THE CONGRUENT NUMBER PROBLEM AND ELLIPTIC CURVES

YE TIAN

ABSTRACT

The Birch and Swinnerton-Dyer (BSD) conjecture and Goldfeld conjecture are fundamental problems in the arithmetic of elliptic curves. The congruent number problem (CNP) is one of the oldest problems in number theory which is, for each integer n, to find all the rational right triangles of area n. It is equivalent to finding all rational points on the elliptic curve $E^{(n)} : ny^2 = x^3 - x$. The BSD conjecture for $E^{(n)}$ solves CNP, and Goldfeld conjecture for this elliptic curve family solves CNP for integers with probability one. In this article, we introduce some recent progress on these conjectures and problems.

MATHEMATICS SUBJECT CLASSIFICATION 2020

Primary 11-06; Secondary 11G05, 11G40

KEYWORDS

Congruent numbers, BSD conjecture, Goldfeld conjecture, quadratic twists, Selmer group, L-function

INTERNATIONAL CONGRESS
OF MATHEMATICIANS
2022 JULY 6–14

Proc. Int. Cong. Math. 2022, Vol. 3, pp. 1990–2010
DOI 10.4171/ICM2022/85

1. CONGRUENT NUMBER PROBLEM

A positive rational number n is called a *congruent number* if the following equivalent conditions hold:

(i) There exists a rational number x such that $x^2 \pm n$ are squares of rational numbers.

(ii) There exists a right triangle with rational side lengths (called a rational right triangle) whose area is n.

In his book *Liber Quadratorum* published in 1225, Fibonacci (1175–1250) named an integer satisfying (i) a “congruum” from the Latin, which means to meet together, since the three squares $x^2 - n$, x^2, and $x^2 + n$ are congruent modulo n.

The congruent number problem (CNP, for short) is to determine, in finitely many steps, whether or not a given rational number is a congruent number, and, if it is, find all the corresponding x in (i) or rational right triangles in (ii). No such algorithm has ever been found. The Persian mathematician Al-Karaji (953–1029), perhaps the first mathematician, stated this problem in terms of (i). A similar question appeared in his Arabic translation of the work of Diophantus in Greek. In an Arab manuscript of the tenth century, Mohammed Ben Alhocain realized the equivalence between (i) and (ii) and stated that this problem is “the principal object of the theory of rational right triangles” (see Dickson’s book [20, CHAP. XVI, P. 459]).

Recall that any rational Pythagorean triple has the following form:

$$2abt, \quad (a^2 - b^2)t, \quad (a^2 + b^2)t$$

for a unique (a, b, t), where t is a positive rational number and $a > b$ are two coprime positive integers with $2 \nmid (a + b)$. We call a rational Pythagorean triple primitive if $t = 1$, i.e., its triangle has coprime integral side lengths. It follows that n is a congruent number if and only if n has the same square-free part as $ab(a + b)(a - b)$, for some integers a and b. For example, by taking $(a, b) = (5, 4)$, $(2, 1)$, and $(16, 9)$, note that $5, 6, 7$ are congruent numbers with corresponding triangles $(20/3, 3/2, 41/6)$, $(3, 4, 5)$, and $(24/5, 35/12, 337/60)$. To consider CNP, it is enough to consider square-free integers. In *Liber Quadratorum*, Fibonacci constructed these right triangles and also claimed that 1 is not a congruent number, but did not give a proof.

In 1640, Fermat discovered his infinite descent method to show that $1, 2, 3$ are noncongruent numbers. The same method could be employed to find more noncongruent numbers, for example, any prime $p \equiv 3 \pmod 8$. In fact, suppose such a prime p is a congruent number, then there exists a primitive Pythagorean triple $(a^2 - b^2, 2ab, a^2 + b^2)$ whose area $ab(a + b)(a - b)$ has the square-free part p. Assume the area is minimal. Since $a, b, a + b, a - b$ are coprime to each other, by modulo 8 consideration, we have

$$a = r^2, \quad b = ps^2, \quad a + b = u^2, \quad a - b = v^2$$

for some positive integers r, s, u, v. Note that the Pythagorean triple $(u - v, u + v, 2r)$ is with smaller area, a contradiction.

More examples of congruent and noncongruent numbers (gray for non-congruent numbers) were found:

$n \bmod 8$	1	2	3	5	6	7
n	1	2	3	5	6	7
	9	10	11	13	14	15
	17	18	19	21	22	23
	25	26	27	29	30	31
	33	34	35	37	38	39
	41	42	43	45	46	47
	⋮	⋮	⋮	⋮	⋮	⋮
	217	218	219	221	222	223
	⋮	⋮	⋮	⋮	⋮	⋮

From the table, one may conjecture that all the positive integers congruent to $5, 6, 7$ modulo 8 are congruent numbers (conjectured by Alter, Curtz, and Kubota in [2]) and the density of positive integers congruent to $1, 2, 3$ modulo 8 being non-congruent is one.

The arithmetic of elliptic curves, in particular the BSD conjecture and the Goldfeld conjecture, provides a systematical and deeper point of view to study CNP. We now recall these conjectures to introduce notation.

For an elliptic curve A over a number field F, the set $A(F)$ of rational points has a finitely generated abelian group structure by Mordell–Weil theorem. Its rank is denoted by $\operatorname{rank}_{\mathbb{Z}} A(F)$. The Hasse–Weil L-function $L(s, A/F)$ of A is defined as an Euler product and conjectured to be entire and to satisfy a functional equation. The vanishing order of $L(s, A/F)$ at $s = 1$ denoted by $\operatorname{ord}_{s=1} L(s, A/F)$ is called the analytic rank of A/F. When $F = \mathbb{Q}$, the conjecture is known by the work of Wiles [54], et al., and the functional equation is given by

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

where $N_A \in \mathbb{Z}_{\geq 1}$ is the conductor of $A/\mathbb{Q}$, and $\epsilon(A) \in \{\pm 1\}$ is the root number.

Conjecture 1 (BSD). *Let A be an elliptic curve over a number field F. Then the following holds:*

(1) $\operatorname{rank}_{\mathbb{Z}} A(F) = \operatorname{ord}_{s=1} L(s, A/F)$.

(2) *The Tate–Shafarevich group $Ш(A/F)$ is finite. For $r = \operatorname{ord}_{s=1} L(s, A/F)$,*

$$\frac{L^{(r)}(1, A/F)}{r!\Omega_A R_A/\sqrt{|D_F|}} = \frac{\prod_v c_v \cdot \#Ш(A/F)}{\#A(F)_{\mathrm{tors}}^2}.$$

Here D_F is the discriminant of F, while Ω_A, R_A, and c_v are the Néron period, the regulator, and the Tamagawa number of A at place v, respectively.

For a prime p, we call the equality of p-valuation on both sides the p-part BSD formula.

One significant fact related to the BSD conjecture for an elliptic curve A over $\mathbb{Q}$ is that if it holds, then there will be an effective algorithm to compute generators of $A(\mathbb{Q})$ [39]. It is easy to see that a positive integer n is a congruent number if and only if the elliptic curve (called a congruent elliptic curve)

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

has Mordell–Weil group $E^{(n)}(\mathbb{Q})$ of positive rank. There exists a one-to-one correspondence between rational right triangles with area n and nontorsion rational points of $E^{(n)}$. In particular, the BSD conjecture for $E^{(n)}$ would solve the CNP.

A fundamental result on the BSD conjecture was obtained by Coates–Wiles [18], Rubin [43], Gross–Zagier [24], and Kolyvagin [36]: If $\operatorname{ord}_{s=1} L(s, A/\mathbb{Q}) \leq 1$, then

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

and $\#\text{Ш}(A/\mathbb{Q}) < \infty$. There are several results on the p-part BSD formula, including Rubin [43], Kato [33], Kolyvagin [36], Skinner–Urban [46], Zhang [56], Jetchev–Skinner–Wan [31]. The full BSD conjecture was verified for a subfamily of congruent elliptic curves, which have both algebraic and analytic rank one.

