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

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

Now put

$$\begin{aligned} K_*^+(x, m, M) &:= \{k \in K^+(x, m, M) : h_3(d_k) = 1\}, \\ K_*^-(x, m, M) &:= \{k \in K^-(x, m, M) : h_3(d_k) = 1\}. \end{aligned}$$

Taya [79] proves the following bound using Theorem 9.2.

PROPOSITION 9.3. *Suppose  $(m, M)$  is a valid pair. Then*

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

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

In particular, the set of real (respectively 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 (respectively 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 9.2. □

We have the following positive density result.

**THEOREM 9.4.** *Suppose  $E/\mathbb{Q}$  is any elliptic curve of conductor  $N = N_{\text{split}}N_{\text{nonsplit}}N_{\text{add}}$  whose mod 3 Galois representation  $E[3]$  is reducible and  $E[3]^{\text{ss}} \cong \mathbb{F}_3(\psi) \oplus \mathbb{F}_3(\psi^{-1}\omega)$ . Let  $d$  be the fundamental discriminant corresponding to the quadratic character  $\psi$ . Suppose that*

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

Let

$$d_0 := \begin{cases} d, & d > 0, \\ -3d, & d < 0, d \not\equiv 0 \pmod{3}, \\ -d/3, & (\text{mod } M) \quad d < 0, d \equiv 0 \pmod{3}, \end{cases} \tag{38}$$

let

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

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

$$\frac{d_0}{2^{r(E)+s_3(d)} \cdot 3} \prod_{\ell|N_{\text{split}}N_{\text{non-split}}, \ell \nmid d, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell|N_{\text{add}}, \ell \nmid d, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell|d, \ell \text{ odd}, \ell \neq 3} \frac{1}{2\ell} \prod_{\ell|3N} \frac{q}{\ell + 1} \tag{39}$$

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)  $h_3(d_0d_K) = 1$ .

If, furthermore, we impose the assumption on  $E$  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 (39) of all imaginary quadratic fields  $K$  have:

- (1)  $d_K$  is odd;
- (2)  $K$  satisfies the Heegner hypothesis with respect to  $3N$ ;
- (3) the Heegner point  $P \in E(K)$  is nontorsion.

*Proof.* We will apply Proposition 9.3 as well as Theorem 7.1. 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

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

- (2) In case (b), let

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

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)  $\ell$  odd prime,  $\ell \neq 3, \ell | N_{\text{split}} \implies m/d_0 \equiv [\text{quadratic residue unit}] \pmod{\ell}$   
and  $2 | N_{\text{split}} \implies m/d_0 \equiv 1 \pmod{8}$ ,
- (3)  $\ell$  odd prime,  $\ell \neq 3, \ell | N_{\text{nonsplit}} \implies m/d_0 \equiv [\text{quadratic residue unit}] \pmod{\ell}$   
and  $2 | N_{\text{nonsplit}} \implies m/d_0 \equiv 1 \pmod{8}$ ,
- (4)  $\ell$  prime,  $\ell \equiv 1 \pmod{3}, \ell | N_{\text{add}}, \ell \nmid d \implies m/d_0 \equiv [\text{quadratic residue unit}] \pmod{\ell}$   
and  $\ell \equiv 1 \pmod{3}, \ell | N_{\text{add}} \implies m \equiv \implies m/d_0 \equiv [\text{quadratic residue unit}] \pmod{\ell}$ ,
- (5)  $\ell$  prime,  $\ell$  odd,  $\ell \equiv 2 \pmod{3}, \ell | N_{\text{add}}$  (which by our assumptions implies  $\ell | d$ )  $\implies m \equiv 0 \pmod{\ell}$  where  $m/d_0 \equiv [\text{quadratic residue unit}] \pmod{\ell}$   
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)  $\ell$  prime,  $\ell \equiv 1 \pmod{3}, \ell | N_{\text{add}} \implies \ell$  splits in  $K$ ,
- (5)  $\ell$  prime,  $\ell \equiv 2 \pmod{3}, \ell | N_{\text{add}} \implies \ell$  splits in  $K$ ,

and  $d_K \equiv 1 \pmod{4}$  (that is,  $d_K$  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 9.1), and assumptions (4) and (5) in the statement of the theorem imply that  $(jd, d^2)$  is also a valid pair whenever  $(j, d) = 1$ . Thus, by Proposition 9.3, for any  $d_0 | M$ ,

$$\lim_{x \rightarrow \infty} \frac{|K_*^-(x, m, M)|}{|K^-(x/d_0, 1, 1)|} \geq \frac{d_0}{2\Phi(M)} \prod_{\ell | M} \frac{q}{\ell + 1}. \tag{40}$$

The left-hand side of (40) is the proportion of imaginary quadratic  $K$  satisfying  $d_0 d_K \equiv m \pmod{M}$  and  $h_3(d_0 d_K) = 1$ . Moreover, note that there are

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

choices for residue classes of  $m \pmod{M}$ . Combining all the above and summing over each valid residue class  $m \pmod{M}$ , we immediately obtain our lower bound (45) 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)  $h_3(d_0 d_K) = 1$ . This proves the part of the theorem before assumption (6) is introduced in the statement.

If we assume that  $E$  satisfies assumption (6) in the statement of the theorem, then for all  $K$  as above, we see that  $E$ ,  $p = 3$  and  $K$  satisfy all the assumptions of Theorem 7.1 (see Remark 7.3), thus implying that  $P$  is nontorsion. The final part of the theorem now follows.  $\square$

Similarly, we have the following positive density result for producing  $E$  which satisfy the assumptions of Theorem 9.4.

