RECENT DEVELOPMENTS ON QUADRATIC TWISTS OF ELLIPTIC CURVES

CHAO LI

Abstract. We begin with a brief history of the congruent number problem, one of the oldest unsolved problems in number theory, to motivate the study of quadratic twists of elliptic curves. Then we survey some recent results on the arithmetic of quadratic twists of elliptic curves, including Goldfeld's conjecture and the full Birch and Swinnerton-Dyer conjecture.

1. An old mystery

In an anonymous Arab manuscript in the year 972, one finds one of the oldest unsolved problems in number theory:

Question 1.1. Given an integer n, does there exist a rational number x such that the 3-term arithmetic progression

$$x - n, x, x + n$$

are all rational squares?

If so, such an integer n is called a *congruent number*. The term originates from the Latin word *congruous*, meaning in agreement or harmony. The problem itself is almost certainly much older, with some authors having traced examples in Babylon and India back to around 800 BC. We refer to Dickson [Dic66, Chap. XVI] for a detailed account of the history of congruent numbers and refer to S. Zhang [Zha13] for a nice recent survey on the congruent number problem.

Example 1.2. The number 24 is congruent by taking $x = 25$:

$$1 = 1^2, \quad 25 = 5^2, \quad 49 = 7^2.$$

By dividing $4 = 2^2$, we know that 6 is also congruent.

The ancient question of determining congruent numbers may seem a bit random at first glance. For example, one may wonder why not ask various analogous questions:

- can one determine all 4-term arithmetic progression consisting of squares?
- can one determine all 3-term arithmetic progression consisting of cubes (or more generally n-th powers for $n \geq 3$)?

For the first question, Euler already proved that there is no such 4-term arithmetic progression except the trivial ones. The second question is equivalent to the Fermat-type equation $x^n + y^n = 2z^n$, and it was shown by Darmon–Merel [DM97] in 1997 that there are only trivial solutions as well. So the congruent number problem is not at all random and the developing a criterion for congruent

Date: September 14, 2018.

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

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

number is indeed an interesting quest. In his famous *Liber Quadratorum* (the Book of Squares), Fibonacci proved the following theorem.

Theorem 1.3 (Fibonacci, around 1220)**.** $5, 6, 7$ *are congruent.*

In fact, the arithmetic progression

$$31^2, 41^2, 49^2, \quad \text{resp.} \quad 113^2, 337^2, 463^2$$

have common difference $12^2 \cdot 5$ and $120^2 \cdot 7$ respectively, hence $n = 5, 7$ are congruent. The case of $n = 5, 6$ were known to the Arabs, and Fibonacci either rediscovered them or learnt them from Arab sources.

The congruent number problem also has an interesting connection to geometry.

Proposition 1.4. *n is congruent if and only if n is the area of a right-angled triangle with rational sides (a, b, c).*

Proof. Consider the bijection $n \mapsto (a, b, c)$ given by

$$a = \sqrt{x+n} - \sqrt{x-n}, \quad b = \sqrt{x+n} + \sqrt{x-n}, \quad c = 2\sqrt{x}.$$

Notice $a^2 + b^2 = c^2$ and the area is indeed given by $ab/2 = ((x+n) - (x-n))/2 = n$. □

This connection to geometry dates back to Diophantus' *Arithmetica* in the 3rd century. Right-angled triangle with rational sides was also stated as the principal object of the theory of rational right triangles in another Arab manuscript in the 10th century.

Fibonacci conjectured that 1 is not congruent, but he was not able to prove it (actually, he gave an incorrect proof of it). Later Fermat rediscovered the problem (in the equivalent geometric form) when reading the appendix of his copy of *Arithmetica* (written by the French translator Bachet). He proved the following theorem using his famous method of infinite descent (creating a smaller solution from a given one which leads to contradiction since there cannot be an infinite sequence of descending positive integers) — the same method he used to show that $x^n + y^n = z^n$ has no nonzero integer solutions when $n = 4$ and which led him to believe that the same statement is true for any integer $n \geq 3$.

Theorem 1.5 (Fermat, around 1640)**.** $1, 2, 3$ *are not congruent.*

Fermat's proof that 1 is not congruent survived in his copy of *Arithmetica*. As Weil remarked ([Wei84, p. 77]), "Fortunately, just for once, he had found room for this mystery in the margin of the very last proposition of Diophantus".

2. Connection with elliptic curves

As we have seen, it took several hundred years to classify all congruent numbers < 10. It would be desirable to find a more systematic criterion. This is where elliptic curves comes into the picture.

Proposition 2.1. *n is congruent if and only if the equation $ny^2 = x^3 - x$ has a rational solution with $y \neq 0$.*

Proof. Let (a, b, c) be the associated Pythagorean triple. Then the association $(a, b, c) \mapsto (x, y)$ given by

$$x = b/(c-a), y = 2/(c-a),$$

is a bijection with inverse

$$a = \frac{x^2-1}{y}, b = \frac{2x}{y}, c = \frac{x^2+1}{y}. \quad \square$$

The equation $ny^2 = x^3 - x$ under the change of variables $y \mapsto n^2 y$ and $x \mapsto nx$ becomes $y^2 = x^3 - n^2 x$, which is an example of an elliptic curve in the Weierstrass form.

Definition 2.2. An *elliptic curve* over $\mathbb{Q}$ is a smooth plane cubic curve defined by a Weierstrass equation

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q}.$$

There is a unique elliptic curve $\mathbb{Q}$ that becomes isomorphic to E over the quadratic field $\mathbb{Q}(\sqrt{d})$ (but not over $\mathbb{Q}$), given by its d-th *quadratic twist* $E^{(d)}$ with the Weierstrass equation

$$E^{(d)} : y^2 = x^3 + Ad^2 x + Bd^3.$$

In particular, the simple family $\{y^2 = x^3 - n^2 x\}$ is an example of *quadratic twists family* of elliptic curves.

