PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 10, Pages 13–32 (February 8, 2023)
https://doi.org/10.1090/bproc/144

A NOTE ON RANK ONE QUADRATIC TWISTS OF ELLIPTIC CURVES AND THE NON-DEGENERACY OF p-ADIC REGULATORS AT EISENSTEIN PRIMES

ASHAY A. BURUNGALE AND CHRISTOPHER SKINNER

(Communicated by Romyar T. Sharifi)

Abstract. We show that for certain non-CM elliptic curves $E_{/\mathbb{Q}}$ such that 3 is an Eisenstein prime of good reduction, a positive proportion of the quadratic twists E_ψ of E have Mordell–Weil rank one *and* the 3-adic height pairing on $E_\psi(\mathbb{Q})$ is non-degenerate. We also show similar but weaker results for other Eisenstein primes. The method of proof also yields examples of middle codimensional algebraic cycles over number fields of arbitrarily large dimension (generalized Heegner cycles) that have non-zero p-adic height. It is not known – though expected – that the archimedian height of these higher-codimensional cycles is non-zero.

1. Introduction

Let $E_{/\mathbb{Q}}$ be an elliptic curve. It is a famous[1] theorem of Gross and Zagier [16] that for a suitably chosen imaginary quadratic field $K/\mathbb{Q}$,

$$L'(E/K,1) = (*)_{E,K} \cdot \langle y_K, y_K \rangle_{\mathrm{NT}}. \tag{1.1}$$

Here $L(E/K,s) = L(E,s)L(E^K,s)$ is the product of the L-functions of E and its quadratic twist E^K, $(*)_{E,K}$ is some non-zero constant, $y_K \in E(K)$ is the Heegner point, and $\langle -,- \rangle_{\mathrm{NT}}$ the Néron–Tate height pairing on $E(K)$. This gets used two ways in applications: On the one hand, if y_K is non-torsion, then, since the Néron–Tate height pairing is non-zero on non-torsion points, (1.1) implies $\mathrm{ord}_{s=1}L(E/K,s) = 1$ (the hypotheses on K already force the order of vanishing to be ≥ 1). On the other hand, if $\mathrm{ord}_{s=1}L(E,s) = 1$, then choosing K such that $L(E^K,1) \neq 0$, (1.1) implies that y_K is non-torsion.[2]

There is also a p-adic analog of (1.1) due to Perrin-Riou [34] when E has good ordinary reduction at p:

$$L'_p(E/K,1) = (*)_{E,K,p} \cdot \langle y_K, y_K \rangle_p. \tag{1.2}$$

Received by the editors December 13, 2021, and, in revised form, May 17, 2022, and August 25, 2022.

2020 *Mathematics Subject Classification.* Primary 11G05, 11G40, 11G50.

Key words and phrases. Elliptic curves, rational points, p-adic height.

The work of the first author was partially supported by the National Science Foundation Grant DMS-2001409, and that of of the second author by the Simons Investigator Grant #376203 from the Simons Foundation and the National Science Foundation Grant DMS-1901985.

[1] Of course, as stated this relies on the also famous theorem of Wiles *et al.* that all such elliptic curves are modular.

[2] In combination with Kolyvagin's theorems on the Euler system of Heegner points [23], this then implies $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 1$, $\#Ш(E/\mathbb{Q}) < \infty$, and $\langle y,y \rangle_{\mathrm{NT}} \neq 0$ for any $y \in E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}}$.

Here $L_p(E/K,s) = L_p(E,s)L_p(E^K,s)$ is the product of the Mazur–Swinnerton-Dyer p-adic L-functions of E and E^K, $(*)_{E,K,p}$ is a non-zero p-adic number, and $\langle -,- \rangle_p$ is the Perrin-Riou–Schneider p-adic height pairing [35]. One obstacle to using (1.2) just as (1.1) is that it is not generally known in this case that the p-adic height is non-zero on non-torsion rational points.[3][4] Consequently, in the non-CM case, one in general cannot use Heegner points and the Gross–Zagier formulas (1.1) and (1.2) to conclude that $\mathrm{ord}_{s=1}L_p(E,s) = 1$ if $\mathrm{ord}_{s=1}L(E,s) = 1$. However, concluding the opposite implication is fine: If $\mathrm{ord}_{s=1}L_p(E,s) = 1$, then $\mathrm{ord}_{s=1}L(E,s) = 1$, with all the concomitant consequences.

The main result of this note provides examples of *arithmetic* families of non-CM elliptic curves (in this case, quadratic twists) such that an explicit positive proportion of the family can be shown to satisfy (1.2) with both sides non-zero (for a well-chosen K) and hence (1.1) also holds with both sides non-zero. In particular, this proves Schneider's conjecture – that the regulator of the p-adic height pairing is non-degenerate [36] – for these curves. Earlier, Wuthrich [42] gave examples of algebraic families of elliptic curves over $\mathbb{Q}$ for which the specialization of an algebraic section has non-zero p-adic height for all but finitely many of the specializations over $\mathbb{Q}$, providing evidence for the expected non-vanishing of p-adic heights. To our knowledge, however, the results in this paper provide the only known cases of infinite families of elliptic curves for which the p-adic regulator is proved to be non-zero for a given prime p of ordinary reduction.

More precisely, our main result – Theorem 2.8 – pins down conditions guaranteeing that for certain quadratic twists E_ψ of elliptic curves admitting rational isogenies of degree 3, $\mathrm{ord}_{s=1}L_p(E_\psi,s) = 1$. Combined with Perrin-Riou's p-adic Gross–Zagier formula (1.2) we then conclude that the p-adic height of a Heegner point $y_K \in E_\psi(K)$ is non-zero (for a well-chosen K) and hence y_K is non-torsion. This then implies via (1.1) and work of Kolyvagin that $\mathrm{ord}_{s=1}L(E_\psi,s) = 1$, $\mathrm{rank}_{\mathbb{Z}}E_\psi(\mathbb{Q}) = 1$, and $Ш(E_\psi/\mathbb{Q})$ is finite. We emphasize that we obtain $\mathrm{ord}_{s=1}L(E_\psi,s) = 1$ as a consequence of proving that $\mathrm{ord}_{s=1}L_p(E_\psi,s) = 1$. While $L(E,s)$ and $L_p(E,s)$ (for any elliptic curve over $\mathbb{Q}$) are expected to have the same order of vanishing at $s=1$, in general it is only known that each order of vanishing has the same parity (at least in the situations considered herein) and so, in particular, one is odd if and only if the other is.

As an example of an application of our main theorem, consider the elliptic curve

$$E : y^2 + xy + y = x^3 - 36x - 70$$

(this is the curve $14.a3$ in the LMFDB list). It satisfies the hypotheses of our main theorem, and so if ψ is an odd quadratic character such that $\psi(3) = -1$, $\psi(2) = \psi(7) = +1$, and $3 \nmid h_{K_\psi}$ (the class number of the imaginary quadratic field K_ψ corresponding to ψ), then $E_\psi(\mathbb{Q})$ has rank one, the p-adic height of a generator is non-zero, and $\mathrm{ord}_{s=1}L_3(E_\psi,s) = 1 = \mathrm{ord}_{s=1}L(E_\psi,s)$. In particular, this holds

[3]It is, however, known for CM curves: this is a theorem of Bertrand [2], proved via transcendental methods.

[4]In contrast to our lack of knowledge in the case of good ordinary reduction, Kobayashi [22] has proved that if E has good supersingular reduction at p, then the p-adic height of a non-torsion rational point (defined by Zahrin in this case) is always non-zero. While this does not in general prove that the p-adic regulator is non-zero in this case, Kobayashi also proved the analog of (1.2).

for the -55-twist[5] of E. The conditions on ψ are in fact satisfied by a positive proportion of imaginary quadratic fields, ordered by discriminant.

There is a variant of the main result – Theorem 2.10 – with 3 replaced by an odd prime p, but the desired results can only be shown to hold for infinitely many quadratic twists (as opposed to a positive proportion of such). For example, the curve $E : y^2+y = x^3-x^2-10x-20$ (this is the curve $11.a2$ in the LMFDB list) has infinitely many quadratic twists E_ψ of rank one such that a generator of $E_\psi(\mathbb{Q})$ is proved to have non-trivial 5-adic height and $\mathrm{ord}_{s=1}L_5(E_\psi, s) = 1 = \mathrm{ord}_{s=1}L(E_\psi, s)$. (It is, of course, expected that this will hold for a positive proportion: it is even a conjecture of Goldfeld that this proportion should always be $\frac{1}{2}$.) For example, this holds for the -7 and -43 twists of E.

Our main results provide additional evidence towards Goldfeld's Conjecture. The classes of characters ψ to which they apply often complement those appearing in previous results (see the paragraph at the end of section 2.2.1). We can also conclude that the p-part of the Birch–Swinnerton-Dyer formula holds for many of the twists E_ψ arising in the proof of our main results and certain even quadratic twists with analytic rank zero (cf. section 3.1). This also complements previous results on the Birch–Swinnerton-Dyer formula at Eisenstein primes.

The proofs of our main results amount to a simple observation about λ-invariants of p-adic Dirichlet L-series. As explained by Greenberg and Vatsal [15] about twenty years ago, for certain elliptic curves admitting rational p-isogenies, $L_p(E, s)$ is congruent modulo p to the the product of two (possibly imprimitive) p-adic Dirichlet L-series and the λ-invariant λ_E of the former is the sum of the latter two. It is then not difficult to describe situations under which this sum of λ-invariants is 1 and so $\lambda_E = 1$. But $\lambda_E = 1$ just means $\mathrm{ord}_{s=1}L_p(E, s) = 1$. In light of (1.2), this implies $\langle y_K, y_K\rangle_p \neq 0$ for a good choice of K. In particular, the Heegner point y_K is non-torsion and so $\mathrm{ord}_{s=1}L(E, s) = 1$ (by (1.1)).