**THEOREM 9.5.** *Suppose  $(N_1, N_2, N_3)$  is a triple of pairwise coprime integers such that  $N_1 N_2$  is square-free,  $N_3$  is square-full and  $N_1 N_2 N_3 = N$ . Let*

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

Then a proportion of at least

$$\frac{1}{2^r \cdot 3} \prod_{\ell|N_1 N_2, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell|N_3, \ell \text{ odd}, \ell \neq 3} \frac{1}{\ell} \prod_{\ell|N, \ell \neq 3} \frac{q}{\ell + 1}$$

of even (respectively odd) quadratic characters  $\psi$  corresponding to real (respectively imaginary) quadratic fields  $\mathbb{Q}(\sqrt{d})$ , where  $d > 0$  (respectively  $d < 0$ ) 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)  $h_3(-3d) = 1$  (respectively  $h_3(d) = 1$ ).

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

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

*Proof.* We will apply Proposition 9.3. 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)  $\ell$  odd prime,  $\ell \neq 3, \ell | N_1 \implies m \equiv -3[\text{quadratic nonresidue}] \pmod{\ell}$ ,  
and  $2 | N_1 \implies m \equiv 1 \pmod{8}$ ;

(3)  $\ell$  odd prime,  $\ell \neq 3, \ell | N_2 \implies m \equiv -3[\text{quadratic residue unit}] \pmod{\ell}$ ,  
and  $2 | N_2 \implies m \equiv 5 \pmod{8}$ ;

(4)  $\ell$  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)  $\ell$  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

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

- If  $m \equiv 2 \pmod{3}$ , let

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

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  $\psi$  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,  $\psi$  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 9.3, if  $m \equiv 2 \pmod{3}$  with corresponding  $M$  as defined above, then

$$\lim_{x \rightarrow \infty} \frac{|K_*^-(x, m, M)|}{|K^+(3x, 3, 9)| + |K^+(3x, 6, 9)|} \geq \frac{1}{6\Phi(M)} \prod_{\ell | M, \ell \neq 3} \frac{q}{\ell + 1}, \quad (41)$$

where the left-hand side of (41) 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

$$\lim_{x \rightarrow \infty} \frac{|K_*^-(x, m, M)|}{|K^-(x, 1, 3)| + |K^-(x, 2, 3)|} \geq \frac{1}{2\Phi(M)} \prod_{\ell | M, \ell \neq 3} \frac{q}{\ell + 1}, \quad (42)$$

where the left-hand side of (42) 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 9.3, if  $m \equiv 3 \pmod{9}$  with corresponding  $M$  as defined above, then

$$\lim_{x \rightarrow \infty} \frac{|K_*^-(x, m, M)|}{|K^+(x/3, 1, 3)| + |K^+(x/3, 2, 3)|} \geq \frac{3}{2\Phi(M)} \prod_{\ell | M, \ell \neq 3} \frac{q}{\ell + 1}, \quad (43)$$

where the left-hand side of (43) 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

$$\lim_{x \rightarrow \infty} \frac{|K_*^-(x, m, M)|}{|K^-(x, 1, 3)| + |K^-(x, 2, 3)|} \geq \frac{1}{2\Phi(M)} \prod_{\ell|M, \ell \neq 3} \frac{q}{\ell + 1}, \tag{44}$$

where the left-hand side of (44) 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

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

choices of residue classes  $m \pmod{M}$  which satisfy congruence conditions (1)–(5). Combining all the above and summing over each of these residue classes  $m \pmod{M}$ , we immediately obtain our lower bounds for the proportions of desired  $d > 0$  from (42) and desired  $d < 0$  from (43).

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

**REMARK 9.6.** Suppose  $E[3]^{\text{ss}} \cong \mathbb{F}_3 \oplus \mathbb{F}_3(\omega)$ . Note that for each  $d$  produced by Theorem 9.5, Theorem 9.4 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  $P \in E^{(d)}(K)$  is nontorsion. In particular, for each such  $d$  there is *at least one*  $K$  such that  $P \in E^{(d)}(K)$  is nontorsion. Thus,  $r_{\text{an}}(E^{(d)}) = 1 - w(E^{(d)})/2$ .

*Proof of Theorem 1.5.* Suppose  $E[3]$  is reducible, that is,  $E[3]^{\text{ss}} \cong \mathbb{F}_3(\psi) \oplus \mathbb{F}_3(\psi^{-1}\omega)$  for some quadratic character  $\psi : \text{Gal}(\mathbb{Q}/\mathbb{Q}) \rightarrow \mu_2$ . Twisting by the quadratic character  $\psi^{-1}$ , we may assume without loss of generality that  $E[3]^{\text{ss}} \cong \mathbb{F}_3 \oplus \mathbb{F}_3(\omega)$ .

Let  $d$  be a fundamental discriminant corresponding to a quadratic character  $\psi$  in the family of  $d$  produced by Theorem 9.5 (with the integers  $N_1 = N_{\text{split}}$ ,  $N_2 = N_{\text{nonsplit}}$  and  $N_3 = N_{\text{odd}}$  as in our setting). In particular,  $E^{(d)}[3]^{\text{ss}} \cong \mathbb{F}_3(\psi) \oplus \mathbb{F}_3(\psi^{-1}\omega)$  satisfies the assumptions of Theorem 9.4, including assumption (6). Hence, we can apply Theorem 9.4 to  $E^{(d)}$  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  $P \in E^{(d)}(K)$  is nontorsion.

Since  $w(E^{(d)})w(E^{(dd_K)}) = w(E/K) = -1$  (the last equality following from the Heegner hypothesis), we have that each such  $K$  satisfies

$$r_{\text{an}}(E^{(dd_K)}) = \frac{1 + w(E^{(d)})}{2}.$$

Hence, there are a positive proportion of quadratic twists of  $E$  with rank  $1 + w(E^{(d)})/2$ , and in fact by Theorem 9.4, a lower bound for this proportion is given by

$$\frac{d_0}{2^{r(E^{(d)})+s_3(d)} \cdot 3} \prod_{\substack{\ell | N_{\text{split}} N_{\text{nonsplit}} \\ \ell \nmid d, \ell \text{ odd}, \ell \neq 3}} \frac{1}{2} \prod_{\substack{\ell | N_{\text{add}} d^2 \\ \ell \nmid d, \ell \text{ odd}, \ell \neq 3}} \frac{1}{2} \prod_{\ell | d, \text{ odd}, \ell \neq 3} \frac{1}{2\ell} \prod_{\ell | 3Nd^2} \frac{q}{\ell + 1} \quad (45)$$

in the notation of the statement of the theorem.