Theorem 2 ([37]). *Let $n \equiv 5 \pmod 8$ be a square-free positive integer, all of whose prime factors are congruent to 1 modulo 4. Assume that $\mathbb{Q}(\sqrt{-n})$ has no ideal class of order 4, then $E^{(n)} : y^2 = x^3 - n^2 x$ has both algebraic and analytic rank 1 and the full BSD conjecture holds.*

For the above congruent number elliptic curves, the 2-part of the BSD formula is proved in [51], [50]. The p-part of the BSD formula, when $p \geq 3$, $p \nmid n$, is the consequence of works by Perrin-Riou [42], Kobayashi [35], etal. The p-part of the BSD formula, when $p \equiv 1 \pmod 4$, $p \mid n$, is proved in Li-Liu-Tian [37]. The generalization of Kobayashi's work to potential supersingular primes together with the argument of Perrin-Riou [42], also implies the p-part BSD formula for primes p of potential supersingular reduction (see [41]).

There is a conjecture on statistical behaviors of analytic ranks for a quadratic twist family of elliptic curves. For an elliptic curve $y^2 = f(x)$ over F, its quadratic twist family consists of elliptic curves $ny^2 = f(x)$ with $n \in F^\times$. Based on minimalist principle, Goldfeld proposed the following:

Conjecture 3 (Goldfeld [14,23]). *Let $\varepsilon \in \{\pm 1\}$ and $\mathcal{A}$ be a quadratic twist family of elliptic curves over F. Then, ordered by norms of conductors, among the quadratic twists $A \in \mathcal{A}$ with $\epsilon(A) = \varepsilon$,*

$$\operatorname{Prob}\big(\operatorname{ord}_{s=1} L(s, A/F) = 0\big) \quad \big(\textit{resp.}\ \operatorname{Prob}\big(\operatorname{ord}_{s=1} L(s, A/F) = 1\big)\big)$$

is one if $\varepsilon = +1$ (resp. -1). In particular, if $F = \mathbb{Q}$, as A runs over a quadratic twist family of elliptic curves,

$$\operatorname{Prob}\big(\operatorname{ord}_{s=1} L(s, A/\mathbb{Q}) = r\big)$$

is equal to $1/2$ for $r = 0, 1$, and 0 for $r \geq 2$.

We refer to $\epsilon = 1$ (resp. -1) case of the conjecture as the even (resp. odd) parity Goldfeld conjecture. The significance of Goldfeld conjecture is that, together with the Gross–Zagier formula (see Section 2), it solves the problem of finding generators of $A(\mathbb{Q})$ for density-one elliptic curves A in a quadratic twist family.

Conjecture 4 (Goldfeld [23], Katz–Sarnak [34], etc.). *Let A run over all elliptic curves over a fixed number field F as ordered by height, then*

$$\mathrm{Prob}\big(\mathrm{ord}_{s=1} L(s, A/F) = r\big)$$

is equal to $1/2$ for $r = 0, 1$, and 0 for $r \geq 2$.

For $n \in \mathbb{Z}_{\geq 0}$, we have

$$\epsilon\big(E^{(n)}\big) = \begin{cases} +1, & n \equiv 1, 2, 3 \pmod 8, \\ -1, & n \equiv 5, 6, 7 \pmod 8). \end{cases}$$

The central L-value of $E^{(n)}$ is related to the following ternary quadratic equation by Tunnell [52]: For a positive square-free integer n, let $a = 1$ if n is odd and $a = 2$ if n is even. Consider the equation

$$2ax^2 + y^2 + 8z^2 = n/a, \quad x, y, z \in \mathbb{Z}.$$

Let $\Sigma(n)$ be the set of its solutions and let

$$\mathcal{L}(n) = \#\big\{(x, y, z) \in \Sigma(n) \mid 2 \mid z\big\} - \#\big\{(x, y, z) \in \Sigma(n) \mid 2 \nmid z\big\}.$$

It is easy to see that $\mathcal{L}(n) = 0$ for positive $n \equiv 5, 6, 7 \pmod 8$. Tunnell proved that for n positive square-free, $\mathcal{L}(n) \neq 0$ if and only if $L(1, E^{(n)}) \neq 0$. The BSD conjecture predicts the following:

Conjecture A. *A positive square-free integer n is a congruent number if and only if $\mathcal{L}(n) = 0$. In particular, any positive integer $n \equiv 5, 6, 7 \pmod 8$ is a congruent number.*

One can determine whether $\mathcal{L}(n) = 0$ in finitely many steps, yet there is no algorithm to find all the rational points of $E^{(n)}$. Tunnell's work was recently generalized to any given quadratic twist family of elliptic curves over $\mathbb{Q}$ in [26].

The even Goldfeld conjecture for the family $E^{(n)}$ can be stated as follows:

Conjecture B1. *Among all square-free positive integers $n \equiv 1, 2, 3 \pmod 8$, the subset of n with $\mathcal{L}(n) \neq 0$ has density one.*

For an elliptic curve $A/\mathbb{Q}$ with root number -1, the BSD conjecture predicts that $A(\mathbb{Q})$ has an infinite-order point. Heegner point construction provides a systematic method to construct rational points. We now give a concrete construction for congruent elliptic curves $E^{(n)}$ with $n \equiv 5, 6, 7 \pmod 8$. Denote by E the elliptic curve $y^2 = x^3 - x$ that has conductor 32. The Abel–Jacobi map induces the complex uniformization

$$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E, \quad z \mapsto \int_O^z dx/2y,$$

where $\Lambda_E = \{\int_\gamma dx/2y \mid \gamma \in H_1(E(\mathbb{C}), \mathbb{Z})\} \subset \mathbb{C}$ is the period lattice. Denote by ϕ the newform of weight 2 and level $\Gamma_0(32)$ associated to E. Let f be the analytic map

$$f : X_0(32)(\mathbb{C}) \to E(\mathbb{C})$$

induced by the above complex uniformization $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$ and

$$\mathcal{H} \to \mathbb{C} : \tau \mapsto \int_{i\infty}^{\tau} 2\pi i \phi(z) dz.$$

We now give a construction of Heegner points. For n a positive square-free integer $\equiv 5, 6, 7 \pmod 8$, let $K = \mathbb{Q}(\sqrt{-n})$, let $\mathcal{O}$ be its ring of integers, and H its Hilbert class field. Let c be the complex conjugation and let $E(K)^{c=-1} \subset E(K)$ be the subgroup on which c acts by -1, then we naturally have $E(K)^{c=-1} \simeq E^{(n)}(\mathbb{Q})$.

Define the Heegner point, which lies in $E^{(n)}(\mathbb{Q}) \otimes \mathbb{Q}$, as follows:

$$y_n := \begin{cases} \mathrm{tr}_{H/K}(1 - [i]) \cdot f(\tau_n), \\ \mathrm{tr}_{H/K}[i] \cdot f(\tau_n), \\ 2\,\mathrm{tr}_{H/K}\, f(\tau_n), \end{cases} \quad \text{where } \mathcal{H} \ni \tau_n = \begin{cases} \frac{1}{4(1-\sqrt{-n})}, \\ \frac{-1}{4\sqrt{-n}}, \\ \frac{-2}{\epsilon+\sqrt{-n}}, \end{cases} \quad \text{if } n \equiv \begin{cases} 5 \pmod 8, \\ 6 \pmod 8, \\ 7 \pmod 8). \end{cases}$$

Here ϵ is an integer such that $\epsilon^2 \equiv -n \pmod{128}$. The construction is natural from an automorphic representation point of view, which will be described in Section 2.

Conjecture B2. *Among all positive integers $n \equiv 5, 6, 7 \pmod 8$, the subset of n with y_n being nontorsion has density one.*

The Gross–Zagier formula (see Section 2) implies that y_n is nontorsion if and only if $L'(1, E^{(n)}) \neq 0$. Furthermore, Kolyvagin's work shows that if y_n is nontorsion, then the rank of $E^{(n)}(\mathbb{Q})$ is one [36]. The Gross–Zagier formula also helps compute y_n and therefore a generator of $E^{(n)}(\mathbb{Q})$ [19].

Remark 5. The combination of *Conjectures B1* and *B2* is equivalent to Goldfeld conjecture for congruent elliptic curves, which would solve the CNP for integers with probability one.