There are analogs of both (1.1) and (1.2) with E replaced by a newform $f \in S_{2k}(\Gamma_0(N))$:

$$L'(f/K, k) = (*)_{f,K}\cdot\langle z_{K,f}, z_{K,f}\rangle_{\mathrm{BB}} \quad \text{and} \quad L'_p(f/K, k) = (*)_{f,K,p}\cdot\langle z_{K,f}, z_{K,f}\rangle_{p,\mathrm{Nek}},$$

where $z_{K,f}$ is the f-isotypical piece of a generalized Heegner cycle (which belongs to the Chow group of the product of a Kuga–Sato variety; cf. [43] [30]). Here $\langle -, -\rangle_{\mathrm{BB}}$ is the Beilinson–Bloch height pairing [1] [5], and $\langle -, -\rangle_{p,\mathrm{Nek}}$ is Nekovář's p-adic height pairing [29]. In contrast to the weight 2 case (heights on abelian varieties), if $2k > 2$ then it is not known in general that if $z_{K,f}$ has infinite order then $\langle z_{K,f}, z_{K,f}\rangle_{\mathrm{BB}} \neq 0$. Similarly, it is not known in general that if $z_{K,f}$ has infinite order then its image in the Bloch–Kato Selmer group $H^1_{\mathrm{f}}(K, V_f)$ is non-zero (where V_f is the p-adic Galois representation such that $L(V_f, s) = L(f, s+k-1)$). As a consequence of our main results, we can exhibit infinitely many examples where $\langle z_{K,f}, z_{K,f}\rangle_{p,\mathrm{Nek}} \neq 0$ (cf. section 3.2) and so the image of $z_{K,f}$ in $H^1_{\mathrm{f}}(K, V_f)$ must be non-zero (and the dimension of $H^1_{\mathrm{f}}(K, V_f)$ is one). Unfortunately, we cannot conclude from this anything about the non-vanishing of $L'(f/K, k)$ because of the aforementioned lack of knowledge of the non-triviality of $\langle z_{K,f}, z_{K,f}\rangle_{\mathrm{BB}}$. The deduction of these higher-dimensional cases from our results for elliptic curves

[5]This is the curve $42350.bl3$. For this curve, the LMFDB entry does not include a computation of any p-adic regulator, but our results show that the 3-adic regulator is non-zero.

is a straightforward application of Hida theory in combination with the Mazur–Kitagawa two-variable p-adic L-functions.

Of course, all of the results in this paper should easily generalize to newforms $f \in S_2(\Gamma_0(N))$ that are residually reducible at some $p \nmid 2N$ at which f is ordinary. We have left the formulation of such results to the interested reader.

2. p-adic L-functions and Eisenstein primes

In this section we prove our main results on the order of vanishing of p-adic L-functions of quadratic twists of an elliptic curve and concomitant non-vanishing of p-adic heights of Heegner points. We also briefly place these results in the context of Goldfeld's Conjecture and prior results towards it.

2.1. **Iwasawa invariants.**

2.1.1. *Backdrop.* Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N, and let p be an odd Eisenstein prime of good reduction. This means $E[p]$ is a reducible $G_{\mathbb{Q}}$-representation, for $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and so

$$E[p]^{\mathrm{ss}} \simeq \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\chi)$$

as $G_{\mathbb{Q}}$-modules, for characters $\phi, \chi : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$. In particular, $\phi\chi = \omega$, the Teichmüller character. Suppose

(2.1) $\quad \phi$ is either odd and unramified at p or even and ramified at p.

As E has good reduction at p, if ϕ is even and ramified at p then χ is odd and unramified at p.

Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. We identify the Iwasawa algebra $\mathbb{Z}_p[\![\Gamma]\!]$ with the power series ring $\mathbb{Z}_p[\![T]\!]$ by fixing a topological generator $\gamma_0 \in \Gamma$ and identifying $\gamma_0 - 1$ with T. Recall that $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \Delta \times \Gamma$ and that the cyclotomic character $\epsilon : \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^{\times}$ induces an isomorphism $\rho : \Gamma \xrightarrow{\sim} 1 + p\mathbb{Z}_p$.

Let $\mathcal{L}_E, \mathcal{L}_\phi \in \mathbb{Z}_p[\![\Gamma]\!]$ be the associated p-adic L-functions. The p-adic L-function $\mathcal{L}_E$ is just the p-adic L-function $\mathcal{L}(E, \mathbb{1}, T)$ of [15, §3] (which belongs to $\mathbb{Z}_p[\![\Gamma]\!]$ by Cor. (3.8) of *op. cit.* in light of the assumption (2.1)). The p-adic L-function $\mathcal{L}_\phi$ is that denoted $\mathcal{L}(C, T)$ in [15] if ϕ is odd, and if ϕ is even then $\mathcal{L}_\phi = \mathcal{L}_{\phi^{-1}\omega}$. Let $\mu(\mathcal{L}_E)$ and $\mu(\mathcal{L}_\phi)$ be the respective μ-invariants of $\mathcal{L}_E$ and $\mathcal{L}_\phi$, and let $\lambda(\mathcal{L}_E)$ and $\lambda(\mathcal{L}_\phi)$ be their respective λ-invariants.

For any finite character $\theta : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$, let A_θ denote the group $\mathbb{Q}_p/\mathbb{Z}_p$ acting via the composition of θ with the Teichmüller lift $\mathbb{F}_p^{\times} \hookrightarrow \mathbb{Z}_p^{\times}$.

For $\ell \neq p$, let

$$r_\ell = p^{\mathrm{ord}_p((\ell^{p-1}-1)/p)},$$

which is just the number of primes v of $\mathbb{Q}_\infty$ over ℓ, and let

$$t_\ell(E) = \mathrm{corank}_{\mathbb{Z}_p}(A_\phi(\mathbb{Q}_{\infty,v})) + \mathrm{corank}_{\mathbb{Z}_p}(A_\chi(\mathbb{Q}_{\infty,v})) - \mathrm{corank}_{\mathbb{Z}_p}(E(\mathbb{Q}_{\infty,v})_{p^\infty\text{-tor}})$$

for any of the primes v of $\mathbb{Q}_\infty$ over ℓ (all the quantities in the sum are independent of the choice of v). By $A_\theta(\mathbb{Q}_{\infty,v})$ we mean the subgroup of A_θ fixed by a decomposition group for v in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\infty)$.

The following simple formula for the λ-invariant $\lambda(\mathcal{L}_E)$ in terms of $\lambda(\mathcal{L}_\phi)$ and the r_ℓs and t_ℓs is the key ingredient in our main results.

Proposition 2.1. *Suppose* (2.1) *holds. Then*

(i) $\mu(\mathcal{L}_E) = 0$,
(ii) $\lambda(\mathcal{L}_E) = 2\lambda(\mathcal{L}_\phi) + \sum_{\ell|N} r_\ell t_\ell(E)$.

Proof. This is a simple consequence of [15, Thm. 3.11]. □

Let $\varepsilon(E) = \pm 1$ denote the root number of the elliptic curve $E_{/\mathbb{Q}}$. This is the sign of the functional equation of $L(E, s)$. As $p \nmid N$ by hypothesis, it is also the 'sign' of the functional equation of $\mathcal{L}_E$ (cf. [27, Ch. I (18.3)]).

Proposition 2.2. *The root number $\varepsilon(E)$ of E equals $(-1)^{\lambda(\mathcal{L}_E)}$.*

Proof. Let $p^\mu f(T)u(T)$ be the Weierstrass preparation of $\mathcal{L}_E = \mathcal{L}_E(T) \in \mathbb{Z}_p[\![T]\!]$. So $\mu = \mu(\mathcal{L}_E)$, $f(T)$ is a monic polynomial of degree $\lambda = \lambda(\mathcal{L}_E)$, and $u(T) = u_0 + u_1 T + \cdots$ is an invertible power-series. Then $\mathcal{L}_E(-T/(1+T)) = p^\mu f(-T/(T+1))u(-T/(T+1))$. As $u(-T/(T+1))$ is a unit with constant term u_0 and $f(-T/(T+1)) \equiv (-1)^\lambda T^\lambda \bmod p$, it follows that the Weierstrass preparation of $\mathcal{L}_E(-T/(1+T))$ is $p^\mu g(T)v(T)$, where $g(T)$ is a monic polynomial of degree λ and $v(T)$ has constant term congruent to $(-1)^\lambda u_0$ modulo p. It follows that
(2.2)
$$\mathcal{L}_E(T) \equiv p^\mu u_0 T^\lambda \pmod{p^{\mu+1}} \text{ and } \mathcal{L}_E(-T/(1+T)) \equiv p^\mu (-1)^\lambda u_0 T^\lambda \pmod{p^{\mu+1}}.$$

The functional equation of $\mathcal{L}_E$ asserts that

$$\mathcal{L}_E(T) = \varepsilon(E)(1+T)^{\log_p N/\log_p \rho(\gamma_0)} \mathcal{L}_E(-T/(1+T)).$$

This follows from [27, Ch. I (18.3)] with $(1+T) = \epsilon(\gamma_0)^s$. From this together with (2.2) it follows that $p^\mu u_0 T^\lambda \equiv \varepsilon(E) p^\mu (-1)^\lambda u_0 T^\lambda \pmod{p^{\mu+1}}$, and hence that $\varepsilon(E)(-1)^\lambda = 1$. □

2.1.2. *Iwasawa invariants for quadratic twists of elliptic curves and quadratic characters.*

Lemma 2.3. *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N and $p \nmid 2N$ a prime of ordinary reduction. Suppose E admits a cyclic p-isogeny with kernel Φ such that the $G_\mathbb{Q}$-action φ on Φ is either odd and ramified at p or even and unramified at p. Let ψ be an odd quadratic character with $(p\mathrm{cond}^{\mathrm{r}}\varphi, \mathrm{cond}^{\mathrm{r}}\psi) = 1$, and let E_ψ be the associated quadratic twist of E. Then*

(i) $\mu(\mathcal{L}_{E_\psi}) = 0$,
(ii) $\lambda(\mathcal{L}_{E_\psi}) = 2\lambda(\mathcal{L}_{\varphi\psi}) + \sum_{\ell|N, \ell\nmid \mathrm{cond}^{\mathrm{r}}\psi\mathrm{cond}^{\mathrm{r}}\varphi} r_\ell t_\ell(E_\psi)$.

Note that this lemma applies to any $E_{/\mathbb{Q}}$ with a rational point of order p for a prime $p \nmid 2N$ (take Φ to be the subgroup generated by such a point).