Now choose any  $K$  as produced by Theorem 9.4 for  $E^{(d)}$  so that  $w(E^{(dd_K)}) = -w(E^{(d)})$ . 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  $E^{(dd_K)}[3]^{\text{ss}} \cong \mathbb{F}_3(\psi \varepsilon_K) \oplus \mathbb{F}_3((\psi \varepsilon_K)^{-1} \omega)$  satisfies all of the assumptions (including (6)) of Theorem 9.4. Hence, we can apply Theorem 9.4 to  $E^{(dd_K)}$  to conclude that a positive proportion of imaginary quadratic fields  $K'$  satisfy the Heegner hypothesis with respect to  $3Nd^2 d_K^2$  and have that the associated Heegner point  $P \in E^{(dd_K)}(K')$  is nontorsion. Since  $w(E^{(dd_K)})w(E^{(dd_K d_K')}) = w(E^{(dd_K)}/K') = -1$ , we have that each such  $K'$  satisfies

$$r_{\text{an}}(E^{(dd_K d_K')}) = \frac{1 + w(E^{(dd_K)})}{2} = \frac{1 - w(E^{(d)})}{2}. \quad (46)$$

Hence, there are a positive proportion of quadratic twists of  $E$  with rank  $1 - w(E^{(d)})/2$ , and in fact by Theorem 9.4, a lower bound for this proportion is given by

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

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

We have thus established Theorem 1.5. □

When  $E$  is semistable, we have  $E[3]^{\text{ss}} \cong \mathbb{F}_3 \oplus \mathbb{F}_3(\omega)$  for the following reason: Suppose  $E[3]^{\text{ss}} \cong \mathbb{F}_3(\psi) \oplus \mathbb{F}_3(\psi^{-1} \omega)$  for some quadratic character  $\psi$ . Then  $\psi$  cannot be ramified at any  $\ell | N$  since the corresponding admissible  $GL_2(\mathbb{Q}_\ell)$

representation is Steinberg of conductor  $\ell$ , but if  $\psi$  was ramified at  $\ell$ , it would force the conductor to be divisible by  $\ell^2$  by the above description of  $E[3]^{\text{ss}}$ . Hence,  $\psi$  is a quadratic character only possibly ramified at 3 and hence must be either 1 or  $\omega$ .

Now we can use Theorem 9.5 to compute explicit lower bounds on the proportion of rank-0 and rank-1 quadratic twists.

**PROPOSITION 9.7.** *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 9.5 (with  $N_1 = N_{\text{split}}$ ,  $N_2 = N_{\text{nonsplit}}$  and  $N_3 = N_{\text{add}} = 1$ , at least*

$$\frac{1}{2^r \cdot 3} \prod_{\ell|N, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell|N, \ell \neq 3} \frac{q}{\ell + 1} \quad (47)$$

*of  $d > 0$  (respectively  $d < 0$ ) have  $r_{\text{an}}(E^{(d)}) = 1$  (respectively  $r_{\text{an}}(E^{(d)}) = 0$ ).*

*If  $3|N$ , then:*

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

$$\frac{1}{2^r \cdot 3} \prod_{\ell|N, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell|N, \ell \neq 3} \frac{q}{\ell + 1} \quad (48)$$

*of  $d > 0$  (respectively  $d < 0$ ) have  $r_{\text{an}}(E^{(d)}) = 1$  (respectively  $r_{\text{an}}(E^{(d)}) = 0$ ).*

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

$$\frac{1}{2^{r+2} \cdot 3} \prod_{\ell|N, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell|N, \ell \neq 3} \frac{q}{\ell + 1} \quad (49)$$

*of  $d > 0$  (respectively  $d < 0$ ) have  $r_{\text{an}}(E^{(d)}) = 0$  (respectively  $r_{\text{an}}(E^{(d)}) = 1$ ), and at least*

$$\frac{1}{2^{r+2}} \prod_{\ell|N, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell|N, \ell \neq 3} \frac{q}{\ell + 1} \quad (50)$$

*of  $d > 0$  (respectively  $d < 0$ ) have  $r_{\text{an}}(E^{(d)}) = 1$  (respectively  $r_{\text{an}}(E^{(d)}) = 0$ ).*

*Proof.* First, we apply Theorem 9.5 to  $N_1 = N_{\text{split}}$ ,  $N_2 = N_{\text{nonsplit}}$  and  $N_3 = N_{\text{add}} = 1$ . For any  $d$  produced by the theorem, Remark 9.6 implies that

$$r_{\text{an}}(E^{(d)}) = \frac{1 - w(E^{(d)})}{2}. \quad (51)$$

Let  $d$  be any fundamental discriminant produced by Theorem 9.5. By the properties of  $d$  produced in Theorem 9.5, the corresponding local characters  $\psi_\ell$  satisfy the implications

$$\ell|N, \ell \nmid d \implies \ell||N \implies \psi_\ell(\ell)w_\ell(E) = -\psi_\ell(\ell)a_\ell(E) = -\psi(\ell)a_\ell(E) = 1, \tag{52}$$

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

$$\ell|(N, d) \implies \ell = 3. \tag{53}$$

We now calculate  $w(E^{(d)})$  using (52) and (53). 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 [3, 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,

$$w(E^{(d)}) = -\psi(-1) \left( \prod_{\text{if } 3|(N,d)} -w_3(E) \right). \tag{54}$$

If  $3 \nmid N$ , then we have  $3 \nmid (N, d)$ , and so  $w(E^{(d)}) = -\psi(-1)$ . Thus, by (51) and the lower bound given in the statement of Theorem 9.5, in the notation of the theorem, we have that at least

$$\frac{1}{2^r \cdot 3} \prod_{\ell|N, \ell \text{ odd}, \ell \neq 3} \frac{1}{2} \prod_{\ell|N, \ell \neq 3} \frac{q}{\ell + 1} \tag{55}$$

of  $d > 0$  have  $r_{\text{an}}(E^{(d)}) = 1$  and at least the same proportion of  $d < 0$  have  $r_{\text{an}}(E^{(d)}) = 0$ . If  $3|N$ , then

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

The desired bounds in this case follow again from (51), the lower bound given in the statement of Theorem 9.5 and the final part of that theorem.  $\square$

REMARK 9.8. It is most likely possible to refine the casework in the proofs of Theorems 9.5 and 9.4 in order to achieve better lower bounds of twists with ranks 0 or 1.