Example 1. For $n = 101, 102$, and 103, the Heegner point y_n is given by

$$\left(\frac{-3975302500}{442723681}, \frac{2808122994457950}{9315348971921}\right), \ (5100, 364140),$$

and

$$\left(\frac{-777848715219380607}{8780605285453456}, \frac{406939902409963977921570495}{822785599723202981879104}\right).$$

And right triangles with area n corresponding to y_n have side lengths

$$\left(\frac{267980280100}{44538033219}, \frac{44538033219}{1326635050}, \frac{2015242462949760001961}{590857159263897259 50}\right), \ \left(\frac{20}{7}, \frac{357}{5}, \frac{2501}{35}\right),$$

and

$$\left(\frac{1628625311094381 6}{441394452081515}, \frac{45463628564396045}{8143126555471908}, \frac{13413066493804722837470200107969 7}{35943308841829573942237085806 20}\right).$$

Heegner [28] in 1952 showed that any prime or double prime $n \equiv 5, 6, 7 \pmod 8$ is a congruent number. Later on, based on Heegner's method, Monsky [40] in 1990 proved that for $(p_1, p_2) \equiv (1, 5) \pmod 8$ (resp. $(p_1, p_2) \equiv (1, 7) \pmod 8$), two primes such that $(\frac{p_1}{p_2}) = -1$, the product $p_1 p_2$ (resp. $2p_1 p_2$) is a congruent number. A natural question is to seek congruent numbers with many prime factors. The following was first conjectured by Monsky in [40].

Theorem 6 (Tian [50]). *Let n be the product of an odd number of primes $\equiv 5 \pmod 8$ that are not quadratic residues to each other, then n is a congruent number.*

Theorem 7 (Burungale–Tian [11]). Conjecture B1 *is true, namely among all square-free positive integers $n \equiv 1, 2, 3 \pmod 8$, the subset of n with $\mathcal{L}(n) \neq 0$ has density one. In particular, the density of noncongruent numbers among square-free positive integers* $\equiv 1, 2, 3 \pmod 8$ *is one.*

Let S be the subset of positive square-free integers $n \equiv 5, 6, 7 \pmod 8$ so that $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/E(\mathbb{Q})[2] = 1$. By the results on distribution of 2-Selmer groups [27, 32, 49], the density of S for all the positive square-free integers $n \equiv 5, 6, 7 \pmod 8$ is

$$2 \prod_{j \geq 1} (1 + 2^{-j})^{-1}.$$

Theorem 8 ([47, 50, 51]). *There is a density-$\frac{2}{3}$ subset of S so that the analytic rank of $E^{(n)}$ is one and the 2-part BSD formula holds. In particular, among all the square-free positive integers $n \equiv 5, 6, 7 \pmod 8$, the density of congruent numbers is greater than*

$$\frac{4}{3} \prod_{j \geq 1} (1 + 2^{-j})^{-1} \quad \left(> \frac{1}{2} \right).$$

The strategy of the proof of Theorems 6 and 8 (resp. Theorem 7) will be given in Section 2 (resp. Section 3).

2. HEEGNER POINT AND EXPLICIT GROSS–ZAGIER FORMULA

Heegner points and Gross–Zagier formula play an important role in the study of elliptic curves. The work of Yuan, Zhang, and Zhang [55] gives the general construction of Heegner points on Shimura curves over totally real fields and establishes the general Gross–Zagier formula. Some arithmetic applications require an explicit form of the formula such as that in [24]. In this section, we introduce the explicit Gross–Zagier formula from [15] and its application to CNP.

We assume as given:

- A—an elliptic curve over $\mathbb{Q}$ with conductor N,
- K—an imaginary quadratic field with discriminant D,
- χ—a ring class character of K with conductor c, which can be viewed as a character on $\mathrm{Gal}(H_c/K)$, where H_c is the ring class field of K with conductor c,

characterized by the reciprocity law

$$t : \mathrm{Gal}(H_c/K) \xrightarrow{\sim} K^\times \backslash \hat{K}^\times / \hat{\mathcal{O}}_c^\times.$$

Here, $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ is an order of $\mathcal{O}_K$. For any abelian group M, denote $\hat{M} = M \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ with $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

Assume that the Rankin–Selberg L-series $L(s, A, \chi)$ associated to (A, χ) has sign -1 in its function equation.

In the following, we shall introduce the construction of the Heegner points and the explicit Gross–Zagier formula for (A, χ) under the assumption $(c, N) = 1$. Let B be the unique indefinite quaternion algebra over $\mathbb{Q}$ whose ramified places are given by all p such that

$$\epsilon_p(A, \chi) = -\chi_p \eta_p(-1),$$

where $\epsilon_p(A, \chi)$ is the local root number of $L(s, A, \chi)$ at p and η_p is the quadratic character of $\mathbb{Q}_p^\times$ associated to $K_p/\mathbb{Q}_p$. In particular, there exists an embedding of K into B. Fix such an embedding once and for all. An order R of B is called *admissible* with respect to (A, χ) if the discriminant of R is N and $R \cap K = \mathcal{O}_c$. Such an order exists and is unique up to conjugaction by $\hat{K}^\times$. Fix such an admissible order R.

Denote by $X_{\hat{R}^\times}$ the Shimura curve over $\mathbb{Q}$ associated to B of level $\hat{R}^\times$. Under an isomorphism $B(\mathbb{R}) \simeq M_2(\mathbb{R})$, it has the following complex uniformization:

$$X_{\hat{R}^\times}(\mathbb{C}) = B^\times \backslash \mathcal{H}^\pm \times \hat{B}^\times / \hat{R}^\times \sqcup \{\text{cusps}\}.$$

Denote by $[z, g]_{\hat{R}^\times}$ the image of $(z, g) \in \mathcal{H}^\pm \times \hat{B}^\times$ in $X_{\hat{R}^\times}(\mathbb{C})$. Let $\xi_{\hat{R}^\times} \in \mathrm{Pic}(X_{\hat{R}^\times}) \otimes \mathbb{Q}$ be the normalized Hodge class with degree 1 on each connected component of $X_{\hat{R}^\times, \bar{\mathbb{Q}}}$ (see [55, SECTION 3.1.3]).

The following proposition follows from the modularity theorem and the Jacquet–Langlands correspondence.

Proposition 9 ([15, PROPOSITION 3.8]). *Up to scalars, there is a unique nonconstant morphism $f : X_{\hat{R}^\times} \to A$ over $\mathbb{Q}$ satisfying the following properties:*

- *f sends $\xi_{\hat{R}^\times}$ to the identity O of A in the sense that if $\xi_{\hat{R}^\times}$ is represented by a divisor $\sum n_i x_i$ on $X_{\hat{R}^\times, \overline{\mathbb{Q}}}$, then $\sum n_i f(x_i) = O$.*
- *For each place $p|(N, D)$,*

  $$T_{\varpi_p} f = \chi_p^{-1}(\varpi_p) f.$$

  Here, T_{ϖ_p} is the automorphism of $X_{\hat{R}^\times}$, which on $X_{\hat{R}^\times}(\mathbb{C})$ is given by $[z, g]_{\hat{R}^\times} \mapsto [z, g\varpi_p]_{\hat{R}^\times}$, with $\varpi_p \in K_p^\times$ being any uniformizer of K_p.

Let $z \in \mathcal{H}$ be the unique point fixed by $K^\times$ and let $P = [z, 1]_{\hat{R}^\times}$. By the theory of complex multiplication, P is defined over the ring class field H_c of K with conductor c and the Galois action is given by

$$[z, 1]_{\hat{R}^\times}^\sigma = [z, t_\sigma]_{\hat{R}^\times}, \quad \sigma \in \mathrm{Gal}(H_c/K),$$

where $\sigma \mapsto t_\sigma$ is the reciprocity map.

Define the Heegner point

$$P_\chi(f)=\sum_{\sigma\in\mathrm{Gal}(H_c/K)} f\left(P^\sigma\right)\chi(\sigma)\in A(H_c)\otimes\mathbb{Q}(\chi).$$

Here $\mathbb{Q}(\chi)$ is the field over $\mathbb{Q}$ generated by image of χ.

Theorem 10 ([15, 55]). *Assume $(N,c)=1$. Then*

$$L'(1,A,\chi)=2^{-\mu(N,D)}\frac{8\pi^2(\phi,\phi)_{\Gamma_0(N)}}{u^2\sqrt{|Dc^2|}}\cdot\frac{\hat{h}_K(P_\chi(f))}{\deg f}.$$

Here, ϕ is the newform associated to A with

$$(\phi,\phi)_{\Gamma_0(N)}=\iint_{\Gamma_0(N)\backslash\mathcal{H}}|\phi(x+iy)|^2dxdy,$$

$u=[\mathcal{O}_c^\times:\mathbb{Z}^\times]$, $\mu(N,D)$ is the number of common prime factors of N and D, $\hat{h}_K$ is the Néron–Tate height on A over K, and $\deg(f)$ *is the degree of the morphism f.*

Remark 11.