Proof. The pair (E_ψ, p) satisfies the hypothesis of Proposition 2.1: $E_\psi[p]^{\mathrm{ss}} = \mathbb{F}_p(\varphi\psi) \oplus \mathbb{F}_p(\omega\varphi^{-1}\psi)$ as a $G_\mathbb{Q}$-module, and (2.1) holds for $\phi = \varphi\psi$. So $\mu(\mathcal{L}_{E_\psi}) = 0$ and

$$\lambda(\mathcal{L}_{E_\psi}) = 2\lambda(\mathcal{L}_{\varphi\psi}) + \sum_{\ell\in\Sigma_\psi} r_\ell t_\ell(E_\psi),$$

where Σ_ψ consists of the primes dividing $N \cdot \mathrm{cond}^{\mathrm{r}}\psi$. For $\ell \mid \mathrm{cond}^{\mathrm{r}}\psi\mathrm{cond}^{\mathrm{r}}\varphi$, $\ell \neq p$, and v a place of $\mathbb{Q}_\infty$ over ℓ, $\varphi\psi|_{G_{\mathbb{Q}_{\infty,v}}}$ and $\omega\varphi^{-1}\psi|_{G_{\mathbb{Q}_{\infty,v}}}$ are non-trivial and so $A_{\varphi\psi}(\mathbb{Q}_{\infty,v})$, $A_{\omega\varphi^{-1}\psi}(\mathbb{Q}_{\infty,v})$ and $E_\psi(\mathbb{Q}_{\infty,v})_{p^\infty-\mathrm{tor}}$ all vanish. Hence $\sum_{\ell\in\Sigma_\psi} r_\ell t_\ell(E_\psi) = \sum_{\ell|N,\ell\nmid \mathrm{cond}^{\mathrm{r}}\psi\mathrm{cond}^{\mathrm{r}}\varphi} r_\ell t_\ell(E_\psi)$. □

The following two examples illustrate the behaviour of the λ-invariants $\lambda(\mathcal{L}_{E_\psi})$ uncovered by this lemma.

Example 1. Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor 11. There is only one isogeny class of such elliptic curves and for these curves $p = 5$ is an Eisenstein prime satisfying (2.1). Let ψ be an odd quadratic character of conductor prime to 55. Then Lemma 2.3 shows that

$$\lambda(\mathcal{L}_{E_\psi}) = 2\lambda(\mathcal{L}_\psi) + \begin{cases} 1 & \text{if 11 splits in the associated imaginary quadratic field } K_\psi \\ 0 & \text{otherwise.} \end{cases}$$

Indeed, $r_{11} = 1$. If $\psi|_{G_{\mathbb{Q}_{11}}}$ is non-trivial, then – since $\omega|_{G_{\mathbb{Q}_{11}}} = 1$ – just as in the proof of Lemma 2.3 we see that $t_{11}(E_\psi) = 0$. If $\psi|_{G_{\mathbb{Q}_{11}}}$ is trivial, then $\mathrm{corank}_{\mathbb{Z}_p}(A_\phi(\mathbb{Q}_{\infty,v})) = \mathrm{corank}_{\mathbb{Z}_p}(A_\psi(\mathbb{Q}_{\infty,v})) = 1$. Furthermore, $\mathrm{corank}_{\mathbb{Z}_p}(E_\psi(\mathbb{Q}_{\infty,v})_{p^\infty-\mathrm{tor}}) = 1$ as $E_\psi \simeq E$ over $\mathbb{Q}_{11}$ and 11 is a prime of split multiplicative reduction for E. So in this case $t_{11}(E_\psi) = 1$.

Example 2. Let $E_{/\mathbb{Q}}$ be the curve $X_0(19)$ (which is just $19.a2$ in the LMFDB list), and let $p = 3$. Then 3 is an Eisenstein prime of E satisfying (2.1) and so

$$\lambda(\mathcal{L}_{E_\psi}) = 2\lambda(\mathcal{L}_\psi) + \begin{cases} 3 & \text{if 19 splits in } K_\psi \\ 0 & \text{otherwise.} \end{cases}$$

Indeed, $r_{19} = 3$ and reasoning analogous to that employed for Example 1 yields the displayed formula. In particular, for quadratic twists E_ψ with root number -1, the λ-invariants $\lambda(E_\psi)$ are all at least 3 (cf. [40]).

Lemma 2.4. *Let ψ be an odd quadratic character and K_ψ the associated imaginary quadratic field. If $p = 3$ we assume that $\psi \neq \omega$.*

(i) *If p splits in K_ψ, then $\lambda(\mathcal{L}_\psi) \geq 1$.*
(ii) *If p is inert in K_ψ and $p \nmid h_{K_\psi}$, then $\lambda(\mathcal{L}_\psi) = 0$.*

Proof. This is surely well-known, but in the absence of a convenient reference we explain a proof. By the interpolation properties of the p-adic L-function, the value of $\mathcal{L}_\psi$ at the trivial character of Γ is $(1 - \psi(p))L(\psi, 0)$, which equals $(1 - \psi(p))2h_{K_\psi}/w_{K_\psi}$, where w_{K_ψ} is the number of roots of unity in K_ψ. If p splits in K_ψ, then $(1 - \psi(p)) = 0$, so the p-adic L-function has a zero at the trivial character, which implies $\lambda(\mathcal{L}_\psi) \geq 1$. If p is inert in K_ψ then $(1 - \psi(p)) = 2$ and the value of the p-adic L-function on the trivial character is $4h_{K_\psi}/w_{K_\psi}$. As $\psi \neq \omega$ if $p = 3$, $w_{K_\psi} = 2$ or 4 if $p = 3$. In particular, if $p \nmid h_{K_\psi}$, then $4h_{K_\psi}/w_{K_\psi}$ is a p-adic unit (recall that p is odd). This implies that $\lambda(\mathcal{L}_\psi) = 0$ in this case. □

Lemma 2.5. *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N and $p > 2$ a prime. Let ψ be a quadratic character, and let E_ψ be the associated quadratic twist of E. Let $\ell \mid N$, $\ell \nmid \mathrm{cond}^{\mathrm{r}}\psi$, be a prime and let v be a prime of $\mathbb{Q}_\infty$ above ℓ. Then*

$$\mathrm{corank}_{\mathbb{Z}_p}(E_\psi(\mathbb{Q}_{\infty,v})_{p^\infty-\mathrm{tor}}) = \begin{cases} 1 & \psi\omega(\ell) = 1 \text{ and } E \text{ has split multiplicative} \\ & \qquad \text{reduction at } \ell \\ 1 & \psi\omega(\ell) = -1 \text{ and } E \text{ has non-split multiplicative} \\ & \qquad \text{reduction at } \ell \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Note that $\mathrm{corank}_{\mathbb{Z}_p}(E_\psi(\mathbb{Q}_{\infty,v})_{p^\infty-\mathrm{tor}})$ is just the rank of $T_pE_\psi^{G_{\mathbb{Q}_{\infty,v}}}$.

Suppose first that E has additive reduction at ℓ. Then $T_pE^{I_\ell}=0$, where $I_\ell\subset G_{\mathbb{Q}_\ell}$ is the inertia subgroup. As ψ is unramified at ℓ, $T_pE_\psi^{I_\ell}=0$. As $\mathbb{Q}_{\infty,v}/\mathbb{Q}_\ell$ is an unramified extension, it follows that $T_pE_\psi^{G_{\mathbb{Q}_{\infty,v}}}=0$. Hence the corank is always 0 in this case.

Suppose then that E has multiplicative reduction at ℓ. In this case the action of $G_{\mathbb{Q}_\ell}$ on T_pE is reducible but indecomposable and equivalent to

$$\begin{pmatrix}\epsilon\alpha^{-1} & *\\ 0 & \alpha\end{pmatrix}$$

where $\alpha: G_{\mathbb{Q}_\ell}\to\{\pm1\}$ is the unramified character such that $\alpha(\mathrm{Fr}_\ell)=+1$ if E has split reduction and $\alpha(\mathrm{Fr}_\ell)=-1$ if E has non-split reduction. As $\mathbb{Q}_{\infty,v}/\mathbb{Q}$ is a pro-p-extension with p-odd, it follows that

$$\begin{aligned}\mathrm{corank}_{\mathbb{Z}_p}(E_\psi(\mathbb{Q}_{\infty,v})_{p^\infty-\mathrm{tor}})=1 &\iff \epsilon\psi\alpha^{-1}\equiv 1 \bmod p\\ &\iff \omega\psi(\ell)=\begin{cases}1 & E \text{ has split reduction at } \ell\\ -1 & E \text{ has non-split reduction at } \ell.\end{cases}\end{aligned}$$

□

2.1.3. *Further preliminaries.*

Lemma 2.6. *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N and $p>2$ a prime. Suppose that E has a rational cyclic subgroup of order p and let φ be the character giving the action of $G_{\mathbb{Q}}$ on such a subgroup (so $E[p]^{\mathrm{ss}}=\mathbb{F}_p(\varphi)\oplus\mathbb{F}_p(\omega\varphi^{-1})$ as a $G_{\mathbb{Q}}$-module). Let $\ell\mid N$, $\ell\neq p$, be a prime.*

(i) *If E has split multiplicative reduction at ℓ, then φ is unramified at ℓ and $(\varphi(\ell),\omega\varphi^{-1}(\ell))=(1,\omega(\ell))$ or $(\omega(\ell),1)$.*
(ii) *If E has non-split multiplicative reduction at ℓ, then φ is unramified at ℓ and $(\varphi(\ell),\omega\varphi^{-1}(\ell))=(-1,\omega(\ell))$ or $(\omega(\ell),-1)$.*
(iii) *If E has additive reduction at ℓ and $p\geq 5$, then φ is ramified at ℓ.*

Proof. If E has multiplicative reduction at ℓ then the claims in (i) and (ii) follow immediately from the action of $G_{\mathbb{Q}_\ell}$ on T_pE as described in the proof of Lemma 2.5. Suppose then that E has additive reduction at ℓ.

If E has potentially multiplicative reduction at ℓ, then $E_{/\mathbb{Q}_\ell}$ is a ramified quadratic twist of an elliptic curve having multiplicative reduction at ℓ. It follows that φ is ramified at ℓ.

If E has potentially good reduction at ℓ, then, as explained by Serre and Tate, in this case the action of I_ℓ is via a non-trivial quotient Φ_ℓ of order dividing 24 that injects into $\mathrm{Aut}(E[p])$ for $p\geq 3$ (cf. [38, §5.6]). So it can only happen that φ is unramified at ℓ if the order of Φ_ℓ is p. In particular, if $p\geq 5$, then it must be that φ is ramified at ℓ. □

Remark 2.7. If $p=3$, then for each of the four possibilities $(s_1,s_2)=(\pm1,\pm1)$ there exists an elliptic curve with a rational cyclic subgroup of order 3 and a prime $\ell\neq p$ of additive – but potentially good – reduction with φ unramified at ℓ and $(\varphi(\ell),\omega\varphi^{-1}(\ell))=(s_1,s_2)$. For example, the curve 196.b2 has additive but potentially good reduction at 7. It has a rational point of order 3, and taking Φ to be the subgroup of order 3 generated by such a point we have $\varphi=\mathbb{1}$ and

$(\varphi(7), \omega\varphi^{-1}(7)) = (1,1)$. Replacing E by a quadratic twist E_ψ with $\psi(7) = -1$ gives an example with $(\varphi(7), \omega\varphi^{-1}(7)) = (-1,-1)$. Similarly, the curve $50.a2$ has additive but potentially good reduction at 5. This curve also has a rational point of order 3, and taking Φ to be the subgroup of order 3 generated by such a point we have $\varphi = \mathbb{1}$ and $(\varphi(5), \omega\varphi^{-1}(5)) = (1,-1)$. A suitable quadratic twist of this curve then gives an example with $(\varphi(5), \omega\varphi^{-1}(5)) = (-1,1)$.

