Journal Pre-proof

The even parity Goldfeld conjecture: congruent number elliptic curves

Ashay Burungale, Ye Tian

PII: S0022-314X(21)00177-3
DOI: https://doi.org/10.1016/j.jnt.2021.05.001
Reference: YJNTH 6783

To appear in: *Journal of Number Theory*

Received date: 13 April 2021
Accepted date: 31 May 2021

Please cite this article as: A. Burungale, Y. Tian, The even parity Goldfeld conjecture: congruent number elliptic curves, *J. Number Theory* (2021), doi: https://doi.org/10.1016/j.jnt.2021.05.001.

THE EVEN PARITY GOLDFELD CONJECTURE: CONGRUENT NUMBER ELLIPTIC CURVES

ASHAY BURUNGALE AND YE TIAN

Abstract. In 1979 Goldfeld conjectured: 50% of the quadratic twists of an elliptic curve defined over the rationals have analytic rank zero. In this expository article we present a few recent developments towards the conjecture, especially its first instance - the congruent number elliptic curves.

Contents

1. Introduction

Representation of integers by ternary quadratic forms has rich history, yet it continues to be alluring. Sometimes, it is closely related to the arithmetic of quadratic twist family of elliptic curves defined over the rationals.

A positive square-free integer is called a congruent number if it is the area of a right triangle with rational side lengths. An important open problem: to determine whether or not a given integer is a congruent number, perhaps one of the oldest open problems (cf. [50]). It is closely related to studying rational points on a certain quadratic twist family of elliptic curves - the congruent number elliptic curves.

We begin with the Birch and Swinnerton-Dyer (BSD) conjecture for the congruent number elliptic curves in the guise of:

Conjecture 1.1. *Let n be a positive square-free integer. The following are equivalent.*

(a) *n is a congruent number.*

(b) *Let $a = 1$ if $2 \nmid n$ and $a = 2$ otherwise. Let $\Sigma(n)$ be the set of integral solutions to the equation*

$$2ax^2 + y^2 + 8z^2 = \frac{n}{a}.$$

Then, $\#\{(x, y, z) \in \Sigma(n) : 2|z\} = \#\{(x, y, z) \in \Sigma(n) : 2 \nmid z\}$.

Define

$$\mathcal{L}(n) = \#\{(x,y,z) \in \Sigma(n) : 2|z\} - \#\{(x,y,z) \in \Sigma(n) : 2 \nmid z\}. \tag{1.1}$$

The non-vanishing of $\mathcal{L}(n)$ may be determined in a finite number of steps, while an algorithm to determine whether a given n is a congruent number remains elusive.

In view of Tunnell's theorem and the Coates–Wiles theorem: if $\mathcal{L}(n) \neq 0$, then n is not a congruent number (cf. [15], [52]). Conjecture 1.1 predicts the converse. One may ask:

$$\text{How often is } \mathcal{L}(n) \neq 0? \tag{Q}$$

1.1. **Main result.** Our recent result [12]:

Theorem 1.2. *For a density one subset of positive square-free integers* $n \equiv 1, 2, 3 \pmod 8$,

$$\mathcal{L}(n) \neq 0.$$

Remark 1.3.

- A priori, an independent assertion: for a density one subset of $n \equiv 1, 2, 3 \pmod 8$, n is not a congruent number (cf. [47]).
- For $n \equiv 5, 6, 7 \pmod 8$, notice $\mathcal{L}(n) = 0$. Conjecture 1.1 predicts that these n are congruent. Over the last decade, arithmetic of Heegner point as pioneered by Heegner [28], [37] has led to a progress: [49], [51], [47]. It is now known that more than 50% square-free positive integers $n \equiv 5, 6, 7 \pmod 8$ are congruent numbers (cf. [51], [47]).

1.1.1. *Congruent number elliptic curves.* Theorem 1.2 yields the first instance of the influential (even parity) Goldfeld conjecture [22], which concerns the distribution of analytic ranks in the quadratic twist family of elliptic curves over the rationals:

The congruent number problem may be rephrased in terms of the arithmetic of quadratic twist family of the congruent number elliptic curves[1]

$$E^{(n)} : ny^2 = x^3 - x.$$

Let $L(s, E^{(n)})$ denote the Hasse–Weil L-function of $E^{(n)}$. The integer $\mathcal{L}(n)$ is closely related to the special L-value $L(1, E^{(n)})$.

1.1.2. *Outline.* Theorem 1.2 is a consequence of the following.

- An explicit Shimura–Shintani–Waldspurger correspondence [52]:

$$\mathcal{L}(n) \neq 0 \iff L(1, E^{(n)}) \neq 0.$$

- A p-converse theorem [12]:

$$\text{For any prime } p,\ \#\text{Sel}_{p^\infty}(E^{(n)}/\mathbb{Q}) < \infty \implies L(1, E^{(n)}) \neq 0, \tag{p-cv}$$

  where $\text{Sel}_{p^\infty}(E^{(n)}/\mathbb{Q})$ denotes the p^∞-Selmer group.
- A key progress towards Selmer-counterpart of the Goldfeld conjecture [47]:

$$\text{Prob}\left(\#\text{Sel}_{2^\infty}(E^{(n)}/\mathbb{Q}) < \infty \;\middle|\; n \equiv 1, 2, 3 \pmod 8 \text{ positive square-free}\right) = 100\%.$$

Our essential contribution is the p-converse theorem, especially for the prime $p = 2$. Now, an equivalent form of Theorem 1.2: the even parity Goldfeld conjecture for the congruent elliptic curves -

For a density one subset of positive square-free integers $n \equiv 1, 2, 3 \bmod 8$, one has $L(1, E^{(n)}) \neq 0$.

Remark 1.4. Since its proposal, the Goldfeld conjecture has been studied via diverse tools, yet an example remained elusive. Perhaps enigmatically the first example turns out to be the classical congruent number family. Time and again, the congruent number curves have influenced the arithmetic of general elliptic curves over $\mathbb{Q}$. Even a key precursor to [47] - the congruent number family [51], [46].

[1] Note that n is a congruent number if and only if $\text{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) > 0$.

1.2. **Plan.** The article is essentially an elaboration of §1.1.2. It also reports on a generalisation of Tunnell's theorem to general quadratic twist families of elliptic curves [26] and a preliminary investigation of a missing case in Smith's work [20]. The article is not meant as a survey. For instance, in view of [7], even the discussion of (p-cv) is succinct.

The text begins with the Goldfeld conjecture in §2. Then §3 presents a recent interrelation among ternary quadratic forms and central L-values of a quadratic twist family of elliptic curves over the rationals - a generalisation of Tunnell's theorem (the case of congruent number elliptic curves). Next an update of p-converse theorems appears in §4. Then §5 briefly recalls a few conjectures regarding the distribution of Selmer groups associated to elliptic curves over a fixed number field and Smith's main result. Finally, §6 presents an exploratory study of a missing case in [46], [47].

Acknowledgement. It is a pleasure to thank John Coates, Wei He, Shinichi Kobayashi, Jinzhao Pan, Dinakar Ramakrishnan, Alex Smith, Richard Taylor and Wei Zhang for helpful discussions and instructive comments. The authors cordially thank Chris Skinner and Shou-Wu Zhang for inspiring conversations. The article owes its existence to a generous suggestion of Dorian Goldfeld. The authors would like to express their sincere gratitude to Dorian Goldfeld also for his enticing conjecture.

A. B. is partially supported by the NSF grant DMS #2001409, and Y. T. by the NSFC grants #11688101 and #11531008.

2. Goldfeld's conjecture

2.1. Backdrop.

2.1.1. *The set-up.* An elliptic curve over the rationals is given by a projective curve with affine equation:

$$A : y^2 = x^3 + ax + b$$

for $a, b \in \mathbb{Z}$ with $\Delta := 4a^3 + 27b^2 \neq 0$.

The associated Hasse–Weil L-function $L(s, A)$ is defined as an Euler product

$$L(s, A) := \prod_{p \text{ a prime}} L_p(p^{-s})^{-1}$$

for $s \in \mathbb{C}$, where

$$L_p(X) = 1 - a_p X + pX^2, \quad a_p = p + 1 - \#A(\mathbb{F}_p)$$

for $p \nmid 2\Delta$. Define

$$\Lambda(s, A) := N^{s/2} \cdot 2(2\pi)^{-s}\Gamma(s)L(s, A)$$

for N the conductor.

In view of the Hasse bound $|a_p| \leq 2\sqrt{p}$, the Euler product is absolutely convergent for $\mathrm{Re}(s) > 3/2$. The elemental modularity:

Theorem 2.1. *The Hasse–Weil L-function $L(s, A)$ has entire continuation, which satisfies the functional equation*

$$\Lambda(s, A) = \varepsilon(A)\Lambda(2 - s, A),$$

where $\varepsilon(A) \in \{\pm 1\}$ denotes the root number.

The central vanishing order - $\mathrm{ord}_{s=1}L(s, A)$ - is referred to as the analytic rank of A.

2.1.2. *The Birch and Swinnerton-Dyer conjecture.*

Conjecture 2.2 (The BSD conjecture)**.** *Let A be an elliptic curve over $\mathbb{Q}$.*

(a) $\mathrm{ord}_{s=1}L(s, A) = \mathrm{rank}_{\mathbb{Z}}A(\mathbb{Q})$

(b) *The Tate–Shafarevich group $Ш(A/\mathbb{Q})$ is finite and*

$$\frac{L^{(r)}(1, A)}{r! \cdot \Omega_A \cdot R_A} = \frac{\prod_\ell c_\ell(A) \cdot \#Ш(A/\mathbb{Q})}{\#A(\mathbb{Q})^2_{\mathrm{tor}}}$$

for $r = \mathrm{ord}_{s=1}L(s, A)$, $\Omega_A \in \mathbb{C}^\times$ the Néron period, R_A the regulator of the Néron–Tate height pairing on $A(\mathbb{Q})$ and $c_\ell(A)$ the Tamagawa number at ℓ.

The Tate–Shafarevich group $Ш(A/\mathbb{Q})$ is defined as

$$Ш(A/\mathbb{Q}) = \mathrm{Ker}\left(H^1(\mathbb{Q}, A) \to \prod_p H^1(\mathbb{Q}_p, A)\right).$$

It may be interpreted as the isomorphism classes of A-torsors C such that $C(\mathbb{Q}_p)$ is non-empty for all primes p.

Remark 2.3. For a brief introduction, one may refer to the recent survey [7].

2.2. **Goldfeld's conjecture.** An individual invariant may often be delicate to study, an emerging theme is to instead investigate its variation in a family[2]. In the late 1970's Goldfeld pioneered the exploration of quadratic twist families of elliptic curves over the rationals.

Let $A : y^2 = x^3 + ax + b$ be an elliptic curve over the rationals as above. For a square-free integer d, consider the quadratic twist $A^{(d)} : dy^2 = x^3+ax+b$. A principal insight of Goldfeld is that the underlying analytic or arithmetic invariants often vary systematically in the quadratic twist family $\{A^{(d)}\}_d$.

2.2.1. *The conjecture.* In 1979 Goldfeld [22] proposed the following

Conjecture 2.4 (Goldfeld's conjecture)**.** *Let A be an elliptic curve over $\mathbb{Q}$.*

Then, for a density one subset of square-free integers d with $\varepsilon(A^{(d)}) = +1$ (resp. $\varepsilon(A^{(d)}) = -1$) :

$$\mathrm{ord}_{s=1} L(s, A^{(d)}) = 0, \quad \textit{(resp. } \mathrm{ord}_{s=1} L(s, A^{(d)}) = 1\textit{)}.$$

We refer to the sign $+1$ (resp. -1) part as the even (resp. odd) parity Goldfeld conjecture. It may be easily seen that 50% of the quadratic twists have sign ± 1.

Remark 2.5. The core of Goldfeld's conjecture is his minimalist principle: Often for natural families of elliptic curves over $\mathbb{Q}$ - not just the quadratic twist families - the subfamily with root number $+1$ (resp. -1) has generic analytic rank 0 (resp. 1). In particular, the distribution of analytic rank is the same as that of the root number.

Remark 2.6. It is natural to seek an analogue of the conjecture over number fields. In general, the root number variation in a quadratic twist family may notably differ.