One of the advantage of working with an elliptic curve is that we can exploit its geometry.

Example 2.3. Consider the elliptic curve

$$E : y^2 = x^3 - 36x.$$

The solution corresponding to the Pythagorean triple $(3, 4, 5)$ is the rational point

$$(x, y) = (6 \cdot 2, 36 \cdot 1) = (12, 36)$$

on E. The tangent line to this point is $y = 11/2 \cdot x - 30$, which intersects the elliptic curve at another rational point

$$(x, y) = (25/4, 35/8).$$

One can repeat this tangent line process to obtain another rational point

$$(x, y) = (1442401/19600, 1726556399/2744000),$$

and so on. In this way one starts from the point $(12, 36)$ to generate infinitely many rational points (with more and more complicated coordinates!) Similarly, if one starts with two rational points, then the secant line through them will also intersect the elliptic curve at a third rational point (this is a distinct property of cubic equations). In fact this tangent-secant process provides an abelian group structure on the elliptic curve E and its rational points $E(\mathbb{Q})$. In this example we have

$$E(\mathbb{Q}) \cong \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2.$$

Though in general the group of rational points $E(\mathbb{Q})$ can be infinite, the Mordell(–Weil) theorem asserts that it cannot be too enormous.

Theorem 2.4 (Mordell, 1928)**.** *The abelian group $E(\mathbb{Q})$ is finitely generated.*

Definition 2.5. The rank of $E(\mathbb{Q})$ (i.e., the number of copies of $\mathbb{Z}$ in $E(\mathbb{Q})$) is known as the *algebraic rank* of E, denoted by $r_{\text{alg}}(E)$. Notice that $E(\mathbb{Q})$ is finite (resp. infinite) when $r_{\text{alg}}(E) = 0$ (resp. > 0).

It is a fact (not obvious, but also not hard) that the only rational points of $E^{(n)} : y^2 = x^3 - n^2 x$ of finite order must have $y = 0$ ([Sil94, Prop. 6.1]). So n is congruent if and only if $r_{\text{alg}}(E^{(n)}) > 0$, and the congruent number problem reduces to:

Question 2.6. Determine all n such that $r_{\mathrm{alg}}(E^{(n)} : y^2 = x^3 - n^2 x) > 0$.

3. Understanding the rank: the BSD conjecture

The bad news is that we still know very little about r_{alg}, and there is no algorithm that provably determines r_{alg} for all elliptic curves. Miraculously, the mysterious algebraic rank should be related to the analytic properties of its L-function $L(E, s)$. Analogous to the Riemann zeta function

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1},$$

one gathers the local information of E at each prime number p and define

$$L(E, s) := \sum_{n \geq 1} \frac{a_n}{n^s} = \prod_p L_p(E, s).$$

Here

$$L_p(E, s) = \begin{cases} (1 - a_p \cdot p^{-s} + p \cdot p^{-2s})^{-1}, & p \text{ good}, \\ (1 \pm p^{-s})^{-1}, & p \text{ multiplicative}, \\ 1, & p \text{ additive}, \end{cases}$$

and $a_p = p + 1 - |E(\mathbb{F}_p)|$. When evaluating its value at $s = 1$, the local factor at a good prime p gives

$$(1 - a_p p^{-1} + p \cdot p^{-2})^{-1} = \frac{p}{p + 1 - a_p} = \frac{p}{|E(\mathbb{F}_p)|}.$$

Notice that each point in $E(\mathbb{Q})$ reduces mod p and gives a point in $E(\mathbb{F}_p)$. So intuitively, when $E(\mathbb{Q})$ has high rank, each local factor tends to be small, thus the larger $r = r_{\mathrm{alg}}(E)$ is, the "smaller" $L(E, 1)$ is. Birch and Swinnerton-Dyer did numerical experiments for the congruent number curves and suggested the heuristic

$$\prod_{p < X} \frac{|E(\mathbb{F}_p)|}{p} \sim c_E \cdot (\log X)^r,$$

for some positive constant c_E depending on E.

The value of $L(E, s)$ at $s = 1$ does not literally make sense since the infinite product only converges when $\Re s > 3/2$ (due to Hasse's bound $|a_p| \leq 2\sqrt{p}$). Nevertheless, thanks to the modularity theorem of Wiles, Taylor, Breuil, Conrad and Diamond, we now know that $L(E, s)$ can be extended to a holomorphic function on the entire complex plane, so one can indeed make sense of the order of vanishing of $L(E, s)$ as a measurement of how "small" $L(E, 1)$ is.

Definition 3.1. We define $\mathrm{ord}_{s=1} L(E, s)$ to be the *analytic rank* of E, denoted by $r_{\mathrm{an}}(E)$.

The famous Birch and Swinnerton-Dyer (BSD) conjecture asserts that the algebraic rank and the analytic rank, though defined in seemingly unrelated manners, should be the same:

Conjecture 3.2 (BSD)**.** $r_{\mathrm{alg}}(E) = r_{\mathrm{an}}(E)$.