2.2. **The main results.** We now combine the preceding results with Perrin-Riou's p-adic Gross–Zagier formula to prove our main theorems.

2.2.1. *Main results for $p = 3$.* Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N such that $3 \nmid N$. Let $\mathcal{S}$, $\mathcal{N}$, and $\mathcal{A}$ be the respective sets of primes $\ell \mid N$ at which E has split multiplicative reduction, non-split multiplicative reduction, and additive reduction.

Theorem 2.8. *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N such that $3 \nmid N$ and E has a rational subgroup Φ of order 3. Suppose that the character φ giving the $G_\mathbb{Q}$-action on Φ is even and unramified at 3. Suppose also that there exists a prime $\ell_0 \mid N$ with $r_{\ell_0} = 1$, φ unramified at ℓ_0, and such that $\ell_0 \equiv -1 \bmod 3$ if $\ell_0 \in \mathcal{A}$. Let ψ be an odd quadratic character such that $(p\mathrm{cond}^{\mathrm{r}}\varphi, \mathrm{cond}^{\mathrm{r}}\psi) = 1$ and*

(a) $\psi(\ell_0) = \begin{cases} +1 & \ell_0 \in \mathcal{S} \\ -1 & \ell_0 \in \mathcal{N} \\ \pm 1 & \ell_0 \in \mathcal{A}, \end{cases}$

(b) *ψ is either ramified at ℓ or $\psi(\ell) = -1$ for all $\ell_0 \neq \ell \in \mathcal{S}$,*

(c) *ψ is either ramified at ℓ or $\psi(\ell) = +1$ for all $\ell_0 \neq \ell \in \mathcal{N}$,*

(d) *ψ is ramified at all $\ell_0 \neq \ell \in \mathcal{A}$ such that φ is unramified at ℓ and $\ell \equiv -1 \bmod 3$,*

(e) *ψ is either ramified or $\psi(\ell) = -\varphi(\ell)$ for all $\ell_0 \neq \ell \in \mathcal{A}$ such that φ is unramified at ℓ and $\ell \equiv 1 \bmod 3$,*

(f) *$\psi(3) = -\varphi(3)$,*

(g) *$3 \nmid h_{K_{\varphi\psi}}$.*

Then $\lambda(\mathcal{L}_{E_\psi}) = 1$ and consequently

- *$\mathrm{rank}_\mathbb{Z}(E_\psi(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E_\psi, s) = 1$, and*
- *the 3-adic height pairing on $E_\psi(\mathbb{Q})$ is non-degenerate.*

Proof. The right three columns of the following table give the possible values of $t_\ell(E_\psi)$ for primes $\ell \mid N$ for which φ and ψ are unramified:

$\omega(\ell)$	$\varphi(\ell)$	$\psi(\ell)$	$\ell \in \mathcal{S}$	$\ell \in \mathcal{N}$	$\ell \in \mathcal{A}$
$+1$	$+1$	$+1$	1	$*$	2
$+1$	$+1$	-1	0	$*$	0
$+1$	-1	$+1$	$*$	0	0
$+1$	-1	-1	$*$	1	2
-1	$+1$	$+1$	1	0	1
-1	$+1$	-1	0	1	1
-1	-1	$+1$	1	0	1
-1	-1	-1	0	1	1

An entry $*$ means that this case cannot happen (these cases are excluded by Lemma 2.6).

By Lemma 2.3(ii), $\lambda(\mathcal{L}_{E_\psi}) = 2\lambda(\mathcal{L}_{\varphi\psi}) + \sum_{\ell|N,\ell\nmid \mathrm{cond}^{\mathrm{r}}\varphi\mathrm{cond}^{\mathrm{r}}\psi} r_\ell t_\ell(E_\psi)$. It follows from Lemma 2.4(ii) and conditions (f) and (g) on ψ that $\lambda(\mathcal{L}_{\varphi\psi}) = 0$, so $\lambda(\mathcal{L}_{E_\psi}) = \sum_{\ell|N,\ell\nmid \mathrm{cond}^{\mathrm{r}}\varphi} r_\ell t_\ell(E_\psi)$. It follows from the hypotheses on ℓ_0, condition (a), and the above table that $t_{\ell_0}(E_\psi) = 1$. It follows that

$$\lambda(\mathcal{L}_{E_\psi}) = 1 + \sum_{\ell|N,\ell\nmid \ell_0\mathrm{cond}^{\mathrm{r}}\varphi\mathrm{cond}^{\mathrm{r}}\psi} r_\ell t_\ell(E_\psi).$$

All the terms in the sum vanish in light of conditions (b)–(e), as we will explain.

The values of $t_\ell(E_\psi)$ for $\ell \in \mathcal{S}\cup\mathcal{N}$, $\ell \nmid \ell_0\mathrm{cond}^{\mathrm{r}}\psi\mathrm{cond}^{\mathrm{r}}\varphi$ are completely explained by the above table. Comparing (b) and (c) with the table shows that $t_\ell(E_\psi) = 0$ in all these cases. It follows from (d) that the only primes $\ell \in \mathcal{A}$ contributing to the sum are for $\ell \equiv 1 \bmod 3$. Comparing (e) with the table shows that $t_\ell(E_\psi) = 0$ in these cases, too. Putting all this together shows

$$\lambda(\mathcal{L}_{E_\psi}) = 1.$$

As $\lambda(\mathcal{L}_{E_\psi}) = 1$, it follows from Proposition 2.2 that $\varepsilon(E_\psi) = -1$. The p-adic L-function $L_p(E_\psi, s)$ is defined to be $L_p(E_\psi, s) = \mathcal{L}_{E_\psi}(\rho^{1-s})$ (by convention, the right-hand side means the image of $\mathcal{L}_{E_\psi}$ under the continuous ring homomorphism $\mathbb{Z}_p[\![\Gamma]\!] \to \mathbb{Z}_p$ extending ρ^{1-s}). The fact that $\varepsilon(E_\psi) = -1$ implies $L_p(E_\psi, 1) = 0$ as the left-hand side is a multiple of $L(E_\psi, 1)$, which is 0 since the root number is -1. Then $L_p(E_\psi, 1) = 0$ means that $\mathcal{L}_{E_\psi} = (\gamma_0 - 1)\mathcal{L}'_{E_\psi}$ for some $\mathcal{L}'_{E_\psi} \in \mathbb{Z}_p[\![\Gamma]\!]$. As $\lambda(\mathcal{L}_{E_\psi}) = 1$, it follows that $\mathcal{L}'_{E_\psi}(\mathbb{1}) \neq 0$: Under the (fixed, but non-canonical) identification of $\mathbb{Z}_p[\![\Gamma]\!]$ with $\mathbb{Z}_p[\![T]\!]$, $\mathcal{L}_{E_\psi}(T) = T\mathcal{L}'_{E_\psi}(T)$ and $\lambda(\mathcal{L}_\psi)$ is just the degree of the distinguished Weierstrass polynomial of $\mathcal{L}_{E_\psi}(T) = T \cdot$ (distinguished polynomial of $\mathcal{L}'_{E_\psi}(T)$). It follows that $\lambda(\mathcal{L}'_{E_\psi}) = 0$ and so $\mathcal{L}'_{E_\psi}(\mathbb{1}) \neq 0$. It then follows that $L'_p(E_\psi, 1) \neq 0$. The conclusion that $\mathrm{ord}_{s=1}L(E_\psi, s) = 1$, $E_\psi(\mathbb{Q})$ has rank one, and the 3-adic height-pairing is non-degenerate on $E_\psi(\mathbb{Q})$ then follows from Perrin-Riou's p-adic Gross–Zagier formula [34] by the arguments used to deduce [34, Cor. 1.8]; the only extra ingredient needed is the theorem of Kolyvagin [23] that allows us to conclude that the rank of $E_\psi(\mathbb{Q})$ is one in this case and not just at least one. □

Note that the set of all odd quadratic characters ψ as in this theorem has positive density among the set of all odd quadratic characters (when ordered by conductor) by the main results of [10], [18], and [4]. This remains true if we fix a choice for each ℓ of the possibilities allowed in (a)–(e). Consequently we obtain the conclusions of the theorem for a positive proportion of odd quadratic twists E_ψ.

Theorem 2.9. *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N such that $3 \nmid N$ and E has a rational subgroup Φ of order 3. Suppose that the $G_{\mathbb{Q}}$-action on Φ is even and unramified at 3 or odd and ramified at 3. Suppose also that there exists a prime $\ell_0 \mid N$ with $r_{\ell_0} = 1$ and such that $\ell_0 \equiv -1 \bmod 3$ if E has additive reduction at ℓ_0. Then for a positive proportion of odd quadratic characters ψ, $\lambda(\mathcal{L}_{E_\psi}) = 1$ and consequently*

- $\mathrm{rank}_{\mathbb{Z}}(E_\psi(\mathbb{Q})) = \mathrm{ord}_{s=1}L(E_\psi, s) = 1$, *and*
- *the 3-adic height pairing on $E_\psi(\mathbb{Q})$ is non-degenerate.*

Proof. Let φ denote the character giving the action of $G_{\mathbb{Q}}$ on Φ. As the $G_{\mathbb{Q}}$-action on any rational cyclic subgroup of E of order p is given by either φ or $\omega\varphi^{-1}$, replacing E with the quotient E/Φ if necessary, we may assume that φ is even and unramified at 3. Furthermore, upon replacing E by an even quadratic twist if necessary, we may suppose that φ is unramified at the prime ℓ_0. We may then appeal to Theorem 2.8 and the results of [10], [18], and [4] to conclude the positive proportion of desired twists E_ψ. □

Examples.

