Congruent Number Problem

by Ye Tian

1. Introduction

A positive integer is called a *congruent number* if it is the area of a right-angled triangle, all of whose sides have lengths in $\mathbb{Q}$. For example, Fermat proved that 1 is not congruent and Fibonacci proved that 5 is congruent because of the existence of the right triangle with sides $\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$. The congruent number problem (see Dickson [10]) is to determine whether a given integer n is congruent and, if so, find all rational right triangles with area n. It can be traced back at least to the 10-th century in Arab manuscripts (Al-Kazin) but it is possibly much older. It turns out to be the oldest unsolved major problem in number theory, and possibly in the whole of mathematics.

We say a right-angled triangle is *rational* if all three lengths are rational, and is *primitive* if all three lengths a, b, c are positive integers and $(a,b,c) = 1$. By a formula of Euclid, for a primitive right-angled triangle, there exist unique positive integers r, s such that its side lengths are given as

$$r^2 - s^2, \quad 2rs, \quad r^2 + s^2.$$

It follows that for any integers $r > s$, $rs(r^2 - s^2)$ is a congruent number. In particular, $(r-1)r(r+1)$ is congruent for any integer $r > 1$.

Proposition 1.1. *A positive integer n is a congruent number if and only if there exist positive integers r, s, t such that $rs(r^2 - s^2) = nt^2$. If so, the rational right-angled triangle with side lengths*

$$\left(\frac{r^2 - s^2}{t}, \frac{2rs}{t}, \frac{r^2 + s^2}{t}\right)$$

has area n.

For example, taking $(r,s) = (5,4)$,

$$5 \cdot 4 \cdot (5+4) \cdot (5-4) = 5 \cdot 6^2,$$

from which we know 5 is a congruent number with a corresponding right-angled triangle

$$\left(\frac{5^2 - 4^2}{6}, \frac{2 \cdot 5 \cdot 4}{6}, \frac{5^2 + 4^2}{6}\right) = \left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right).$$

Taking (r,s) to be

$$(2,1), \quad (16,9), \quad (5^2 \cdot 13, \ 6^2), \quad (8,1), \quad (4,1), \quad (4,3), \quad (50,49), \quad (156^2, 133^2),$$

square-free parts of $rs(r+s)(r-s)$

$$6, \quad 7, \quad 13, \quad 14, \quad 15, \quad 21, \quad 22, \quad 23$$

are then congruent numbers. By the same numerical method, one can show that the following numbers in the beginning of positive integers (not being divisible by 4) are congruent numbers:

$$5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47, \ldots.$$

The sequence of its residue modulo 8 is

$$5, 6, 7, \ 5, \ 6, \ 7, \ 5, \ 6, \ 7, \ 5, \ 6, \ 7, \ 2, \ 5, \ 6, \ 7, \ 1, \ 5, \ 6, \ 7, \ldots.$$

There is a conjecture:

Conjecture 1.2. *Any positive integer congruent to $5, 6, 7$ modulo 8 is a congruent number.*

The following example shows that the verification of a number being congruent is not trivial. It is known by Heegner that any prime number $\equiv 5 \bmod 8$ is congruent, but Zagier found that the "smallest" rational right angled triangle with area $157 \equiv 5 \bmod 8$ has side lengths:

$$a = \frac{411340519227716149383203}{21666555693714761309610},$$

$$b = \frac{6803298487826435051217540}{411340519227716149383203},$$
$$c = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

Let us remark that there are infinitely many square-free congruent numbers in each residue class of $1, 2, 3$ modulo 8. One can easily show this by using the fact that $(r-1)r(r+1)$ is a congruent number and by using Dirichlet's result on prime numbers on arithmetic progressions. In fact, the first congruent numbers congruent to $1, 2, 3$ modulo 8 are $41, 34$, and 219, respectively. To see $41, 34, 219$ are congruent, one may take (r, s) to be

$$(25,16),\ (41,9); \qquad (17,1),\ (25,9); \qquad (73,48),\ (169,73),$$

respectively.

Is 1 congruent? No one could find a rational right angled triangle with area 1. People began to try to prove that there was no such triangle, and many people falsely claimed a proof. For example, in his memoir "Liber Quadratorum" (1225), Fibonacci made the statement that 1 is not congruent but with a false proof, and its proof had to wait for four centuries. We owe to Fermat, in the middle of the 17-th century, a marvellous proof that 1 is not congruent by introducing infinite descent method. Not only did this proof introduce ideas that had a vast development in the 20-th century, but Fermat noted that his proof also showed that there are no integers x, y, z with $xyz \neq 0$ such that

$$x^4 + y^4 = z^4.$$

He subsequently went on to state, without proof, that there are no integers x, y, z with $xyz \neq 0$ such that

$$x^n + y^n = z^n$$

when n is any integer ≥ 3. It is A. Wiles in 1994 who proved this so-called Fermat's Last Theorem.

Theorem 1.3 (Fermat). *1 is not a congruent number.*

Proof. Suppose, on the contrary, that 1 is congruent, therefore there exists a primitive right angled triangle whose area is a square integer. By Euclid's formula, it has side lengths

$$r^2 - s^2, \quad 2rs, \quad r^2 + s^2$$

for some positive integer r, s. Then $r > s > 0$, $2 \nmid r + s$, and $(r, s) = 1$. Since the area $rs(r+s)(r-s)$ is square and the numbers $r, s, r+s, r-s$ are coprime pairwise, we may write

$$r = x^2, \qquad s = y^2, \qquad r + s = u^2, \qquad r - s = v^2,$$

for some positive integers x, y, u, v. Now one can check that

$$\left(\frac{u+v}{2}, \frac{u-v}{2}, x\right)$$

is again a right angled triangle with integral sides and square area. In fact,

$$\left(\frac{u+v}{2}\right)^2 + \left(\frac{u-v}{2}\right)^2 = \frac{u^2+v^2}{2} = x^2,$$
$$\frac{1}{2} \cdot \frac{u+v}{2} \cdot \frac{u-v}{2} = \frac{u^2-v^2}{8} = \frac{y^2}{4}.$$

Note that the hypotenuse of the new triangle is less than the one we started:

$$x = \sqrt{r} < r^2 + s^2.$$

Thus we constructed a new primitive right angled triangle with square area with smaller hypotenuse. Clearly this process can be repeated. But this gives rise to an infinite decreasing sequence of positive integers, a contradiction. $\square$

By a similar argument, one can show that any prime $p \equiv 3 \bmod 8$ is not a congruent number. Also, one can prove the following numbers are non-congruent:

$$1, 2, 3, 9, 10, 11, 17, 18, 19, 25, 26, 27, 33, \quad 35, \quad 42, 43, \ldots$$