- A counterpart over number fields: [34, Conj. 7.12].
- One may also seek a variant of the conjecture for a self-contragredient cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ for F a number field. Such an investigation appears in [1]. Also see Conjecture 2.8 below.
- An instance of a contrasting root number variation: Let E/F be an elliptic curve with everywhere good reduction, F with no real places but odd (resp. even) number of complex places. Then the root number is given by $\varepsilon(E) = -1$ (resp. $\varepsilon(E) = +1$), further any quadratic twist of E also has root number -1 (resp. $+1$). Such examples perhaps first appeared in [19]. Over $\mathbb{Q}(\sqrt[6]{-11})$, the elliptic curve
$$y^2 = x^3 + \frac{5}{4}x^2 - 2x + 7$$
has everywhere good reduction and its any quadratic twist E' satisfies $\varepsilon(E') = -1$. In contrast, over $\mathbb{Q}(\sqrt[4]{-37})$, the elliptic curve
$$y^2 = x^3 + x^2 - 12x - \frac{67}{4}$$
has everywhere good reduction and its any quadratic twist E' satisfies $\varepsilon(E') = +1$.

2.2.2. *An existence.* We recall a mild, yet general result towards Conjecture 2.4 (cf. [21]).

Let F be a number field and π a self-contragredient cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$. Then its root number $\varepsilon(\pi) \in \{\pm 1\}$ satisfies

$$(-1)^{\mathrm{ord}_{s=1/2} L(s,\pi)} = \varepsilon(\pi),$$

where $L(s, \pi)$ is the L-function of π. Any quadratic twist of π is also self-contragredient.

Theorem 2.7. *Let $\varepsilon \in \{\pm 1\}$ and χ be a quadratic character over F such that $\varepsilon(\pi \otimes \chi) = \varepsilon$. Let S be a finite set of places of F.*

Then, among the quadratic characters χ' over F with $\chi'_v = \chi_v$ for $v \in S$: there exist infinitely many χ' such that $\mathrm{ord}_{s=1/2} L(s, \pi \otimes \chi') = 0$ (resp. 1) if $\varepsilon = +1$ (resp. -1).

[2] which may shed some light on the individual invariant

2.2.3. *The conjecture, again.* In light of Goldfeld's minimalist principle, one may naturally propose:

Conjecture 2.8. *Let π be a self-contragredient cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$. Let χ be a quadratic character over F with $\varepsilon(\pi\otimes\chi)=\varepsilon$ and let S be a finite set of places of F.*

Then, among the quadratic characters χ' over F with

(i) *$\varepsilon(\pi\otimes\chi')=\varepsilon$ and*
(ii) *$\chi'_v=\chi_v$ for $v\in S$,*

the density of χ' with $\mathrm{ord}_{s=1/2}L(s,\pi\otimes\chi')=0$ (resp. 1) is one if $\varepsilon=+1$ (resp. -1).

3. Tunnel's theorem, generalised

The section reports on a recent generalisation [26] of Tunnell's theorem to general quadratic twist families of elliptic curves over $\mathbb{Q}$ (cf. Theorem 3.12) . The strategy - a departure from Tunnell's method - employs general explicit Waldspurger formula [13] and explicit theta liftings.

3.0.1. *Notation.* For $n\in\mathbb{Q}^\times$, let χ_n be the quadratic character over $\mathbb{Q}$ corresponding to the extension $\mathbb{Q}(\sqrt{n})$. For $N\in\mathbb{Z}$ a positive integer, $\chi:(\mathbb{Z}/N\mathbb{Z})^\times\to\mathbb{C}^\times$ a Dirichlet character, and $k\in\frac{1}{2}\mathbb{Z}$ such that $4|N$ if $k\notin\mathbb{Z}$, let $M_k(N,\chi)$ (resp. $S_k(N,\chi)$) denote the space of modular forms (resp. cusp forms) of weight k, level $\Gamma_0(N)$, and character χ. These spaces are endowed with Hecke action.

3.1. Tunnell's theorem.

3.1.1. *The theorem.* Let $E^{(n)}: y^2=x^3-n^2x$ be the congruent elliptic curve, where n is a positive square-free integer.

A link among the central L-values and ternary quadratic forms:

Theorem 3.1 (Tunnell's theorem)**.** *There are weight $3/2$ modular forms,*

$$\sum_{n=1}^{\infty}a_nq^n\in S_{3/2}(128,\mathbf{1}),\quad \sum_{n=1}^{\infty}b_nq^n\in S_{3/2}(128,\chi_2)$$

such that for all positive square-free integers n,

$$\mathcal{L}(n)=\begin{cases}a_n,\\ b_{n/2},\end{cases},\ \frac{L(1,E^{(n)})}{\Omega/\sqrt{n}}=\mathcal{L}(n)^2\cdot\begin{cases}\frac{1}{16},& \text{if } 2\nmid n\\ \frac{1}{8},& \text{if } 2\mid n\end{cases}.$$

Here $\mathcal{L}(n)$ as in (1.1) and $\Omega=\displaystyle\int_1^\infty\frac{\mathrm{d}x}{\sqrt{x^3-x}}$. (cf. [52], [41])

In light of Tunnell's theorem, the central L-values of the quadratic twist family of congruent elliptic curves are modular. Furthermore, the theorem gives an effective way to compute the L-values.

3.1.2. *Tunnell's proof.* The key tool is a fundamental theorem of Waldspurger, which connects

- The Fourier coefficients of half weight modular forms that are Shimura equivalent to a given elliptic newform φ,
- The central L-values of the quadratic twists of φ.

Shimura equivalence. The Shimura equivalence connects - weight 2 and weight 3/2 - Hecke eigenforms.

Given a newform $\varphi\in S_2(M,\chi^2)$ and an positive integer $N\in4\mathbb{Z}\cap2M\mathbb{Z}$, the subspace of $S_{3/2}(N,\chi)$ Shimura equivalent to φ is given by

$$S_{3/2}(N,\chi,\varphi):=\left\{f\in S^\perp_{3/2}(N,\chi)\;\middle|\;T_{p^2}f=a_p(\varphi)f\text{ for all }p\nmid N\right\}.$$

Here $S^\perp_{3/2}(N,\chi)$ is the subspace of $S_{3/2}(N,\chi)$ orthogonal to one variable theta series.

Let $\varphi\in S_2(M,\chi^2)$ be a newform and $\pi=\otimes_v\pi_v$ the irreducible automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ associated to φ. After Flicker, there exists an integer N such that $S_{3/2}(N,\chi,\varphi)\neq0$ if and only if the following hypothesis holds: If $\pi_v=\pi(\xi_{1,v},\xi_{2,v})$ is a principal series with associated characters $\xi_{1,v}$, $\xi_{2,v}$, then

$$\xi_{1,v}(-1)=\xi_{2,v}(-1)=1. \tag{H}$$

Theorem 3.2 (Waldspurger). *Let $\varphi \in S_2(M, \chi^2)$ be a newform that satisfies the hypothesis (H). Let $f = \sum a_n q^n \in S_{3/2}(N, \chi, \varphi)$ with $N \in 4\mathbb{Z} \cap 2M\mathbb{Z}$.*

If n_1, n_2 are positive square-free integers with $n_1/n_2 \in \mathbb{Q}_p^{\times 2}$ for all $p|N$, then

$$a_{n_1}^2 \cdot L\left(1, \varphi \otimes \chi_0^{-1}\chi_{n_2}\right)\sqrt{n_2}\chi(n_2/n_1) = a_{n_2}^2 \cdot L\left(1, \varphi \otimes \chi_0^{-1}\chi_{n_1}\right)\sqrt{n_1}.$$

Here $\chi_0(n) = \chi(n)\left(\frac{-1}{n}\right)$. (cf. [53])

Remark 3.3. A consequence: Assume that $a_n \neq 0$ for a positive square-free n. Then $L(1, \varphi\otimes\chi_0^{-1}\chi_n) \neq 0$, moreover, for any positive square-free m with $m/n \in \mathbb{Q}_p^{\times 2}$ for all $p|N$, one has

$$a_m \neq 0 \iff L(1, \varphi \otimes \chi_0^{-1}\chi_m) \neq 0.$$

Let φ be the newform associated to $E : y^2 = x^3 - x$ of weight 2 and level 32. Now, consider inverse image of the Shimura equivalence for φ. As $S_{3/2}(64, \chi)$ with $\chi^2 = 1$ is generated by one variable theta series, one may resort to $S_{3/2}(128, \chi)$, which is interlaced with weight 1/2 modular forms. Indeed, $S_{3/2}(128, \chi)$ and $M_{1/2}(128, \chi)$ are 3-dimensional, the latter generated by one variable theta series, so multiplication by the unique newform in $S_1(128, \chi_{-2})$ induces an explicit isomorphism

$$M_{1/2}(128, \chi\chi_2) \xrightarrow{\sim} S_{3/2}(128, \chi).$$

This gives rise to $f_1 \in S_{3/2}(128, \mathbf{1})$ and $f_2 \in S_{3/2}(128, \chi_2)$, which are Shimura equivalent to φ satisfying

$$a_1(f_1),\ a_3(f_1),\ a_1(f_2) \text{ and } a_5(f_2) \text{ are non-zero.}$$

Then Theorem 3.1 is just a special case of Theorem 3.2.

Remark 3.4. If the genus class of a definite integral ternary quadratic form consists of only two forms, then the difference of the associated theta series is an eigen cusp form of weight 3/2. Qin found the above weight 3/2 modular forms as such (cf. [41]).

3.2. **General counterpart.** One may seek a generalisation of Tunnell's theorem: As A varies in the quadratic twist family $\mathcal{E}$ of an elliptic curve over $\mathbb{Q}$ -

(a) Encapsulate modularity of a certain "square root" of

$$L^{\mathrm{alg}}(1, A) := \frac{L(1, A)}{\Omega_A} \in \mathbb{Q}.$$

(b) Offer an effective algorithm to compute $L^{\mathrm{alg}}(1, A)$ in terms of ternary quadratic forms. In particular, an algorithm to determine non-vanishing[3] of $L(1, A)$.

The first is essentially addressed by Waldspurger [53]. The second has been studied extensively, a notable progress due to Gross [24] - quadratic twists of elliptic curves with prime conductor - via Waldspurger formula for toric periods. (See also an extension [4] of Gross' work to the square-free conductor case under some local conditions.) Definite ternary quadratic forms are elemental to the approach.

In a recent joint work [26] of the second author, a Waldspurger-style result is reproven in the context of automorphic forms via theta lifting and Waldspurger formula for toric periods (via the local test vector theory developed in [13]). The approach leads to a generalization of the aforementioned results - due to Tunnell and Gross - for any quadratic twist family. In light of the explicit Waldspurger formula [13], (b) is now available for the general quadratic twist family of weight 2 newforms with trivial character.

In general, due to potential local obstruction arising from the action of Atkin–Lehner operators, it is essential to consider a particular subset of the integral solutions of relevant ternary quadratic form. We call them oriented solutions (cf. (ot)). The previous results toward (*b*) implicitly assume the vanishing of the local obstruction (cf. Remark 3.13).

In addition, perhaps surprisingly, it is crucial[4] to resort to certain indefinite ternary quadratic forms (cf. Remark 3.13).

[3] In turn to determine positivity of $\mathrm{rank}_{\mathbb{Z}} A(\mathbb{Q})$ in finitely many steps as $L(1, A) \neq 0 \Rightarrow \mathrm{rank}_{\mathbb{Z}} A(\mathbb{Q}) = 0$ (cf. [15], [31], [35], [45]). Assuming (the rank part of) the BSD conjecture, this is an effective algorithm.

[4] If $\mathcal{E}$ is a family of CM curves or there exists $A \in \mathcal{E}$ such that the conductor of A is not a square, then definite ternary quadratic forms suffice.

3.2.1. *Theta lifting.* The theory of theta lifting generalizes the classical construction of half weight modular forms from quadratic forms.

Let $B/\mathbb{Q}$ be a definite quaternion algebra. Then $V := B^{\mathrm{tr}=0}$ is a quadratic space with quadratic form q given by minus of the reduced norm. Let $H = \mathrm{SO}(V) = PB^\times$ and $\mathbb{G} = \widetilde{\mathrm{SL}_2(\mathbb{A})}$ be the metaplectic double cover of $\mathrm{SL}_2(\mathbb{A})$. Fix a non-trivial additive character ψ of $\mathbb{Q}\backslash\mathbb{A}$. There is a Weil representation w (associated to ψ) of $H(\mathbb{A})\times\mathbb{G}$ on $\mathcal{S}(V(\mathbb{A}))$. Let $\mathcal{A}_0(H)$ (resp. $\mathcal{A}_0(\mathbb{G})$) be the space of automorphic forms on $H(\mathbb{A})$ (resp. $\mathbb{G}$). Theta lifting (associated to ψ) is a systematic mechanism to construct automorphic forms on $\mathbb{G}$ from H and Schwartz functions $\mathcal{S}(V(\mathbb{A}))$, via the Weil representation. For each $\phi\in\mathcal{S}(V(\mathbb{A}))$, the theta kernel function

$$\theta_\phi : (h,g)\mapsto \sum_{x\in V}(w(h,g)\phi)(x)$$

is an automorphic form on $H(\mathbb{A})\times\mathbb{G}$ and gives a $(H(\mathbb{A})\times\mathbb{G})$-equivariant map

$$\theta : \mathcal{A}_0(H)\times\mathcal{S}(V(\mathbb{A}))\to\mathcal{A}_0(\mathbb{G}),\quad (f,\phi)\mapsto\left(\theta_f^\phi : g\mapsto\int_{H(\mathbb{Q})\backslash H(\mathbb{A})} f(h)\theta_\phi(h,g)dh\right).$$

Let $\pi\subset\mathcal{A}_0(H)$ be an irreducible cuspidal representation. Recall the theta lifting of π is defined to be

$$\theta(\pi) := \{\theta_f^\phi \;\big|\; f\in\pi,\phi\in\mathcal{S}(V(\mathbb{A}))\},$$

which is an irreducible cuspidal automorphic representation of $\mathbb{G}$. It is known that $\theta(\pi)\neq 0$ if and only if $L(\frac{1}{2},\pi)\neq 0$.