By the modularity theorem, we also know that $L(E, s)$ satisfies a functional equation of the type

$$L(E, s) \longleftrightarrow \varepsilon(E) \cdot L(E, 2 - s),$$

where $\varepsilon(E) \in \{\pm 1\}$ is the *root number* of E. More precisely, let

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

be the complete L-function of E, where N is the conductor of E. Then

$$\Lambda(E, s) = \varepsilon(E) \cdot \Lambda(E, 2 - s).$$

In particular, $r_{\mathrm{an}}(E)$ is odd if and only if $\varepsilon(E) = -1$. The root number $\varepsilon(E)$ are relatively easy to compute. For example, it is an amusing exercise involving Gauss sums ([Kob93, p. 84]) to find the following closed formulas for congruent number curves,

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

The deep BSD conjecture allows us to exploit the tiny bit of knowledge (the sign $\varepsilon(E^{(n)})$) to make the following very concrete prediction about congruent numbers, which in particular gives a conceptual explanation as to why 5, 6, and 7 are congruent numbers (Theorem 1.3).

Proposition 3.3. *BSD $\Rightarrow$ any square-free $n \equiv 5, 6, 7 \pmod 8$ is congruent.*

4. Goldfeld's conjecture

The BSD conjecture is still widely open in general. The current best results is the following theorem.

Theorem 4.1 (Gross–Zagier[GZ86], Kolyvagin [Kol88])**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then*

$$r_{\mathrm{an}}(E) = 0 \Rightarrow r_{\mathrm{alg}}(E) = 0, \quad r_{\mathrm{an}}(E) = 1 \Rightarrow r_{\mathrm{alg}}(E) = 1.$$

In other words, the BSD conjecture holds whenever $r_{\mathrm{an}}(E) \leq 1$. We emphasize that even in these low rank cases, we still do not know how to prove the converse implications

$$r_{\mathrm{alg}}(E) = 0 \overset{?}{\Rightarrow} r_{\mathrm{an}}(E) = 0, \quad r_{\mathrm{alg}}(E) = 1 \overset{?}{\Rightarrow} r_{\mathrm{an}}(E) = 1.$$

So our current knowledge about the BSD conjecture is a bit asymmetric and one may think that r_{an} is a slightly stronger invariant than r_{alg} for the moment. Motivated by the congruent number problem, we ask the following natural question:

Question 4.2. Given an elliptic curve E over $\mathbb{Q}$, how does $r_{\mathrm{an}}(E^{(d)})$ vary when d varies?

The celebrated conjecture of Goldfeld asserts that $E^{(d)}$ tends to have the minimal rank ($= 0, 1$) compatible with its root number $\varepsilon(E^{(d)}) \in \{\pm 1\}$. It is easy to see that the root number is $+1$ (resp. -1) for 50% fundamental discriminant d's. So in the quadratic twists family $\{E^{(d)}\}$, r_{an} should be 0 (resp. 1) for 50% of d's. Although $r_{\mathrm{an}} \geq 2$ occurs infinitely often, its occurrence should be sparse and accounts for only 0% of d's. Namely,

Conjecture 4.3 (Goldfeld, [Gol79])**.** *In the quadratic twists family $\{E^{(d)}\}$, we have*

$$r_{\mathrm{an}}(E^{(d)}) \begin{cases} = 0, & 50\%\ d\text{'s}, \\ = 1, & 50\%\ d\text{'s}, \\ \geq 2, & 0\%\ d\text{'s}. \end{cases}$$

More precisely, let

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

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

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

Here d runs over all fundamental discriminants.

Remark 4.4. Heuristics developed by various authors predict that

$$N_{\geq 2}(E,X) \stackrel{?}{=} X^{3/4+o(1)},$$

see Park–Poonen–Voight–Wood [PPVM16, §3.3] for a summary. The expected asymptotic for $r \geq 3$ is less clear, and there seem to be contradictory predictions in the literature (see [PPVM16, §3.4]). It is known [ST95, Theorem 3] that

$$N_{\geq 2}(E,X) \gg X^{1/7}/\log^2 X,$$

if $j(E) \neq 0, 1728$. We refer to Silverberg [Sil07] for a nice survey on results for $N_r(E,X)$ when $r \geq 2$.

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

Conjecture 4.5 (Weak Goldfeld)**.** *For $r \in \{0,1\}$, $N_r(E,X) \gg X$.*

Remark 4.6. Katz–Sarnak [KS99] conjectured the analogue of GC for the 2-parameter family $\{E_{A,B} : y^2 = x^3 + Ax + B\}$ of all elliptic curves over $\mathbb{Q}$. The weak version in this case is now known due to the recent work of Bhargava–Skinner–W. Zhang [BSZ14]. However, their method does not directly apply to quadratic twists families.

Our knowledge of the weak Goldfeld conjecture (WGC for short) is in better shape. Heath-Brown ([HB04, Thm. 4]) proved the implication

$$\text{GRH} \Rightarrow \text{WGC}.$$

More precisely, one assumes GRH (Grand Riemann Hypothesis) for the L-functions $L(E^{(d)}, s)$ for this implication. The recent breakthrough of Smith [Smi17] establishes the implication

$$\text{BSD} \Rightarrow \text{GC for the congruent number curve,}$$

and more generally for elliptic curves with full rational 2-torsion and without rational cyclic subgroup of order 4. In particular, the result of Smith has the remarkable consequence (compare Theorem 1.5 and Prop. 3.3) that

$$\text{BSD} \Rightarrow 100\% \text{ of square-free integers } n \equiv 1, 2, 3 \pmod 8 \text{ are not congruent.}$$

5. Unconditional results on Goldfeld's conjecture

As GRH and BSD are widely believed to be true, the works mentioned provide strong evidence towards GC. However, it is still desirable to prove results towards GC without assuming these deep conjectures. We now describe some recent unconditional results in two directions: to establish WGC for some special examples of elliptic curves, and to establish good lower bounds for $N_r(E,X)$ ($r \in \{0,1\}$) for more general elliptic curves.