Modulo 8, we have the sequence of residues modulo 8 of non-congruent numbers:

$$1, 2, 3, 1, 2, 3, 1, 2, 3, 1, 2, 3, 1, \quad 3, \quad 2, 3, \ldots$$

If $\mathcal{D}$ is an infinite set of positive integers, $\mathcal{D}'$ is a subset of $\mathcal{D}$, if the following limit exists:

$$\lim_{N \to +\infty} \frac{\#\{n \in \mathcal{D}' \mid n < N\}}{\#\{n \in \mathcal{D} \mid n < N\}},$$

then it is called the density of $\mathcal{D}'$ in $\mathcal{D}$. Using this notation, there is a conjecture that

Conjecture 1.4. *The congruent numbers in all positive integers congruent to 1, 2, 3 modulo 8 have density 0.*

Beside conjectures 1.2 and 1.4, it is natural to ask the following question.

Question 1.5. *Is there an algorithm which determines whether or not a given positive integers is congruent in a finite number of steps?*

How to understand these conjectures and question? In fact, many results on congruent numbers lie on the arithmetic of elliptic curves. We have seen that a positive integer n is a congruent number if and only if there exist positive integers $r > s, m$ such that

$$rs(r+s)(r-s) = nm^2.$$

Namely $(r/s, m/s^2)$ is a rational point on the following curve:

$$E^{(n)}: \quad ny^2 = x(x+1)(x-1).$$

The curve $E^{(n)}$ has 3 obvious rational points $(0,0), (\pm 1, 0)$, all of which have y-coordinates 0. In fact, we have

Proposition 1.6. *A positive integer n is a congruent number if and only if the curve $E^{(n)}$ has a rational point (x,y) with $y \neq 0$. Moreover, there is a bijection between the following sets:*

- $\{(a,b,c) \in \mathbb{Q}^3 : a^2+b^2=c^2, n = ab/2\}$
- $\{(x,y) \in \mathbb{Q}^2 : ny^2 = x^3 - x\}$

given by

$$(a,b,c) \longmapsto \left(\frac{-b}{a+c}, \frac{2}{a+c}\right),$$
$$(x,y) \longmapsto \left(\frac{1-x^2}{y}, \frac{-2x}{y}, \frac{1+x^2}{y}\right).$$

The curve $E^{(n)}$ has a plane projective model, still denoted by $E^{(n)}$

$$E^{(n)}: \quad ny^2z = x(x+z)(x-z),$$

or equivalently, $y^2z = x(x+nz)(x-nz)$. The curve $E^{(n)}$ is an elliptic curve over $\mathbb{Q}$, i.e. a projective smooth curve over $\mathbb{Q}$ of genus one, together with a rational point at infinite $z=0$, namely $O=[0:1:0]$. There is a rich theory on arithmetic of elliptic curves. We will give a quick review on arithmetic theory of general elliptic curves over $\mathbb{Q}$ in next section.

2. Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$, that is, a projective smooth curve over $\mathbb{Q}$ of genus one with a rational point O on E. Elliptic curves over $\mathbb{Q}$ has a plane model and can be defined by a Weirstrass equation

$$E: \quad y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Q},$$

(or projective one: $y^2z = x^3+axz^2+bz^3$) such that $x^3 + ax + b = 0$ has distinct roots, or equivalently, $4a^3 + 27b^2 \neq 0$; now the rational point O on E is the point at infinite, namely $O = [0:1:0]$.

Let $E(\mathbb{Q})$ denote the set of rational points on E. There is a natural abelian group structure on $E(\mathbb{Q})$ with O as zero element such that $P+Q+R=O$ if and only if P, Q, R are collinear. We call $E(\mathbb{Q})$ the Mordell-Weil group of E over $\mathbb{Q}$.

Theorem 2.1 (Mordell). *The Mordell-Weil group $E(\mathbb{Q})$ is a finitely generated abelian group.*

Hence, there is a non-negative integer r such that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus (\text{a finite abelian group}).$$

The rank r of Mordell-Weil group $E(\mathbb{Q})$ is denoted by $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$. There is an other important arithmetic invariant of E, called Shafarevich-Tate group and defined by

$$\text{Ш}(E) := \mathrm{Ker}(H^1(\mathbb{Q}, E) \longrightarrow \prod_v H^1(\mathbb{Q}_v, E)),$$

where v runs over all places of $\mathbb{Q}$. We have much deeper understand for arithmetic of elliptic curves when Birch and Swinnerton-Dyer studied the link of arithmetic of elliptic curves with their complex L-series.

Recall that the L-series of E is defined as an Euler product

$$L(E,s) = \prod_p L_p(E,s),$$

where the Euler factor $L_p(E,s)$ at a prime p is given as follows:

- $L_p(E,s) = \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$ if E has good reduction at p, here a_p is an integer such that $p+1-a_p$ is the number of points of the reduction of E at $\mathbb{F}_p$; in particular, if $p \nmid 16(4a^3+27b^2)$ then E has good reduction at p and $p+1-a_p$ is the number of solutions of $y^2z = x^3+axz^2+bz^3$ over the finite field $\mathbb{F}_p$.
- $L_p(E,s) = (1-p^{-s})^{-1}$ (resp. $(1+p^{-s})^{-1}$) if E has split (resp. non-split) multiplicative reduction at p.
- $L_p(E,s) = 1$ if E has additive reduction at p.

For the precise definition of the reduction type, see [26]. The completed L-series of E is defined to be

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

which a priori is defined on the complex half plane $\mathrm{Re}(s) > 3/2$. There is a positive integer N_E, called the conductor of E, whose prime factors are exactly the primes on which E has bad reduction, measures the badness of the reductions of E. The following is conjectured first by Taniyama and Shimura, nowadays called the modularity theorem, and is proved by Wiles, Taylor-Wiles and Breuil-Conrad-Diamond-Taylor:

Theorem 2.2. *Let E be an elliptic curve over $\mathbb{Q}$, then its L-series has an analytic continuation to the whole complex plane and satisfies a functional equation with central point $s=1$, namely*

$$\Lambda(E,s) = \epsilon(E)N_E^{1-s} \cdot \Lambda(E, 2-s),$$

where $\epsilon(E) = \pm 1$ is called the root number of E, or called the sign of the L-function $L(E,s)$.