EXAMPLE 9.9. 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  $E[3]^{\text{ss}} = \mathbb{F}_3 \oplus \mathbb{F}_3(\omega)$ . Note that  $N = N_{\text{split}} = 19$  and the root number  $w(E) = +1$ . Consider the set of fundamental discriminant  $d > 0$  (respectively  $d < 0$ ) such that

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

The first few such  $d > 0$  are

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

and the first few such  $d < 0$  are

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

Note that the root number  $w(E^{(d)}) = \psi_d(-19) = -1$  (respectively  $+1$ ), we know from Theorem 9.4 that

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

The explicit lower bounds in Proposition 9.7 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 [32, page 640]).

## 10. The sextic twist family

10.1. **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 10.1. For  $d \in \mathbb{Z}$ , we denote  $E_d$  as the  $d$ th sextic twist of  $E$ ,

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

Note 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 10.2. 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 [88, Section 1] or [86, Section 1] for an overview.

LEMMA 10.3. *We have an isomorphism of  $G_{\mathbb{Q}}$ -representations*

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

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

*Proof.* Note 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 semisimplification of the mod 3 Galois representations. Note 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,

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

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

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

The result then follows. □

LEMMA 10.4. Assume that

- (1)  $d$  is a fundamental discriminant;
- (2)  $d \equiv 0 \pmod{3}$ .

Then the root number of  $E_d$  is given by

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

*Proof.* We use the closed formula for the local root numbers  $w_\ell(E_d)$  in [46, Section 9].

- (1) Since  $d$  is a fundamental discriminant, we have  $d \equiv 1 \pmod{4}$ ,  $d = 4d'$  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

$$w_2(E_d) = \begin{cases} +1, & 2 \nmid d \text{ or } 4 \parallel d, \\ -1, & 8 \parallel d. \end{cases} \tag{56}$$

- (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) Note that if  $2 \nmid d$  or  $4 \parallel d$ , then the number of prime factors  $\ell \mid d$  such that  $\ell \geq 5$  and  $\ell \equiv 2 \pmod{3}$  is odd if and only if  $|d'| \equiv 2 \pmod{3}$ . Similarly, if  $8 \parallel d$ , then the number of prime factors  $\ell \mid d$  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

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

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

$$\prod_{\ell \geq 5} w_\ell(E_d) = \begin{cases} -\text{sign}(d), & 2 \nmid d \text{ or } 4 \parallel d, \\ \text{sign}(d), & 8 \parallel d. \end{cases} \tag{57}$$

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 10.5. *Assume that*

- (1)  $d$  is a fundamental discriminant;
- (2)  $d \equiv 2 \pmod{3}$ .

Then the root number of  $E_d$  is given by

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

*Proof.* The proof is similar to Lemma 10.4 using [46, Section 9].

- (1) Since  $d$  is a fundamental discriminant, we again have the formula (56).
- (2) Note 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 (57).

Now the result again follows from the product formula.  $\square$

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

**THEOREM 10.6.** *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

$$\log_{\omega_{E_d}} P_d \not\equiv 0 \pmod{3}. \quad (58)$$

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 7.1 for  $p = 3$  and noting that  $|\tilde{E}_d^{\text{ns}}(\mathbb{F}_3)| = 3$  since  $E_d$  has additive reduction at 3. It remains to check that all the assumptions of Theorem 7.1 are satisfied. By Lemma 10.3, we have that  $E[3]$  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  $\ell | N_{\text{add}}(E_d)$ , 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 noting 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 (35) (see also Corollary 8.3).  $\square$

**COROLLARY 10.7.** *Assume that we are in the situation of Theorem 10.6.*

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

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

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

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

*Proof.* It follows immediately from Theorem 10.6 using the root number calculation in Lemmas 10.4 and 10.5.  $\square$

**COROLLARY 10.8.** *The weak Goldfeld's conjecture holds for the sextic twist family  $\{E_d\}$ . In fact,  $E_d$  has analytic rank 0 (respectively 1) for at least 1/6 of fundamental discriminants  $d$ .*

*Proof.* By Theorem 9.5, at least 1/3 of all (positive or negative) fundamental discriminants  $d$  satisfy the assumptions of Theorem 10.6, and by Remark 9.6, 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 10.6. The final part of Theorem 9.5 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  $r_{\text{an}}(E_d) = 0$  (respectively 1) by Corollary 10.7. The desired density 1/6 then follows.  $\square$

REMARK 10.9. One can also obtain  $r_{\text{an}}(E_d) \in \{0, 1\}$  for many  $d$ 's which are not fundamental discriminants. From the proof of Theorem 10.6, 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 that  $d$  is a fundamental discriminant only to simplify the root number computation in Lemmas 10.4 and 10.5.

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

THEOREM 10.10. *Assume that we are in the situation of Theorem 10.6. Assume that 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 [28, V.2.2]

$$u_K \cdot c_{E_d} \cdot \prod_{\ell|N(E_d)} c_\ell(E_d) \cdot |\text{III}(E_d/K)|^{1/2} = [E_d(K) : \mathbb{Z}P_d], \quad (59)$$

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 that we are in the situation of Theorem 10.6. 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

$$\prod_{\ell|N(E_d)} c_\ell(E_d) \cdot |\text{III}(E_d/K)|^{1/2} = \frac{[E_d(K) : \mathbb{Z}P_d]}{c_{E_d}}. \quad (60)$$

We will prove BSD(3) by computing the 3-part of both sides of (60) explicitly.