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

Theorem 5.1 (Kriz–L.[KL16]). *WGC is true for any E with a rational 3-isogeny.*

Example 5.2. We also have an explicit lower bound for the proportion. For example, when $E = X_0(19)$, our lower bound is $19/160 = 11.875\%$ of $d < 0$ for $r = 0$ and $19/160 = 11.875\%$ of $d > 0$ for $r = 1$ (which is slightly better than the previous ones $19/240 = 7.92\%$).

Theorem 5.1 gives so far the most general results for WGC (see [KL16, §1.7] for a comparison with previous methods). There are two more known examples for which WGC are valid and are not covered by Theorem 5.1: the congruent number curves $\{y^2 = x^3 - d^2x\}$ and the sextic twists family $\{y^2 = x^3 + d\}$ of j-invariant 0 curves.

Theorem 5.3 (Tian–Yuan–S. Zhang [TYZ14], Smith [Smi16]). *WGC holds for the congruent number curves family $\{y^2 = x^3 - d^2x\}$. In fact, the proportion is at least 41.9% for $r = 0$ and at least 55.9% for $r = 1$.*

Theorem 5.4 (Kriz–L.[KL16]). *WGC holds for the sextic twists family $\{y^2 = x^3 + d\}$. In fact, the proportion is at least $1/6$ for $r = 0$ and at least $1/6$ for $r = 1$.*

Remark 5.5. In a recent work, Bhargava–Elkies–Shnidman [BES16] prove the analogue of Theorem 5.4 for 3-Selmer ranks 0,1, by determining the exact average size of 3-isogeny Selmer groups. The same method also works for quadratic twists family of any elliptic curve with a 3-isogeny ([BKLS]). We remark that their method however does not have the same implication for analytic rank $r = 0, 1$ (or algebraic rank 1), since the p-converse to the theorem of Gross–Zagier and Kolyvagin is not known for p an additive and Eisenstein prime.

Remark 5.6. Browning [Bro17] has used Theorem 5.4 as a key input to show that a positive proportion of cubic surfaces of the form $f(x, y) = g(w, z)$ has a $\mathbb{Q}$-point, where f, g are binary cubic forms.

5.2. **General E.** When $r = 0$, the best result towards GC was due to Ono-Skinner [OS98]: they showed that for any elliptic curve $E/\mathbb{Q}$,

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

When $r = 1$, the best general result was due to Perelli-Pomykala [PP97]: they showed in general that for any $\varepsilon > 0$,

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

We improve both bounds for a wide class of elliptic curves satisfying some technical assumption on Heegner points (see §6.3).

Theorem 5.7 (Kriz–L.[KL16]). *Assume that $E(\mathbb{Q})[2] = 0$. Assume that there exists a Heegner point $y_K \in E(K)$ for some imaginary quadratic field K such that*

$$\textit{2 splits in } K \textit{ and } \frac{|\tilde{E}^{\mathrm{ns}}(\mathbb{F}_2)|}{2} \cdot \log_2(y_K) \not\equiv 0 \pmod 2.$$

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

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

Remark 5.8. Notice the improvement in $r = 0$ is on the exponent of $\log X$, and the improvement in $r = 1$ is more essential. We remark that in contrast to previous methods, the rank 0 and 1 twists in Theorem 5.7 are all explicitly constructed, in the spirit of Mazur–Rubin's work [MR10] on 2-Selmer ranks in quadratic twists families. For these explicit twists, we have also proved the 2-part of the refined Birch and Swinnerton–Dyer formula (see §7).

Remark 5.9. There are also similar but slightly weaker results for certain elliptic curves with $E(\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z}$ ([KL17]). For elliptic curves E appearing in Theorem 5.7 and [KL17], one obtain as a consequence that Silverman's conjecture holds for E, namely there exist infinitely many primes p such that $E^{(\pm p)}$ has rank 0 (resp. rank > 0).

Remark 5.10. For certain elliptic curves with $E(\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z}$, the work of Coates–Y. Li–Tian–Zhai [CLTZ15] also improves the current bounds, using a generalization of the classical method of Heegner and Birch for prime twists.

6. Congruences between Heegner points

6.1. **Congruences between L-values.** The starting point of the proof of Theorem 5.7 is the simple observation that quadratic twisting does not change the mod 2 Galois representations

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

More generally, suppose we have two elliptic curves E, E' such that

$$E[p] \cong E'[p],$$

as Galois representations, or in terms of the associated modular forms, we have a congruence

$$f_E \equiv f_{E'} \pmod{p}.$$

One expects that such a congruence induces a certain "congruence" between special L-values

$$L(E,1) \overset{?}{\equiv} L(E',1) \pmod{p}$$

Making sense of this congruence is more subtle as both sides are transcendental numbers. So one needs to replace the L-value $L(E,1)$ by its suitable algebraic part $L^{\mathrm{alg}}(E,1)$. Notice that when E and E' have root number -1, both sides of the congruence are 0 and thus it is better to consider "congruence" between the first derivatives

$$L'(E,1) \overset{?}{\equiv} L'(E',1) \pmod{p}.$$

Again making precise sense of this congruence is a bit subtle. General theory of p-adic L-functions provides a framework to systematically treat these types of congruences. Let us not go into this general theory but take a more concrete point view, namely, we will replace $L(E,1)$ or $L'(E,1)$ by its algebraic or p-adic incarnation provided by Heegner points.