The conjecture of Birch and Swinnerton-Dyer (BSD, for short) for an elliptic curve E over $\mathbb{Q}$ relates the leading term of the Taylor expansion of $L(E,s)$ at $s=1$ with arithmetic invariants of E, which says that

Conjecture 2.3 (Birch and Swinnerton-Dyer)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then*

(1) the rank part of BSD says that

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

(2) Let $\Omega(E), c_\ell, R(E), Ш(E)$ be the period, Tamagawa number at prime ℓ, regulator, and Shafarevich-Tate group of E, respectively (see [26] for their definitions). The refined part of BSD says that $Ш(E)$ is finite and satisfies the following formula

$$\begin{aligned}\#Ш(E) &= \#Ш_{\mathrm{an}}(E)\\ &:= \left(\frac{\Omega(E)\prod_\ell c_\ell \cdot R(E)}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}\right)^{-1} \cdot \lim_{s\to 1}\frac{L(E,s)}{(s-1)^r}.\end{aligned}$$

For a general elliptic curve $E: y^2 = x^3+ax+b$ over $\mathbb{Q}$ and a square-free integer n, we define the quadratic twist of E by $E^{(n)}: ny^2 = x^3+ax+b$, and $\epsilon(n) = \epsilon(E^{(n)})$ the sign of $E^{(n)}$ in its functional equation. According to the behavior of $\mathrm{ord}_{s=1}L(E^{(n)},s)$, D. Goldfeld [15] (see also Katz–Sarnak [17]) has the following conjecture

Conjecture 2.4 (Goldfeld conjecture)**.** *Among all square-free positive integers n with $\epsilon(n) = +1$ (resp. -1), there is a subset with density one with $\mathrm{ord}_{s=1}L(E^{(n)},s) = 0$ (resp. $=1$).*

Theorem 2.5 (Gross-Zagier [14] and Kolyvagin [19])**.** *If $r := \mathrm{ord}_{s=1}L(E,s) \le 1$, then $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r$.*

Goldfeld's conjecture, together with the theorems of Coates-Wiles and Gross-Zagier-Kolyvagin, predicts Conjecture 1.4 and the following conjecture

Conjecture 2.6 (Rank version of Goldfeld conjecture)**.** *Among all square-free positive integers n with $\epsilon(n) = +1$ (resp. -1), there is a subset of n with density one such that $\mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0$ (resp. $=1$).*

3. L-Values and Tunnell's Theorem

Back to the congruent elliptic curve $E: y^2 = x^3 - x$ and its quadratic twist $E^{(n)}: ny^2 = x^3 - x$. It is not hard to see that the torsion subgroup of $E^{(n)}(\mathbb{Q})$ consisting of $O, (0,0), (\pm 1, 0)$, hence by Mordell's theorem and Proposition 1.6, we have

Proposition 3.1. *A positive integer n is a congruent number if and only if the rank of Mordell-Weil group $E^{(n)}(\mathbb{Q})$ is larger than 0. Moreover, if n is a congruent number, then there are infinitely many rational right angled triangles with area n.*

For example, the Morell-Weil group of $E^{(6)}: 6y^2z = x(x+z)(x-z)$ is of rank one and is, modulo its torsion, generated by the point $P := (2,-1)$. The point P gives rise to the triangle $(3,4,5)$ by the correspondence in Proposition 1.6. The point $2P := \left(\frac{25}{24}, -\frac{70}{24^2}\right)$ gives rise to the triangle $\left(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}\right)$.

It was already known in the middle of 19th century that the L-series $L(E^{(n)},s)$ of the congruent elliptic curve $E^{(n)}: ny^2 = x^3 - x$ is equal to the L-function of a Hecke character over the quadratic imaginary field $\mathbb{Q}(\sqrt{-1})$ and which implies the following (a special case of modularity theorem).

Theorem 3.2. *The L-function $L(E^{(n)},s)$ of $E^{(n)}$ has analytic continuation to an entire function in $s \in \mathbb{C}$ and satisfies the functional equation*

$$\Lambda(E^{(n)},s) := 2(2\pi)^{-s}\Gamma(s)L(E^{(n)},s) = \epsilon(n)N^{1-s}\cdot\Lambda(E^{(n)},2-s),$$

where

$$\epsilon(n) = \begin{cases} +1, & \text{if } n \equiv 1,2,3 \bmod 8, \\ -1, & \text{if } n \equiv 5,6,7 \bmod 8. \end{cases} \qquad N = \begin{cases} 32n^2, & \text{if } 2 \nmid n, \\ 16n^2, & \text{if } 2 \mid n. \end{cases}$$

It is therefore clear that the vanishing order $\mathrm{ord}_{s=1}L(E^{(n)},s)$ of the L-series at $s=1$, is odd if and only if $\epsilon(n) = -1$, and therefore if and only if $n \equiv 5,6,7 \bmod 8$. Thus the BSD conjecture predicts Conjecture 1.2.

Using work of Shimura and Waldspurger on Shimura correspondence and Theorem 2.5 (which was proven by Coates-Wiles for CM elliptic curve with $r=0$), Tunnell established a special values formula of $L(E^{(n)},1)$ and therefore obtained the following theorem.

Theorem 3.3 (Tunnell [33])**.** *Let n be a square-free positive integer and let $a=1$ for n odd and $a=2$ for n even. If n is a congruent number, then*

$$\begin{aligned}\#&\left\{(x,y,z)\in\mathbb{Z}^3 \;\middle|\; \frac{n}{a} = 2ax^2+y^2+8z^2,\ 2\nmid z\right\}\\ &= \#\left\{(x,y,z)\in\mathbb{Z}^3 \;\middle|\; \frac{n}{a} = 2ax^2+y^2+8z^2,\ 2\mid z\right\}.\end{aligned}$$

If the Birch and Swinnerton-Dyer conjecture is true for $E^{(n)}$, then, conversely, the equality implies that n is a congruent number.

Thus there is a conjectural (which will be true assuming the rank part of the BSD conjecture) algorithm which decides in a finite number of steps whether or not a given positive integer is congruent. Tunnell's theorem gives a sufficient condition for a positive integer being non-congruent number. Next section, we introduce the theory of Heegner points, and give a sufficient condition for a positive integer being congruent number.