Let $\mathcal{A}_{0,2}(H)$ denote the space of cuspidal automorphic forms on $H(\mathbb{A})$ with the $H(\mathbb{R})$-action being trivial and let $\pi\subset\mathcal{A}_{0,2}(H)$ be an irreducible. Our goal is to explore precise relation between Fourier coefficients of θ_f^ϕ and the central L-values of quadratic twists of π, by choosing explicit test vectors $f\in\pi$ and $\phi\in\mathcal{S}(V(\mathbb{A}))$.

First of all, the Fourier coefficients of theta liftings θ_f^ϕ have a natural connection with ternary quadratic forms and toric periods.

For $m\in\mathbb{Q}$, $f\in\mathcal{A}_0(H)$ and $\phi\in\mathcal{S}(V(\mathbb{A}))$, define the m-th Fourier coefficient of θ_f^ϕ by

$$W_m(\theta_f^\phi) = \int_{\mathbb{Q}\backslash\mathbb{A}}\theta_f^\phi\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\psi(-mx)dx.$$

Pick $f\in\pi$, then f is constant at infinity and fixed by an open compact subgroup U of $H(\mathbb{A}_f)$. Pick $\phi\in\mathcal{S}(V(\mathbb{A}))$ such that $\phi|_{V_m(\mathbb{A})}\in\mathcal{S}(V_m(\mathbb{A}))^U$, where $V_m(\cdot)=\{x\in V(\cdot)\;\big|\; q(x)=m\}$ for $\cdot=\mathbb{Q},\mathbb{Q}_p,\mathbb{A}$. Assume that $\phi=\phi_{\mathrm{fin}}\otimes\phi_\infty$ with finite part given by $\phi_{\mathrm{fin}}=\mathbf{1}_Z$ for an open compact set $Z\subset V(\mathbb{A}_f)$ and that ϕ_∞ factors through the reduced norm. Say $Z=\widehat{L}$ for a lattice L in V.

On the one hand, $W_m(\theta_f^\phi)$ has expression in terms of ternary quadratic forms:

$$W_m(\theta_f^\phi)\doteq\sum_{[h]\in B^\times\backslash\widehat{B}^\times/U}\frac{f(h)}{w_h}\cdot\#(V_m(\mathbb{Q})\cap Z^h)\tag{FT}$$

with $w_h=\#H(\mathbb{Q})\cap hUh^{-1}$ and $Z^h=hZh^{-1}$. Here '$\doteq$' denotes equality up to an explicit non-zero constant depending on ϕ_∞ and choice of measure.

On the other hand, using Witt theorem, $W_m(\theta_f^\phi)$ can be expressed in terms of toric period: For $x\in V_m(\mathbb{Q})$,

$$W_m(\theta_f^\phi)=\int_{T_x(\mathbb{A})\backslash H(\mathbb{A})}\phi(h^{-1}\cdot x)P_{T_x}(f^h)dh.\tag{FP}$$

Here $\cdot$ denotes the conjugate action of H on V, $T_x\subset H$ is the stabilizer of x, and $P_{T_x}(f)$ is the toric period

$$P_{T_x}(f):=\int_{T_x(\mathbb{Q})\backslash T_x(\mathbb{A})}f(t)dt.$$

For $f\in\pi$, $\phi\in\mathcal{S}(V(\mathbb{A}))$, we seek a relation between the Fourier coefficients $W_m(\theta_f^\phi)$ of θ_f^ϕ and the quadratic twist central L-values $L(\frac{1}{2},\pi\otimes\chi_m)$ as m varies. Let M be the conductor of the Jacquet–Langlands correspondence σ of π.

Definition 3.5. *Let $C\subset\mathbb{Q}^\times$ be an equivalence class with respect to the relation:*

$$a\sim b\quad\Longleftrightarrow\quad a/b\in\mathbb{Q}_v^{\times 2}\quad\text{for all}\quad v\mid 2M\infty.$$

We call C an M-equivalence class.

The root number of $\sigma \otimes \chi_m$ is independent of $m \in C$, denoted by $\varepsilon(C)$. Assume $\varepsilon(C) = 1$ and that (π, C) satisfies the Tunnell–Saito condition (cf. (TS)). In the explicit Waldspurger formula [13] (see Theorem 3.8), as m varies in C, one can find a common vector $f \in \pi$, such that the toric period $P_{T_x}(f)$, is proportional to the base change central L-value $L(\frac{1}{2}, \pi_{K_m}) = L(\frac{1}{2}, \pi)L(\frac{1}{2}, \pi \otimes \chi_m)$. Here $x \in V$ with $q(x) = m$ and $K_m = \mathbb{Q}(\sqrt{m})$.

The following notion of an admissible pair (f, ϕ) for $f \in \pi$ and $\phi \in \mathcal{S}(V(\mathbb{A}))$ is elemental in the context of Shimura equivalence. It is purely local, perhaps easier to check and more flexible than Shimura equivalence.

From now on, further choose ψ in the Weil representation with $\psi_\infty(x) = e^{2\pi i c x}$ for $c \in \mathbb{Q}_{<0}$.

Definition 3.6. *Let $f = \otimes f_v \in \pi$ and $\phi = \otimes_v \phi_v \in \mathcal{S}(V(\mathbb{A}))$ be pure tensors. We call (f, ϕ) an admissible pair if*

- *for $p \nmid 2M\infty$, f_p is spherical and $\phi_p = \mathbf{1}_{M_2(\mathbb{Z}_p)^{\mathrm{tr}=0}}$,*
- *$\phi_\infty(x) = e^{2\pi|c|q(x)}$,*
- *for $p|2M$, $\phi_p \in \mathcal{S}(V(\mathbb{Q}_p))$ is invariant under left multiplication by $1 + 2p\mathbb{Z}_p$.*

Define normalized Fourier coefficients of θ_f^ϕ:

$$a_n(\theta_f^\phi) := e^{2\pi|c|n} W_{-n}(\theta_f^\phi), \quad n \in \mathbb{Q}.$$

Relation of explicit Waldspurger formulae with different test vector is given in [13]. We compare $a_m(\theta_f^\phi)$ with the toric periods defined by another test vector in [13]. It turns out, for an admissible pair (f, ϕ), the ratio is constant as m varies in an equivalence class. We have (cf. [26]):

Theorem 3.7. *Let $\pi \subset \mathcal{A}_{0,2}(H)$ with $L(\frac{1}{2}, \pi) \neq 0$. Let (f, ϕ) be an admissible pair. Then for any positive square-free integers n_1, n_2 with $n_1/n_2 \in \mathbb{Q}_p^{\times 2}$ for all $p|2M$,*

$$a_{n_1}^2(\theta_f^\phi) L\left(\frac{1}{2}, \pi \otimes \chi_{-n_2}\right) \sqrt{n_2} = a_{n_2}^2(\theta_f^\phi) L\left(\frac{1}{2}, \pi \otimes \chi_{-n_1}\right) \sqrt{n_1}.$$

However, the above theorem is ineffective since it does not offer construction of an admissible pair such that the Fourier coefficient with a given index is non-zero. Actually, the construction is the crux of the main result of [26], which relates quadratic twist L-values to ternary quadratic forms.

3.2.2. *Quadratic twist subfamilies.* Let $\mathcal{E}$ be the quadratic twist family of an irreducible cuspidal automorphic representation of $\mathrm{PGL}_2(\mathbb{A})$ whose infinite component is the discrete series of weight 2. We first partition the family into finitely many subfamilies and then for each subfamily, we construct an admissible pair that is effective for this subfamily: the Fourier coefficients of its theta lifting interpret the central L-values of the representations in this subfamily. Furthermore, we also seek to relate the Fourier coefficients to ternary quadratic forms.

Let $\sigma \in \mathcal{E}$ be such that $L(\frac{1}{2}, \sigma) \neq 0$ and M denote the conductor of σ. Let $C \subset \mathbb{Q}^\times$ be an M-equivalence class. Then we have a subfamily of $\mathcal{E}$ given by

$$\mathcal{E}_C := \{\sigma \otimes \chi_m \mid m \in C\} \subset \mathcal{E}.$$

Actually, $\mathcal{E}$ can be covered by finitely many $\mathcal{E}_C$'s (σ may differ).

Notice it suffices to consider a set-up: $L(\frac{1}{2}, \sigma) \neq 0$ and C an M-equivalence class with $\varepsilon(C) = 1$. Let B be the quaternion algebra over $\mathbb{Q}$ such that (σ, C) satisfies Tunnell–Saito condition, i.e. for each $K = \mathbb{Q}(\sqrt{m})$, $m \in C$:

$$\varepsilon(\sigma_v, \mathbf{1}_{K_v}) = \eta_v(-1)\epsilon(B_v) \tag{TS}$$

holds for all places v of $\mathbb{Q}$. Here $\varepsilon(\sigma_v, \mathbf{1}_{K_v})$ is the local root number at v of the Rankin–Selberg L-function $L(s, \sigma \times \mathbf{1}_K)$, η_v the quadratic character associated to the extension $K_v/\mathbb{Q}_v$ and $\epsilon(B_v) \in \{\pm 1\}$ the invariant of B at v. Let $H = PB^\times$ and $\pi \subset \mathcal{A}_0(H)$ be with $\pi^{\mathrm{JL}} = \sigma$.

For simplicity, we often assume σ corresponds to an elliptic curve over $\mathbb{Q}$ and that B is definite[5].

[5] In fact, to construct half weight modular forms effectively for $\mathcal{E}_C$ and to connect with ternary quadratic forms, the ensuing approach works well for a general quaternion algebra.

3.2.3. *Quadratic twist L-values and toric periods.* We first present the explicit Waldspurger formula in [13] which connects toric periods to quadratic twist L-values.

Let $\pi \subset \mathcal{A}_{0,2}(H)$ be irreducible with conductor M. For simplicity, assume that π corresponds to an elliptic curve over $\mathbb{Q}$ via Jacquet-Langlands correspondence. Let $C \subset \mathbb{Q}^\times$ be an M-equivalence class. Assume (π, C) satisfies the Tunnell–Saito condition (TS).

Let $K \subset B$ with $K \simeq \mathbb{Q}(\sqrt{m})$, $m \in C$. An order $R \subset B$ is called admissible (with respect to (π, K)) if its discriminant equals M and $R \cap K = \mathcal{O}_K$. Then the following space is one dimensional:

$$V(\pi, K) := \left\{ f \in \pi \;\middle|\; f \text{ is invariant under } \widehat{R}^\times \text{ and } K_p^\times \text{ for any } p|M \text{ ramified in } K \right\}.$$

We call its generator an admissible test vector for $(\pi, \mathbf{1}_K)$ with level $\widehat{R}^\times$. (A proof of the fact that the space $V(\pi, K)$ is one dimensional and consists of pure tensors appears in [13], which generalizes the newform theory.) Let $\Sigma_C \subset C$ denote the subset of fundamental discriminants in C. A vector $f_0 \in \pi$ is admissible for C if there exists $x \in V_{D_0}(\mathbb{Q})$ for some $D_0 \in \Sigma_C$ and an admissible order R_0 (with respect to $(\pi, \mathbb{Q}(x))$) such that f_0 is an admissible test vector for $(\pi, \mathbf{1}_{\mathbb{Q}(x)})$ with level $\widehat{R}_0^\times$. Let f_0 be admissible for C, then for any $D \in \Sigma_C$ and $x_D \in V_D(\mathbb{Q})$, there exists $h_D \in H(\mathbb{A})$ such that $f_D := f_0^{h_D}$ is an admissible test vector for $(\pi, \mathbf{1}_{\mathbb{Q}(x_D)})$ with level $\widehat{R}_D^\times$ for $R_D := h_D \widehat{R}_0 h_D^{-1} \cap B$ (an admissible order).