(1) To compute Heegner points (if non-torsion) via CM theory and modular parameterization, one only gets an approximation. The precise computation can be carried out since one knows the height of Heegner point via the above formula (see [53]).

(2) One may use different Heegner points to construct rational points on A by choosing different K. The case $(D,N)\neq 1$ sometimes provides points with smaller height. The above formula with $(D,N)\neq 1$ was conjectured by Gross and Hayashi in [25] and employed in [53] for the computation of rational points.

Some arithmetic problems lead to the situation $(c,N)\neq 1$. Consider the following: a nonzero rational number is called a *cube sum* if it is of form a^3+b^3 with $a,b\in\mathbb{Q}^\times$. For any $n\in\mathbb{Q}^\times$, consider the elliptic curve $C_n: x^3+y^3=2n$. If n is not a cube, then $2n$ is a cube sum if and only if the rank of $C_n(\mathbb{Q})$ is positive.

Theorem 12 ([16]). *For any odd integer $k\geq 1$, there exist infinitely many cube-free odd integers n with exactly k distinct prime factors such that*

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

Here, a certain Heegner point is considered for the pair (A,χ) where $A=X_0(36): x^2=y^3+1$ is an isogeny to C_1 and χ is a certain cubic ring class character over the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$ with conductor $3n^*$ where n^* is the product of prime factors in n. In particular, the pair (A,χ) has joint ramification at the prime 3.

In fact, the explicit Gross–Zagier formula is proved for any pair (π,χ) where

- π is a cuspidal automorphic representation on GL_2 over a totally real field F with central character ω_π, discrete series of weight 2 at all archimedean places,

- $\chi : K^\times \backslash \hat{K}^\times \to \mathbb{C}^\times$ is a character of finite order for a totally imaginary quadratic extension K over F such that

  (i) $\omega_\pi \cdot \chi|_{\mathbb{A}_F^\times} = 1$,

  (ii) the root number of the Rankin–Selberg L-series $L(s, \pi, \chi)$ is -1.

Based on the work of Yuan–Zhang–Zhang [55], the above explicit formula is established via generalizing Gross–Prasad local test vector theory.

The relevant problem in local harmonic analysis is the following. Let $\mathcal{B}$ be a quaternion algebra over a local field $\mathcal{F}$ with a quadratic sub-$\mathcal{F}$-algebra $\mathcal{K}$. Let π be an irreducible smooth admissible representation on $\mathcal{B}^\times$ which is of infinite dimension if $\mathcal{B}$ is split. Let χ be a character of $\mathcal{K}^\times$ such that $\chi|_{\mathcal{F}^\times}$ is the inverse of the central character of π. Consider the functional space

$$\mathcal{P}(\pi, \chi) := \mathrm{Hom}_{\mathcal{K}^\times}(\pi, \chi^{-1}).$$

In general, $\dim_{\mathbb{C}} \mathcal{P}(\pi, \chi) \leq 1$. In the case $\mathcal{P}(\pi, \chi) \neq 0$, a vector φ is called a *test vector* for (π, χ) if $\ell(\varphi) \neq 0$ for any nonzero $\ell \in \mathcal{P}(\pi, \chi)$.

Moreover, for an unitary (π, χ), $\mathcal{P}(\pi, \chi)$ is nonzero if and only if the bilinear form $\alpha \in \mathcal{P}(\pi, \chi) \otimes \mathcal{P}(\bar{\pi}, \bar{\chi})$ defined as the toric integral of matrix coefficients

$$\alpha(\varphi_1 \otimes \varphi_2) = \int_{\mathcal{F}^\times \backslash \mathcal{K}^\times} \langle \pi(t)\varphi_1, \varphi_2 \rangle \chi(t) dt, \quad \varphi_1 \in \pi, \varphi_2 \in \bar{\pi}$$

is nonzero. Here, $\bar{\pi}$ (resp. $\bar{\chi}$) is the complex conjugate of π (resp. χ) and $\langle \cdot, \cdot \rangle$ is a nondegenerate invariant pairing on $\pi \otimes \bar{\pi}$. In particular, if $\mathcal{P}(\pi, \chi) \neq 0$, φ is a test vector for (π, χ) if and only if $\alpha(\varphi, \bar{\varphi}) \neq 0$.

For any pair (π, χ) as above, in [15] we find an *admissible* order $\mathcal{R}$ for (π, χ) which is unique up to $\mathcal{K}^\times$-conjugacy. The invariant subspace $\pi^{\mathcal{R}^\times}$ of π by $\mathcal{R}^\times$ is at most of dimension 2. By studying the toric integral α, there is a line in $\pi^{\mathcal{R}^\times}$ containing test vectors for (π, χ).

Our explicit Gross–Zagier formula satisfies the following properties: First, the test vector only depends on the local type π_v, χ_v, for v dividing the conductor of π. It is useful when considering horizontal variation (quadratic twist, for example), see [7, 13], or vertical variation (in Iwasawa theory) of the character χ. We also have a so-called S-version formula which says that for a different choice of a pure tensor test vector, for example, at a finite set of places S, the new explicit formula can be obtained by modifying the original one by local computations at S, for example, see [16].

In the rest of this section, we sketch a proofs of Theorems 6 and 8. In Heegner's work, the point y_n is not 2-divisible. In [50, 51], Heegner's results were generalized to many prime factors by induction on 2-divisibility of Heegner points via the Waldspurger and Gross–Zagier formulas.

For $E : y^2 = x^3 - x$, $K = \mathbb{Q}(\sqrt{-n})$, $n \equiv 5, 6, 7$ positive square-free, the explicit Gross–Zagier formula for (E, K) gives

$$\hat{h}_{\mathbb{Q}}(y_n) = 2^a \frac{L'(1, E^{(n)})}{\Omega_{E^{(n)}}}$$

where $a = 1, 0, 1$ in the case $n \equiv 5, 6, 7 \pmod 8$, respectively. Now if y_n is nontorsion, then the BSD conjecture becomes

$$\left[E^{(n)}(\mathbb{Q})/E^{(n)}(\mathbb{Q})_{\mathrm{tor}} : \mathbb{Z}\cdot y_n\right] = 2^{\mu(n)-1}\sqrt{\#Ш\left(E^{(n)}/\mathbb{Q}\right)},$$

where $\mu(n)$ is the number of odd prime factors of n. If n is a prime then the 2-part of the BSD conjecture is equivalent to 2-indivisibility of y_n, this is exactly Heegner's case. As $\mu(n)$ becomes large, the 2 divisibility of y_n becomes high and the original Heegner's argument does not work directly. Whenever $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/E^{(n)}(\mathbb{Q})[2] = 1$, the 2-divisibility of y_n fully comes from Tamagawa numbers. The 2-divisibility can be proved via induction; to do this, one employs various relations between different Heegner points.

We employ the induction method (see [50]) in the case $n \equiv 5 \pmod 8$ with all prime factors $\equiv 1 \pmod 4$. Let $z_n := f(\tau_n)$ and let y_n be the Heegner points as in the Section 1. Denote by H the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$ and let $H_0 \subset H$ be the genus subfield determined by $\mathrm{Gal}(H_0/K) \simeq 2\,\mathrm{Cl}(K)$. For each $d|n$ with the same above property as n, let $y_0 = \mathrm{tr}_{H/H_0} z_n$ and $y_{d,0} = \mathrm{tr}_{H/K(\sqrt{-d})} z_n$. Then these points satisfy the following relation:

$$y_n + \sum_{\substack{1\le d|n, d\neq n,\\ d\equiv 5 \pmod 8}} y_{d,0} = 2^{\mu(n)} y_0 \quad \left(\mathrm{mod}\ E[2]\right).$$

Furthermore, the Gross–Zagier formula implies that whenever $y_{d,0}$ is nontorsion, both $y_{d,0}$ and y_d lie in the one-dimensional space $E(\mathbb{Q}(\sqrt{-d}))^{c=-1} \otimes \mathbb{Q}$ and

$$[y_{d,0} : y_d]^2 = \frac{L^{\mathrm{alg}}(1, E^{(n/d)})}{L^{\mathrm{alg}}(1, E)}, \quad \text{where } L^{\mathrm{alg}}(1, E^{(n/d)}) = \frac{L(1, E^{(n/d)})}{\Omega_{E^{(n/d)}}}.$$

By induction on the 2 divisibility of y_d and 2 divisibility of $\frac{L^{\mathrm{alg}}(1,E^{(n/d)})}{L^{\mathrm{alg}}(1,E)}$, one gets the following 2 divisibility of y_n whenever $\mathrm{Cl}(K)$ has no element of order 4:

$$y_n \in \left(2^{\mu(n)-1}E(K)^{c=-1} + E(K)_{\mathrm{tor}}\right)\backslash\left(2^{\mu(n)}E(K)^{c=-1} + E(K)_{\mathrm{tor}}\right).$$

Thus Theorem 6 follows.