4. Heegner Points and Congruence Numbers

In this section we consider the congruent elliptic curve $E: y^2 = x^3 - x$ and its quadratic twists $E^{(n)}: ny^2 = x^3 - x$. One of our main result is the following weak version of Goldfeld conjecture:

Theorem 4.1. *Among the set of all positive square-free integers $n \equiv 5,6,7 \mod 8$, there is a subset of integers n with density more than 50% such that $L(E^{(n)},s)$ has a simple zero at $s=1$ (and therefore n is a congruent number).*

4.1 Heegner-Birch Argument

For a positive square-free integer n, let $\#\text{Ш}_{\text{an}}(n) = \#\text{Ш}_{\text{an}}(E^{(n)})$ be the hypothetical size of the Shafarevich-Tate group of $E^{(n)}$ predicted by the refined BSD conjecture; it is known to be a positive rational number when the analytic rank $r^{(n)} := \text{ord}_{s=1} L(E^{(n)},s)$ is ≤ 1. In particular, $\#\text{Ш}_{\text{an}}(E) = \#\text{Ш}(E) = 1$. We start with the simplest case of Heegner point.

Theorem 4.2. *Any prime $p \equiv 7 \mod 8$ is a congruent number, and $r^{(p)} = 1$ and $\#\text{Ш}_{\text{an}}(p)$ is a 2-adic unit.*

Proof. Let $K = \mathbb{Q}(\sqrt{-p})$ and $E: y^2 = x^3 - x$, which has conductor 32. Note that $X_0(32)$ is a genus one curve over $\mathbb{Q}$ with the cusp ∞ rational. There is a degree 2 modular parametrization

$$f: X_0(32) \longrightarrow E, \qquad \infty \mapsto O,$$

Since the prime 2 is split in K, there is an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/32\mathbb{Z}$. The point P on $X_0(N)$ representing the isogeny $(\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1})$ is defined over the Hilbert class field H_K of K. Define the Heegner point on E to be

$$y = \text{Tr}_{H_K/K} f(P) \in E(K).$$

Using the theory of complex multiplication, one can show that there is a 2-torsion point $T \neq O$ such that

$$f(P) + f(P)^c = T$$

where c is the complex conjugation. Since $[H_K:K]$ is odd, we have $y + y^c = T$. Now we have $2y \in E(K)^-$, the subgroup of points in $E(K)$ where the action of complex conjugation is equal to the inverse. If y is torsion, then $4y = O$. But $E[4] \cap E(K) = E[2]$ and then y is defined over $\mathbb{Q}$. Thus $2y = y + y^c = O \neq T$, a contradiction.

Under the twisting isomorphism

$$E(K)^- \cong E^{(p)}(\mathbb{Q}), \qquad (x,y) \mapsto (-x, y/\sqrt{-p}),$$

we may view $2y$ as a rational point on $E^{(p)}$. One can derive the following formula from the Gross-Zagier formula for E over K (see Theorem 4.4)

$$\#\text{Ш}_{\text{an}}(p) = [E^{(p)}(\mathbb{Q}) : \mathbb{Z}(2y) + E^{(p)}(\mathbb{Q})_{\text{tor}}]^2.$$

Therefore, we know that $\#\text{Ш}_{\text{an}}(E^{(p)})$ is a 2-adic unit since $2y$ is not 2-divisible in $E^{(p)}(\mathbb{Q})$. □

Theorem 4.3. *Any prime $p \equiv 3 \mod 8$ is not a congruent number and $\#\text{Ш}_{\text{an}}(E^{(p)})$ is a 2-adic unit.*

One can show that a prime $p \equiv 3 \mod 8$ is not congruent exactly as Fermat show that 1 is not congruent. But we now give a proof using L-values, parallel to the previous case.

Proof. Let B be the quaternion algebra over $\mathbb{Q}$ ramified exactly at $2, \infty$. Since 2 is inert in $K = \mathbb{Q}(\sqrt{-p})$, there is an embedding of K into B as $\mathbb{Q}$-algebras. Fix such an embedding and let R be an order of B of discriminant 32 such that $R \cap K = \mathcal{O}_K$. Such an order R is unique up to conjugation by $\widehat{K}^\times$ (there is a conjugation action of $\widehat{B}^\times$ on the set of orders with fixed discriminant). Here, for an abelian group M, $\widehat{M} = M \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$, where $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. with p running over all primes.

Consider the Shimura set $X_{\widehat{R}^\times} := B^\times \backslash \widehat{B}^\times / \widehat{R}^\times$. By the reduction theory of definite quadratic forms, the set $X_{\widehat{R}^\times}$ is finite. For any odd p, there is a Hecke action T_p on the free abelian group $\mathbb{Z}[X_{\widehat{R}^\times}]$ (for precise definition, see (4.1)). Let $\sum_n a_n q^n \in S_2(\Gamma_0(32))$ be the newform associated to E. By Jacquet-Langlands correspondence, there is a unique free of rank one $\mathbb{Z}$-submodule in the subspace of $\mathbb{Z}[X_{\widehat{R}^\times}]$ with degree zero where T_p acts as the Fourier coefficient a_p. Let f be its base (unique up to ± 1). It turns out that f takes odd value on cosets of $\widehat{B}^{\times 2}$.

Denote by $\mathcal{C} = K^\times \backslash \widehat{K}^\times / \widehat{\mathcal{O}}_K$ the ideal class group of K, which has odd cardinality. The embedding of K into B induces a morphism from $\mathcal{C}$ to $X_{\widehat{R}^\times}$. Thus we obtain a function, still denote by f, from $\mathcal{C}$ to $\mathbb{Z}$. Since the ideal class number is odd, $\mathcal{C} = \mathcal{C}^2$ and f takes odd values on $\mathcal{C}$. Therefore the period

$$y := \sum_{t \in \mathcal{C}} f(t)$$

is odd. The following formula can be derived from the Waldspurger formula 4.5 by noting $\#\text{Ш}_{\text{an}}(1) = 1$.

$$|y|^2 = [\mathcal{O}_K^\times : \mathbb{Z}^\times]^2 \cdot \#\text{Ш}_{\text{an}}(p).$$

We then know that the analytic Sha $\#\text{Ш}_{\text{an}}(p)$ is a 2-adic unit and therefore p is non-congruent number by Theorem 2.5. □

One can easy to show that $\text{Ш}(E^{(p)})[2^\infty]$ is trivial for primes $p \equiv 3 \mod 4$ and therefore the 2-part of refined BSD conjecture holds for $E^{(p)}$.

For a general n with many prime factors, the ideal class number of $K = \mathbb{Q}(\sqrt{-n})$ is not odd any more. The Heegner-Birch argument does not apply directly. We will use all Heegner points for genus characters and an induction argument to obtain a criterion with positive density. To do that, we need general Gross-Zagier formula and Waldspurger formula (see [14], [36] and [5]), which we review next.

4.2 Heegner Points and Gross-Zagier Formula

4.2.1 Gross-Zagier Formula

Given a triple (E,K,χ) where

- E: an elliptic curve of conductor N defined over $\mathbb{Q}$;
- K: an imaginary quadratic field of discriminant D and $\eta : \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \to \pm 1$ the associated character;
- χ: an anticyclotomic character of conductor c.