(E1) Consider the curve $14.a3$ from the LMFDB, which has minimal Weierstrass equation $E : y^2 + xy + y = x^3 - 36x - 70$. This curve has a rational 3-torsion point and satisfies the hypotheses of Theorem 2.8. In this case $\varphi = \mathbb{1}$, $\mathcal{S} = \{7\}$, $\mathcal{N} = \{2\}$, and $\mathcal{A} = \emptyset$. Note that $r_7 = 1$ so we may take $\ell_0 = 7$. By [18] there exists a positive proportion of odd quadratic characters ψ satisfying

$$\psi(7) = 1,\ \psi(2) = 1 \text{ or } \psi \text{ is ramified at } 2,\ \psi(3) = -1,\ 3 \nmid h_{K_\psi}.$$

These correspond to the conditions (a), (c), (f), and (g) of Theorem 2.8, and so the conclusions of the theorem hold for E_ψ. In particular, they hold for for the -55-twist of E (the curve $42350.bl3$ in the LMFDB).

(E2) Consider the curve $20.a3$, which has minimal Weierstrass equation $E : y^2 = x^3 + x^2 - x$. This curve has a rational 3-torsion point and satisfies the conditions of Theorem 2.8. In particular, $\varphi = \mathbb{1}$, $\mathcal{S} = \emptyset$, $\mathcal{N} = \{5\}$, and $\mathcal{A} = \{2\}$. As $r_2 = 1$, we may take $\ell_0 = 2$. By [18] there exists a positive proportion of odd quadratic characters ψ satisfying

$$\psi(2) = \pm 1,\ \psi(5) = 1 \text{ or } \psi \text{ is ramified at } 5,\ \psi(3) = -1,\ 3 \nmid h_{K_\psi}.$$

For all such ψ, the twists E_ψ satisfy the conclusion of Theorem 2.8. In particular, they hold for the -19-twist of E (the curve $7220.f3$).

(E3) The elliptic curves $26.a2$, $34.a3$, $35.a2$, $38.a2$, $44.a2$, $50.a2$, $106c2$ all also have rational 3-torsion points and satisfy the hypotheses of Theorem 2.8.

Relation with Schneider's and Goldfeld's conjectures. For non-CM elliptic curves E, Theorem 2.8 provides some of the first systematic theoretical evidence towards the conjectural non-vanishing of the p-adic regulator for primes p of ordinary reduction (this was first conjectured in [36]). Theorem 2.8 – in the guise of Theorem 2.9 – also provides additional evidence for Goldfeld's conjecture, which predicts the distribution of analytic ranks in the quadratic twist family E_ψ of a given elliptic curve E over the rationals (cf. [14]). Previous evidence has been supplied by the results in [32], [33], [31], [24], [25], among others. For many of the curves to which Theorem 2.9 applies, the class of characters ψ for which the conclusions are proved to hold include a positive proportion of characters not included in these prior results. For example, for the curve in Example (E1), the results of [24] and [25] apply to twists E_ψ that have no primes of split multiplicative reduction, while the characters ψ in (E1) are such that E_ψ always has split multiplicative reduction at 7. In fact, a similar phenomenon always holds whenever $\ell_0 \in \mathcal{S}$.

2.2.2. *The main result for general Eisenstein primes p.* Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N. As before, let $\mathcal{S}$, $\mathcal{N}$, and $\mathcal{A}$ be the respective sets of primes $\ell \mid N$

at which E has split multiplicative reduction, non-split multiplicative reduction, and additive reduction.

Theorem 2.10. *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N and $p \nmid 6N$ a prime. Suppose E has a rational subgroup Φ of order p such that the character φ giving the action of $G_{\mathbb{Q}}$ on Φ has order dividing 2 and is even and unramified at p. Suppose that there exists a prime $\ell_0 \mid N$, $\ell_0 \notin \mathcal{A}$, such that $r_{\ell_0} = 1$. Let ψ be an odd quadratic character such that $(p\mathrm{cond}^{\mathrm{r}}\varphi, \mathrm{cond}^{\mathrm{r}}\psi) = 1$ and*

(a) $\psi(\ell_0) = \begin{cases} +1 & \ell_0 \in \mathcal{S} \\ -1 & \ell_0 \in \mathcal{N}, \end{cases}$
(b) *ψ is either ramified at ℓ or $\psi(\ell) = -1$ for all $\ell_0 \neq \ell \in \mathcal{S}$,*
(c) *ψ is either ramified at ℓ or $\psi(\ell) = +1$ for all $\ell_0 \neq \ell \in \mathcal{N}$,*
(d) *$\psi(p) = -\varphi(p)$,*
(e) *$p \nmid h_{K_{\varphi\psi}}$.*

Then $\lambda(\mathcal{L}_{E_\psi}) = 1$ and consequently

- *$\mathrm{rank}_{\mathbb{Z}}(E_\psi(\mathbb{Q})) = \mathrm{ord}_{s=1}L(E_\psi, s) = 1$, and*
- *the p-adic height pairing on $E_\psi(\mathbb{Q})$ is non-degenerate.*

Proof. This can be proved by the same arguments employed to prove Theorem 2.8. The relevant table is:

$\omega(l)$	$\varphi(l)$	$\psi(l)$	$\ell \in \mathcal{S}$	$\ell \in \mathcal{N}$
$+1$	$+1$	$+1$	1	$*$
$+1$	$+1$	-1	0	$*$
$+1$	-1	$+1$	$*$	0
$+1$	-1	-1	$*$	1
-1	$+1$	$+1$	1	0
-1	$+1$	-1	0	1
-1	-1	$+1$	1	0
-1	-1	-1	0	1
ζ	$+1$	$+1$	1	$*$
ζ	$+1$	-1	0	$*$
ζ	-1	$+1$	$*$	0
ζ	-1	-1	$*$	1

for $\zeta \notin \{\pm 1\}$ a root of unity. An entry $*$ means that this case cannot occur. Note that the need for a column for $\ell \in \mathcal{A}$ is ruled out by Lemma 2.6(iii). □

The analog of the positive proportion results of [10], [18], and [4] are not yet known for primes $p \geq 5$. Consequently we are unable to deduce an analog of the positive proportion result of Theorem 2.9. However, the results of [41] do allow for a weaker result in the case $p = 5$.

Theorem 2.11. *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N with $5 \nmid N$. Suppose E has a rational subgroup Φ of order 5 such that the action of $G_{\mathbb{Q}}$ on Φ has order dividing 2 and is even and unramified at 5. Suppose that there exists a prime $\ell_0 \mid N$ such that $r_{\ell_0} = 1$ and such that E has potential multiplicative reduction at ℓ_0 if $\ell_0 \in \mathcal{A}$. Suppose further that*

(i) *N is odd and for all $\ell_0 \neq \ell \mid N$, $\ell \not\equiv -1 \bmod 5$ and if $\ell \equiv 1 \bmod 5$ then $\ell \not\equiv -1 \bmod 4$,*
(ii) *if $\ell_0 \in \mathcal{S}$, then $\ell_0 \not\equiv -1 \bmod 5$ if $\varphi(\ell_0) = +1$ and either $\ell_0 \not\equiv 1 \bmod 5$ or $\ell_0 \not\equiv -1 \bmod 4$ if $\varphi(\ell_0) = -1$,*
(iii) *if $\ell_0 \in \mathcal{N}$, then $\ell_0 \not\equiv -1 \bmod 5$ if $\varphi(\ell_0) = -1$ and either $\ell_0 \not\equiv 1 \bmod 5$ or $\ell_0 \not\equiv -1 \bmod 4$ if $\varphi(\ell_0) = +1$.*

Then for infinitely many odd quadratic ψ, $\lambda(\mathcal{L}_{E_\psi}) = 1$ and consequently

- $\mathrm{rank}_{\mathbb{Z}}(E_\psi(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E_\psi, s) = 1$, *and*
- *the 5-adic height pairing on $E_\psi(\mathbb{Q})$ is non-degenerate.*

Proof. If E has potentially multiplicative reduction at ℓ_0, then after replacing ℓ_0 by a suitable even quadratic twist we reduce to the case where $\ell_0 \notin \mathcal{A}$. It remains to observe that in this case the set of characters ψ satisfying (a)–(e) of Theorem 2.10 is an infinite set. This is a consequence of the main result of [41] in light of the hypotheses (i)–(iii) on the primes dividing N and the condition (a) on the characters ψ. □

While the fact that $p = 5$ is not used in the proof of Theorem 2.11, the theorem would be vacuously true for $p > 5$. This is a consequence of the hypothesis that N is odd, a restriction made in order to appeal to the main result of [41] (which only allows for prescribed behaviour for ψ at odd primes): If E has odd conductor N and a rational subgroup Φ of order p on which $G_{\mathbb{Q}}$ acts via a character of order at most 2, then $a_2(E) \equiv \pm(1 + 2) \bmod p$. The Riemann hypothesis bound $|a_2(E)| \leq 2\sqrt{2}$ then implies that $p \leq 5$. However, it is still possible to show in some cases that if there exists *one* character ψ as in Theorem 2.10, then there exist infinitely many. An example for $p = 7$ is given in Example (E5).

Examples.

(E4) The elliptic curve 11.a2 in the LMFDB list, which has minimal Weierstrass equation $E : y^2 + y = x^3 - x^2 - 10x - 20$, satisfies the hypotheses of Theorem 2.10 for $p = 5$. This curve has a rational 5-torsion point. In this case $\mathcal{S} = \{\ell_0\} = \{11\}$ and $\varphi = \mathbb{1}$. Note that $\ell_0 \neq -1 \bmod 5$. In particular, if ψ is an odd character such that

$$\psi(11) = +1,\ \psi(5) = -1,\ 5 \nmid h_{K_\psi},$$

then the conclusions of the theorem hold for E_ψ. In particular, they hold for the -7 and -43 twists of E.

(E5) The elliptic curve 26b2 on the LMFDB list, which has minimal Weierstrass equation $E : y^2 + xy + y = x^3 - x^2 - 3x + 3$, has a rational point of order 7. In this case $\mathcal{S} = \{2\}$, $\mathcal{N} = \{13\}$ and $\varphi = \mathbb{1}$. Note that $r_{13} = 1$, so we may take $\ell_0 = 13$. Let ψ_0 be the quadratic character associated with the field $K_0 = \mathbb{Q}(\sqrt{-2})$. Then $\psi_0(7) = -1 = \psi_0(13)$. As $h_{K_0} = 2$, it follows that ψ_0 satisfies the conditions of Theorem 2.10 and so the conclusions of that theorem hold for E_{ψ_0}. Furthermore, [20, Thm. 7.5] ensures that there are infinitely many odd quadratic characters ψ such that ψ equals ψ_0 on decomposition groups at 2, 7, and 13 and such that $7 \nmid h_{K_\psi}$. That is, there are infinitely many ψ satisfying the conditions in Theorem 2.10 for the curve 26b2.