6.2. **Algebraic incarnation.** Let $K = \mathbb{Q}(\sqrt{d_K})$ be an imaginary quadratic field. Assume K satisfies the *Heegner hypothesis for* E: any prime dividing the conductor $N = N(E)$ of E is split in K (this forces E/K to have root number -1). The theory of complex multiplication then provides *Heegner points* $y_K \in E(K)$ (defined up to torsion and sign, see [Gro84]). The Gross-Zagier formula relates $L'(E/K, 1)$ with the Neron-Tate height pairing of the Heegner point y_K,

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

here $(*)$ is an explicit nonzero constant depending on E/K. Since the Neron-Tate height pairing

$$\langle , \rangle_{\mathrm{NT}} : E(K) \times E(K) \to \mathbb{R}$$

is non-degenerate modulo the torsion part $E(K)_{\mathrm{tor}}$. We know that

$$r_{\mathrm{an}}(E/K) = 1 \Leftrightarrow y_K \text{ is of infinite order.} \tag{1}$$

This provides a way to access the analytic rank by studying the Heegner point y_K, which we may think of as an algebraic incarnation of $L(E, 1)$ or $L'(E, 1)$. We refer to W. Zhang [Zha14] for a recent survey on Heegner points.

6.3. **p-adic incarnation.** For the purpose of mod p congruences, it would be better to use a p-adic invariant associated to y_K. Recall that we have a formal logarithm

$$\log_p : \hat{E}(p\mathbb{Z}_p) \to \mathbb{Z}_p, \quad (t = -x/y) \mapsto \int_0^t \omega_E(T).$$

given by integrating the invariant differential $\omega_E(T)$ on the formal group $\hat{E}$. Linearly extending gives a p-adic logarithm,

$$\log_p : E(\mathbb{Q}_p) \to \mathbb{Q}_p,$$

whose kernel consists exactly the torsion points in $E(\mathbb{Q}_p)$. If $\log_p(y_K) \neq 0$, then y_K is of infinite order in $E(K_p)$, and hence y_K is of infinite order in $E(K)$ and by (1) we obtain $r_{\mathrm{an}}(E/K) = 1$. Finally, using

$$r_{\mathrm{an}}(E/K) = r_{\mathrm{an}}(E) + r_{\mathrm{an}}(E^{(d_K)}),$$

we arrive at the following implication that

$$\log_p(y_K) \neq 0 \Rightarrow \{r_{\mathrm{an}}(E), r_{\mathrm{an}}(E^{(d_K)})\} = \{0, 1\}. \tag{2}$$

In this way, we are able to access the analytic rank using the p-adic logarithm $\log_p(y_K)$, which we may think of as the p-adic incarnation of $L(E, 1)$ or $L'(E, 1)$.

6.4. **The main congruence formula.** Coming back to the situation of two elliptic curves E, E' with an isomorphism

$$E[p] \cong E'[p]$$

of Galois representations. Let K be an imaginary quadratic field satisfying the Heegner hypothesis for both E and E'. Then one may expect a mod p congruence

$$\log_p(y_K) \stackrel{?}{\equiv} \log_p(y'_K) \pmod{p}.$$

This identity of course would not be true without further modification: for example if $\log_2(y_K) \neq 0 \pmod 2$, then applying the identity for $E' = E^{(d)}$ and $p = 2$ would imply that $r_{\mathrm{an}}(E^{(d)}) \in \{0, 1\}$ for any d, which is not true (see Remark 4.4). Fortunately, we are able to prove the following main congruence formula.

Theorem 6.1 (Kriz–L.[KL16]). *Let E, E' be two elliptic curves such that*

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

as semisimple $G_{\mathbb{Q}}$-representations. Let M be the product of all primes $\ell | \gcd(N, N')$ such that $a_\ell(E) \equiv a_\ell(E') \pmod{p^m}$. Assume K satisfies Heegner hypothesis for E, E' and let y_K, y'_K be the associated Heegner points. Assume p splits in K. Then we have a congruence

$$\left(\prod_{\ell | pNN', \ell \nmid M} \frac{|\tilde{E}^{\mathrm{ns}}(\mathbb{F}_\ell)|}{\ell} \right) \cdot \log_p(y_K) \equiv \pm \left(\prod_{\ell | pNN', \ell \nmid M} \frac{|\tilde{E'}^{\mathrm{ns}}(\mathbb{F}_\ell)|}{\ell} \right) \cdot \log_p(y'_K) \pmod{p^m}.$$

Remark 6.2. Recall that $\tilde{E}^{\mathrm{ns}}(\mathbb{F}_\ell)$ denotes the number of $\mathbb{F}_\ell$-points of the nonsingular part of the mod ℓ reduction of E, which is $\ell + 1 - a_\ell(E)$ if $\ell \nmid N$, $\ell \pm 1$ if $\ell || N$ and ℓ if $\ell^2 | N$. The factors in the above congruence can be understood as the result of removing the Euler factors of $L(E, 1)$ and $L(E', 1)$ at bad primes.

Remark 6.3. The link between the p-adic logarithm of Heegner points and p-adic L-functions dates back to Rubin [Rub92] in the CM case and was recently established in great generality by Bertolini–Darmon–Prasanna [BDP13] and Liu–S. Zhang–W. Zhang [LZZ15].

Remark 6.4. The congruence formula in Theorem 6.1 can be viewed as a congruence between the special values (at the trivial character) of the BDP p-adic L-functions for two congruent modular forms of weight 2. Recently, under the Heegner hypothesis, Hatley–Lei [HL17] study the variation of anticyclotomic algebraic μ-invariants and λ-invariants for Selmer groups under congruences, which can be viewed as an algebraic analogue of Theorem 6.1. If one can extend Theorem 6.1 to more general anticyclotomic characters, then one can hope to use [HL17] and the method of Greenberg–Vatsal [GV00] to propagate the validity of the anticyclotomic Iwasawa main conjecture under congruences.