The above induction argument was improved in [51] to handle the general case. For a positive integer d, let $g(d) = \#2\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ be the genus class number of $\mathbb{Q}(\sqrt{-d})$. For $n \equiv 5, 6, 7 \pmod 8$, let

$$\mathcal{L}(n) = \begin{cases} [L'(1, E^{(n)})/(2^{2\mu(n)-2-a(n)} \cdot \Omega_{E^{(n)}} R_{E^{(n)}})]^{1/2}, & \text{if } \mathrm{ord}_{s=1} L(1, E^{(n)}) = 1, \\ 0, & \text{otherwise,} \end{cases}$$

where $a(n) = 0$ if n is even and $a(n) = 1$ if n is odd.

Then the BSD conjecture for $E^{(n)}$ is equivalent to $\mathcal{L}(n)^2 = \#Ш(E^{(n)}/\mathbb{Q})$ whenever $L'(1, E^{(n)}) \neq 0$. We have the following criterion for the 2-indivisibility of $\mathcal{L}(n)$:

Theorem 13 ([51]). *For $n \equiv 5, 6, 7 \pmod 8$ positive square-free, $\mathcal{L}(n)$ is an integer and $2^{-\rho(n)}\mathcal{L}(n)$ is odd if*

$$\begin{cases} \sum_{\substack{n=d_0\cdots d_\ell \\ d_i\equiv 1 \ (\mathrm{mod}\ 8), i>0}} \prod_i g(d_i) \equiv 1 \pmod 2 \ \textit{or} \\ \sum_{\substack{n=d_0\cdots d_\ell, \\ d_0\equiv 5,7 \ (\mathrm{mod}\ 8) \\ d_1\equiv 1,3 \ (\mathrm{mod}\ 8) \\ d_i\equiv 1 \ (\mathrm{mod}\ 8), i>1}} \prod_i g(d_i) \equiv 1 \pmod 2, & \textit{if } n \equiv 5, 7 \pmod 8, \\ \sum_{\substack{n=d_0\cdots d_\ell, \\ d_0\equiv 5,6,7 \ (\mathrm{mod}\ 8) \\ d_1\equiv 1,2,3 \ (\mathrm{mod}\ 8) \\ d_i\equiv 1 \ (\mathrm{mod}\ 8), i>1}} \prod_i g(d_i) \equiv 1 \pmod 2, & \textit{if } n \equiv 6 \pmod 8, \end{cases}$$

where $\rho(n)$ is a positive integer (defined in [51]*) arising from an isogeny between $E^{(n)}$ and $2ny^2 = x^3 + x$.*

Let

$$\begin{aligned} s(n) &= \dim_{\mathbb{F}_2} \mathrm{Sel}_2\big(E^{(n)}/\mathbb{Q}\big)/E^{(n)}(\mathbb{Q})[2] \\ &= \mathrm{rank}_{\mathbb{Z}}\, E^{(n)}(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш\big(E^{(n)}/\mathbb{Q}\big)[2]. \end{aligned}$$

Consider the following sets for $i = 5, 6, 7$:

- Σ_i—the set of all square-free positive integers $n \equiv i \pmod 8$,
- $\Sigma_i' \subset \Sigma_i$—the subset of n with $s(n) = 1$,
- $\Sigma_i'' \subset \Sigma_i$—the subset of n satisfying the conditions in the Theorem 13.

Theorem 14 (Heath-Brown [27], Swinnerton-Dyer [49], Kane [32]). *The density of Σ_i' in Σ_i is*

$$2\prod_{k=1}^{\infty}\big(1 + 2^{-k}\big)^{-1} = 0.8388\ldots$$

Theorem 15 (Smith [47]). *The set Σ_i'' is contained in Σ_i' with density $\frac{3}{4}$, $\frac{1}{2}$, $\frac{3}{4}$ for $i = 5, 6, 7$, respectively.*

Observe that Theorem 8 is a consequence of Theorems 13, 14, and 15.

3. SELMER GROUPS: P-CONVERSE AND DISTRIBUTION

The n-Selmer group for an elliptic curve A over a number F is defined by

$$\mathrm{Sel}_n(A/F) = \ker\Big(H^1\big(F, A[n]\big) \to \prod_v H^1(F_v, A)\Big)$$

and fits into the short exact sequence

$$0 \to A(F)/nA(F) \to \mathrm{Sel}_n(A/F) \to Ш(A/F)[n] \to 0.$$

The group $\mathrm{Hom}(\mathrm{Sel}_{p^\infty}(A/F), \mathbb{Q}_p/\mathbb{Z}_p)$ is known to be a finitely generated $\mathbb{Z}_p$-module, its rank of free part is called p^∞-Selmer corank of A, denoted by $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/F)$.

Conjecture 16 (BSD, reformulation). *Let A/F be an elliptic curve over a number field, $r \in \mathbb{Z}_{>0}$, and p be a prime. Then the following are equivalent:*

(1) $\mathrm{ord}_{s=1} L(s, A/F) = r$,

(2) $\mathrm{rank}_{\mathbb{Z}} A(F) = r$ *and* $Ш(A/F)$ *is finite,*

(3) $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/F) = r$.

Notation (p-converse). *The implication*

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

is referred to as rank r p-converse.

We can also consider a Selmer variant of Goldfeld's Conjecture 3. The following was conjectured by Bhargava–Kane–Lenstra–Poonen–Rains.

Conjecture 17 ([4]). *Let F be a global field, p be a prime, and G a finite symplectic p-group. If all elliptic curves A over F are ordered by height, then for $r = 0, 1$ we have*

$$\mathrm{Prob}\big(\mathrm{Sel}_{p^\infty}(A/F) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus G\big) = \frac{1}{2} \cdot \frac{(\#G)^{1-r}}{\#\mathrm{Sp}(G)} \cdot \prod_{i \geq r} \big(1 - p^{1-2i}\big).$$

In particular, the density of rank 0 (or 1) elliptic curves over F is $\frac{1}{2}$.

3.1. Distribution of Selmer groups and Goldfeld conjecture

The following Smith's result shows that even for a quadratic twist family, the distribution follows the same pattern as the above conjecture.

Theorem 18 (Smith [48]). *Let $A/\mathbb{Q}$ be an elliptic curve satisfying A has full rational 2-torsion, but no rational cyclic subgroup of order 4. Then, among the quadratic twists $A^{(d)}$ of A, a distribution law as in Conjecture 17 holds for $p = 2$.*

In particular, among all quadratic twists $A^{(d)}$ with sign $+1$ (resp. -1), there is a subset of density one with $\mathrm{corank}_{\mathbb{Z}_2} \mathrm{Sel}_{2^\infty}(A^{(d)}/\mathbb{Q}) = 0$ (resp. 1).

Remark 19. Smith's work is based on the following results of Heath-Brown, Swinnerton-Dyer, and Kane on distribution of 2-Selmer groups, which is the first step to understand the distribution of 2^∞-Selmer groups.

Theorem 20 ([27,32,49]). *Let $A/\mathbb{Q}$ be an elliptic curve satisfying*

- *A has full rational 2-torsion, but no rational cyclic subgroup of order 4.*

Then for $r \in \mathbb{Z}_{\geq 0}$, among the quadratic twists $A^{(d)}$ of A,

$$\mathrm{Prob}\big(\dim_{\mathbb{F}_2} \mathrm{Sel}_2\big(A^{(d)}/\mathbb{Q}\big)/A^{(d)}(\mathbb{Q})[2] = r\big) = \prod_{j=0}^{\infty} \big(1 + 2^{-j}\big)^{-1} \prod_{i=1}^{r} \frac{2}{2^i - 1}.$$

In general, for a quadratic twist family of elliptic curves over $\mathbb{Q}$, its distribution of 2-Selmer groups may exhibit new behavior. For example, the quadratic twist family of Tiling number elliptic curves has

$$A^{(d)} : dy^2 = x(x-1)(x+3) \quad \text{with } A^{(1)}(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

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 20. For example, if $d \neq 1$, $d \equiv 1 \pmod{12}$ is positive square-free, then

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2\big(A^{(-d)}/\mathbb{Q}\big)/A^{(-d)}(\mathbb{Q})[2] \geq 2.$$

A preliminary study suggests that for such elliptic curves, the distribution of 2-Selmer groups may look more like that of the 4-ranks of ideal class groups of the underlying imaginary quadratic fields.