In particular, we may choose $h_{D_0} = 1$ and then $f_0 = f_{D_0}$. From now, fix such choices.

For $D \in \Sigma_C$, let $K_D = \mathbb{Q}(x_D)$ and $\mathcal{O}_D$ the ring of integers of K_D. Denote

$$P^0_{K_D}(f_D) := \sum_{t \in \mathrm{Cl}(K_D)} f_D(t).$$

Theorem 3.8 (Explicit Waldspurger formula)**.** *Let f_0 be a non-zero C-admissible test vector, valued in the rationals.*

Then there exists a constant $k_C \in \mathbb{Q}^\times$ dependent only on π and C :

$$\frac{\sqrt{D} \cdot L\left(\frac{1}{2}, \pi_K\right)}{\Omega_\sigma^+ \Omega_\sigma^-} = k_C \cdot \frac{|P^0_K(f_D)|^2}{[\mathcal{O}_D^\times : \mathbb{Z}^\times]^2} \in \mathbb{Q}$$

for all $D \in \Sigma_C$, $K = \mathbb{Q}(\sqrt{D})$. Here $(\Omega_\sigma^+, \Omega_\sigma^-) \in (\mathbb{R}^\times \times i\mathbb{R}^\times)$ are Shimura's fundamental periods associated to σ. (cf. [13])

3.2.4. *Optimal choices.* For B and $f_0 = f_{D_0} \in \pi$ a $\mathbb{Z}$-primitive C-admissible test vector as in Theorem 3.8, one may seek a ϕ_0 inherent to the ternary quadratic form such that exactly one toric period appears in the Fourier coefficients[6] of $\theta_{f_0}^{\phi_0}$. One may even consider all $D \in \Sigma_C$ simultaneously.

To begin, choose h_D for $D \in \Sigma_C$: for $v|2M\infty$ and $D, D' \in \Sigma_C$,

$$h_{D',v}^{-1} \cdot (\sqrt{D/D'} x_{D'}) = h_{D,v}^{-1} \cdot x_D \in V(\mathbb{Q}_v).$$

Here for $p|2M$, view $\sqrt{D/D'}$ as an element in $(1 + 2p\mathbb{Z}_p)$. A simple yet key result [26]:

Proposition 3.9. *There exists a lattice $L_0 \subset V$ and an open compact subgroup $U_0 \subset \widehat{R}_0^\times$ such that*

$$L_D := h_D \widehat{L}_0 h_D^{-1} \cap V$$

is an x_D-distinguished lattice with level $U_D := h_D U_0 h_D^{-1} \subset \widehat{R}_D^\times$ for any $D \in \Sigma_C$ - the definition being:

$$L_{D,p} \cap V_D(\mathbb{Q}_p) = U_{D,p} \cdot \{\pm x_D\}$$

for all prime p.

For unique toric integral to appear in the Fourier coefficients, it is essential to isolate a certain symmetry arising from the abelian group structure of lattices, thereby switching to a finer structure: For a prime $p|2M$, define a local condition $L^o_{D,p} \subset L_{D,p}$ by

$$L^o_{D,p} = \left\{ \ell \in L_{D,p} \;\middle|\; \ell \in U_{D,p} \cdot ((1 + 2p\mathbb{Z}_p) x_D) \right\}$$

Now let $\phi_D = \phi_{D,\mathrm{fin}} \otimes e^{2\pi|c|q(\cdot)}$: $\phi_{D,\mathrm{fin}}$ the characteristic function of $\widehat{L}_D^{(2M)} \cdot \prod_{p|2M} L^o_{D,p}$.

Definition 3.10. *The special admissible pairs (f_D, ϕ_D), $D \in \Sigma_C$ are called distinguished.*

[6] Note that the D-th Fourier coefficient $W_D(\theta_f^\phi)$ only depends on the restriction $\phi|_{V_D(\mathbb{A})}$

The theta lifting

$$\theta_C := \theta_{f_D}^{\phi_D}$$

does not depend on the choice of D. Now let $(f, \phi, L, U, \{L_p^o\}_{p|2M})$ be any one of

$$\big(f_D, \phi_D, L_D, U_D, \{L_{D,p}^o\}_{p|2M}\big), \qquad D \in \Sigma_C.$$

Definition 3.11. *For each $[h] \in X_U := B^\times \backslash \widehat{B}^\times / U$, let $L_h^o \subset L_h := h\widehat{L}h^{-1} \cap V$ be the subset*

$$L_h^o = \left\{ \ell \in L_h \;\middle|\; \ell \in h \cdot L_p^o \text{ for all } p|2M \right\}. \tag{ot}$$

We refer to $L_h^o \subset L_h$ as the oriented solutions of the underlying ternary quadratic form.

In light of (FP), (FT), it now follows: For each $D \in \Sigma_C$, normalized Fourier coefficients of θ_C satisfy

$$a_{|D|}(\theta_C) = \frac{P_{K_D}^0(f_D)}{[\mathcal{O}_D^\times : \mathbb{Z}^\times]}$$

and

$$a_{|D|}(\theta_C) = \sum_{[h] \in X_U} \frac{f(h)}{w_h} \cdot \#(L_h^o \cap V_D(\mathbb{Q})),$$

where $w_h := \#(hUh^{-1} \cap H(\mathbb{Q}))$ is a finite group.

3.2.5. *Main result.* Let $\pi \subset \mathcal{A}_{0,2}(H)$ and M the conductor of the Jacquet–Langlands transfer. Let C be an M-equivalence class with $\varepsilon(C) = 1$ such that (π, C) satisfies Tunnell–Saito condition (TS).

Theorem 3.12. *Assume B is definite and $L(\frac{1}{2}, \pi) \neq 0$. Let (f, ϕ) be a distinguished pair as in §3.2.4. Then there exists an explicit constant $k_C \in \mathbb{Q}^\times$ such that for each $D \in \Sigma_C$,*

$$\frac{\sqrt{D} \cdot L\left(\frac{1}{2}, \pi \otimes \chi_D\right)}{\Omega_\sigma^-} = k_C \cdot \left(\sum_{[h] \in X_U} \frac{f(h)}{w_h} \cdot \#(L_h^o \cap V_D(\mathbb{Q})) \right)^2.$$

Here the notation is as in §3.2.4. (cf. [26])

Remark 3.13.

(i) A more general set-up appears in [26]: weight k and indefinite quaternion algebras[7].

(ii) If for each $v|M$, $\varepsilon(\pi_v) = \epsilon(B_v)$, then the local obstruction of Atkin–Lehner operator disappears. The oriented solutions in Theorem 3.12 may thus be replaced by the whole lattice solutions - switching the constant k_C with a 2-power multiple.

(iii) If $\mathcal{E}$ is CM or there exists $A \in \mathcal{E}$ with non-square conductor, then there exists $n_1 > 0$, $n_2 < 0$: both $L(s, E^{(n_1)})$ and $L(s, E^{(n_2)})$ have sign $+1$ and also do not vanish at the center. In this case, there exists a partition of $\mathcal{E}$ such that each $\mathcal{E}_C$ corresponds to a definite quaternion algebra.

3.3. **Congruent Number L-values, revisited.** As an application of Theorem 3.12, we recover Tunnell's theorem and exhibit a new interpretation of the central L-values of the congruent number elliptic curves in terms of ternary quadratic forms.

3.3.1. *Tunnell's theorem, again.* Let σ be the irreducible cuspdial automorphhic representation associated to $E : y^2 = x^3 - x$, its conductor $M = 32$. We first use Theorem 3.7 to recover Tunnell's result. Let $C \subset \mathbb{Q}_{<0}$ be an M-equivalence class consisting of negative rationals. Then $\varepsilon(C) = 1$ if and only if $C = [-1], [-2], [-10], [-3]$, where $[n]$ denotes the M-equivalence class of $n \in \mathbb{Q}^\times$. Now pick C with $\varepsilon(C) = 1$ to be one of $[-1], [-2], [-3]$.

The quaternion algebra determined by C such that (σ, C) satisfies Tunnell–Saito condition (TS) is the quaternion algebra B over $\mathbb{Q}$ ramified exactly at 2 and infinity, i.e.

$$B = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

with $i^2 = j^2 = -1$, $ij = k = -ji$. Let $H = PB^\times$ and $\pi \subset \mathcal{A}_{0,2}(H)$ be irreducible: the Jacquet–Langlands correspondence of π is σ. For the existence of admissible pairs, we begin with the computation of the space $V(\pi, K)$ (cf. [51]).

Let $K = \mathbb{Q}(x) \subseteq B$ with

$$x = i, \quad i + j, \quad i + j + k, \qquad \text{for } C = [-1],\ [-2],\ [-3], \quad \text{respectively.}$$

[7] Accordingly, the infinite component π_∞ may be non-trivial and in general, one needs to account for infinitely many integral solutions with fixed reduced norm in an indefinite lattice.

Let $\mathcal{O}_B$ be the maximal order of B generated over $\mathbb{Z}$ by $i, j, \dfrac{1+i+j+k}{2}$. Then

$$R = \mathcal{O}_K + 4\mathcal{O}_B$$

is an admissible order for $(\pi, \mathbf{1}_K)$. The (finite) Shimura set $X_{\widehat{R}^\times}$ of level $\widehat{R}^\times$ has representatives given by elements in $H(\mathbb{Q}_2)$:

$$X_{\widehat{R}^\times} = \begin{cases} \{1_2, (1+2j)_2, (1+1+i+j+k)_2, (1+1+i-j+k)_2\}, & \text{if } C=[-1], \\ \{1_2, (1+2j)_2\}, & \text{if } C=[-2], \\ \{1_2, (1+2j)_2\}, & \text{if } C=[-3]. \end{cases}$$

A basis $f : X_{\widehat{R}^\times} \to \mathbb{Z}$ of the one dimensional space $V(\pi, K)$ with respect to the above representatives of $X_{\widehat{R}^\times}$ (cf. [51]):

$$f = \begin{cases} (1,-1,0,0), & \text{if } C=[-1], \\ (1,-1), & \text{if } C=[-2], \\ (3,-1), & \text{if } C=[-3]. \end{cases}$$

Let $L \subset V$ be the lattice with level $\begin{cases} 128, & \text{if } C=[-1],[-3] \\ 256, & \text{if } C=[-2] \end{cases}$ and character $\mathbf{1}$ given by

$$L = \begin{cases} \mathbb{Z}i \oplus \mathbb{Z}(j+k) \oplus \mathbb{Z}4(j-k), & \text{if } C=[-1],[-3] \\ \mathbb{Z}(i+j) \oplus \mathbb{Z}2(i-j) \oplus \mathbb{Z}8k, & \text{if } C=[-2]. \end{cases}$$

Put $\phi = \mathbf{1}_{\widehat{L}} \otimes e^{2\pi|c|q(\cdot)} \in \mathcal{S}(V(\mathbb{A}))$. Then (f, ϕ) is an admissible pair.

In view of Theorem 3.7 and (FT), finally Tunnell's result:

For any positive square-free integer n,

$$\frac{L(1, E^{(n)})}{\Omega/\sqrt{n}} = \frac{1}{16} \cdot \begin{cases} (\#L_1 \cap V_{-n}(\mathbb{Q}) - \#L_2 \cap V_{-n}(\mathbb{Q}))^2, & \text{if } n \equiv 1,3 \pmod 8 \\ 2(\#L_1' \cap V_{-n}(\mathbb{Q}) - \#L_2' \cap V_{-n}(\mathbb{Q}))^2, & \text{if } n \equiv 2 \pmod 8. \end{cases}$$

Here $\Omega = \int_1^\infty \frac{dx}{\sqrt{x^3-x}}$, $\{L_1, L_2\}$, $\{L_1', L_2'\}$ the genus class of lattices in V given by

$$\{L_1 = \mathbb{Z}i \oplus \mathbb{Z}(j+k) \oplus \mathbb{Z}4(j-k), L_2 = \mathbb{Z}(i+j) \oplus \mathbb{Z}2k \oplus \mathbb{Z}(2i-2j+k)\}$$

and

$$\{L_1' = \mathbb{Z}(i+j) \oplus \mathbb{Z}2(i-j) \oplus \mathbb{Z}8k, L_2' = \mathbb{Z}2(i-j) \oplus \mathbb{Z}2(i+j) \oplus \mathbb{Z}(i+j-4k)\}.$$

Note that the ternary quadratic forms corresponding to L_1, L_2, L_1', L_2' are given by

$$x^2+2y^2+32z^2, \quad 2x^2+4y^2+9z^2+4yz,$$

$$2x^2+8y^2+64z^2, \quad 8x^2+8y^2+18z^2+8yz,$$

respectively.

3.3.2. *Congruent number L-values, anew.* In light of Theorem 3.12, one may obtain central L-value formulae for congruent number elliptic curves in term of different ternary quadratic forms (or equivalently different lattices).