Notice that Theorem 6.1 allows us to propagate the non-vanishing (mod p) of the p-adic logarithm of Heegner points through congruences, as long as the extra Euler factors are p-adic units. We apply to the case $p = 2$ and $E' = E^{(d)}$ and construct an explicit set of d's such that the p-adic logarithm of $P^{(d)} \in E^{(d)}(K)$ is nonzero and counting the size of such set of d's allows us to prove Theorem 5.7. We illustrate this construction by an example.

Example 6.5. Consider the curve $37a1$ in Cremona's table,

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

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

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

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

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

generates $E(\mathbb{Q}) = E(K) \cong \mathbb{Z}$. The formal logarithm associated to ω_E is

$$\log_2(t) = t + 1/2 \cdot t^4 - 2/5 \cdot t^5 + 6/7 \cdot t^7 - 3/2 \cdot t^8 + 2/3 \cdot t^9 + \cdots$$

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

$$\log_2 y_K = \log_2 5y_K = 2 + 2^5 + 2^6 + 2^8 + 2^9 + \cdots \in 2\mathbb{Z}_2^\times.$$

Hence

$$\frac{|\tilde{E}(\mathbb{F}_2)| \cdot \log_2 y_K}{2} \in \mathbb{Z}_2^\times.$$

So the assumptions in Theorem 5.7 are satisfied. Consider the set $\mathcal{N}$ consisting of square-free products of the signed primes

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

For any $d \in \mathcal{N}$, we have the (rank part of) BSD conjecture is true for $E^{(d)}$ and $E^{(-7d)}$. and

$$\begin{cases} r_{\mathrm{an}}(E^{(d)}) = 1, & r_{\mathrm{an}}(E^{(-7d)}) = 0, \quad d > 0, \\ r_{\mathrm{an}}(E^{(d)}) = 0, & r_{\mathrm{an}}(E^{(-7d)}) = 1, \quad d < 0. \end{cases}$$

Since $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$, it follows that

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

6.5. **Heegner points at Eisenstein primes.** The proof of WGC in Theorems 5.1 and 5.4 also replies on a congruence formula involving the p-adic logarithm of Heegner points. Now suppose p is an *Eisenstein prime* for E (i.e., $E[p]$ is a reducible $G_{\mathbb{Q}}$-representation, or equivalently, E admits a rational p-isogeny). In this case, we have

$$\text{the modular form } f_E \equiv \text{an Eisenstein series} \pmod{p},$$

and one may expect a congruence

$$\log_p(y_K) \stackrel{?}{\equiv} \text{a Katz } p\text{-adic } L\text{-value} \pmod{p} \tag{3}$$

We prove a precise congruence of this kind in [KL16]. Next,

- By Gross' factorization (since the relevant character is a restriction from $\mathbb{Q}$ to K), the Katz p-adic L-value factorizes as a product of two Kubota–Leopoldt p-adic L-values.
- The Kubota–Leopoldt p-adic L-values evaluates to the Bernoulli numbers, which are related to relative p-class number of degree $p-1$ abelian CM number fields by the class number formula.

The upshot is that the Eisenstein series side of the congruence can be evaluated explicitly, and we arrive at a congruence formula of the type

$$\log_p(y_K) \equiv \text{ product of two relative } p\text{-class numbers} \pmod{p} \tag{4}$$

(up to certain Euler factors that can be made precise, but we ignore them here).

Remark 6.6. When $E/\mathbb{Q}$ has CM by $\mathbb{Q}(\sqrt{-p})$ (of class number 1), Rubin [Rub83] proved a mod p congruence formula between the algebraic part of $L(E, 1)$ and certain Bernoulli numbers. Notice that E admits a p-isogeny (multiplication by $\sqrt{-p}$), our congruence formula (4) specializes to provide a mod p congruence between the p-adic logarithm of the Heegner point on E and certain Bernoulli numbers, which can be viewed as a generalization of Rubin's formula from the rank 0 case to the *rank 1* case.

Remark 6.7. Analogous to Remark 6.4, the congruence formula (3) can be viewed as an congruence between the BDP p-adic L-function and the anticyclotomic Katz p-adic L-function. One can hope to use the known cases of the Iwasawa main conjecture for Katz p-adic L-functions to prove new cases of the anticyclotomic main conjecture for elliptic curves when $E[p]$ is reducible.

When $p = 3$, the relative p-class numbers becomes the 3-class numbers of two quadratic fields. Our final ingredient to finish the proof of WGC in Theorems 5.1 and 5.4 is Davenport–Heilbronn's theorem ([DH71]) (enhanced by Nakagawa–Horie [NH88] with congruence conditions), which allows one to find a positive proportion of twists such that both 3-class numbers in question are trivial.

We illustrate this explicit criterion by the example of sextic twists family in Theorem 5.4.

Example 6.8. Let $E : y^2 = x^3 - 432$ (isomorphic to $x^3 + y^3 = 1$ and $j(E) = 0$). Let

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

be the d-th sextic twist of E. Then E_d admits a 3-isogeny and we have the following explicit criterion for analytic rank one in terms the 3-class numbers (denoted by $h_3(-)$) of quadratic fields. Suppose K satisfies the Heegner hypothesis for $3d$ (all prime factors of $3d$ are split in K). Assume that

(1) d is a fundamental discriminant.
(2) $d \equiv 2, 3, 5, 8 \pmod 9$.
(3) If $d > 0$, $h_3(-3d) = h_3(d_K d) = 1$. If $d < 0$, $h_3(d) = h_3(-3d_K d) = 1$.