Remark 2.12. The infinitude of characters in Theorem 2.11 (see also Example (E5)) can be partly quantified (cf. [32], [33]).

3. Supplementa

We conclude by recording some consequences for the p-part of the Birch and Swinnerton-Dyer formula for the curves arising from Theorems 2.8 and 2.10 and with an observation on non-vanishing of p-adic heights for some higher codimensional (generalized Heegner) cycles.

3.1. **The Birch and Swinnerton-Dyer formula at Eisenstein primes.** We prove theorems for both analytic ranks one and zero.

Theorem 3.1. *Let $E_{/\mathbb{Q}}$, p, and ψ be as in Theorem* 2.8 *or* 2.10. *Then* $\mathrm{ord}_{s=1}L(E_\psi,1)=1$ *and*

$$\left|\frac{L'(E_\psi,1)}{\mathrm{reg}(E_\psi)\cdot\Omega_{E_\psi}}\right|_p^{-1}=\left|Ш(E_\psi)\prod_{\ell\nmid\infty}c_\ell(E_\psi)\right|_p^{-1},$$

that is, the p-part of the BSD formula holds for E_ψ.

Here, as usual, $\mathrm{reg}(E_\psi)$ is the regulator of $E_\psi(\mathbb{Q})$, $\Omega_{E_\psi}=\int_{E_\psi(\mathbb{R})}\omega_{E_\psi}$ is the real Néron period associated to the Néron differential ω_{E_ψ}, $c_\ell(E_\psi)$ the Tamagawa number at the prime ℓ, and $Ш(E_\psi)$ is the Tate–Shafarevich group of E_ψ over $\mathbb{Q}$.

Proof. The curve E_ψ satisfies the hypothesis of Theorem (1.3) of [15] for the prime p, and consequently the Iwasawa Main Conjecture is true for E_ψ at the prime p. Since the conclusions of Theorems 2.8 and 2.10 are that $\mathrm{ord}_{s=1}L(E_\psi,s)=1$, $\mathrm{rank}_{\mathbb{Z}}E_\psi(\mathbb{Q})=1$, and the p-adic regulator is non-degenerate for E_ψ, the p-part of the Birch–Swinnerton-Dyer formula for E_ψ is then a consequence of [36, Thm. 2′]. □

As an immediate consequence we obtain the following; the proof is just as for Theorem 2.9.

Theorem 3.2. *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N such that $3\nmid N$ and E has a rational subgroup Φ of order 3. Suppose that the $G_{\mathbb{Q}}$-action on Φ is even and unramified at 3 or odd and ramified at 3. Suppose also that there exists a prime $\ell_0\mid N$ with $r_{\ell_0}=1$ and such that $\ell_0\equiv-1 \bmod 3$ if E has additive reduction at ℓ_0. Then for a positive proportion of odd quadratic characters ψ, $\mathrm{ord}_{s=1}L(E_\psi,s)=1$ and the p-part of the BSD formula holds for $L'(E_\psi,1)$.*

There is also a corresponding result for $p=5$, but with 'a positive proportion of' replaced by 'infinitely many,' just as in Theorem 2.11. There is a similar result for other p given the existence of at least one ψ satisfying the conditions of Theorem 2.10; see Example (E5). We leave the formulation of these results to the interested reader.

For *real* quadratic twists of rank zero we deduce the following results.

Theorem 3.3. *Let $E_{/\mathbb{Q}}$, p, and ψ be as in Theorem* 2.8 *or* 2.10 *(so* $\mathrm{ord}_{s=1}L(E_\psi,s)=1$*). Let N_ψ be the conductor of E_ψ. Let $K/\mathbb{Q}$ be an imaginary quadratic field such that*

(i) *the discriminant D_K of K is odd and satisfies $D_K<-4$;*
(ii) *every prime dividing pN_ψ splits in K;*

(iii) $\mathrm{ord}_{s=1} L(E_\psi/K, s) = 1$.

Let ψ_K be the quadratic character associated with K and let $\chi = \psi\psi_K$. Then $L(E_\chi, 1) \neq 0$ and

$$\left|\frac{L(E_\chi, 1)}{\Omega_{E_\chi}}\right|_p^{-1} = \left|Ш(E_\chi)\prod_{\ell\nmid\infty} c_\ell(E_\chi)\right|_p^{-1}.$$

That is, the p-part of the BSD formula holds for E_χ.

Proof. We have $E_\psi[p]^{ss} = \mathbb{F}_p(\phi)\oplus\mathbb{F}_p(\omega\phi^{-1})$ with $\phi = \varphi\psi$ odd and unramified at p. Moreover $\phi(p) = -1$. As explained in the proof of [9, Thm. 5.3.1], the p-part of the BSD formula then holds for $L'(E_\psi/K, 1)$. The key point is that the hypotheses (i)–(iii) of the theorem then imply that the conditions (a)–(d) in *loc. cit.* hold for the curve E_ψ and imaginary quadratic field K. As $L'(E_\psi/K, 1) = L'(E_\psi, 1)L(E_\chi, 1)$ and the p-part of the BSD formula holds for $L'(E_\psi, 1)$ by Theorem 3.1, it follows – just as in the proof of [9, Thm. 5.3.1] – that it also holds for $L(E_\chi, 1)$. □

Corollary 3.4. *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N such that $3 \nmid N$ and E has a rational subgroup Φ of order 3. Suppose that the character φ giving the $G_\mathbb{Q}$-action on Φ is even and unramified at 3 or odd and ramified at 3. Suppose also that there exists a prime $\ell_0 \mid N$ with $r_{\ell_0} = 1$ and such that $\ell_0 \equiv -1 \bmod 3$ if E has additive reduction at ℓ_0. For primes $\ell \in \mathcal{A}\setminus\{\ell_0\}$ at which φ is unramified, suppose that $\ell \equiv 1 \bmod 3$. Let χ be an even quadratic character such that $(3N, \mathrm{cond}^{\mathrm{r}}\chi) = 1$ and*

(a) $\chi(\ell_0) = \begin{cases} +1 & \ell_0 \in \mathcal{S} \\ -1 & \ell_0 \in \mathcal{N} \\ \pm 1 & \ell_0 \in \mathcal{A}, \end{cases}$

(b) $\chi(\ell) = -1$ *for all* $\ell_0 \neq \ell \in \mathcal{S}$,

(c) $\chi(\ell) = +1$ *for all* $\ell_0 \neq \ell \in \mathcal{N}$,

(d) $\chi(\ell) = -\varphi(\ell)$ *for all* $\ell_0 \neq \ell \in \mathcal{A}$ *such that φ is unramified at ℓ and* $\ell \equiv 1 \bmod 3$,

(e) $\chi(3) = -\varphi(3)$.

If $L(E_\chi, 1) \neq 0$, then

$$\left|\frac{L(E_\chi, 1)}{\Omega_{E_\chi}}\right|_3^{-1} = \left|Ш(E_\chi)\prod_{\ell\nmid\infty} c_\ell(E_\chi)\right|_3^{-1}.$$

Proof. Let ψ be an odd quadratic character as in Theorem 2.8 such that $(\mathrm{cond}^{\mathrm{r}}\psi, 3N\mathrm{cond}^{\mathrm{r}}\chi) = 1$, $\chi\psi(l) = +1$ for $l|3N$, and the characters of $\mathbb{Q}_2^\times$ determined by χ and ψ are the same. The condition on the local characters of $\mathbb{Q}_2^\times$ imposes local conditions at 2 on ψ when N is odd; these conditions are in addition to the conditions (a)–(f) of Theorem 2.8 (which are conditions for the primes $\ell \mid 3N$), but in light of the main results of [4] it is still possible to choose ψ to also satisfy condition (g) of the theorem. Observe that the imaginary quadratic field K associated to the character $\chi\psi$ then satisfies the conditions (i)–(iii) of Theorem 3.3. □

Using Theorem 2.11 one can formulate a variant of Corollary 3.4 for $p = 5$. In particular, the 5-part of the BSD formula holds for any even quadratic twist E_χ of the curve $E = X_0(11)$ for which $\chi(11) = +1$, $\chi(5) = -1$ and $L(E_\chi, 1) \neq 0$. A similar result holds for other Eisenstein primes p given the existence of an odd quadratic

ψ satisfying the conditions of Theorem 2.10. We leave the precise formulation of such results to the interested reader.

Next there is a rank zero analog of Theorem 3.1:

Theorem 3.5. *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N such that $3 \nmid N$ and E has a rational subgroup Φ of order 3. Suppose that the $G_{\mathbb{Q}}$-action on Φ is even and unramified at 3 or odd and ramified at 3. Suppose also that there exists a prime $\ell_0 \mid N$ with $r_{\ell_0} = 1$ and such that $\ell_0 \equiv -1 \bmod 3$ if E has additive reduction at ℓ_0. Then for a positive proportion of even quadratic characters χ, $L(E_\chi, 1) \neq 0$ and the 3-part of the BSD formula holds for $L(E_\chi, 1)$.*

Proof. Fix a character ψ satisfying the conditions of Theorem 2.8 (there are infinitely many such – see the proof of Theorem 2.9). It remains to note that a positive proportion of imaginary quadratic fields K satisfy conditions (i), (ii), and (iii) of Theorem 3.3.

By the $r = 0$ case of [9, Thm. 5.2.1], if a K satisfies conditions (i) and (ii) of Theorem 3.3 and $\mathrm{Sel}_{3^\infty}(E_\chi)$ is finite, then $L(E_\chi, 1) \neq 0$, so it also satisfies condition (iii) of Theorem 3.3. We conclude the positive proportion of such K from the main results of [3], especially [3, Thm. 2.4], as follows.