(I) Let $x = 2i \in B$ and $R = \mathbb{Z}[i] + 4\mathcal{O}_B$. Let f be the test vector in the last subsection for $C=[-1]$. Consider the genus class of lattices in V with level 128 and character $\mathbf{1}$ consisting of

$$L_1 = \mathbb{Z}i \oplus \mathbb{Z}4(j-k) \oplus \mathbb{Z}4(j+k),$$
$$L_2 = \mathbb{Z}2i \oplus \mathbb{Z}(i+4k) \oplus \mathbb{Z}(4j-i),$$
$$L_3 = \mathbb{Z}2i \oplus \mathbb{Z}(i+2j+2k) \oplus \mathbb{Z}4(j-k).$$

Then the lattice $2L_1$ is x-distinguished and $(f, \mathbf{1}_{2\widehat{L}_1} \otimes e^{2\pi|c|q(\cdot)})$ a distinguished pair.

Proposition 3.14. *For any positive square free integer* $n \equiv 1 \pmod 8$,

$$\frac{L(1, E^{(n)})}{\Omega/\sqrt{n}} = \frac{1}{16}\big(\#L_1 \cap V_{-n}(\mathbb{Q}) - \#L_2 \cap V_{-n}(\mathbb{Q})\big)^2.$$

(II) We now construct a new distinguished pair whose Fourier coefficients interpret the L-values $L(1, E^{(n)})$ for positive square-free integers $n \equiv 1 \pmod 8$.

Let $\sigma' = \sigma \otimes \chi_2$ be with conductor $M' = 64$. Consider the M'-equivalence class $C = [-2]$ with $\varepsilon(C) = 1$. The pair (σ', C) gives the quaternion algebra B as in §3.3.1. Let $\pi' := \pi \otimes \chi_2 \subset \mathcal{A}_{0,2}(H)$ and $K := \mathbb{Q}(x) \subset B$ with $x := 2(i + j)$.

Then

$$R := \mathcal{O}_K + 4(i + j)\mathcal{O}_B$$

is an admissible order for $(\pi', \mathbf{1}_K)$. The Shimura set $X_{\widehat{R}^\times}$ has representatives given by elements in $H(\mathbb{Q}_2)$:

$$X_{\widehat{R}^\times} = \{1_2, (1 + 2j)_2, (1 + 2(1 + i + j + k))_2, (1 + 3(1 + i + j + k))_2\}.$$

A $\mathbb{Z}$-primitive test vector in $V(\pi', K)$ is given by

$$f' = (1, 1, -1, -1).$$

Consider the genus class of lattices in V with level 512 and character $\mathbf{1}$ consisting of

$$\begin{aligned} L_1' &= \mathbb{Z}(i + j) \oplus \mathbb{Z}8(i - j) \oplus \mathbb{Z}8k, \\ L_2' &= \mathbb{Z}2(i + j) \oplus \mathbb{Z}8k \oplus \mathbb{Z}(-3i + 5j - 4k), \\ L_3' &= \mathbb{Z}8k \oplus \mathbb{Z}16i \oplus \mathbb{Z}(9i + j), \\ L_4' &= \mathbb{Z}2(i + j) \oplus \mathbb{Z}8(i - j) \oplus \mathbb{Z}(i + j + 4k). \end{aligned}$$

Then the lattice $2L_1'$ is x-distinguished and $(f', \mathbf{1}_{\widehat{2L_1'}} \otimes e^{2\pi|c|q(\cdot)})$ a distinguished pair.

Proposition 3.15. *For any positive square-free integer $n \equiv 1 \pmod 8$,*

$$\frac{L(1, E^{(n)})}{\Omega/\sqrt{n}} = \frac{1}{16}\left(\#L_1' \cap V_{-2n}(\mathbb{Q}) + \#L_2' \cap V_{-2n}(\mathbb{Q}) - \#L_3' \cap V_{-2n}(\mathbb{Q}) - \#L_4' \cap V_{-2n}(\mathbb{Q})\right)^2.$$

Remark 3.16. Let θ, θ' be the theta lifting of the distinguished pairs as in (I), (II) respectively. For positive square-free $n \equiv 1 \pmod 8$, one has

$$a_{4n}^2(\theta) = a_{8n}^2(\theta')$$

(cf. Proposition 3.14 and Proposition 3.15). However, as n varies in positive square-free integers with $n \equiv 1 \pmod 8$, note that the sequence $\{a_{4n}(\theta)\}$ is not proportional[8] to $\{a_{8n}(\theta')\}$.

4. p-CONVERSE

4.0.1. *The Birch and Swinnerton-Dyer conjecture, bis.* Let A be an elliptic curve over $\mathbb{Q}$ and p a prime.

The p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(A/\mathbb{Q})$ appears as the middle term of the short exact sequence

$$0 \to A(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(A/\mathbb{Q}) \to Ш(A/\mathbb{Q})[p^\infty] \to 0, \tag{4.1}$$

for $Ш(A/\mathbb{Q})[p^\infty]$ the p-primary part of $Ш(A/\mathbb{Q})$.

In view of the exact sequence (4.1), Conjecture 2.2 suggests:

Conjecture 4.1. *Let A be an elliptic curve over $\mathbb{Q}$. The following are equivalent.*

(a) $\mathrm{rank}_{\mathbb{Z}} A(\mathbb{Q}) = r$ *and* $Ш(A/\mathbb{Q})$ *is finite.*
(b) $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/\mathbb{Q}) = r$ *for p a prime.*
(c) $\mathrm{ord}_{s=1} L(s, A) = r$.

Part (b) follows from part (a) just by (4.1). That $(c) \implies (a)$ is a spectacular result[9] towards the Birch and Swinnerton-Dyer conjecture due to Coates–Wiles [15] and Rubin [42] (the CM case), and Gross–Zagier [25] and Kolyvagin [35] (the general case).

After Skinner, nowadays, '$(b) \implies (c)$' is referred to as a p-converse: a p-adic criterion to have analytic rank r. For $r = 0$, an important progress towards the p-converse - Rubin [43] (the CM case) and Skinner–Urban [45] (the ordinary non-CM case). The $r = 1$ case remained widely open until the breakthrough due to Zhang [55] and Skinner [44] (the ordinary non-CM case) a few years back. Since then, the p-converse is undergoing a revival, in light of which one may hope a complete resolution of:

[8] For example, $a_4(\theta) = a_8(\theta')$ but $a_{4\cdot 57}(\theta) = -a_{8\cdot 57}(\theta')$.
[9] For a brief introduction, one may see [7, §3.1–3.2].

Conjecture 4.2 (p-converse)**.** *Let A be an elliptic curve over $\mathbb{Q}$, p a prime and $r = 0, 1$. Then,*

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(A/\mathbb{Q}) = r \quad \Longrightarrow \quad \mathrm{ord}_{s=1}L(s, A) = r.$$

Our study concerns some of the missing cases, notably the CM curves (cf. [11], [12], [8], [9], [10]). For a brief overview of the current progress towards Conjecture 4.2, one may refer to [7, §3.1–3.2].

4.0.2. *The Goldfeld conjecture, bis.* In view of Conjecture 2.4 and Conjecture 4.2:

Conjecture 4.3. *Let A be an elliptic curve over $\mathbb{Q}$ and p a prime.*
Then, for a density one subset of square-free integers d with $\varepsilon(A^{(d)}) = +1$ (resp. $\varepsilon(A^{(d)}) = -1$) :

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(A^{(d)}/\mathbb{Q}) = 0, \quad \textit{(resp. } \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(A^{(d)}/\mathbb{Q}) = 1\textit{)}.$$

4.0.3. *p-converse to a theorem of Coates–Wiles and Rubin.*

Theorem 4.4. *Let A be a CM elliptic curve over $\mathbb{Q}$ and p a prime. Then*

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(A/\mathbb{Q}) = 0 \implies L(1, A) \neq 0.$$

In the early 1990's Rubin [43] proved this p-converse when $p \nmid \#\mathcal{O}_K^\times$ for K the CM field - the hypothesis being essential to utilise the Euler system of elliptic units. The case $p = 2$ remained open since then. The unconditional p-converse is quite recent [12].

Now, in view of Theorem 3.1:

Corollary 4.5. *For a positive square-free integer $n \equiv 1, 2, 3 \bmod 8$, let $E^{(n)}$ be the congruent elliptic curve $ny^2 = x^3 - x$. Let p be a prime. Then,*

$$\mathcal{L}(n) \neq 0 \iff \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E^{(n)}/\mathbb{Q}) = 0.$$

Approach. Unconventionally - for the CM case - the approach employs the Beilinson–Kato elements [31]. It is inherently Iwasawa theoretic, principle:

$$\text{Galois actions on arithmetic objects} \longleftrightarrow \text{zeta values}.$$

(cf. [32]). Indeed, the decisive shift is to consider Kato's main conjecture for A (cf. [31, Conj. 12.10]) instead of the habitual elliptic units main conjecture for K (cf. [43]). The heart of [12] is the proof of Kato's main conjecture, which via an Iwasawa descent implies Theorem 4.4.

Remark 4.6. Unlike [43], our approach uniformly treats the ordinary and non-ordinary primes.

4.0.4. *p-converse to a theorem of Gross–Zagier, Kolyvagin and Rubin.*

Theorem 4.7. *Let A be a CM elliptic curve over the rationals with conductor N and $p \nmid 6N$ a prime. Then,*

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(A/\mathbb{Q}) = 1 \implies \mathrm{ord}_{s=1}L(s, A) = 1.$$

For p also a prime of ordinary reduction, this p-converse was proved in [12]. It is a rare instance where the non-CM case [44], [55] preceded the CM case. The supersingular case will appear in [10] (cf. [5], [6]). Another approach, which generalizes to CM curves over totally real fields, is given in [9].

A salient feature of [12], [9]: the arithmetic of auxiliary Heegner points over the CM field. For CM curves, the CM field does not satisfy the Heegner hypothesis - while - it is natural to seek to utilise the arithmetic of the CM field. The generality of the Gross–Zagier formula [54] allows us to still introduce auxiliary Heegner points over the CM field. The core of the approach: an interplay between Iwasawa theory of the auxiliary Heegner points [38] and CM Iwasawa theory [43]. For a more detailed account of the strategy, one may refer to [7, §4].

5. Distribution of Selmer groups

5.1. **Conjectures.** The subsection presents conjectures on the distribution of Selmer groups of elliptic curves over a fixed number field following [40], [2]. As an instructive introduction, one may refer to [39].

Let A be an elliptic curve over a number field F and p a prime. For the p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(A/F)$, the exact sequence

$$0 \to A(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\kappa} \mathrm{Sel}_{p^\infty}(A/F) \to Ш(A/F)[p^\infty] \to 0 \qquad (\mathrm{Seq}_A)$$

of cofinitely generated $\mathbb{Z}_p$-modules is split.

5.1.1. *The mod p Selmer groups.* We recall the distribution model for the mod p Selmer groups $\mathrm{Sel}_p(A/F)$ due to Poonen and Rains [40].

Consider the infinite dimensional locally compact hyperbolic quadratic space

$$V := \prod_v{}' H^1(F_v, A[p]).$$

Here the restricted product arises from $\{A(F_v)/pA(F_v)\}_v$ and the quadratic form Q : the sum of local quadratic forms Q_v corresponding to the map

$$H^1(F_v, A[p]) \to H^2(F_v, \mathbb{G}_m) \hookrightarrow \mathbb{Q}/\mathbb{Z},$$

which arises from the short exact sequence

$$0 \to \mathbb{G}_m \to \mathcal{H} \to A[p] \to 0$$

of G_{F_v}-modules for $\mathcal{H}$ the Heisenberg group scheme as in [40].

By definition, $\mathrm{Sel}_p(A/F)$ is the intersection of two maximal isotropic subspaces: the images of $H^1(F, A[p])$ under the restriction map and the local Kummer maps:

$$\begin{array}{ccc} \prod_v A(F_v)/pA(F_v) & & \\ & \xrightarrow{\kappa_v} & \\ & & \prod_v{}' H^1(F_v, A[p]) \\ & \xrightarrow{\mathrm{Res}} & \\ H^1(F, A[p]) & & \end{array}$$

This perhaps suggests the following model.

Let $(V = W \oplus W^\vee, Q)$ be a hyperbolic quadratic space over $\mathbb{F}_p$ of dimension $2n$ with the natural quadratic form and I_V the set of maximal isotropic subspaces.