Then $r_{\mathrm{an}}(E_d/K) = 1$.

Remark 6.9. More generally, the Cohen–Lenstra heuristic for p-class groups of number fields together with the congruence formula (4) should imply WGC for any elliptic curve with a rational p-isogeny. Unfortunately, very little is known at the moment for the Cohen–Lenstra heuristic when $p \geq 5$.

6.6. **Rubin–Silverberg families and sieves.** Let us end our discussion on congruences between Heegner points with an application to other families of elliptic curves. Since the modular curve $X(N)$ has genus zero when $N = 2, 3, 4, 5$, there are infinitely families of elliptic curves with the same mod $N = 2, 3, 4, 5$ representation. Rubin and Silverberg [RS01], [RS95], [Sil97] computed explicit equations $E_t : y^2 = x^3 + A(t)x + B(t)$ for the universal elliptic curves with constant mod N Galois representation. It is a natural question to understand the rank distribution in these Rubin–Silverberg families $\{E_t\}$. Using Theorem 6.1, we can produce explicit analytic rank 0 or 1 curves E_t by only requiring E_t satisfying certain desired *local* properties.

Let us illustrate this idea by an example. Consider

$$E = 256b1 : y^2 = x^3 - 2x$$

of j-invariant 1728. Then the 1-parameter family

$$E_t : y^2 = x^3 + A(t)x + B(t), \quad A(t) = 2(108t^4 - 36t^2 - 1), B(t) = 16t(108t^4 + 1),$$

has constant mod 3 representation $E_t[3] \cong E[3]$. Let $P(t) = 108t^4 + 36t^2 - 1$. The

$$\Delta(E_t) = -2^9 \cdot P(t)^3 = -\Delta(E) \cdot P(t)^3.$$

We can prove the following theorem:

Theorem 6.10 (Kriz–L.)**.** *Suppose $t \in \mathbb{Z}$ such that for any prime $\ell | P(t)$, we have*
(1) $\ell^4 \nmid P(t)$.

(2) $6B(t) \in (\mathbb{F}_\ell^\times)^2$ *if and only if* $\ell \equiv 2 \pmod 3$.
Then $r_{\mathrm{an}}(E_t) \leq 1$.

Question 6.11. Can one count how many $|t| < X$ satisfying the two assumptions of Theorem 6.10?

Such counting would give a lower bound on the number of analytic rank 0 or 1 curves in the family $\{E_t\}$. This leads to an interesting and nontrivial question in sieve theory. Brun's sieve allows one to obtain an asymptote $\frac{X}{\log^k X}$ for the number of $|t| < X$ such that $P(t)$ has a bounded number of prime factors (where $k > 0$ is related to the dimension of the sieve). However, adding the condition (2) for each prime factor $\ell | P(t)$ seems to be causing difficulty and new ideas are needed.

7. The full BSD conjecture

Besides the rank conjecture $r_{\mathrm{alg}}(E) = r_{\mathrm{an}}(E)$, Birch and Swinnerton-Dyer further conjectured a precise formula

$$\frac{L^{(r)}(E/\mathbb{Q}, 1)}{r!\Omega(E/\mathbb{Q})R(E/\mathbb{Q})} = \frac{\prod_p c_p(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})|}{|E(\mathbb{Q})_{\mathrm{tor}}|^2} \tag{5}$$

for the leading coefficient of the Taylor expansion of $L(E/\mathbb{Q}, s)$ at $s = 1$ (here $r = r_{\mathrm{an}}(E)$) in terms of various important arithmetic invariants of E. This is known as the *full BSD conjecture*, or the *refined BSD formula*. See [Gro11] for detailed definitions of invariants appearing in the formula. Here we mention that the *Shafarevich–Tate group* $Ш(E/\mathbb{Q})$ is defined to be

$$Ш(E/\mathbb{Q}) = \ker(H^1(\mathbb{Q}, E) \to \prod_v H^1(\mathbb{Q}_v, E)),$$

where v runs over all places of $\mathbb{Q}$. It is conjectured to be always finite, which is proved when $r \leq 1$ by Gross–Zagier and Kolyvagin. We remark that there is still no example of an elliptic curve $E/\mathbb{Q}$ with $r \geq 2$ for which we can prove the finiteness of $Ш(E/\mathbb{Q})$.

When $r \leq 1$, both sides of the BSD formula (5) are known to be positive rational numbers. To prove that (5) is indeed an equality, it suffices to prove that it is an equality up to a p-adic unit, for each prime p. This is known as the *p-part of the BSD formula* (BSD(p) for short).

Much progress for BSD(p) for p odd has been made recently (see [KL16, Rem. 1.22] for a summary of results) using deep methods from Iwasawa theory. However, there are real technical difficulties at present in using Iwasawa theory to prove BSD(p) when $p = 2$. As an application of Theorem 6.1, we are able to prove BSD(2) when $r \leq 1$ for many quadratic twists of an elliptic curve in Theorem 5.7. Using different methods based on modular symbols, Zhai [Zha16] and Cai-L.-Zhai [CLZ17] are also able to prove BSD(2) for many quadratic twists of a wide class of elliptic curves, and an analogue of Theorem 5.7 when $r = 0$ for these elliptic curves. Combining BSD(p) for all p's allows one prove the full BSD conjecture for infinitely many quadratic twists of a wide class of elliptic curves, and finally lead to the following theorem (see [Wan14, Theorem 9.3]).