LEMMA 10.11. *We have  $E_d(K)[3] = 0$ .*

*Proof.* By Lemma 10.3, we have  $E_d[3]^{\text{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega)$ . Since neither  $\psi_d$  nor  $\psi_d\omega$  becomes trivial when restricted to  $G_K$ , we know that  $E_d(K)[3] = 0$ .  $\square$

LEMMA 10.12. *If  $\ell|N(E_d)$  and  $\ell \neq 3$  (equivalently,  $\ell|d$ ), then  $3 \nmid c_\ell(E_d)$ .*

*Proof.* By Lemma 10.3, we have  $E_d[3]^{\text{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega)$ . Because  $\psi_d$  and  $\psi_d\omega$  are both nontrivial at  $\ell$  (in fact, ramified at  $\ell$ ), we know that  $E_d(\mathbb{Q}_\ell)[3] = 0$ .

Since  $E_d(\mathbb{Q}_\ell)$  has a pro- $\ell$ -subgroup ( $\ell \neq 3$ ) of finite index and  $E_d(\mathbb{Q}_\ell)$  has trivial 3-torsion, we know that  $3 \nmid c_\ell(E_d)$ .  $\square$

**DEFINITION 10.13.** 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  $\mathcal{L}_v = H_{\text{ur}}^1(F_v, E_d[3])$  is the unramified subspace. Note 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

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

We will consider the following four types of local conditions:

- (1) The *Kummer conditions*  $\mathcal{L}$  given by  $\mathcal{L}_v = \text{im}(E(F_v)/3E(F_v) \rightarrow H^1(F_v, E_d[3]))$ . The 3-Selmer group  $\text{Sel}_3(E_d/F) = H_{\mathcal{L}}^1(F, E_d[3])$  is cut out by the Kummer conditions.
- (2) The *unramified conditions*  $\mathcal{U}$  given by  $\mathcal{U}_v = H_{\text{ur}}^1(F_v, E_d[3])$ .
- (3) The *strict conditions*  $\mathcal{S}$  given by  $\mathcal{S}_v = \mathcal{U}_v$  for  $v \nmid 3$  and  $\mathcal{S}_v = 0$  for  $v \mid 3$ .
- (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  $v \mid 3$ .

**LEMMA 10.14.**  $H_{\mathcal{U}}^1(K, E_d[3]) = H_{\mathcal{S}}^1(K, E_d[3]) = 0$ .

*Proof.* By Shapiro's lemma, we have

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

By Lemma 10.3, we have an exact sequence

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

Restricting to the unramified Selmer group, we obtain a map

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

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

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

Similarly, we have

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

By the assumptions on the 3-class numbers in Theorem 10.6 and Scholz's reflection theorem ([69]; see also [85, 10.2]), we know that the four 3-class numbers appearing above are all trivial. Hence,  $H_{\mathcal{U}}^1(K, E_d[3]) = 0$ . Since by definition, we have

$$H_S^1(K, E_d[3]) \subseteq H_{\mathcal{U}}^1(K, E_d[3]),$$

and we also know that  $H_S^1(K, E_d[3]) = 0$ . □

LEMMA 10.15.  $\dim H_{\mathcal{R}}^1(K, E_d[3]) = 2$ .

*Proof.* It follows from [17, Theorem 2.18] that

$$\dim H_{\mathcal{R}}^1(K, E_d[3]) - \dim H_S^1(K, E_d[3]) = \frac{1}{2} \sum_{v|3} \dim \mathcal{R}_v. \quad (61)$$

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 10.3,  $E_d[3]^{\text{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega)$ . 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 10.14 and formula (61). □

LEMMA 10.16.  $\text{Sel}_3(E_d/K) \cong \mathbb{Z}/3\mathbb{Z}$ . In particular,  $\text{III}(E_d/K)[3] = 0$ .

*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  $\mathcal{L}_v = H_{\text{ur}}^1(K_v, E_d[3])$  by [27, Lemma 6].
- (2) If  $v|\infty$ , then  $v$  is complex and  $H^1(K_v, E_d[3]) = 0$ . So  $\mathcal{L}_v = H_{\text{ur}}^1(K_v, E_d[3]) = 0$ .
- (3) If  $v|d$ , then  $v$  is split in  $K$  and thus  $K_v \cong \mathbb{Q}_\ell$ . By Lemma 10.12,  $c_\ell(E)$  is coprime to 3. It follows that  $\mathcal{L}_v = H_{\text{ur}}^1(K_v, E_d[3])$  by [27, Lemma 6].

It follows from the claim that

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

So  $\dim \text{Sel}_3(E_d/K) \leq 2$  by Lemma 10.15.

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 [19, Theorem 1.8], we know that  $\dim \text{Sel}_3(E_d/K)$  is odd and thus must be 1. Hence,  $\text{Sel}_3(E_d/K) \cong \mathbb{Z}/3\mathbb{Z}$  as desired.  $\square$

LEMMA 10.17. *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  $\text{ord}_3(c_3(E_d)) = \text{ord}_3([E_d(K) : \mathbb{Z}P_d]/c_{E_d})$ .*

*Proof.* The first part follows directly from Tate's algorithm [72, IV.9] (see also the formula in [68, 0.5]).

Suppose  $\text{ord}_3(c_3(E_d)) = 0$ . We need to show that  $\text{ord}_3([E_d(K) : \mathbb{Z}P_d]) = 0$ . If not, then since  $E_d(K)[3] = 0$  (Lemma 10.11), we know that there exists some  $Q \in E_d(K)$  such that  $3Q = nP_d$  for some  $n$  coprime to 3. Let  $\omega_{E_d}$  be the Néron differential of  $E_d$  and let  $\log_{E_d} := \log_{\omega_{E_d}}$ . By the very definition of the Manin constant, we have  $c_{E_d} \cdot \omega_{E_d} = \omega_{E_d}$  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,

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

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

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

which contradicts formula (58).