Assume that the Rankin-Selberg L-function $L(s,E,\chi)$ has sign -1 in its function equation and assume that $(c,N)=1$. Let B be the indefinite quaternion algebra over $\mathbb{Q}$ whose finite ramified places are exactly those v with

$$\epsilon(E_v,\chi_v) = -\chi_v\eta_v(-1).$$

where $\epsilon(E_v,\chi_v)$ is the local root number of $L(s,E,\chi)$ at v. Let R be an order of B with discriminant N such that $R\cap K = \mathcal{O}_c$ with respect to a fixed embedding of K into B. Such order exists and is unique up to the action of $\widehat{K}^{\times}$. Let $X_{\widehat{R}^{\times}}$ be the Shimura curve over $\mathbb{Q}$ associated to B of level $\widehat{R}^{\times}$. Its complex points forms a Riemann surface as follows

$$X_{\widehat{R}^{\times}}(\mathbb{C}) \cong B_+^{\times}\backslash\mathcal{H}\times\widehat{B}^{\times}/\widehat{R}^{\times}\cup\{\text{cusps}\}.$$

Here, $B_+^{\times}$ denotes elements in $B^{\times}$ with positive reduced norms and $B_+^{\times}$ acts on $\mathcal{H}$ via an isomorphism $B(\mathbb{R})\cong M_2(\mathbb{R})$. The set of cusps is non-empty if and only if B is split. We denote $[z,g]_{\widehat{R}^{\times}}$ the image of $(z,g)\in\mathcal{H}\times\widehat{B}^{\times}$ in $X_{\widehat{R}^{\times}}(\mathbb{C})$.

On the curve $X_{\widehat{R}^{\times}}$, there is a distinguished class $\xi_{\widehat{R}^{\times}}\in\mathrm{Pic}(X_{\widehat{R}^{\times}})_{\mathbb{Q}}$ with degree equal to one on every connected component of $X_{\widehat{R}^{\times}}$. In the case of the modular curve $X_0(N)$, one may work with the divisor class of the cusp at infinity. In general, one uses a normalized Hodge class i.e. the unique line bundle, which has degree one on each geometrically connected components, and is parallel to

$$\omega_{X_{\widehat{R}^{\times}}/\mathbb{Q}} + \sum_{x\in X_{\widehat{R}^{\times}}(\overline{\mathbb{Q}})}(1-e_x^{-1})x.$$

Here $\omega_{X_{\widehat{R}^{\times}}/\mathbb{Q}}$ is the canonical bundle of $X_{\widehat{R}^{\times}}$, e_x is the ramification index of x in the complex uniformization of $X_{\widehat{R}^{\times}}$, i.e. for a cusp x, $e_x=\infty$ so that $1-e_x^{-1}=1$; for a non-cusp x, e_x is the ramification index of any preimage of x in the map $X_{U'}\to X_{\widehat{R}^{\times}}$ for any sufficiently small open compact subgroup U' of $\widehat{R}^{\times}$ such that each geometrically connected component of $X_{U'}$ is a free quotient of $\mathcal{H}$ under the complex uniformization.

By the modularity theorem and Jacquet-Langlands correspondence, there is a modular parametrization, that is, a non-constant morphism over $\mathbb{Q}$

$$f : X_{\widehat{R}^{\times}} \longrightarrow E$$

satisfying the following conditions

- mapping the normalized Hodge class $\xi_{\widehat{R}^{\times}}$ to O, that is, there is an integral multiple of $\xi_{\widehat{R}^{\times}}$ represented by a divisor $\sum_i n_ix_i$ with integral coefficients n_i such that $\sum_i a_if(x_i)=O$ in $E(\mathbb{Q})$.
- for each $p\mid(N,D)$, $T_{\varpi_{K_p}}f = \chi_p^{-1}(\varpi_{K_p})f$. Here, for each place $p\mid(N,D)$, $K_p^{\times}$ normalizes $R_p^{\times}$ and a uniformizer ϖ_{K_p} of K_p induces an automorphism $T_{\varpi_{K_p}}$ on $X_{\widehat{R}^{\times}}$ over $\mathbb{Q}$, which, on $X_{\widehat{R}^{\times}}(\mathbb{C})$, is given by $[z,g]_{\widehat{R}^{\times}}\mapsto[z,g\cdot\varpi_{K_p}]_{\widehat{R}^{\times}}$. Also note that for such p, $\chi_p(\varpi_{K_p})=\pm1$.

Moreover, if f' is another such parametrization, then there exist nonzero integers n,n' such that $nf=n'f'$.

The multiplicity one property follows from the following result in local representation theory. Let $p<\infty$. Let π_p be the p-component of the Jacquet-Langlands correspondence on $B_{\mathbb{A}}^{\times}$ of the cuspidal automorphic representation associated to E. Then

- if $\mathrm{ord}_p(N_p)\le 1$ or $K_p/\mathbb{Q}_p$ is unramified, then the space $\pi_p^{R_p^{\times}}$ of π_p invariant under $R_p^{\times}$ is of dimension one.
- if $\mathrm{ord}_p(N_p)\ge 2$ and $K_p/\mathbb{Q}_p$ is ramified, then $\dim_{\mathbb{C}}\pi_p^{R_p^{\times}}\le 2$ and there is a unique line in $\pi_p^{R_p^{\times}}$ at where $K_p^{\times}$ acts by χ_p^{-1}.

Let z_0 be the unique point on $\mathcal{H}$ fixed by $K^{\times}$ and P the point on $X_{\widehat{R}^{\times}}$ represented by the double coset $[z_0,1]_{\widehat{R}^{\times}}$ in the above complex uniformization. The Shimura's reciprocity law asserts that $P\in X_{\widehat{R}^{\times}}(K^{\mathrm{ab}})$ and for any $t\in\widehat{K}^{\times}$, denote by $\sigma_t\in\mathrm{Gal}(K^{\mathrm{ab}}/K)$ the image of t under the Artin map $\widehat{K}^{\times}/K^{\times}\to\mathrm{Gal}(K^{\mathrm{ab}}/K)$, then

$$[z,1]_{\widehat{R}^{\times}}^{\sigma_t} = [z,t]_{\widehat{R}^{\times}}.$$

Therefore, by $R\cap K=\mathcal{O}_c$ we have $P\in X_{\widehat{R}^{\times}}(H_c)$, where H_c is the ring class field of K of conductor c, characterized by the property that the Artin map induces an isomorphism $\mathrm{Gal}(H_c/K)\cong K^{\times}\backslash\widehat{K}^{\times}/\widehat{\mathcal{O}}_c^{\times}$. Define the Heegner point

$$P_\chi(f) := \sum_{\sigma\in\mathrm{Gal}(H_c/K)} f(P)^{\sigma}\chi(\sigma).$$

Theorem 4.4 (Gross-Zagier Formula). *Assume that (E,χ) has sign -1 and $(c,N)=1$. Then the Heegner point $P_\chi(f)$ satisfies the following height formula:*

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

Here

- *ϕ is the newform associated to E 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.
- $\widehat{h}_K$ *is the Neron-Tate height on* E *over* K.
- $\deg(f)$ *is the degree of the morphism* f.