Suppose K satisfies conditions (i) and (ii) of Theorem 3.3. Let $\chi = \psi\psi_K$. This is the quadratic character associated with the real quadratic field $\mathbb{Q}(\sqrt{\mathrm{cond}^{\mathrm{r}}(\psi)|D_K|})$, where D_K is the discriminant of K. Let $\phi_\chi : E_\chi \to E'_\chi$ be the quotient of E_χ by the sugroup $\Phi_\chi \subset E_\chi[3]$ for Φ_χ the χ-twist of Φ. In the notation of [3], $E_\chi = E_s$ for $s = \mathrm{cond}^{\mathrm{r}}(\psi)|D_K| \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, and $\phi_\chi = \phi_s$ for ϕ the quotient of E by Φ. As K varies, s runs over a family $\Sigma \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ defined by local conditions in the sense of [3, Thm. 2.4]. The choices of ψ and K ensure that the global Selmer ratio of [3] satisfies $c(\phi_\chi) = c(\phi_s) = 1$; this is a case-by-case but straight-forward calculation. It then follows from [3, Thm. 2.4] that the average rank of $\mathrm{Sel}_3(E_\chi)$ is ≤ 1. As the root number of E_χ is $+1$ by the choice of χ and $E_\chi[3](\mathbb{Q}) = 0$, the dimension of $\mathrm{Sel}_3(E_\chi)$ is even (see [12]). It follows that a positive proportion of the K's must be such that $\mathrm{Sel}_3(E_\chi) = 0$ (and so $\mathrm{Sel}_{3^\infty}(E_\chi)$ is finite). □

As with Theorem 3.2, there is also a corresponding result for $p = 5$, but with 'a positive proportion of' replaced by 'infinitely many,' just as in Theorem 2.11, and a similar result for other p given the existence of at least one ψ satisfying the conditions of Theorem 2.10. The existence of infinitely many imaginary quadratic fields K as required in the proof follows from now standard analytic results, such as [13, Thm. A]. We also leave the formulation of these results to the interested reader.

Remark 3.6. Theorems 3.1 and 3.2 provide many families of twists that complement the prior results towards the Birch and Swinnerton-Dyer formula for elliptic curves with analytic rank one (cf. [44], [19], [9], [8]). Notice in particular that [9] treats a general yet completely complementary Eisenstein case: $\varphi\psi$ being either ramified at p and odd, or unramified at p and even. Similarly, the prior results in the rank zero case (cf. [26], [15], [39], [9]) exclude the twists covered by Theorems 3.3 and 3.5 and Corollary 3.3.

3.2. **Non-vanishing of p-adic heights: higher-codimensional algebraic cycles.** Finally, we note that as a by-product of our main results and the two-variable p-adic L-function of Kitagawa and Mazur, we can conclude the non-vanishing of

the p-adic heights of some generalized Heegner cycles of codimension greater than one. This is explained as part of the proof of Theorem 3.7.

Let $E_{/\mathbb{Q}}$, p, and ψ be as in Theorem 2.8 or Theorem 2.10. Let $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(N_\psi))$ be the newform associated with the quadratic twist E_ψ of E. As E has ordinary reduction at p and ψ is unramified at p, f is ordinary at p. There is then a Hida family of p-stabilised p-ordinary newforms $\mathbf{f}$ of tame level N_ψ associated with f. Let $\mathbb{I}$ be the finite integral extension of the Hida-Iwasawa algebra $\mathbb{Z}_p[\![X]\!]$ generated by the eigenvalues of $\mathbf{f}$, so we may view $\mathbf{f}$ as an element $\mathbf{f} = \sum_{n=1}^{\infty} \mathbf{a}_n q^n \in \mathbb{I}[\![q]\!]$: if $\phi : \mathbb{I} \to \overline{\mathbb{Q}}_p$ is a continuous $\mathbb{Z}_p$-homomorphism such that $\phi(1+X) = (1+p)^{k-2}$ for $k \geq 2$, then $f_\phi = \sum_{n=1}^{\infty} \phi(\mathbf{a}_n) q^n$ is a p-stabilised p-ordinary newform of weight k, character ω^{2-k}, and tame level N_ψ, and there exists ϕ_0 such that $\phi_0(1+X) = 1$ and f_{ϕ_0} is the p-ordinary stabilisation of f. Let $\mathcal{O}_\phi \subset \overline{\mathbb{Z}}_p$ be the integral closure of $\phi(\mathbb{I})$ (so a finite extension of $\mathbb{Z}_p$) and let $F_\phi \subset \overline{\mathbb{Q}}_p$ be the field of fractions of $\mathcal{O}_\phi$ (so a finite extension of $\mathbb{Q}_p$). Let V_ϕ be the usual two-dimensional F_ϕ-representation of $G_\mathbb{Q}$ associated with f_ϕ.

Theorem 3.7. *Suppose $\mathbb{I} = \mathbb{Z}_p[\![X]\!]$. Let $\phi : \mathbb{I} \to \overline{\mathbb{Q}}_p$ be the continuous $\mathbb{Z}_p$-homomorphism such that $\phi(1+X) = (1+p)^{k-2}$ for an even integer $k > 2$ satisfying $k/2 \equiv 1 \bmod p-1$.*

(i) $\dim_{F_\phi} H^1_{\mathrm{f}}(\mathbb{Q}, V_\phi(1-k/2)) = 1$,

(ii) *the p-adic height pairing[6] on $H^1_{\mathrm{f}}(\mathbb{Q}, V_\phi(1-k/2))$ is non-degenerate,*

where $H^1_{\mathrm{f}}(\cdot)$ denotes the Bloch–Kato Selmer group.

Proof. Let $\mathcal{L}_{\mathbf{f}} \in \mathbb{I}[\![\Gamma]\!] = \mathbb{I}[\![T]\!]$ be the p-adic L-function of Mazur–Kitagawa associated with $\mathbf{f}$ (see [21] and note especially that Condition (B) of [21, §5.5] holds). This has the property that for any $\phi : \mathbb{I} \to \overline{\mathbb{Q}}$ as above, $\mathcal{L}_{\mathbf{f}}$ specializes under ϕ to an element $\mathcal{L}_{f_\phi} \in \mathcal{O}_\phi[\![T]\!]$ that is an $F_\phi^\times$-multiple of the usual p-adic L-function of the newform associated with f_ϕ (cf. [27]), and in particular $\mathcal{L}_{f_{\phi_0}} = \mathcal{L}_{E_\psi}$.

Suppose ϕ is such that $k > 2$ is an even integer and $k/2 \equiv 1 \bmod p-1$. Let $\mathcal{L}_p(f_\phi) = \mathcal{L}_{f_\phi}(\epsilon(\gamma_0)^{k/2-1}(1+T)-1)$. Note that $\mathcal{L}_p(f_\phi)$ is congruent to $\mathcal{L}_p(f_{\phi_0}) = \mathcal{L}_{E_\psi}$ modulo the maximal ideal of the ring of integers of any finite extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$ containing both F_ϕ and F_{ϕ_0}. Since $\mu(\mathcal{L}_{E_\psi}) = 0$ by Lemma 2.3 and $\lambda(\mathcal{L}_{E_\psi}) = 1$ by Theorem 2.8, it follows that $\mathcal{L}_p(f_\phi) \equiv T \bmod \varpi_\phi$, where $\varpi_\phi \in \mathcal{O}_\phi$ is any uniformiser. It follows that the μ- and λ-invariants of $\mathcal{L}_p(f_\phi) \in \mathcal{O}_\phi[\![T]\!]$ are $\mu(\mathcal{L}_p(f_\phi)) = 0$ and $\lambda(\mathcal{L}_p(f_\phi)) = 1$. It then follows from the functional equation of the usual p-adic L-function of f_ϕ that the root number $\varepsilon(f_\phi)$ of the newform associated with f_ϕ equals $(-1)^{\lambda(\mathcal{L}_p(f_\phi))} = -1$; the proof is just as for Proposition 2.2. We thus have

$$\varepsilon(f_\phi) = -1 \quad \text{and} \quad \mathrm{ord}_{T=0}\mathcal{L}_p(f_\phi) = 1. \tag{3.1}$$

Now let K be any imaginary quadratic field such that every prime $\ell \mid pN$ splits in K and $L(f_\phi \otimes \chi_K, k/2) \neq 0$, where χ_K is the odd Dirichlet character associated with K and $f_\phi \otimes \chi_K$ is the corresponding twist of f_ϕ. As $\varepsilon(f_\phi \otimes \chi_K) = \chi_K(-N_\psi)\varepsilon(f_\phi) = +1$, there are infinitely many such K (cf. [13, Thm. A]). Noting that the newform associated with $f_\phi \otimes \chi_K$ is also p-ordinary, we then consider

$$\mathcal{L}_p(f_\phi/K) = \mathcal{L}_p(f_\phi)\mathcal{L}_p(f_\phi \otimes \chi_K).$$

[6]Since f_ϕ is p-ordinary, the ordinary filtration on V_ϕ yields a canonical p-adic height pairing (cf. [29]).

This is an $F_\phi^\times$-multiple of the function denoted $L_p(f_\phi \otimes K, 1)$ in [30]. As the value of $\mathcal{L}_p(f_\phi \otimes \chi_K)$ at $T = 0$ is a non-zero multiple of $L(f_\phi \otimes \chi_K, k/2)$, which is non-zero by the choice of K, it then follows from (3.1) that $\mathrm{ord}_{T=0}\mathcal{L}_p(f_\phi/K) = 1$ and so, in the notation of [30], $L_p'(f_\phi \otimes K, 1, 1) \neq 0$. So by [29, Thm. A] (see also [37]) the p-adic height of the f_ϕ-isotypic piece of the corresponding Heegner cycle – which is a codimension $k/2$-cycle in the $k-1$-dimensional Kuga–Sato variety (the non-singular compactification of the $k-2$-fold self-product of the universal elliptic curve over $Y(N_\phi)$) is non-zero. In particular, the image $z_{f_\phi,1} \in H^1_{\mathrm{f}}(K, V_\phi(1-k/2))$ of this cycle under the p-adic Abel–Jacobi map is also non-zero, and so the conclusions of the theorem follow from [28, Thm. 13.1] (but see also [30, Rem. 6.5] and the note added in proof at the end of *op. cit.* for an explanation of why $p \nmid 2N_\phi$ and f_ϕ ordinary is all that is required of p for the conclusion of [28, Thm. 13.1] to hold). □

The non-vanishing of p-adic heights for Heegner cycles on Kuga–Sato varieties that appears in the preceding proof provides one of the first infinite families of middle codimensional algebraic cycles on varieties over number fields such that the codimension is at least two and the p-adic height is (shown to be) non-zero. An infinite family corresponding to CM newforms was given in [7] and [11] (see also [6]).

As the Hida families for different choices of the character ψ are disjoint, our results in fact yield infinitely many infinite families. Moreover, by appealing to [11], for example, it should be possible to deduce similar non-vanishing results for generalised Heegner cycles (corresponding to twists by infinite order anticyclotomic characters of K). Additionally, other families of Heegner cycles with non-zero p-adic height should similarly arise from the results of [17] and corresponding analogs of Theorems 2.8 and 2.10.