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

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

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

Since  $c_3(E_d) = 3$  and  $\tilde{E}_d^{\text{ns}}(\mathbb{F}_3) = \mathbb{Z}/3\mathbb{Z}$ , 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

$$E_d(\mathbb{Q}_3)/\hat{E}_d(3\mathbb{Z}_3) \cong \mathbb{Z}/9\mathbb{Z}. \tag{62}$$

Now by formula (58), 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 (62), 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,  $\text{Sel}_3(E_d/K)$  is equal to the strict Selmer group  $H^1_S(K, E_d[3])$ , a contradiction to Lemmas 10.14 and 10.16. □

*Proof of Theorem 10.10.* Theorem 10.10 follows immediately from the equivalent formula (60) and Lemmas 10.12, 10.16 and 10.17. □

### 11. Cubic twist 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 sixth-power-free integer. Recall that for a cube-free positive integer  $D$ , the  $D$ th cubic twist  $E_d$  is the curve  $E_{dD^2}$  (see Definition 10.1). For  $r \geq 0$ , we define

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

to be the counting function for the number of cubic twists of  $E_d$  of analytic rank  $r$ . Recall that by Lemma 10.3,  $E_d[3]^{\text{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega)$ .

**THEOREM 11.1.** *Assume for any prime  $\ell | N(E_d)$ , we have  $\psi_d(\ell) \neq 1$  and  $\psi_d\omega(\ell) \neq 1$ . Assume that 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 11.2.** Note 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)  $\ell$  is split in  $K$ ;
- (2)  $\psi_d(\ell) = -1$  ( $\ell$  is inert in  $\mathbb{Q}(\sqrt{d})$ );
- (3)  $\omega(\ell) = 1$  ( $\ell$  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  $E_{dD^2}[3]^{\text{ss}} \cong \mathbb{F}_3(\psi_d) \oplus \mathbb{F}_3(\psi_d\omega)$ . 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 7.1 ( $p = 3$ ) to  $E_{dD^2}$  and conclude that

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

The root number  $w(E_{dD^2})$  is  $+1$  (respectively  $-1$ ) 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 the standard application of Ikehara's tauberian theorem as in the proof of Theorem 1.12, we know that

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

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

**EXAMPLE 11.3.** 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 11.1 are satisfied. The set  $\mathcal{N}$  in the proof of Theorem 11.1 consists of square-free products of the primes

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

Note 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  $D \in \mathcal{N}$ ,

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

### Acknowledgements

We are grateful to M. Bhargava, J. Coates, D. Goldfeld, B. Gross, B. Mazur, K. Prasanna, P. Sarnak, A. Shnidman, C. Skinner, E. Urban, X. Wan, A. Wiles, S. Zhang and W. Zhang for helpful conversations or comments. Our debt to the two papers [5] and [45] should be clear to the readers. The examples in this article are computed using Sage [67].

### References

- [1] A. Abbes and E. Ullmo, ‘À propos de la conjecture de Manin pour les courbes elliptiques modulaires’, *Compos. Math.* **103**(3) (1996), 269–286.
- [2] A. Agashe, K. Ribet and W. A. Stein, ‘The Manin constant’, *Pure Appl. Math. Q.* **2**(2, part 2) (2006), 617–636.
- [3] N. Balsam, ‘The parity of analytic ranks among quadratic twists of elliptic curves over number fields’, arXiv e-prints, April 2014, <https://arxiv.org/abs/1404.4964>.
- [4] A. Berti, M. Bertolini and R. Venerucci, ‘Congruences between modular forms and the Birch and Swinnerton–Dyer conjecture’, in *Elliptic Curves, Modular Forms and Iwasawa Theory: In Honour of John H. Coates’ 70th Birthday*, Cambridge, UK, March 2015 (eds. D. Loeffler and S. L. Zerbes) (Springer International Publishing, Cham, 2016), 1–31.
- [5] M. Bertolini, H. Darmon and K. Prasanna, ‘Generalized Heegner cycles and  $p$ -adic Rankin  $L$ -series’, *Duke Math. J.* **162**(6) (2013), 1033–1148. With an appendix by Brian Conrad.
- [6] 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.
- [7] 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.
- [8] M. Bhargava, Z. Klagsbrun, R. Lemke Oliver and A. Shnidman, ‘Selmer groups in families of quadratic twists with a 3-isogeny’, arXiv e-prints, September 2017, <https://arxiv.org/abs/1709.09790>.
- [9] T. D. Browning, ‘Many cubic surfaces contain rational points’, *Mathematika* **63**(3) (2017), 818–839.
- [10] A. A. Burungale, H. Hida and Y. Tian, ‘Horizontal variation of Tate–Shafarevich groups’, arXiv e-prints, December 2017.
- [11] D. Byeon, D. Jeon and C. H. Kim, ‘Rank-one quadratic twists of an infinite family of elliptic curves’, *J. Reine Angew. Math.* **633** (2009), 67–76.