To use primitive Heegner points, we actually use parametrization $f_0 : X_U \to E$ with higher level than $\widehat{R}^\times$, such that a multiple of f_0 factors through $X_{\widehat{R}^\times}$ becomes to f and the same Gross-Zagier formula also holds.

4.2.2 Waldspurger Formula

To do our induction argument, we also need Waldspurger formula. Given the same triple (E,K,χ) as before but assume the sign of $L(s,E,\chi)$ is $+1$. Still assume $(c,N)=1$. As before, let B be the definite quaternion algebra over $\mathbb{Q}$ ramified precisely at $\varepsilon(E_v,\chi_v) = -\chi_v\eta_v(-1)$ and R an order of B with discriminant N such that $R\cap K = \mathcal{O}_c$ under a fixed embedding $K \hookrightarrow B$. Instead of the Shimura curve, we now consider the Shimura set $X_{\widehat{R}^\times} = B^\times\backslash\widehat{B}^\times/\widehat{R}^\times$.

For any prime $p\nmid N$, there is a Hecke action T_p on the free abelian group $\mathbb{Z}[X_{\widehat{R}^\times}]$ which is defined as follows. For $p\nmid N$, $B_p^\times/R_p^\times \cong \mathrm{GL}_2(\mathbb{Q}_p)/\mathrm{GL}_2(\mathbb{Z}_p)$ can be identified with the set of $\mathbb{Z}_p$-lattices in a 2-dimensional vector space over $\mathbb{Q}_p$. Then for any $g=(g_v)\in\widehat{B}^\times$,

$$T_p([g]) = \sum_{h_p}[g^{(p)}h_p], \tag{4.1}$$

where $g^{(p)}$ is the p-off part of g, namely $g^{(p)} = (g_v^{(p)})$ with $g_v^{(p)} = g_v$ for all $v\neq p$ and $g_p^{(p)} = 1$, and if g_p corresponds to lattice Λ, then h_p runs over $p+1$ lattices $\Lambda'\subset\Lambda$ with $[\Lambda:\Lambda'] = p$.

By Jacquet-Langlands correspondence, there is function

$$f : X_{\widehat{R}^\times} \longrightarrow \mathbb{Z}$$

such that for each $p\nmid N$, the Hecke operator T_p acts on f by a_p and for each $p\mid(N,D)$, $f(\cdot\varpi_{K,p}) = \chi_p(\varpi_{K,p})^{-1}f$. Such f is unique up to scalar. The reason for the multiplicity one property is the same as the one in Gross-Zagier formula.

Consider the toric period

$$P_\chi(f) = \sum_{\sigma\in\mathrm{Gal}(H_c/K)} f(t)\chi(t)$$

where $\mathrm{Gal}(H_c/K)\cong K^\times\backslash\widehat{K}^\times/\widehat{\mathcal{O}}_c^\times \to X_{\widehat{R}^\times}$ induced from the fixed embedding $K\hookrightarrow B$.

Theorem 4.5 (Waldspurger Formula). *Assume that* (E,χ) *has sign* $+1$ *and* $(c,N)=1$. *Then we have that*

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

Here, if $f=\sum_i f(g_i)[g_i]$ *where* $\{[g_i]\}$ *is a system of representatives of* $X_{\widehat{R}^\times}$, *then*

$$\deg f = \sum_i f(g_i)^2 w_i^{-1}$$

where w_i *is the cardinality of* $(B^\times\cap g_i\widehat{B}^\times g_i^{-1})/\{\pm1\}$.

4.3 Genus Character and Birch's Conjecture

For a positive square-free integer n, if the analytic rank of $E^{(n)}$ is ≤ 1, let $\mathcal{L}(n)$ be the positive real number such that $\mathcal{L}(n)^2 = \#\text{Ш}_{\mathrm{an}}(E^{(n)})$; if the analytic rank of $E^{(n)}$ is ≥ 2, let $\mathcal{L}(n)=0$.

If the sign of $E^{(d)}$ is -1, let α_d be a generator of $E(\mathbb{Q}(\sqrt{d}))^-$ modulo torsion if $\mathcal{L}(d)\neq 0$ and $\alpha_d = 0$ otherwise. Denote by $\mathcal{P}(d) = \mathcal{L}(d)\alpha_d$.

For a genus character χ corresponding to $D=d_0d_1$, that is, the character corresponding to the quadratic extension $\mathbb{Q}(\sqrt{d_0},\sqrt{d_1})/K$, the above version Gross-Zagier and Waldspurger formulae relate $P_\chi(f)$ to $\mathcal{L}(d_0)\mathcal{L}(d_1)$ if sign is $+1$ and $\mathcal{P}(d_0)\mathcal{L}(d_1)$ if sign is -1. Here the choice of d_0 is such that $E^{(d_0)}$ has sign -1.

Proposition 4.6. *Let* E *be the curve* $y^2 = x^3-x$. *For each square-free positive integer* n, *let* f *be the primitive test vector for* E *and the trivial character over* $K_n := \mathbb{Q}(\sqrt{-n})$, *which has a multiple as in the previous formulaes. Let* χ *be a unramified genus character over* K_n. *Let* $h_2(n)$ *be the* 2*-rank of ideal class group of* K_n.