Theorem 21 ([22]). *Let A be the elliptic curve $y^2 = x(x-1)(x+3)$. Among the set of positive square-free integers $d \equiv 7 \pmod{24}$ (resp. $d \equiv 3 \pmod{24}$), the subset of d such that both of $A^{(\pm d)}$ have $\operatorname{Sel}_2(A^{(\pm d)}/\mathbb{Q})/A^{(\pm d)}(\mathbb{Q})[2]$ trivial has density $\frac{1}{2}\prod_{i=1}^{\infty}(1-2^{-i}) > 14.4\%$ (resp. of density $\prod_{i=1}^{\infty}(1-2^{-i}) > 28.8\%$).*

In general, for $r \in \mathbb{Z}_{\geq 0}$, for the set of positive square-free integers $d \equiv 3 \pmod{24}$,

$$\begin{aligned}&\operatorname{Prob}\big(\dim_{\mathbb{F}_2} \operatorname{Sel}_2\big(A^{(d)}/\mathbb{Q}\big)/A^{(d)}(\mathbb{Q})[2] = 2r\big)\\ &= \left(\sum_{k=0}^{r} 2^{-(r+k)(3r+3k-1)/2} \prod_{i=1}^{r+k}\big(1-2^{-i}\big)^{-2} \prod_{i=0}^{2k-1}\big(2^{r+k-i}-1\big) \prod_{i=1}^{k} \frac{4^{i-1}}{4^i-1}\right) \cdot \prod_{i=1}^{\infty}\big(1-2^{-i}\big).\end{aligned}$$

An approach to Goldfeld conjecture. The Goldfeld conjecture for a quadratic twist family of elliptic curves over $\mathbb{Q}$ is a consequence of the following steps:

(1) Distribution of p^∞-Selmer groups in the quadratic twist family, which should be a certain variant of general distribution law for all elliptic curves in [4].

(2) The rank zero and rank one p-converse.

Proof of Theorem 7. It is a direct consequence of Tunnell's work on quadratic twist L-values of congruent elliptic curves [52], Theorem 18 of Smith on distribution of 2^∞-Selmer groups, and Theorem 22 below on the rank zero p-converse for CM elliptic curves for $p = 2$. ■

3.2. Recent progress: *p*-converse

In the remaining part of this section, we discuss the p-converse theorem in the CM case. For a few other p-converse theorems, see [6, 8–10]. Fix a prime p.

Theorem 22 (Rubin [43, 44], Burungale–Tian [11]). *Let $A/\mathbb{Q}$ be a CM elliptic curve. Then,*

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

Remark 23. Assume that $A/\mathbb{Q}$ has CM by K and $p \nmid \#\mathcal{O}_K^\times$. Then the above theorem is due to Rubin [43, 44].

Remark 24. Skinner–Urban [46] established the rank zero p-converse for certain elliptic curves over $\mathbb{Q}$ without CM.

Theorem 25 (W. Zhang [56], Skinner [45], Castella–Wan [17]). *Let $A/\mathbb{Q}$ be a non-CM elliptic curve and $p \geq 3$. Then,*

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

under certain assumptions.

Their methods essentially excludes the CM case. For CM elliptic curves:

Theorem 26 (Burungale–Tian [12], Burungale–Skinner–Tian [8]). *Let A be a CM elliptic curve over $\mathbb{Q}$ and $p \nmid 6N_A$ a prime. Then*

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

3.2.1. Rank zero CM p-converse

We outline the proof of Theorem 22. Unconventionally for the CM elliptic curves, this approach is based on Kato's main conjecture [33], which we recall now.

Let $f \in S_k(\Gamma_0(N))$ be an elliptic newform of even weight $k \geq 2$, level $\Gamma_0(N)$, and Hecke field F. Fix an embedding $\iota_p : \mathbb{Q} \to \overline{\mathbb{Q}}_p$. Let λ be the place of F induced by ι_p, F_λ be the completion of F at λ, and O_λ the integer ring. Let $V_{F_\lambda}(f)$ be the two-dimensional representation of $G_{\mathbb{Q}}$ over F_λ associated to f. We first introduce the related Iwasawa cohomology. For $n \in \mathbb{Z}_{\geq 0}$, let

$$G_n = \operatorname{Gal}\bigl(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\bigr), \quad G_\infty = \varprojlim_n G_n = \operatorname{Gal}\bigl(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}\bigr).$$

Let $\Lambda = O_\lambda[[G_\infty]]$ be a two-dimensional complete semilocal ring. For $q \in \mathbb{Z}_{\geq 0}$, consider the $\Lambda_{\mathbb{Q}_p} = \Lambda \otimes \mathbb{Q}$-module

$$\mathbb{H}^q\bigl(V_{F_\lambda}(f)\bigr) = \varprojlim_n H^q\bigl(\mathbb{Z}[\zeta_{p^n}, 1/p], T\bigr) \otimes \mathbb{Q},$$

where $T \subset V_{F_\lambda}(f)$ is any $G_{\mathbb{Q}}$-stable O_λ-lattice and H^q denotes the étale cohomology. The following holds [33]:

(1) $\mathbb{H}^2(V_{F_\lambda}(f))$ is a torsion $\Lambda_{\mathbb{Q}_p}$-module, and

(2) $\mathbb{H}^1(V_{F_\lambda}(f))$ is a free $\Lambda_{\mathbb{Q}_p}$-module of rank one.

Now we introduce the submodule of $\mathbb{H}^1(V_{F_\lambda}(f))$ generated by Beilinson–Kato elements. We have the following existence of zeta elements for the p-adic Galois representation corresponding to an elliptic newform [33, THM. 12.5]:

(1) There exists a nonzero F_λ-linear morphism

$$V_{F_\lambda}(f) \to \mathbb{H}^1\bigl(V_{F_\lambda}(f)\bigr); \ \gamma \mapsto z_\gamma(f).$$

(2) Let $Z(f)$ be the $\Lambda_{\mathbb{Q}_p}$-submodule of $\mathbb{H}^1(V_{F_\lambda}(f))$ generated by $z_\gamma(f)$ for all $\gamma \in V_{F_\lambda}(f)$. Then $\mathbb{H}^1(V_{F_\lambda}(f))/Z(f)$ is a torsion $\Lambda_{\mathbb{Q}_p}$-module.

Remark 27. For a characterizing property of the morphism $\gamma \mapsto z_\gamma(f)$ in terms of the underlying critical L-values, we refer to [33, THM. 12.5 (1)].

Conjecture 28 (Kato's Main Conjecture [33]). *The following equality of ideals holds in $\Lambda_{\mathbb{Q}_p}$:*

$$\mathrm{Char}\big(\mathbb{H}^2\big(V_{F_\lambda}(f)\big)\big) = \mathrm{Char}\big(\mathbb{H}^1\big(V_{F_\lambda}(f)\big)/Z(f)\big).$$

Theorem 29 (Burungale–Tian [11]). *Kato's main conjecture holds for any CM modular form f and any prime p.*

As observed by Kato [33], the CM case of Kato's main conjecture is closely related to an equivariant main conjecture for the underlying imaginary quadratic field. This is based on an intrinsic relation between the Beilinson–Kato elements and elliptic units.

As a consequence of Theorem 29, we have the following result, which implies Theorem 22.

Theorem 30 ([11]). *Assume that f is CM. Let $H^1_{\mathrm{f}}(\mathbb{Q}, V_{F_\lambda}(f)(k/2))$ be the corresponding Bloch–Kato Selmer group (see Kato [33]). Then,*

$$H^1_{\mathrm{f}}\big(\mathbb{Q}, V_{F_\lambda}(f)(k/2)\big) = 0 \implies \mathrm{ord}_{s=k/2} L(s,f) = 0.$$

3.3. Rank one CM p-converse

In the following, we focus on the proof of the rank one CM p-converse theorem for ordinary primes p. The key is an auxiliary Heegner point main conjecture (HPMC, for short).