A key proposal [40]:

Conjecture 5.1.

$$\mathrm{Prob}\left(\dim \mathrm{Sel}_p(A/F) = d\right) = \lim_{\dim V \to \infty} \mathrm{Prob}\left(\dim(Z_1 \cap Z_2) = d \;\middle|\; Z_1, Z_2 \in I_V\right)$$

It may be seen that

$$C_{p,d} := \lim_{\dim V \to \infty} \mathrm{Prob}\left(\dim(Z_1 \cap Z_2) = d \;\middle|\; Z_1, Z_2 \in I_V\right) = \prod_{j=0}^{\infty}(1+p^{-j})^{-1} \prod_{i=1}^{d} \frac{p}{p^i - 1}.$$

In particular, when ordered by height, the elliptic curves with $\mathrm{rank}_{\mathbb{Z}} A(F) \geq 2$ have density $\leq \frac{p+1}{p^2}$. In light of the BSD conjecture, the Poonen–Rains conjecture thus implies the following.

Conjecture 5.2 (Rank conjecture)**.** *Let $r \in \{0, 1\}$. When ordered by height, 50% of the elliptic curves over F have Mordell–Weil rank r.*

5.1.2. *The p^∞-Selmer groups.* Following Bhargava, Kane, Lenstra, Poonen and Rains (cf. [2]), we now switch to the p^∞-Selmer group.

Equip $\mathbb{Z}_p^{2n}$ with the hyperbolic quadratic form $Q : \mathbb{Z}_p^{2n} \to \mathbb{Z}_p$ given by

$$Q(x_1, \cdots, x_n, y_1, \cdots, y_n) = \sum_{i=1}^{n} x_i y_i.$$

A direct summand Z of $\mathbb{Z}_p^{2n}$ is called maximal isotropic if $Q|_Z = 0$ and the rank of Z is n. Let $\mathrm{OGr}_n(\mathbb{Z}_p)$ be the set of the maximal isotropic $\mathbb{Z}_p$-submodules of $\mathbb{Z}_p^{2n}$. Let OGr_n be the underlying smooth projective scheme over $\mathbb{Z}$. Consider the natural probability measure ν_n on $\mathrm{OGr}_n(\mathbb{Z}_p)$:

$$\nu_n(S) := \lim_{e \to \infty} \frac{\#\mathrm{Im}\left(S \to \mathrm{OGr}_n(\mathbb{Z}/p^e\mathbb{Z})\right)}{\#\mathrm{OGr}_n(\mathbb{Z}/p^e\mathbb{Z})}$$

for $S \subset \mathrm{OGr}_n(\mathbb{Z}_p)$ an open and closed subset. Fix $W := \mathbb{Z}_p^n \times 0$ and Z at random[10].

[10] In fact, equivalent to choose both Z and W at random, since $O(V, Q)$ acts transitively on $\mathrm{OGr}_n(\mathbb{Z}_p)$.

In the spirit of §5.1.1 define

$$R := (Z \cap W) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p,$$
$$S := (Z \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \cap (W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p),$$
$$T := S/R.$$

Note that T is finite, endowed with a canonical non-degenerate alternate pairing. Let $\mathcal{Q}_{2n}$ be the distribution of the isomorphism class of the short exact sequences

$$0 \to R \to S \to T \to 0, \tag{5.1}$$

induced from ν_n. It may be seen that the limit of $\mathcal{Q}_{2n}$ exists, say $\mathcal{Q}$.

A fundamental proposal [2]:

Conjecture 5.3. *Let F be a global field and $\mathcal{S}$ a short exact sequence of $\mathbb{Z}_p$-modules as in (5.1). When ordered by height, the density of*

$$\{A : \mathrm{Seq}_A \simeq \mathcal{S}\}$$

equals the $\mathcal{Q}$-probability of $\mathcal{S}$.

More precisely, let G be a finite symplectic p-group. Then

$$\mathrm{Prob}\left(\mathrm{Sel}_{p^\infty}(A/F) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus G\right) = \frac{(\#G)^{1-r}}{\#\mathrm{Sp}(G)} \times \begin{cases} \frac{1}{2}\prod_{i=r+1}^{\infty}(1-p^{1-2i}), & \text{if } r = 0, 1, \\ 0, & \text{if } r \geq 2. \end{cases}$$

The scheme OGr_n is a disjoint union of two isomorphic subschemes $\mathrm{OGr}_n^{\pm}$ such that - for any field k - $\mathrm{OGr}_n^{+}(k)$ (resp. $\mathrm{OGr}_n^{-}(k)$) parameterize $Z \in \mathrm{OGr}_n(k)$ with $\dim(Z \cap W_k)$ even (resp. odd). Further, the locus with $\dim(Z \cap W_k) \geq 2$ has lower dimension (cf. [2]). Thus Conjecture 5.3 implies Conjecture 5.2. Assuming independence in p, it also implies:

Conjecture 5.4. *Let $n \in \mathbb{Z}_{\geq 1}$. When ordered by height, the average of $\#\mathrm{Sel}_n(A/F)$ is $\sigma(n) := \sum_{d|n} d$.*

In particular, the average of $\#\mathrm{Sel}_{2^n}(A/F)$ is conjecturally $2^{n+1} - 1$, which resonates through the following subsection.

5.2. **Smith's work.** In his remarkable thesis, Smith [47] made the following breakthrough towards the distribution of the 2^∞-Selmer groups in the quadratic twist family of elliptic curves over $\mathbb{Q}$ (cf. [23]).

Theorem 5.5. *Let $A/\mathbb{Q}$ be an elliptic curve such that*

$$A[2] \subset A(\mathbb{Q}) \text{ and } A \text{ has no cyclic subgroup of order 4 defined over } \mathbb{Q}. \tag{ord}$$

Let $r \in \mathbb{Z}_{\geq 0}$ and G be a symplectic 2-group.

Then, as d varies over square-free integers:

$$\mathrm{Prob}\left(\mathrm{Sel}_{2^\infty}(A^{(d)}/\mathbb{Q}) \cong (\mathbb{Q}_2/\mathbb{Z}_2)^r \oplus G\right) = \frac{(\#G)^{1-r}}{\#\mathrm{Sp}(G)} \times \begin{cases} \frac{1}{2}\prod_{i=r+1}^{\infty}(1-2^{1-2i}), & \text{if } r = 0, 1, \\ 0, & \text{if } r \geq 2. \end{cases}$$

A couple of striking consequences:

Corollary 5.6. *Let A be an elliptic curve over $\mathbb{Q}$ as in Theorem 5.5.*

Then, for a density one subset of square-free integers d with $\varepsilon(A^{(d)}) = +1$ (resp. $\varepsilon(A^{(d)}) = -1$) :

$$\mathrm{corank}_{\mathbb{Z}_2}\mathrm{Sel}_{2^\infty}(A^{(d)}/\mathbb{Q}) = 0, \quad \textit{(resp. } \mathrm{corank}_{\mathbb{Z}_2}\mathrm{Sel}_{2^\infty}(A^{(d)}/\mathbb{Q}) = 1\textit{)}.$$

Corollary 5.7. *The density of non-congruent numbers in all positive square-free integers $n \equiv 1, 2, 3 \bmod 8$ is one.*

Remark 5.8. The quadratic twist family of elliptic curves is complementary to Conjecture 5.3, yet intriguingly Theorem 5.5 echoes the same principal.

Remark 5.9.

- Very recently, Smith has announced: Theorem 5.5 also holds for elliptic curves $A/\mathbb{Q}$ with $A(\mathbb{Q})[2] = 0$. When ordered by height, a density one subset of elliptic curves over $\mathbb{Q}$ satisfies the hypothesis.
- Suppose $A(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and let A' be the isogenous curve arising from the 2-torsion. If $\mathbb{Q}(A[2]) \neq \mathbb{Q}(A'[2])$, Smith has announced: Corollary 5.6 still holds.

5.3. **Goldfeld's conjecture: an instance.** By Corollary 5.6 and Theorem 4.4,

Corollary 5.10. *Let $E^{(n)} : y^2 = x^3 - n^2x, n \in \mathbb{N}$, be congruent number elliptic curves. Then,*

$$L(1, E^{(n)}) \neq 0 \text{ for a density one subset of positive square-free integers } n \equiv 1, 2, 3 \bmod 8.$$

Remark 5.11. In light of Remark 5.9 and Theorem 4.4: The even parity Goldfeld conjecture holds for quadratic twist family of CM elliptic curves over $\mathbb{Q}$, once the CM field differs from $\mathbb{Q}(\sqrt{-2})$.

6. Distribution of 2-Selmer groups: exceptional case

Let E be a fixed elliptic curve over $\mathbb{Q}$. Recall that the 2-Selmer group $\mathrm{Sel}_2(E/\mathbb{Q})$ appears in the fundamental short exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\kappa} \mathrm{Sel}_2(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0.$$

In particular, if $\mathrm{Sel}_2(E/\mathbb{Q}) = \kappa(E(\mathbb{Q})_{\mathrm{tor}})$, then E has Mordell–Weil rank 0 and $Ш(E/\mathbb{Q})[2] = 0$. On the other hand, if $\mathrm{Sel}_2(E/\mathbb{Q})/\kappa(E(\mathbb{Q})_{\mathrm{tor}})$ is non-trivial and E has Mordell–Weil rank 0 : $Ш(E/\mathbb{Q})[2]$ is non-trivial.

The 2-parity conjecture, proved by Monsky [36] (see also [18]), asserts that

$$\dim_{\mathbb{F}_2}\left(\mathrm{Sel}_2(E/\mathbb{Q})/\kappa(E(\mathbb{Q})_{\mathrm{tor}})\right) \equiv \operatorname*{ord}_{s=1} L(s, E) \bmod 2.$$

For simplicity assume that $E[2] \subset E(\mathbb{Q})$. For a square-free integer n, let $E^{(n)}$ be the quadratic twist of E by $\mathbb{Q}(\sqrt{n})$ and define the rational number

$$\mathscr{L}(n) := \frac{L(1, E^{(n)})}{\Omega_{E^{(n)}}} \cdot \left(\frac{\prod_\ell c_\ell(E^{(n)})}{\#E^{(n)}(\mathbb{Q})^2_{\mathrm{tor}}}\right)^{-1},$$

the analytic Sha of $E^{(n)}$ if $L(1, E^{(n)}) \neq 0$.

Given a residue class a mod M, one may seek to study: among all positive (or negative) square-free integers n in this residue class, the minimal value of $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/\kappa(E^{(n)}(\mathbb{Q})_{\mathrm{tor}})$ and the 2-adic valuation of $\mathscr{L}(n)$ of $E^{(n)}$, and the distribution of n which $\mathrm{ord}_2\mathscr{L}(n)$ attains the minimum.

6.0.1. *A precursor.* If E satisfies (ord), then the results of Heath-Brown [27], Swinnerton-Dyer [48] and Kane [30] exhibit the minimal value of 2-Selmer ranks and its distribution among the residue classes. The results suggest that the distribution of 2-Selmer groups in a quadratic twist family (modulo the contribution of torsion points) still mirrors the Poonen–Rains principle[11] (cf. Conjecture 5.1). The phenomenon inspired and resonates through Smith's work on 2^∞-Selmer groups [46], [47].

The main results of [27], [48], [30]:

Theorem 6.1. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying (ord). Let n_0 be a square-free integer and $d_0 = \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(n_0)}/\mathbb{Q})/\kappa(E^{(n_0)}(\mathbb{Q})_{\mathrm{tor}})$. Let N be the conductor of E, and $[n_0] \subset \mathbb{Q}^\times$ the N-equivalence class[12] which contains n_0.*

(i) *For $d, k \in \mathbb{Z}_{\geq 0}$, let $\pi_{d,k}$ denote the following probability among square-free integers n with k distinct prime factors such that $n \in [n_0]$:*

$$\pi_{d,k} := \mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/\kappa(E^{(n)}(\mathbb{Q})_{\mathrm{tor}}) = d\right).$$

Then

$$\lim_{k\to\infty} \pi_{d,k} = \begin{cases} 2\prod_{j=0}^{\infty}(1+2^{-j})^{-1}\prod_{i=1}^{d}\frac{2}{2^i-1}, & \text{if } d \equiv d_0 \pmod 2, \\ 0, & \text{if } d \not\equiv d_0 \pmod 2. \end{cases}$$

(ii) *For $d \in \mathbb{Z}_{\geq 0}$, among square-free integers $n \in [n_0]$:*

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/\kappa(E^{(n)}(\mathbb{Q})_{\mathrm{tor}}) = d\right) = \begin{cases} 2\prod_{j=0}^{\infty}(1+2^{-j})^{-1}\prod_{i=1}^{d}\frac{2}{2^i-1}, & \text{if } d \equiv d_0 \pmod 2, \\ 0, & \text{if } d \not\equiv d_0 \pmod 2. \end{cases}$$

In particular, for $d \in \mathbb{Z}_{\geq 0}$, among square-free integers n :

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/\kappa(E^{(n)}(\mathbb{Q})_{\mathrm{tor}}) = d\right) = \prod_{j=0}^{\infty}(1+2^{-j})^{-1}\prod_{i=1}^{d}\frac{2}{2^i-1}.$$

[11] though their framework excludes the quadratic twist family

[12] See Definition 3.5.