- [12] L. Cai, Y. Chen and Y. Liu, 'Heegner points on modular curves', *Trans. Amer. Math. Soc.* **370** (2018), 3721–3743.
- [13] F. Castella, 'On the  $p$ -part of the Birch–Swinnerton–Dyer formula for multiplicative primes', *Cambridge J. Math.* **6**(1) (2018), 1–23.
- [14] J. Coates, 'Lectures on the Birch–Swinnerton–Dyer conjecture', *ICCM Not.* **1**(2) (2013), 29–46.
- [15] J. Coates, Y. Li, Y. Tian and S. Zhai, 'Quadratic twists of elliptic curves', *Proc. Lond. Math. Soc.* (3) **110**(2) (2015), 357–394.
- [16] R. F. Coleman, 'Torsion points on curves and  $p$ -adic abelian integrals', *Ann. of Math.* (2) **121**(1) (1985), 111–168.
- [17] H. Darmon, F. Diamond and R. Taylor, 'Fermat's last theorem', in *Elliptic Curves, Modular Forms & Fermat's Last Theorem (Hong Kong, 1993)* (International Press, Cambridge, MA, 1997), 2–140.
- [18] H. Davenport and H. Heilbronn, 'On the density of discriminants of cubic fields. II', *Proc. R. Soc. Lond. A* **322**(1551) (1971), 405–420.
- [19] T. Dokchitser and V. Dokchitser, 'Root numbers and parity of ranks of elliptic curves', *J. Reine Angew. Math.* **658** (2011), 39–64.
- [20] 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*, Progress in Mathematics, 108 (Birkhäuser Boston, Boston, MA, 1993), 61–84.
- [21] D. Goldfeld, 'Conjectures on elliptic curves over quadratic fields', in *Number Theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois University, Carbondale, IL, 1979)*, Lecture Notes in Mathematics, 751 (Springer, Berlin, 1979), 108–118.
- [22] C. D. Gonzalez-Avilés, 'On the conjecture of Birch and Swinnerton–Dyer', *Trans. Amer. Math. Soc.* **349**(10) (1997), 4181–4200.
- [23] F. Q. Gouvêa, *Arithmetic of  $p$ -Adic Modular Forms*, Lecture Notes in Mathematics, 1304 (Springer, Berlin, 1988).
- [24] B. H. Gross, 'On the factorization of  $p$ -adic  $L$ -series', *Invent. Math.* **57**(1) (1980), 83–95.
- [25] B. H. Gross, 'Heegner points on  $X_0(N)$ ', in *Modular Forms (Durham, 1983)*, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res. (Horwood, Chichester, 1984), 87–105.
- [26] B. H. Gross, 'Lectures on the conjecture of Birch and Swinnerton–Dyer', in *Arithmetic of  $L$ -Functions*, IAS/Park City Math. Ser., 18 (American Mathematical Society, Providence, RI, 2011), 169–209.
- [27] B. H. Gross and J. A. Parson, 'On the local divisibility of Heegner points', in *Number Theory, Analysis and Geometry* (Springer, New York, 2012), 215–241.
- [28] B. H. Gross and D. B. Zagier, 'Heegner points and derivatives of  $L$ -series', *Invent. Math.* **84**(2) (1986), 225–320.
- [29] D. R. Heath-Brown, 'The size of Selmer groups for the congruent number problem. II', *Invent. Math.* **118**(2) (1994), 331–370. With an appendix by P. Monsky.
- [30] D. R. Heath-Brown, 'The average analytic rank of elliptic curves', *Duke Math. J.* **122**(3) (2004), 591–623.
- [31] H. Hida and J. Tilouine, 'Anti-cyclotomic Katz  $p$ -adic  $L$ -functions and congruence modules', *Ann. Sci. Éc. Norm. Supér.* (4) **26**(2) (1993), 189–259.
- [32] K. James, ' $L$ -series with nonzero central critical value', *J. Amer. Math. Soc.* **11**(3) (1998), 635–641.
- [33] K. James, 'Elliptic curves satisfying the Birch and Swinnerton–Dyer conjecture mod 3', *J. Number Theory* **76**(1) (1999), 16–21.
- [34] D. Jetchev, C. Skinner and X. Wan, 'The Birch and Swinnerton–Dyer formula for elliptic curves of analytic rank one', *Camb. J. Math.* **5**(3) (2017).

- [35] D. Kane, 'On the ranks of the 2-Selmer groups of twists of a given elliptic curve', *Algebra Number Theory* **7**(5) (2013), 1253–1279.
- [36] K. Kato, ' $p$ -adic Hodge theory and values of zeta functions of modular forms', *Astérisque* (295) (2004), ix, 117–290. Cohomologies  $p$ -adiques et applications arithmétiques. III.
- [37] N. M. Katz, 'Higher congruences between modular forms', *Ann. of Math. (2)* **101** (1975), 332–367.
- [38] N. M. Katz, ' $p$ -adic interpolation of real analytic Eisenstein series', *Ann. of Math. (2)* **104**(3) (1976), 459–571.
- [39] N. M. Katz, ' $p$ -adic  $L$ -functions for CM fields', *Invent. Math.* **49**(3) (1978), 199–297.
- [40] N. M. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues, and Monodromy*, American Mathematical Society Colloquium Publications, 45 (American Mathematical Society, Providence, RI, 1999).
- [41] S. Kobayashi, 'The  $p$ -adic Gross–Zagier formula for elliptic curves at supersingular primes', *Invent. Math.* **191**(3) (2013), 527–629.
- [42] D. Kriz, 'Generalized Heegner cycles at Eisenstein primes and the Katz  $p$ -adic  $L$ -function', *Algebra Number Theory* **10**(2) (2016), 309–374.
- [43] B. V. Le Hung and C. Li, 'Level raising mod 2 and arbitrary 2-Selmer ranks', *Compos. Math.* **152**(8) (2016), 1576–1608.
- [44] 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.
- [45] Y. Liu, S. Zhang and W. Zhang, 'A  $p$ -adic Waldspurger formula', *Duke Math. J.* **167**(4) (2018), 743–833.
- [46] E. Liverance, 'A formula for the root number of a family of elliptic curves', *J. Number Theory* **51**(2) (1995), 288–305.
- [47] B. Mazur, 'On the arithmetic of special values of  $L$  functions', *Invent. Math.* **55**(3) (1979), 207–240.
- [48] B. Mazur and K. Rubin, 'Ranks of twists of elliptic curves and Hilbert's tenth problem', *Invent. Math.* **181**(3) (2010), 541–575.
- [49] B. Mazur and K. Rubin, 'Diophantine stability', *Amer. J. Math.* **140**(3) (2018), 571–616. With an appendix by M. Larsen.
- [50] B. Mazur, 'Rational points of abelian varieties with values in towers of number fields', *Invent. Math.* **18** (1972), 183–266.
- [51] R. L. Miller, 'Proving the Birch and Swinnerton–Dyer conjecture for specific elliptic curves of analytic rank zero and one', *LMS J. Comput. Math.* **14** (2011), 327–350.
- [52] J. S. Milne, *Arithmetic Duality Theorems*, Perspectives in Mathematics, 1 (Academic Press, Inc., Boston, MA, 1986).
- [53] J. S. Milne, *Arithmetic Duality Theorems*, second edition, (BookSurge, LLC, Charleston, SC, 2006).
- [54] P. Monsky, 'Generalizing the Birch–Stephens theorem. I. Modular curves', *Math. Z.* **221**(3) (1996), 415–420.
- [55] J. Nakagawa and K. Horie, 'Elliptic curves with no rational points', *Proc. Amer. Math. Soc.* **104**(1) (1988), 20–24.
- [56] J. Nekovář, 'Class numbers of quadratic fields and Shimura's correspondence', *Math. Ann.* **287**(4) (1990), 577–594.
- [57] K. Ono, 'A note on a question of J. Nekovář and the Birch and Swinnerton–Dyer conjecture', *Proc. Amer. Math. Soc.* **126**(10) (1998), 2849–2853.
- [58] K. Ono, 'Nonvanishing of quadratic twists of modular  $L$ -functions and applications to elliptic curves', *J. Reine Angew. Math.* **533** (2001), 81–97.