- *for* $n\equiv 1,2,3 \bmod 8$ *and* $\mathrm{sign}(E,\chi)=+1$, *the period* $P_\chi(f)\neq 0$ *only if we may write* $n=d_0d_1$ *with* $0<d_1\equiv 1 \bmod 8$ *such that* χ *is the character associated to* $K_n(\sqrt{d_1})$. *In that case,*

$$P_\chi(f) = \pm 2^{h_2(n)-\delta}u_{K_n}\mathcal{L}(d_1)\mathcal{L}(d_2).$$

Here $\delta=1$ *if* $n\equiv 1 \bmod 8$ *and* $\delta = 0$ *otherwise.*
- *for* $n\equiv 5,6,7 \bmod 8$ *and* $\mathrm{sign}(E,\chi)=-1$, *the point* $P_\chi(f)$ *is non-torsion only if we may write* $n=d_0d_1$ *with* $0<d_0\equiv 5,6,7 \bmod 8$ *and* $0<d_1\equiv 1,2,3 \bmod 8$ *and* $\chi=\chi_{d_0,d_1}$ *is the genus character associated to* $K_n(\sqrt{d_1})$ *for* $n\equiv 5,6 \bmod 8$ *or* $K_n(\sqrt{d_1^*})$ *for* $n\equiv 7 \bmod 8$. *In this case*

$$P_\chi(f) = \epsilon(d_0,d_1)2^{h_2(n)}\mathcal{P}(d_0)\mathcal{L}(d_1).$$

Here $\epsilon(d_0,d_1)=\pm i$ *if* $(d_0,d_1)\equiv(5,3) \bmod 8$ *and* $\epsilon(d_0,d_1)=\pm 1$ *otherwise.*

The point here is as follows. Suppose $d_0\equiv 5,6,7 \bmod 8$ is a positive and want to understand the "Heegner point" $\mathcal{P}(d_0)$. We need to compare its different realization P_χ of genus characters $\chi=\chi_{d_0,d_1}$. Let $n=d_0d_1$ and $n'=d_0d_1'$ be such situation. Choose e_0 such that e_0d_1, e_0d_1' are in the situation of sign $+1$.

If we write $P(d_0,d_1)$ (resp. $P(e_0,d_1)$) for corresponding points (resp. periods). Then we have the comparison:

$$\begin{aligned}[P(d_0,d_1):P(d_0,d_1')] &\sim [\mathcal{P}(d_0)\mathcal{L}(d_1):\mathcal{P}(d_0)\mathcal{L}(d_1')]\\ &= [\mathcal{L}(e_0)\mathcal{L}(d_1):\mathcal{L}(e_0)\mathcal{L}(d_1')] \sim [P(e_0,d_1):P(e_0,d_1')]\end{aligned}$$

namely we obtain comparison of Heegner points in term of periods.

4.4 Induction Argument

Given $n\equiv 5,6,7 \bmod 8$, let $f: X_{\widehat{R}^\times} \longrightarrow E$ be the primitive modular parametrization for E and trivial character over $K_n=\mathbb{Q}(\sqrt{-n})$. Then we have

$$\sum_\chi P_\chi(f)=2^kQ_n, \qquad Q_n:=\mathrm{Tr}_{H_{K_n}/H_0}P.$$

Here $\chi=\chi_{d_0,d_1}$ runs over all genus characters of K. Recall that we relates $P_\chi(f)$ to $\mathcal{P}(d_0)\mathcal{L}(d_1)$. By an induction, express $\mathcal{P}(n)$ in term of the genus points Q_d's with $d\equiv 5,6,7 \bmod 8$ and $\mathcal{L}(d)$'s with $d\equiv 1,2,3 \bmod 8$. Their 2-adic non-trivialities are related to the genus class number $g(d)$'s as initial cases. Here $g(d)$ is the cardinality of $2\mathcal{C}_d$ where $\mathcal{C}_d$ is the ideal class group of $K_d=\mathbb{Q}(\sqrt{-d})$. Then $g(d)$ is odd if and only if K_d has no ideal class of order 4. By Gauss' genus theory, it is easy to determine the parity of $g(d)$.

4.5 The Main Result

Our main result is

Theorem 4.7 (T-Yuan-Zhang). *The number $\mathcal{L}(n)$ is an integer. For $n\equiv 5,7 \pmod 8$, $2^{-\rho(n)}\mathcal{L}(n)$ is odd if*

$$\sum_{\substack{n=d_0\cdots d_\ell\\ d_i\equiv 1 \pmod 8,\ i>0}} \prod_i g(d_i)\equiv 1 \bmod 2, \quad \textit{or}$$

$$\sum_{\substack{n=d_0\cdots d_\ell,\\ d_0\equiv 5,7 \pmod 8\\ d_1\equiv 2,3 \pmod 8\\ d_i\equiv 1 \pmod 8,\ i>1}} \prod_i g(d_i)\equiv 1 \pmod 2.$$

For $n\equiv 6 \bmod 8$, $2^{-\rho(n)}\mathcal{L}(n)$ is odd if

$$\sum_{\substack{n=d_0\cdots d_\ell,\\ d_0\equiv 5,6,7 \pmod 8\\ d_1\equiv 2,3 \pmod 8\\ d_i\equiv 1 \pmod 8,\ i>1}} \prod_i g(d_i)\equiv 1 \pmod 2.$$

Here all decompositions $n=d_0\cdots d_\ell$ are non-ordered with $d_i>1$.

Here $\rho(n)$ is an integer with $0\le\rho(n)\le \operatorname{rank} E^{(n)}(\mathbb{Q})$ defined as follows. Let $A=(X_0(32),\infty): 2v^2=u^3+u$ and $A_n: 2nv^2=u^3+u$. Let $\varphi_n: A_n\to E^{(n)}$ be a degree 2-isogeny and define a non-negative integer ρ to be such that $2^{\rho(n)}=[E^{(n)}(\mathbb{Q}):\varphi_n(A_n(\mathbb{Q}))+E^{(n)}[2]]$.

Let $s(n)$ denote the $\mathbb{F}_2$-dimension of the 2-Selmer group of $E^{(n)}: ny^2=x^3-x$ modulo the $E^{(n)}[2]$. Then

$$s(n)=\operatorname{rank} E^{(n)}(\mathbb{Q})+\dim_{\mathbb{F}_2} Ш(E^{(n)}/\mathbb{Q})[2].$$

Theorem 4.8 (Heath-Brown, Daniel M. Kane). *Let Σ be all square-free positive integers $n\equiv 5 \bmod 8$ (resp $n\equiv 6,7 \bmod 8$), then the density of the subset $\Sigma_1\subset\Sigma$ of n with $s(n)=1$ is*

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

Theorem 4.9 (Smith). *Let Σ_1 be the set of square-free positive integers $n\equiv 5 \bmod 8$ (resp. $n\equiv 6,7 \bmod 8$) with $s(n)=1$. Let Σ_1' be the set of square-free positive integers $n\equiv 5 \bmod 8$ (resp. $n\equiv 6,7 \bmod 8$) satisfying the sufficient conditions in the above Theorem. Then $\Sigma_1'\subset\Sigma_1$ with density $\frac{3}{4}$ (resp. $\frac{1}{2}$, $\frac{3}{4}$).*

Combining Theorems 4.7, 4.8 and 4.9, we obtain Theorem 4.1. and its analogues for sign $+1$ case. we have the following:

Theorem 4.10. *1. Among the set of all positive square-free integers $n\equiv 1,2,3 \bmod 8$, there is a subset of integers n with density more than 40% such that $L(E^{(n)},1)\neq 0$.*

2. Among the set of all positive square-free integers $n\equiv 5,6,7 \bmod 8$, there is a subset of integers n with density more than 50% such that $L'(E^{(n)},1)\neq 0$.