Example.

(E6) Let E be the elliptic curve 14.a3 in the LMFDB list and let ψ be the odd quadratic character of conductor 55. Then Theorem 2.8 applies to E, ψ, and $p = 3$ (see Example (E1)). The modular form associated with E is 14.2.$a.a$ in the LMFDB list. There are exactly 3 newforms of weight 2, trivial character, and level dividing $42 = 3 \cdot 14$. These are the forms 14.2.$a.a$, 21.2.$a.a$, and 42.2.$a.a$ in the LMFDB list. Each has rational Fourier coefficients and so corresponds to an isogeny class of elliptic curves. Of these isogeny classes, only that associated with 14.2.$a.a$ (so the isogeny class of E) admits rational isogenies of degree 3. From this it follows that the ordinary 3-stabilisation of 14.2.$a.a$ is the unique 3-ordinary eigenform of weight 2, trivial character, and level 42 with residually reducible 3-adic Galois representation, and consequently the Hida family associated to 14.2.$a.a$ has $\mathbb{I} = \mathbb{Z}_p[\![X]\!]$. The same is then true for the Hida family associated with any twist of 14.2.$a.a$ by a quadratic character of conductor prime to 42. In particular, it holds for the newform associated with E_ψ (which has level $42350 = 14 \cdot 55^2$). Let g be the weight 6 newform in the Hida family for the newform associated with E_ψ. It then follows that for any imaginary quadratic field K in which each prime $\ell \mid 2 \cdot 3 \cdot 5 \cdot 11$ splits and $L(g \otimes \chi_K, 3) \neq 0$, the 3-adic height of the corresponding Heegner cycle is non-zero. Furthermore, $\dim_{\mathbb{Q}_3} H^1_{\mathrm{f}}(\mathbb{Q}, V_g(-2)) = \dim_{\mathbb{Q}_3} H^1_{\mathrm{f}}(K, V_g(-2)) = 1$ and $H^1_{\mathrm{f}}(K, V_g(-2))$ is

spanned by the image of this cycle. That there are infinitely many such K follows from the main result of [13].

Acknowledgment

We thank the referee for helpful comments.

References

[1] A. Beĭlinson, *Height pairing between algebraic cycles*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, pp. 1–24, DOI 10.1090/conm/067/902590. MR902590

[2] Daniel Bertrand, *Propriétés arithmétiques de fonctions thêta à plusieurs variables* (French), Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 17–22, DOI 10.1007/BFb0099438. MR756080

[3] Manjul Bhargava, Zev Klagsbrun, Robert J. Lemke Oliver, and Ari Shnidman, *3-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field*, Duke Math. J. **168** (2019), no. 15, 2951–2989, DOI 10.1215/00127094-2019-0031. MR4017518

[4] Manjul Bhargava and Ila Varma, *The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders*, Proc. Lond. Math. Soc. (3) **112** (2016), no. 2, 235–266, DOI 10.1112/plms/pdv062. MR3471250

[5] Spencer Bloch, *Height pairings for algebraic cycles*, Proceedings of the Luminy conference on algebraic K-theory (Luminy, 1983), J. Pure Appl. Algebra **34** (1984), no. 2-3, 119–145, DOI 10.1016/0022-4049(84)90032-X. MR772054

[6] Ashay A. Burungale, *Non-triviality of generalised Heegner cycles over anticyclotomic towers: a survey*, p-adic aspects of modular forms, World Sci. Publ., Hackensack, NJ, 2016, pp. 279–306. MR3587960

[7] Ashay A. Burungale and Daniel Disegni, *On the non-vanishing of p-adic heights on CM abelian varieties, and the arithmetic of Katz p-adic L-functions* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **70** (2020), no. 5, 2077–2101. MR4245607

[8] Ashay A. Burungale, Christopher Skinner, and Ye Tian, *The Birch and Swinnerton-Dyer conjecture: a brief survey*, Nine mathematical challenges—an elucidation, Proc. Sympos. Pure Math., vol. 104, Amer. Math. Soc., Providence, RI, [2021] ©2021, pp. 11–29. MR4337415

[9] Francesc Castella, Giada Grossi, Jaehoon Lee, and Christopher Skinner, *On the anticyclotomic Iwasawa theory of rational elliptic curves at Eisenstein primes*, Invent. Math. **227** (2022), no. 2, 517–580, DOI 10.1007/s00222-021-01072-y. MR4372220

[10] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420, DOI 10.1098/rspa.1971.0075. MR491593

[11] Daniel Disegni, *The universal p-adic Gross-Zagier formula*, Invent. Math. **230** (2022), no. 2, 509–649, DOI 10.1007/s00222-022-01133-w. MR4493324

[12] Tim Dokchitser and Vladimir Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596, DOI 10.4007/annals.2010.172.567. MR2680426

[13] Solomon Friedberg and Jeffrey Hoffstein, *Nonvanishing theorems for automorphic L-functions on* GL(2), Ann. of Math. (2) **142** (1995), no. 2, 385–423, DOI 10.2307/2118638. MR1343325

[14] Dorian Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118. MR564926

[15] Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63, DOI 10.1007/s002220000080. MR1784796

[16] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, DOI 10.1007/BF01388809. MR833192

[17] Yuichi Hirano, *Congruences of modular forms and the Iwasawa λ-invariants* (English, with English and French summaries), Bull. Soc. Math. France **146** (2018), no. 1, 1–79, DOI 10.24033/bsmf.2752. MR3864870

[18] Jin Nakagawa and Kuniaki Horie, *Elliptic curves with no rational points*, Proc. Amer. Math. Soc. **104** (1988), no. 1, 20–24, DOI 10.2307/2047452. MR958035

[19] Dimitar Jetchev, Christopher Skinner, and Xin Wan, *The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one*, Camb. J. Math. **5** (2017), no. 3, 369–434, DOI 10.4310/CJM.2017.v5.n3.a2. MR3684675

[20] N. Jochnowitz, *Congruences between modular forms of half integral weights and implications for class numbers and elliptic curves*, preprint.

[21] Koji Kitagawa, *On standard p-adic L-functions of families of elliptic cusp forms*, p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), Contemp. Math., vol. 165, Amer. Math. Soc., Providence, RI, 1994, pp. 81–110, DOI 10.1090/conm/165/01611. MR1279604

[22] Shinichi Kobayashi, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*, Invent. Math. **191** (2013), no. 3, 527–629, DOI 10.1007/s00222-012-0400-9. MR3020170

[23] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $SH(E,\mathbf{Q})$ for a subclass of Weil curves* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671, DOI 10.1070/IM1989v032n03ABEH000779; English transl., Math. USSR-Izv. **32** (1989), no. 3, 523–541. MR954295

[24] Daniel Kriz, *Generalized Heegner cycles at Eisenstein primes and the Katz p-adic L-function*, Algebra Number Theory **10** (2016), no. 2, 309–374, DOI 10.2140/ant.2016.10.309. MR3477744

[25] Daniel Kriz and Chao Li, *Goldfeld's conjecture and congruences between Heegner points*, Forum Math. Sigma **7** (2019), Paper No. e15, 80, DOI 10.1017/fms.2019.9. MR3954912

[26] B. Mazur, *On the arithmetic of special values of L functions*, Invent. Math. **55** (1979), no. 3, 207–240, DOI 10.1007/BF01406841. MR553997

[27] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48, DOI 10.1007/BF01388731. MR830037

[28] Jan Nekovář, *Kolyvagin's method for Chow groups of Kuga-Sato varieties*, Invent. Math. **107** (1992), no. 1, 99–125, DOI 10.1007/BF01231883. MR1135466

[29] Jan Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202, DOI 10.1007/s10107-005-0696-y. MR1263527

[30] Jan Nekovář, *On the p-adic height of Heegner cycles*, Math. Ann. **302** (1995), no. 4, 609–686, DOI 10.1007/BF01444511. MR1343644

[31] Ken Ono, *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves*, J. Reine Angew. Math. **533** (2001), 81–97, DOI 10.1515/crll.2001.027. MR1823865

[32] Ken Ono and Christopher Skinner, *Fourier coefficients of half-integral weight modular forms modulo l*, Ann. of Math. (2) **147** (1998), no. 2, 453–470, DOI 10.2307/121015. MR1626761

[33] Ken Ono and Christopher Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), no. 3, 651–660, DOI 10.1007/s002220050275. MR1660945

[34] Bernadette Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques* (French), Invent. Math. **89** (1987), no. 3, 455–510, DOI 10.1007/BF01388982. MR903381

[35] Peter Schneider, *p-adic height pairings. I*, Invent. Math. **69** (1982), no. 3, 401–409, DOI 10.1007/BF01389362. MR679765

[36] Peter Schneider, *p-adic height pairings. II*, Invent. Math. **79** (1985), no. 2, 329–374, DOI 10.1007/BF01388978. MR778132

[37] Ariel Shnidman, *p-adic heights of generalized Heegner cycles* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **66** (2016), no. 3, 1117–1174. MR3494168

[38] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (French), Invent. Math. **15** (1972), no. 4, 259–331, DOI 10.1007/BF01405086. MR387283

[39] Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), no. 1, 1–277, DOI 10.1007/s00222-013-0448-1. MR3148103

[40] V. Vatsal, *Rank-one twists of a certain elliptic curve*, Math. Ann. **311** (1998), no. 4, 791–794, DOI 10.1007/s002080050209. MR1637976

[41] A. Wiles, *On class groups of imaginary quadratic fields*, J. Lond. Math. Soc. (2) **92** (2015), no. 2, 411–426, DOI 10.1112/jlms/jdv031. MR3404031

[42] Christian Wuthrich, *On p-adic heights in families of elliptic curves*, J. London Math. Soc. (2) **70** (2004), no. 1, 23–40, DOI 10.1112/S0024610704005277. MR2064750

[43] Shouwu Zhang, *Heights of Heegner cycles and derivatives of L-series*, Invent. Math. **130** (1997), no. 1, 99–152, DOI 10.1007/s002220050179. MR1471887
[44] Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2** (2014), no. 2, 191–253, DOI 10.4310/CJM.2014.v2.n2.a2. MR3295917

Department of Mathematics, California Institute of Technology, 1200 E California Blvd, Pasadena, California 91125; and The University of Texas at Austin, Austin, Texas 78712
Email address: ashayburungale@gmail.com

Department of Mathematics, Princeton University, Princeton, New Jersey 08544-1000
Email address: cmcls@princeton.edu