- [59] K. Ono and C. Skinner, 'Non-vanishing of quadratic twists of modular  $L$ -functions', *Invent. Math.* **134**(3) (1998), 651–660.
- [60] A. Perelli and J. Pomykala, 'Averages of twisted elliptic  $L$ -functions', *Acta Arith.* **80**(2) (1997), 149–163.
- [61] B. Perrin-Riou, 'Points de Heegner et dérivées de fonctions  $L$   $p$ -adiques', *Invent. Math.* **89**(3) (1987), 455–510.
- [62] R. Pollack and K. Rubin, 'The main conjecture for CM elliptic curves at supersingular primes', *Ann. of Math. (2)* **159**(1) (2004), 447–464.
- [63] K. Prasanna, 'On  $p$ -adic properties of central  $L$ -values of quadratic twists of an elliptic curve', *Canad. J. Math.* **62**(2) (2010), 400–414.
- [64] K. Rubin, 'Congruences for special values of  $L$ -functions of elliptic curves with complex multiplication', *Invent. Math.* **71**(2) (1983), 339–364.
- [65] K. Rubin, 'The 'main conjectures' of Iwasawa theory for imaginary quadratic fields', *Invent. Math.* **103**(1) (1991), 25–68.
- [66] K. Rubin, ' $p$ -adic  $L$ -functions and rational points on elliptic curves with complex multiplication', *Invent. Math.* **107**(2) (1992), 323–350.
- [67] The Sage Developers. SageMath, the Sage Mathematics Software System (Version 7.2), 2016. <http://www.sagemath.org>.
- [68] P. Satgé, 'Groupes de Selmer et corps cubiques', *J. Number Theory* **23**(3) (1986), 294–317.
- [69] A. Scholz, 'Über die Beziehung der Klassenzahlen quadratischer Körper zueinander', *J. Reine Angew. Math.* **166** (1932), 201–203.
- [70] J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* **15**(4) (1972), 259–331.
- [71] J.-P. Serre, 'Divisibilité de certaines fonctions arithmétiques', *Enseign. Math. (2)* **22**(3–4) (1976), 227–260.
- [72] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 151 (Springer, New York, 1994).
- [73] C. Skinner and W. Zhang, 'Indivisibility of Heegner points in the multiplicative case', arXiv e-prints, July 2014.
- [74] C. Skinner and E. Urban, 'The Iwasawa main conjectures for  $GL_2$ ', *Invent. Math.* **195**(1) (2014), 1–277.
- [75] A. Smith, 'The congruent numbers have positive natural density', arXiv e-prints, March 2016.
- [76] A. Smith, ' $2^\infty$ -Selmer groups,  $2^\infty$ -class groups, and Goldfeld's conjecture', arXiv e-prints, February 2017.
- [77] F. Sprung, 'The Iwasawa main conjecture for elliptic curves at odd supersingular primes', arXiv e-prints, October 2016.
- [78] G. Stevens, 'Stickelberger elements and modular parametrizations of elliptic curves', *Invent. Math.* **98**(1) (1989), 75–106.
- [79] H. Taya, 'Iwasawa invariants and class numbers of quadratic fields for the prime 3', *Proc. Amer. Math. Soc.* **128**(5) (2000), 1285–1292.
- [80] Y. Tian, X. Yuan and S. Zhang, 'Genus periods, genus points and congruent number problem', *Asian J. Math.* **21**(4) (2017), 721–773.
- [81] Y. Tian, 'Congruent numbers and Heegner points', *Camb. J. Math.* **2**(1) (2014), 117–161.
- [82] V. Vatsal, 'Rank-one twists of a certain elliptic curve', *Math. Ann.* **311**(4) (1998), 791–794.
- [83] V. Vatsal, 'Canonical periods and congruence formulae', *Duke Math. J.* **98**(2) (1999), 397–419.
- [84] X. Wan, 'Iwasawa main conjecture for supersingular elliptic curves', arXiv e-prints, November 2014.

- [85] L. C. Washington, *Introduction to Cyclotomic Fields*, second edition, Graduate Texts in Mathematics, 83 (Springer, New York, 1997).
- [86] M. Watkins, 'Rank distribution in a family of cubic twists', in *Ranks of Elliptic Curves and Random Matrix Theory*, London Mathematical Society Lecture Note Series, 341 (Cambridge University Press, Cambridge, 2007), 237–246.
- [87] H. Yoo, 'Non-optimal levels of a reducible mod  $l$  modular representation', *Trans. Amer. Math. Soc.* **371** (2019), 3805–3830.
- [88] D. Zagier and G. Kramarz, 'Numerical investigations related to the  $L$ -series of certain elliptic curves', *J. Indian Math. Soc. (N.S.)* **52** (1987), 51–69 (1988).
- [89] S. Zhai, 'Non-vanishing theorems for quadratic twists of elliptic curves', *Asian J. Math.* **20**(3) (2016), 475–502.
- [90] W. Zhang, 'Selmer groups and the indivisibility of Heegner points', *Camb. J. Math.* **2**(2) (2014), 191–253.