Part (i) is due to Swinnerton-Dyer [48], a key: $(\pi_{d,k})_{d=0}^{\infty}$ is connected by a Markov chain as k varies. Via analytic tools, Kane [30] proved that part (i) implies part (ii) - a transition from the density for integers with restricted prime factors to natural density. The above theorem for the congruent number elliptic curve $y^2 = x^3 - x$ is also due to Heath-Brown [27], an independent approach.

6.0.2. *An exceptional case.* Some quadratic twist families of elliptic curves over $\mathbb{Q}$ satisfy neither (ord) nor the hypotheses in Remark 5.9.

A key missing case:

$$E[2] \subset E(\mathbb{Q}) \text{ and } E \text{ has rational 4-torsion points.} \tag{exc}$$

For example, the quadratic twist family of tiling number elliptic curves

$$E^{(n)} : y^2 = x(x-n)(x+3n).$$

Notice $E(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Perhaps surprisingly, in light of the presence of such rational 4-torsion, the distribution of 2-Selmer groups no longer seems to be as in Theorem 6.1. A suggestive example [20]:

Proposition 6.2. *Let E be the elliptic curve $y^2 = x(x-1)(x+3)$. If $n \neq 1$, $n \equiv 1 \pmod{12}$ is positive square-free, then*

$$\dim_{\mathbb{F}_2} \text{Sel}_2(E^{(-n)}/\mathbb{Q})/\kappa(E^{(-n)}(\mathbb{Q})_{\text{tor}}) \geq 2,$$

and the corresponding $\mathscr{L}(-n)$ is also even.

6.1. **Main results.** Our preliminary study suggests that for elliptic curves satisfying (exc), the distribution of 2-Selmer groups may resemble that of the 4-ranks of ideal class groups of the underlying imaginary quadratic fields.

Let $g(n) := \#2\text{Cl}(\mathbb{Q}(\sqrt{-n}))$, in particular, $g(n)$ is odd if and only if $\mathbb{Q}(\sqrt{-n})$ has no ideal class of exact order 4.

A main result of [20]:

Theorem 6.3. *Let E be the elliptic curve $y^2 = x(x-1)(x+3)$. Let $n \equiv 3, 7 \pmod{24}$ be a positive square-free integer. Let $\epsilon \in \{\pm 1\}$. Then the followings are equivalent.*

(a) *The genus invariant*

$$\begin{cases} g(n) + \sum\limits_{\substack{d \mid n \\ d \equiv 11 \bmod 24}} g(n/d)g(d), & \text{if } n \equiv 7 \bmod 24 \text{ and } \epsilon = -1, \\ g(n), & \text{otherwise,} \end{cases}$$

is odd.

(b) $\text{Sel}_2(E^{(\epsilon n)}/\mathbb{Q})/\kappa(E^{(\epsilon n)}(\mathbb{Q})_{\text{tor}}) = 0$.

(c) $L(1, E^{(\epsilon n)}) \neq 0$ *and the analytic Sha $\mathscr{L}(\epsilon n)$ of $E^{(\epsilon n)}$ is odd.*

As in [49], the core of the approach: a link between $\mathscr{L}(\pm n)$ and $g(n)$. In light of [48], [30], [46], the link also allows us to deduce the following positive density [20].

Theorem 6.4. *Let E be the elliptic curve $y^2 = x(x-1)(x+3)$. Among the set of positive square-free integers $n \equiv 7 \pmod{24}$ (resp. $n \equiv 3 \pmod{24}$), the subset of n - for which the analytic Sha $\mathscr{L}(\pm n)$ of $E^{(\pm n)}$ is odd and $\text{Sel}_2(E^{(\pm n)}/\mathbb{Q})/\kappa(E^{(\pm n)}(\mathbb{Q})_{\text{tor}})$ trivial - has density $\frac{1}{2}\prod_{i=1}^{\infty}(1-2^{-i}) \approx 14.4\%$ (resp. $\prod_{i=1}^{\infty}(1-2^{-i})$).*

Remark 6.5. A salient feature: $\mathscr{L}(\pm n)$ mirrors the ideal class groups of imaginary quadratic fields, unlike [30], [46].

In the following we exhibit methods to study Theorem 6.3.

6.2. **2-descent in a quadratic twist family.** Let $E/\mathbb{Q}$ be an elliptic curve.

6.2.1. *The set-up.* In the following we assume $E[2] \subset E(\mathbb{Q})$.

One may suppose that E is given by a Weierstrass equation $y^2 = x(x-e_1)(x-e_2)$ with $e_1, e_2 \in \mathbb{Z}$. Let m be a square-free integer, and $E^{(m)} : y^2 = x(x-e_1m)(x-e_2m)$. Let S be the set of primes dividing $2me_1e_2(e_1-e_2)\infty$ and $\mathbb{Q}(S,2)$ the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ supported on S.

Then elements in $\mathrm{Sel}_2(E^{(m)}/\mathbb{Q})$ can be realized as curves $C_\Lambda/\mathbb{Q}$ with $C_\Lambda(\mathbb{A}_\mathbb{Q}) \neq \emptyset$. Here for $\Lambda = (b_1, b_2) \in \mathbb{Q}(S,2)^2$, the curve:

$$C_\Lambda : \quad \begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_1 m t^2 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_2 m t^2 \end{cases}$$

Note that $C_\Lambda(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ if and only if $C_\Lambda(\mathbb{Q}_v) \neq \emptyset$ for all $v \in S$. The 2-torsion points O, $(0,0)$, $(e_1m, 0)$, and $(e_2m, 0)$ correspond to $(b_1, b_2) = (1,1)$, $(e_2/e_1, -e_1m)$, $(e_1m, (e_1-e_2)/e_1)$, and $(e_2m, (e_2-e_1)m)$.

6.2.2. *The strategy.* Let $S' \subset S$ be the set of primes dividing $2e_1e_2(e_1-e_2)$, which is independent of m. Let $n > 0$ be the prime-to-S' part of m, and let $q = m/n$. Write $n = \ell_1 \cdots \ell_k$.

Let $A = (a_{ij}) \in M_{k\times k}(\mathbb{F}_2)$ be the Rédei matrix associated to n, defined by $a_{ij} = \left[\frac{\ell_j}{\ell_i}\right] := \frac{1}{2}\left(1 - \left(\frac{\ell_j}{\ell_i}\right)\right)$ (the additive Legendre symbol) if $i \neq j$, and $\sum_j a_{ij} = 0$ for all i, namely $a_{ii} = \left[\frac{n/\ell_i}{\ell_i}\right]$. For $\Lambda = (b_1, b_2) \in \mathbb{Q}(S,2)^2$, $t = 1, 2$, write $b_t = c_t \prod_i \ell_i^{x_{t,i}}$ and $c_t = \prod_{p \in S'\cup\{-1\}} p^{y_t^{(p)}}$ for $x_t = (x_{t,1}, \cdots, x_{t,k})^{\mathrm{T}} \in \mathbb{F}_2^k$ and $y_t^{(p)} \in \mathbb{F}_2$ for $p \in S' \cup \{-1\}$.

Then the condition that $C_\Lambda(\mathbb{Q}_v) \neq \emptyset$ for all $v \in S \setminus (S' \cup \{\infty\}) = \{\ell_1, \cdots, \ell_k\}$ can be rephrased as a linear equation in $\mathbb{F}_2$ involving A and x_t. For example, consider $E : y^2 = x(x-1)(x+3)$, then the linear equation [20]:

$$\begin{pmatrix} A + D_q & D_{-3} \\ & A + D_{-q} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} z_{c_1} \\ z_{c_2} \end{pmatrix}.$$

Here for an integer d prime to n, $z_d := \left(\left[\frac{d}{\ell_1}\right], \cdots, \left[\frac{d}{\ell_k}\right]\right)^{\mathrm{T}} \in \mathbb{F}_2^k$, and $D_d := \mathrm{diag}(z_d) \in M_{k\times k}(\mathbb{F}_2)$.

Similarly, for each $v \in S' \cup \{\infty\}$, the condition that $C_\Lambda(\mathbb{Q}_v) \neq \emptyset$ can also be rephrased in terms of linear algebra. This allows us to describe $\mathrm{rank}_{\mathbb{F}_2}\mathrm{Sel}_2(E^{(m)}/\mathbb{Q})$ in terms of the corank of certain "generalized Rédei matrix". Via elementary linear algebra, one may then establish the equivalence of parts (a) and (b) of Theorem 6.3.

Remark 6.6. The approach is employed in several previous works, for example, [27], [48], [30], [46].

6.3. **An induction.** Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and ϕ the associated newform.

6.3.1. *The set-up.* For a positive square-free integer n, let $K = \mathbb{Q}(\sqrt{-n})$ be an imaginary quadratic field, D its discriminant, and η the associated quadratic character.

Let $\chi : \mathrm{Gal}(H/K) \cong \mathrm{Cl}(K) \to \{\pm 1\}$ be an unramified quadratic character over K, where H is the Hilbert class field of K. Such characters are in one-to-one correspondence with the unramified quadratic extensions $K(\sqrt{-d})/K$, where $d > 0$ is a divisor of n with $d \equiv 3 \bmod 4$ (resp. $d \equiv 3 \bmod 4$ or $d \equiv n \bmod 8$) if $n \equiv 3 \bmod 4$ (resp. $2 \mid n$). We usually denote such χ associated to $K(\sqrt{-d})/K$ by χ_d. In particular, taking $d = n$, we obtain the trivial character $\mathbf{1}_K = \chi_n$ over K.

Let Σ be the set of places $v \mid N\infty$ such that

$$\varepsilon_v(E, \chi) \cdot \chi_v\eta_v(-1) = -1.$$

Here $\varepsilon_v(E,\chi)$ is the local root number at v of the Rankin–Selberg L-series $L(s, E \times \chi)$. Note that $\infty \in \Sigma$ and for any finite place $v \in \Sigma : v$ non-split in K. Assume that Σ has even cardinality, equivalently, the sign of the functional equation of $L(s, E \times \chi)$ is $+1$.

Let B be the definite quaternion algebra over $\mathbb{Q}$ ramified exactly at the places in Σ. Then there exists an embedding of K into B, which we fix once and for all. Let $R \subset B$ be an order of discriminant N with $R \cap K = \mathcal{O}_K$. The Shimura set

$$X := B^\times \backslash \widehat{B}^\times / \widehat{R}^\times$$

is a finite set endowed with Hecke correspondences T_p for $p \nmid N$ and $K_v^\times$-actions for $v \mid (N, D)$ by right multiplication (cf. [13, Lem. 3.4]). Let $\mathbb{C}[X]$ be the set of $\mathbb{C}$-valued functions on X, which is endowed with a natural Hermitian inner product $\langle\ ,\ \rangle$, Hecke operators T_p for $p \nmid N$ and $K_v^\times$-actions for $v \mid (N, D)$. Let $\mathbb{C}[X]^0 \subset \mathbb{C}[X]$ be the orthogonal complement of the functions on X which factor through the reduced norm map $\widehat{B}^\times \to \widehat{\mathbb{Q}}^\times$.

Let π be the cuspidal automorphic representation of $B^\times$ whose Jacquet–Langlands transfer to GL_2 is the automorphic representation generated by ϕ.

6.3.2. *Toric periods.* The subspace $V(\pi,\chi)$ of $\pi^{\widehat{R}^\times}\subset\mathbb{C}[X]^0$ where T_p acts as $a_p(\phi)=a_p(E)$ for all $p\nmid N$ and $K_v^\times$ acts via χ_v for all $v\mid(N,D)$ turns out to be one-dimensional (cf. [13]). A generator of this space is referred to as a test vector. In fact, since the coefficients of T_p-actions and the values of χ_v are integral, $V(\pi,\chi)$ has a basis $f\in\mathbb{Z}[X]$ of integral values. One may choose a $\mathbb{Z}$-primitive test vector $f:X\to\mathbb{Z}$, i.e. the image generates $\mathbb{Z}$. Such f is unique up to ±1.

The inclusion $K\to B$ induces a map $\iota:\mathrm{Cl}(K)\to X$, in view of which, define the toric period $P^0_\chi(f)$ associated to (E,χ):

$$P^0_\chi(f)=\sum_{t\in\mathrm{Cl}(K)}\chi(t)f(\iota(t))\in\mathbb{Z}.$$

An explicit Waldspurger formula [13].