Classically, HPMC is only formulated for pairs (A, K') where $A/\mathbb{Q}$ is an elliptic curve and K' is an imaginary quadratic field satisfying the Heegner hypothesis. To show the rank 1 p-converse for a CM elliptic curve, we utilize a certain anticyclotomic Iwasawa theory over the CM field. The key is to construct relevant Heegner points for auxiliary Rankin–Selberg pairs, and consider the underlying HPMC.

Let $A/\mathbb{Q}$ be a CM elliptic curve with CM by K and with p^∞-Selmer corank one. Let λ be the associated Hecke character over K and θ_λ the corresponding theta series.

Lemma 31. *There exists a finite order Hecke character χ over K such that $L(1, \lambda^*/\chi^* \cdot \chi) \neq 0$, where $*$ is the involution given by nontrivial automorphism of K, so that the L-function for the Rankin pair $(f := \theta_{\lambda/\chi}, \ \chi)$,*

$$L(s, f \times \chi) = L(s, \lambda) L\big(s, \lambda^*/\chi^* \cdot \chi\big),$$

has sign -1 and the same vanishing order at the center as $L(s,\lambda) = L(s, A/\mathbb{Q})$.

We have the relevant Heegner point $P_0 \in B(K) \otimes \mathbb{Q}$ on the abelian variety $B := A_{f\times\chi}$ associated to the pair $(f = \theta_{\lambda/\chi}, \chi)$. The Gross–Zagier formula of Yuan–Zhang–Zhang [55] implies that $0 \neq P_0 \in B(K) \otimes \mathbb{Q}$ if and only if $\mathrm{ord}_{s=1} L(s, f \times \chi) = 1$.

Note that p is split in K. Let K_∞/K be the anticyclotomic extension with Galois group $\Gamma \cong \mathbb{Z}_p$. For each $n \geq 1$, let $K_n \subset K_\infty$ be the degree p^n subextension over K.

One can construct a family of norm compatible Heegner points $P_n \in B(K_n)$. Denote by $\Lambda = \mathcal{O}_{\mathfrak{p}}[[\Gamma]]$ and $\Lambda_{\mathbb{Q}_p} = \Lambda \otimes \mathbb{Q}$. Here $\mathcal{O}$ is the endomorphism ring of B (viewed as a subring of $\overline{\mathbb{Q}}$), $\mathfrak{p}|p$ the prime ideal of $\mathcal{O}$ induced by ι_p, and $\mathcal{O}_{\mathfrak{p}}$ the completion of $\mathcal{O}$ at $\mathfrak{p}$.

Proposition 32. *The $\Lambda_{\mathbb{Q}_p}$-modules*

$$S(B/K_\infty) := \big(\varprojlim_n \varprojlim_m \mathrm{Sel}_{\mathfrak{p}^m}(B/K_n)\big)_{\mathbb{Q}_p}, \quad X(B/K_\infty) := \big(\varinjlim_n \varinjlim_m \mathrm{Sel}_{\mathfrak{p}^m}(B/K_n)\big)^\vee_{\mathbb{Q}_p}$$

are finitely generated $\Lambda_{\mathbb{Q}_p}$-modules of rank one. Moreover, the element

$$\kappa = (P_n) \in S(B/K_\infty)$$

is not $\Lambda_{\mathbb{Q}_p}$-torsion so that $S(B/K_\infty)/\Lambda_{\mathbb{Q}_p} \cdot \kappa$ is a finitely generated torsion $\Lambda_{\mathbb{Q}_p}$-module.

Conjecture 33 (HPMC). *With the above notations,*

$$\big(\mathrm{Char}\big(S(B/K_\infty)/(\kappa)\big)\big)^2 = \mathrm{Char}\big(X(B/K_\infty)_{\mathrm{tor}}\big).$$

The control theorem gives

$$\#\big(S(B/K_\infty)/(\kappa)\big)_\Gamma < \infty \Rightarrow 0 \neq P_0 \in B(K),$$
$$\mathrm{corank}_{\mathcal{O}_\mathfrak{p}} \mathrm{Sel}_{\mathfrak{p}^\infty}(B/K) = 1 \Rightarrow \#\big(X(B/K_\infty)_{\mathrm{tor}}\big)_\Gamma < \infty.$$

The rank one p-converse in the CM case is a consequence of HPMC. In fact, by descent,

$$\#\big(X(B/K_\infty)_{\mathrm{tor}}\big)_\Gamma < \infty \Leftrightarrow \#\big(S(B/K_\infty)/(\kappa)\big)_\Gamma < \infty. \quad (*)$$

Now $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/\mathbb{Q}) = 1$ implies that the left-hand side of $(*)$ holds. On the other hand, under the Gross–Zagier formula, $\mathrm{ord}_{s=1} L(s, A/\mathbb{Q}) = 1$ is a consequence of the right-hand side of $(*)$.

First proof of HPMC. The two variable Rankin–Selberg p-adic L-function $\mathcal{L}_p(f \times \chi)$ (see [21]) associated to (f, χ) has a decomposition in terms of $\mathcal{L}_p(\lambda)$ and $\mathcal{L}_p(\lambda^*/\chi^* \cdot \chi)$, where $\mathcal{L}_p(\lambda)$, $\mathcal{L}_p(\lambda^*/\chi^* \cdot \chi)$ are the Katz p-adic L-functions (see [29]) associated to λ and $\lambda^*/\chi^* \cdot \chi$, respectively. Note that $\mathcal{L}_p(f \times \chi)$ and $\mathcal{L}_p(\lambda)$ vanish along the anticyclotomic line, thus we may consider their derivatives with respect to the cyclotomic variable, i.e.,

$$\big(\mathcal{L}'_p(f \times \chi)\big) = \big(\mathcal{L}'_p(\lambda)\big)\big(\mathcal{L}_p(\lambda^*/\chi^* \cdot \chi)\big).$$

The HPMC is based on Λ-adic Gross–Zagier formula and Rubin's main conjecture.

On the one hand, the Λ-adic Gross–Zagier formula [21] connects Heegner point with $\mathcal{L}'_p(f \times \chi)$ as

$$\big(\mathcal{L}'_p(f \times \chi)\big) = \big(\langle \kappa, \kappa \rangle\big) = \mathrm{Char}\big(S(B/K_\infty)/(\kappa)\big) R(f \times \chi),$$

where $\langle \cdot, \cdot \rangle$ is the Λ-adic height pairing and $R(f \times \chi)$ is the Λ-adic regulator of $f \times \chi$ which is nonzero by the rigidity principle [5]. On the other hand, Rubin's main conjecture [1, 43] implies

$$\big(\mathcal{L}'_p(\lambda)\big) = \mathrm{Char}\big(X(\lambda)_{\mathrm{tor}}\big) R(\lambda), \quad \big(\mathcal{L}_p(\lambda^*/\chi^* \cdot \chi)\big) = \mathrm{Char}\big(X\big(\lambda^*/\chi^* \cdot \chi\big)\big),$$

where $R(\lambda)$ is the Λ-adic regulator which is nonzero [5], $X(\lambda)$ and $X(\lambda^*/\chi^* \cdot \chi)$ are certain anticyclotomic Selmer groups. Then, the HPMC follows from the decomposition

$$\mathrm{Char}\big(X(B/K_\infty)_{\mathrm{tor}}\big) = \mathrm{Char}\big(X(\lambda)_{\mathrm{tor}}\big)\,\mathrm{Char}\big(X\big(\lambda^*/\chi^* \cdot \chi\big)\big)$$

and the comparison of Λ-adic regulators, $R(\lambda) = R(f \times \chi)$. ■

Second proof of HPMC. Via Λ-adic Waldspurger formula and nontriviality of κ, the HPMC is equivalent to the BDP main conjecture [45]. Let $p = v\bar{v}$ where v is determined by ι_p. ■

Proposition 34. *The $\Lambda_{\mathbb{Q}_p}$-modules*

$$S_v(B/K_\infty) := \big(\varprojlim_n \varprojlim_m \mathrm{Sel}_{\mathfrak{p}^m,v}(B/K_n)\big)_{\mathbb{Q}_p},$$
$$X_v(B/K_\infty) := \big(\varinjlim_n \varinjlim_m \mathrm{Sel}_{\mathfrak{p}^m,v}(B/K_n)\big)^\vee_{\mathbb{Q}_p}$$

are finitely generated torsion $\Lambda_{\mathbb{Q}_p}$-modules. Here $\mathrm{Sel}_{\mathfrak{p}^m,v}$ is the $\mathfrak{p}^m$-Selmer group with v-relaxed and $\bar{v}$-strict local Selmer condition [45].