Theorem 7.1. *The full BSD conjecture holds for infinitely many elliptic curves over* $\mathbb{Q}$ *without complex multiplication (and of analytic rank 0).*

Remark 7.2. This theorem is due to the work of many people. We refer to Skinner's Arizona Winter School 2018 notes [Ski] for a nice survey on the Iwasawa theory of elliptic curves (for p odd). Here we content ourselves by listing the authors for proving the corresponding BSD(p) ($r = 0$):

- p odd, good ordinary: Kato, Skinner–Urban,

- p odd, good supersingular: Kobayashi, Wan, Sprung,
- p odd, multiplicative: Skinner,
- p odd, additive: Wan,
- $p = 2$: Kriz–L., Zhai, Cai–L.–Zhai.

Remark 7.3. The analogue of Theorem 7.1 in the CM case was known earlier for $r \leq 1$ (see [KL16, Rem. 1.24] for the references for p odd and Zhao [Zha97] and Tian [Tia14] for $p = 2$).

8. Acknowledgments

I would like to thank the referee for helpful comments. This work is partly done during the ICCM 2017 at Guangzhou and the Pan Asia Number Theory Conference 2018 at IMS, National University of Singapore, and I would like to thank the organizers and IMS for their hospitality.

References

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

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

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

[BKLS] Manjul Bhargava, Zev Klagsbrun, Robert Lemke Oliver, and Ari Shnidman. Selmer groups in families of quadratic twists with a 3-isogeny. in preparation.

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

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

[CLTZ15] John Coates, Yongxiong Li, Ye Tian, and Shuai Zhai. Quadratic twists of elliptic curves. *Proc. Lond. Math. Soc. (3)*, 110(2):357–394, 2015.

[CLZ17] L. Cai, C. Li, and S. Zhai. On the 2-part of the Birch and Swinnerton-Dyer conjecture for quadratic twists of elliptic curves. *ArXiv e-prints*, December 2017.

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

[Dic66] Leonard Eugene Dickson. *History of the theory of numbers. Vol. II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.

[DM97] Henri Darmon and Loï c Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

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

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

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

[GV00] Ralph Greenberg and Vinayak Vatsal. On the Iwasawa invariants of elliptic curves. *Invent. Math.*, 142(1):17–63, 2000.

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

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

[HL17] J. Hatley and A. Lei. Comparing anticyclotomic Selmer groups of positive coranks for congruent modular forms. *ArXiv e-prints*, June 2017.

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

[KL16] D. Kriz and C. Li. Goldfeld's conjecture and cocongruence between Heegner points. *preprint*, 2016.

[KL17] D. Kriz and C. Li. Prime twists of elliptic curves. *ArXiv e-prints, to appear in Math. Res. Lett.*, October 2017.

[Kob93] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[Kol88] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and Ш$(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

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

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

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

[MR10] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and Hilbert's tenth problem. *Invent. Math.*, 181(3):541–575, 2010.

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

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

[PP97] A. Perelli and J. Pomykala. Averages of twisted elliptic L-functions. *Acta Arith.*, 80(2):149–163, 1997.

[PPVM16] J. Park, B. Poonen, J. Voight, and M. Matchett Wood. A heuristic for boundedness of ranks of elliptic curves. *ArXiv e-prints*, February 2016.

[RS95] K. Rubin and A. Silverberg. Families of elliptic curves with constant mod p representations. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 148–161. Int. Press, Cambridge, MA, 1995.

[RS01] K. Rubin and A. Silverberg. Mod 2 representations of elliptic curves. *Proc. Amer. Math. Soc.*, 129(1):53–57, 2001.

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

[Rub92] Karl Rubin. p-adic L-functions and rational points on elliptic curves with complex multiplication. *Invent. Math.*, 107(2):323–350, 1992.

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

[Sil97] Alice Silverberg. Explicit families of elliptic curves with prescribed mod N representations. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 447–461. Springer, New York, 1997.

[Sil07] A. Silverberg. The distribution of ranks in families of quadratic twists of elliptic curves. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 171–176. Cambridge Univ. Press, Cambridge, 2007.

[Ski] C. Skinner. Lectures on the Iwasawa theory of ellptic curves. `http://swc.math.arizona.edu/aws/2018/2018SkinnerNotes.pdf`.

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

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

[ST95] C. L. Stewart and J. Top. On ranks of twists of elliptic curves and power-free values of binary forms. *J. Amer. Math. Soc.*, 8(4):943–973, 1995.

[Tia14] Ye Tian. Congruent numbers and Heegner points. *Camb. J. Math.*, 2(1):117–161, 2014.

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

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

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

[Wan14] X. Wan. Iwasawa Main Conjecture for Supersingular Elliptic Curves. *ArXiv e-prints*, November 2014.

[Wei84] André Weil. *Number theory*. Birkhäuser Boston, Inc., Boston, MA, 1984. An approach through history, From Hammurapi to Legendre.

[Zha97] Chunlai Zhao. A criterion for elliptic curves with lowest 2-power in $L(1)$. *Math. Proc. Cambridge Philos. Soc.*, 121(3):385–400, 1997.

[Zha13] Shou-Wu Zhang. Congruent numbers and Heegner points. *Asia Pac. Math. Newsl.*, 3(2):12–15, 2013.

[Zha14] Wei Zhang. The Birch–Swinnerton-Dyer conjecture and Heegner points: a survey. In *Current developments in mathematics 2013*, pages 169–203. Int. Press, Somerville, MA, 2014.

[Zha16] Shuai Zhai. Non-vanishing theorems for quadratic twists of elliptic curves. *Asian J. Math.*, 20(3):475–502, 2016.

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

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