Theorem 6.7. *Let E and χ be as above. Then*

$$L(1,E\times\chi)=2^{-\mu(N,D)}\cdot\frac{8\pi^2(\phi,\phi)_{\Gamma_0(N)}}{u^2\sqrt{|D|}}\cdot\frac{|P^0_\chi(f)|^2}{\langle f,f\rangle}.$$

Here $\mu(N,D)$ is the number of common prime factors of N and D, $u=[\mathcal{O}_K^\times:\mathbb{Z}^\times]$ and $(\phi,\phi)_{\Gamma_0(N)}$ the Petersson norm of ϕ.

Now we fix a $\mathbb{Z}$-primitive test vector $f\in V(\pi,\mathbf{1}_K)$ for E and the trivial character $\mathbf{1}_K$. Define the genus period

$$P_0(f):=\sum_{t\in2\mathrm{Cl}(K)}f(\iota(t))\in\mathbb{Z}.$$

An evident yet key fact: if $f|_{(\widehat{B}^\times)^2}$ only takes odd integeral values, then $P_0(f)\equiv g(n)\bmod 2$. Let $k=\mu(n)$ be the number of prime factors of n, let $c=0$ if $n\equiv1\bmod4$, and $c=1$ otherwise. In particular, $\mathrm{Cl}(K)/2\mathrm{Cl}(K)\cong\mathrm{Gal}(H_0/K)\cong(\mathbb{Z}/2\mathbb{Z})^{k-c}$ for H_0 the genus class field of K.

Then as χ varies,

$$\sum_{\chi:\mathrm{Gal}(H/K)\to\{\pm1\}}P^0_\chi(f)=2^{k-c}P_0(f).\tag{6.1}$$

Remark 6.8. For χ such that $f\notin V(\pi,\chi)$, notice $P^0_\chi(f)=0$.

6.3.3. *Induction.* In the following we assume that $E[2]\subset E(\mathbb{Q})$. Notice

$$L(s,E\times\chi)=L(s,E^{(n/d)})L(s,E^{(-d)}).$$

By considering the variation of local arithmetic invariants of elliptic curves in a quadratic twist family, Theorem 6.7 (the Waldspurger formula) may be rephrased as [20]:

$$|P^0_\chi(f)|^2=C_{n,d}\cdot4^{\mu(n)}u^2\mathscr{L}(n/d)\mathscr{L}(-d)\cdot\left(\frac{4}{\#E^{(n/d)}(\mathbb{Q})_{\mathrm{tor}}}\right)^2\left(\frac{4}{\#E^{(-d)}(\mathbb{Q})_{\mathrm{tor}}}\right)^2.\tag{6.2}$$

Here $\mathscr{L}(n/d)$ and $\mathscr{L}(-d)$ are the analytic Sha of $E^{(n/d)}$ and $E^{(-d)}$ in the rank 0 case, and $C_{n,d}$ an explicit non-zero rational constant which depends just on the residue classes (n mod M, d mod M) - where M an explicit constant intrinsic to E.

We moreover assume that $E^{(m)}(\mathbb{Q})_{\mathrm{tor}}=E^{(m)}[2]$ for all square-free integers $m\neq\pm1$, and that $L(1,E)\neq0$ and $L(1,E^{(-1)})\neq0$.

Now, in light of (6.1) and (6.2), for $f\notin V(\pi,\chi_1)$:

$$2^cu\left(\pm\sqrt{C_{n,n}\mathscr{L}(1)\mathscr{L}(-n)}\cdot\frac{4}{\#E(\mathbb{Q})_{\mathrm{tor}}}+\sum_{\substack{\chi_d:\mathrm{Gal}(H/K)\to\{\pm1\}\\ f\in V(\pi,\chi_d)\\ d\neq1,n}}\pm\sqrt{C_{n,d}\mathscr{L}(n/d)\mathscr{L}(-d)}\right)=P_0(f).$$

When $f\in V(\pi,\chi_1)$, an analogous formula holds. Finally, by replacing E with $E^{(-1)}$, we obtain formulae relating $\mathscr{L}(-1)\mathscr{L}(n)$ with $\mathscr{L}(-n/d)\mathscr{L}(d)$. Note that in these formulae, the number of prime factors of $\pm n/d$ and $\pm d$ are strictly smaller than that of $\pm n$. This allows us to execute an induction argument on the number $k=\mu(n)$ of prime factors of n, proving the lower bounds for the 2-adic valuations and the congruence formula modulo 2 for $\mathscr{L}(\pm n)$.

The induction leads to an equivalence of parts (a) and (c) of Theorem 6.3. Here the presence of 4-torsion reduces the length of the recursion formula for $\mathscr{L}(\pm n)$, which yields a very concise formula relating $\mathscr{L}(\pm n)$ and $g(n)$, unlike [51].

Remark 6.9. The induction method was introduced in [49] and it has been employed in several previous works, for example [14], [51].

References

[1] N. Balsam, *The Parity of Analytic Ranks among Quadratic Twists of Elliptic Curves over Number Fields*, thesis, Columbia 2015.

[2] M. Bhargava, D. Kane, H. Lenstra, B. Poonen and E. Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich–Tate groups of elliptic curves*, Cambridge J. Math. 3 (2015), 275–321.

[3] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, 333–400, Progr. Math., 86, Birkhäuser Boston, Boston, MA, 1990.

[4] S. Bocherer and R. Schulze-Pillot, *On a theorem of Waldspurger and on Eisenstein series of Klingen type*, Math. Ann. 288 (1990), no. 3, 361–388.

[5] A. Burungale, S. Kobayashi and K. Ota, *Rubin's conjecture on local units in the anticyclotomic tower at inert primes*, preprint 2021.

[6] A. Burungale, S. Kobayashi and K. Ota, *p-adic L-functions and rational points on CM elliptic curves at inert primes*, preprint 2021.

[7] A. Burungale, C. Skinner and Y. Tian, *The Birch and Swinnerton-Dyer conjecture: a brief survey*, The Linde Hall Inaugural Math Symposium, Proc. Sympos. Pure. Math., to appear.

[8] A. Burungale, C. Skinner and Y. Tian, *p-converse to a theorem of Gross–Zagier and Kolyvagin: CM elliptic curves over totally real fields*, preprint 2019.

[9] A. Burungale, C. Skinner and Y. Tian, *Elliptic curves and Beilinson–Kato elements: rank one aspects*, preprint 2020.

[10] A. Burungale, C. Skinner and Y. Tian, *p-converse to a theorem of Gross–Zagier, Kolyvagin and Rubin, II*, in progress.

[11] A. Burungale and Y. Tian, *p-converse to a theorem of Gross-Zagier, Kolyvagin and Rubin*, Invent. Math. 220 (2020), no. 1, 211–253.

[12] A. Burungale and Y. Tian, *A rank zero p-converse to a theorem of Gross–Zagier, Kolyvagin and Rubin*, preprint 2019, submitted.

[13] L. Cai, J. Shu and Y. Tian, *Explicit Gross–Zagier formula and Waldspurger formula*, Algebra Number Theory 8 (2014), no. 10, 2523–2572.

[14] J. Coates, Y. Li, Y. Tian and S.Zhai, *Quadratic twists of elliptic curves*, Proc. London Math. Soc. (3) 110 (2015) 357-394.

[15] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), no. 3, 223–251.

[16] C. Delaunay, *Heuristics on Tate–Shafarevich groups of elliptic curves defined over* $\mathbb{Q}$, Experiment. Math. 10(2) (2001), 191–196.

[17] J. Desjardins, *Root number of the twists of an elliptic curve*, Journal de Théorie des Nombres de Bordeaux, Tome 32 (2020) no. 1, pp. 73–101.

[18] T. Dokchitser and V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) 172 (2010), no. 1, 567–596.

[19] T. Dokchitser and V. Dokchitser, *Elliptic curves with all quadratic twists of positive rank*, Acta Arith. 137 (2009), no. 2, 193–197.

[20] K. Feng, Q. Liu, J. Pan and Y. Tian, *Toric periods and non-tiling numbers*, preprint 2021.

[21] S. Friedberg and J.Hoffstein, *Non-vanishing theorems for automorphic L-functions on* GL(2), Ann. of Math. (2) 142 (1995), no. 2, 385–423.

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

[23] D. Goldfeld and S. Munao, *Alexander Smith wins the first David Goss prize in number theory*, Notices Amer. Math. Soc. 66 (2019), no. 11, 1875–1878.

[24] B. Gross, *Heights and the special values of L-series*. Number theory (Montreal, Que., 1985), 115–187, CMS Conf. Proc., 7, Amer. Math. Soc., Providence, RI, 1987.

[25] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), no. 2, 225–320.

[26] W. He, Y. Tian, W. Xiong, *Explicit theta lifting and quadratic twist L-values*, preprint.

[27] D.R. Heath-Brown, *The size of Selmer groups for congruent number problem, II*, Inv. Math. 118, 331–370 (1994).

[28] Heegner, K. *Diophantische analysis und modulfunktionenMath*, Math. Z. 56 (1952), 227–253.

[29] J. Johnson-Leung and G. Kings, *On the equivariant main conjecture for imaginary quadratic fields*, J. Reine Angew. Math. 653 (2011), 75–114.

[30] D. Kane, *On the ranks of the 2-Selmer groups of twists of a given elliptic curve*, Algebra Number Theory 7, no. 5, 1253–1279 (2013).

[31] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétiques. III. Astérisque No. 295 (2004), ix, 117–290.

[32] K. Kato, *Iwasawa theory and generalizations*, International Congress of Mathematicians. Vol. I, 335–357, Eur. Math. Soc., Zurich, 2007.

[33] N. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, 45. American Mathematical Society, Providence, RI, 1999. xii+419 pp.

[34] Z. Klagsbrun, B. Mazur and K. Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) 178 (2013), no. 1, 287–320.

[35] V. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, 435–483, Progr. Math., 87, Birkhäuser Boston, Boston, MA, 1990.
[36] P. Monsky, *Generalizing the Birch–Stephens theorem. I. Modular curves*, Math. Z. 221 (1996), no. 3, 415–420.
[37] P. Monsky, *Mock Heegner Points and Congruent Numbers*, Math. Z. 204 (1990), no. 1, 45–67.
[38] B. Perrin-Riou, *p-adic L-functions, Iwasawa theory and Heegner points*, Bull. Soc. Math. France 115 (1987), no. 4, 399–456.
[39] B. Poonen, *Heuristics for the arithmetic of elliptic curves*, Proceedings of the International Congress of Mathematicians–Rio de Janeiro 2018. Vol. II. Invited lectures, 399–414, World Sci. Publ., Hackensack, NJ, 2018.
[40] B. Poonen and E. Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. 25 (2012), no. 1, 245–269.
[41] H. R. Qin, *Congruent numbers, quadratic forms and K_2*, preprint 2020.
[42] K. Rubin, *Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. 89 (1987), no. 3, 527–559.
[43] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), no. 1, 25–68.
[44] C. Skinner, *A converse to a theorem of Gross, Zagier and Kolyvagin*, Ann. of Math. (2) 191 (2020), no. 2, 329–354.
[45] C. Skinner and E. Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. 195 (2014), no. 1, 1–277.
[46] A. Smith, *The congruent numbers have positive natural density*, preprint, arXiv:1603.08479.
[47] A. Smith, *2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture*, preprint, arXiv:1702.02325.
[48] P. Swinnerton-Dyer, *The effect of twisting on 2-Selmer groups*, Mathematical Proceedings of the Cambridge Philosophical Society, vol. 145(2008), 513–526.
[49] Y. Tian, *Congruent Numbers and Heegner Points*, Cambridge Journal of Mathematics, 2 (2014), 117-161.
[50] Y. Tian, *Congruent number problem*, Proceedings of the Sixth International Congress of Chinese Mathematicians. Vol. I, 135–151, Adv. Lect. Math. (ALM), 36, Int. Press, Somerville, MA, 2017.
[51] Y. Tian, X. Yuan and S. Zhang, *Genus periods, genus points and congruent number problem*, Asian J. Math. 21 (2017), no. 4, 721–773.
[52] J.B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. 72(2), 323–334 (1983).
[53] J.L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. pures et appl. 60 (1981), 375–484.
[54] X. Yuan, S.-W. Zhang and W. Zhang, *The Gross-Zagier formula on Shimura curves*, Annals of Mathematics Studies, vol 184. (2013) viii+272 pages.
[55] W. Zhang, *Selmer groups and the indivisibility of Heegner points*, Cambridge Journal of Math., Vol. 2 (2014), No. 2, 191–253.

Ashay A. Burungale: California Institute of Technology, 1200 E California Blvd, Pasadena CA 91125
Email address: ashayburungale@gmail.com

Ye Tian: Academy of Mathematics and Systems Science, MCM, HLM, Chinese Academy of Sciences, Beijing 100190, and School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 10049
Email address: ytian@math.ac.cn