Let $\mathcal{L}_v(B/K_\infty)$ be the anticyclotomic BDP p-adic L-function in [3,38].

Conjecture 35 (BDP Main Conjecture). $\mathrm{Char}(X_v(B/K_\infty)) = (\mathcal{L}_v(B/K_\infty))$.

The $\Lambda_{\mathbb{Q}_p}$-modules $S_v(B/K_\infty)$, $X_v(B/K_\infty)$, $(\mathcal{L}_v(B/K_\infty))$ can be decomposed in terms of Selmer groups and p-adic L-functions of λ, $\lambda^*/\chi^* \cdot \chi$. Then, we approach the BDP main conjecture based on Iwasawa main conjecture for imaginary quadratic fields proved by Rubin [43].

The second approach generalizes to CM elliptic curves over totally real field [6,30].

ACKNOWLEDGMENTS

The author thanks Ashay Burungale, John Coates, Henri Darmon, Yifeng Liu, Christopher Skinner, Xinyi Yuan, Shou-Wu Zhang, and Wei Zhang for their helpful comments, discussions, and constant support.

FUNDING

This work was partially supported by NSFC grant #11688101.

REFERENCES

[1] A. Agboola and B. Howard, Anticyclotomic Iwasawa theory of CM elliptic curves. *Ann. Inst. Fourier (Grenoble)* **56** (2006), no. 4, 1001–1048.

[2] R. Alter, T. B. Curtz, and K. K. Kubota, Remarks and results on congruent numbers. In *Proceedings of the Third Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, FL, 1972)*, pp. 27–35, Florida Atlantic Univ., Boca Raton, FL, 1972.

[3] M. Bertolini, H. Darmon, and K. Prasanna, Generalized Heegner cycles and p-adic Rankin L-series. With an appendix by Brian Conrad. *Duke Math. J.* **162** (2013), no. 6, 1033–1148.

[4] 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. *Camb. J. Math.* **3** (2015), 275–321.

[5] A. Burungale, On the μ-invariant of the cyclotomic derivative of a Katz p-adic L-function. *J. Inst. Math. Jussieu* **14** (2015), no. 1, 131–148.

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

[7] A. Burungale, H. Hida, and Y. Tian, Horizontal variation of Tate–Shafarevich groups. 2017, arXiv:1712.02148.

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

[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, The Birch and Swinnerton-Dyer conjecture: a brief survey. (English summary) Nine mathematical challenges, *Proc. Sympos. Pure Math.* **104** (2021), 11–29.

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

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

[13] A. Burungale and Y. Tian, Horizontal non-vanishing of Heegner points and toric periods. *Adv. Math.* **362** (2020), 106938, 35 pp.

[14] A. Burungale and Y. Tian, The even parity Goldfeld conjecture: congruent number elliptic curves. *J. Number Theory* **230** (2022), 161–195.

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

[16] L. Cai, J. Shu, and Y. Tian, Cube sum problem and an explicit Gross–Zagier formula. *Amer. J. Math.* **139** (2017), no. 3, 785–816.

[17] F. Castella and W. Xin, Perrin-Riou's main conjecture for elliptic curves at supersingular primes. arXiv:1607.02019.

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

[19] J. E. Cremona, *Algorithms for modular elliptic curves*. 2nd edn. Cambridge University Press, Cambridge, 1997, vi+376 pp. ISBN: 0-521-59820-6.

[20] L. E. Dickson, *History of the theory of numbers, vol. II: diophantine analysis*. Chelsea Publishing Co., New York, 1966, xxv+803 pp.

[21] D. Disegni, The p-adic Gross–Zagier formula on Shimura curves. *Compos. Math.* **153** (2017), no. 10, 1987–2074.

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

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

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

[25] Y. Hayashi, The Rankin's L-function and Heegner points for general discriminants. *Proc. Japan Acad. Ser. A Math. Sci.* **71** (1995), no. 2, 30–32.

[26] W. He, Y. Tian, and W. Xiong, Explicit theta lifting and quadratic twist L-values. Preprint, 2021.

[27] D. R. Heath-Brown, The size of Selmer groups for congruent number problem, II. *Invent. Math.* **118** (1994), no. 2, 331–370.

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

[29] H. Hida and J. Tilouine, Anti-cyclotomic Katz p-adic L-functions and congruence modules. *Ann. Sci. Éc. Norm. Supér. (4)* **26** (1993), no. 2, 189–259.

[30] M. L. Hsieh, Eisenstein congruence on unitary groups and Iwasawa main conjectures for CM fields. *J. Amer. Math. Soc.* **27** (2014), no. 3, 753–862.

[31] D. Jetchev, C. Skinner, and X. Wan, The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one. *Camb. J. Math.* **5** (2017), no. 3, 369–434.

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

[33] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Cohomologies p-adiques et applications arithmétiques. III. *Astérisque* **295** (2004), 117–290.

[34] N. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*. Amer. Math. Soc. Colloq. Publ. 45, American Mathematical Society, Providence, RI, 1999, xii+419 pp.

[35] S. Kobayashi, The p-adic Gross–Zagier formula for elliptic curves at supersingular primes. *Invent. Math.* **191** (2013), no. 3, 527–629.

[36] V. Kolyvagin, Euler systems. In *The Grothendieck Festschrift, Vol. II*, pp. 435–483, Progr. Math. 87, Birkhäuser Boston, Boston, MA, 1990.

[37] Y. X. Li, Y. Liu, and Y. Tian, On The Birch and Swinnerton-Dyer Conjecture for CM Elliptic Curves over $\mathbb{Q}$. arXiv:1605.01481.

[38] Y. F. Liu, S. W. Zhang, and W. Zhang, A p-adic Waldspurger formula. *Duke Math. J.* **167** (2018), no. 4, 743–833.

[39] Y. Manin, Cyclotomic fields and modular curves. *Uspekhi Mat. Nauk* **26** (1971), no. 6(162), 7–71 (Russian).

[40] P. Monsky, Mock Heegner points and congruent numbers. *Math. Z.* **204** (1990), no. 1, 45–67.

[41] J. Pan, *The p-adic BSD conjecture for elliptic curves over $\mathbb{Q}$ at potentially supersingular primes*. Ph.D. Thesis, 2017 (in Chinese).

[42] B. Perrin-Riou, Points de Heegner et dérivées de fonctions L p-adiques. *Invent. Math.* **89** (1987), no. 3, 455–510.

[43] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.* **103** (1991), no. 1, 25–68.

[44] K. Rubin, p-adic variants of the Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, pp. 71–80, Contemp. Math. 165, Amer. Math. Soc., Providence, RI, 1994.

[45] C. Skinner, A converse to a theorem of Gross, Zagier and Kolyvagin. *Ann. of Math. (2)* **191** (2020), no. 2, 329–354.

[46] C. Skinner and E. Urban, The Iwasawa main conjectures for GL_2. *Invent. Math.* **195** (2014), no. 1, 1–277.

[47] A. Smith, The congruent numbers have positive natural density. 2016, arXiv:1603.08479.

[48] A. Smith, 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. 2017, arXiv:1702.02325.

[49] P. Swinnerton-Dyer, The effect of twisting on 2-Selmer groups. *Math. Proc. Cambridge Philos. Soc.* **145** (2008), 513–526.

[50] Y. Tian, Congruent numbers and Heegner points. *Camb. J. Math.* **2** (2014), 117–161.

[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** (1983), no. 2, 323–334.

[53] M. Watkins, Some remarks on Heegner point computations. In *Explicit methods in number theory*, pp. 81–97, Panor. Synthèses 36, Soc. Math. France, Paris, 2012.

[54] A. Wiles, Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)* **141** (1995), no. 3, 443–551.

[55] X. Yuan, S.-W. Zhang, and W. Zhang, The Gross-Zagier formula on Shimura curves. *Ann. of Math. Stud.* **184** (2013), viii+272 pages.

[56] W. Zhang, Selmer groups and the indivisibility of Heegner points. *Camb. J. Math.* **2** (2014), no. 2, 191–253.

YE TIAN

Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China, ytian@math.ac.cn