5. Distribution of 2-Selmer Groups

Let E be an elliptic curve over $\mathbb{Q}$. For each $1\le k\le\infty$, the. 2^k-Selmer group of E is defined to be

$$\mathrm{Sel}_{2^k}(E)=\mathrm{Ker}\left(H^1(\mathbb{Q},E[2^k])\longrightarrow\prod_v H^1(\mathbb{Q}_v,E)[2^k]\right).$$

Then there is an exact sequence of $\mathbb{Z}_2$-modules

$$0\longrightarrow E(\mathbb{Q})\otimes_{\mathbb{Z}}(\mathbb{Q}_2/\mathbb{Z}_2)\longrightarrow \mathrm{Sel}_{2^\infty}\longrightarrow Ш(E)[2^\infty]\longrightarrow 0$$

and therefore,

$$\mathrm{Sel}_{2^\infty}(E)\cong(\mathbb{Q}_2/\mathbb{Z}_2)^r\oplus\bigoplus_i(\mathbb{Z}/2^i\mathbb{Z})^{r_i}$$

with $r\ge 0$, and r_i non-negative even integers and almost all 0. Let $m_i=r+\sum_{j\ge i}r_j$. Thus $\underline{m}:=(m_1\le m_2\le\cdots)$ is a decreasing sequence of non-negative integers. such that $m_i\equiv r \bmod 2$ for all i where $r:=\lim_i m_i$. The structure of $Ш_{2^\infty}(E)$ is determined by the sequence $\underline{m}$, called the 2^∞-Selmer type of E. It is know that $r\equiv \mathrm{ord}_{s=1}L(E,s) \bmod 2$ by Dokchitser brothers [11].

Definition 5.1. A sequence $\underline{m}$ of non-negative integers is called admissible if (i) its is decreasing $m_1\ge m_2\ge\cdots$; (ii) $m_i\equiv r \bmod 2$ for all i, where $r:=\lim_i m_i$ is called the rank of $\underline{m}$.

Given an elliptic curve E over $\mathbb{Q}$, for a square-free integer n, denote by $E^{(n)}$ its quadratic twist over $\mathbb{Q}(sqrtn)$, $\underline{m}^{(n)}$ its 2^∞-Selmer type, and $\epsilon(n) = \pm 1$ the sign in its functional equation.

Given an admissible $\underline{m}$ with rank r, let $P(E, \underline{m})$ denote the density, among all square-free integers n with $\epsilon(n) \equiv r \mod 2$, of those n for which $E^{(n)}$ has 2^∞-Selmer type $\underline{m}$. By work of Heath-Brown, Kane, and Smith, we have

Theorem 5.2. *Let E be an elliptic curve over $\mathbb{Q}$ with full rational 2-torison points and E has no cyclic subgroup of order 4 defined over $\mathbb{Q}$. Let $\underline{m}$ be an admissible sequence with rank r. Then the density $P(E, \underline{m}) > 0$ if and only if $r \leq 1$. In the case $r \leq 1$, we have*

$$P(E, \underline{m}) = \delta(m_1) \prod_{i \geq 1} \delta(m_i, m_{i+1}),$$

where

- *for each $m \geq j \geq 0$, $\delta(m, j)$ denote the probability that an arbitrary $m \times m$-alternating matrix with entries in $\mathbb{F}_2$ has a kernel of dimension j. Here $A \in M_{m \times m}(\mathbb{F}_2)$ is called alternating of $A^t = -A$ and diagonals of A are zero.*
- *for each $m \geq 0$, $\delta(m) = \lim_{j \geq 0} \delta(m + 2j, m)$.*

Remark. 1. Heath-Brown and Kane showed that the density, among all square-free n, of those n such that $m_1^{(n)} = m_1$ is $\delta(m_1)$. Let m, j be any non-negative integers with $m \geq j$. For any integer $k \geq 1$, let

$$\mathfrak{R}_k(m, j) = \left\{ \text{square-free } n \mid m_k^{(n)} = m, m_{k+1}^{(n)} = j \right\},$$

$$\mathfrak{S}_k(m) = \left\{ \text{square-free } n \mid m_k^{(n)} = m \right\}.$$

Smith [29] proved that the density of $\mathfrak{R}_k(m, j)$ in $\mathfrak{S}_k(m)$ exists and is equal to $\delta(m, j)$.

2. By a remark in the draft of Heath-Brown

$$\delta(m, j) = 2^j \prod_{i=1}^{j} (2^i - 1)^{-1} \cdot \prod_{i=m-j+1}^{m} (1 - 2^{-i}) \cdot \prod_{i=0}^{(m-j)/2-1} (1 - 2^{-1-2i}).$$

$$\delta(m) = \lim_{l \to \infty} P(m + 2j, m) = \lambda \cdot 2^m \cdot \prod_{i=1}^{m} (2^i - 1)^{-1},$$

$$\lambda = \prod_{i=1}^{\infty} (1 - 2^{-1-2i}) = 0.4194 \cdots.$$

What is remarkable about the above result is that, while it does not tell us the precise structure of any particular 2^n-Selmer group, it does give the asymptotic distribution of these groups, and shows that this asymptotic distribution is exactly as predicted by the probabilistic model given in [1] Moreover, it is shown in [1] that the above result implies corresponding part of Rank version of Goldfeld's conjecture.

6. Full BSD Conjecture

The following theorem shows that there are infinitely many elliptic curves over $\mathbb{Q}$ of rank one for which the full BSD conjecture hold.

Theorem 6.1 (Li-Liu-T). *Let $n \equiv 5 \mod 8$ be a positive integer with all prime factors congruent to 1 modulo 4 and assume that $\mathbb{Q}(\sqrt{-n})$ has no ideal class of exact order 4. Then n is a congruent number and the full BSD conjecture holds for the elliptic curve $E^{(n)} : ny^2 = x^3 - x$.*

For example, the number 1493 is the minimal prime $p \equiv 5 \mod 8$ such that $E^{(p)}$ has rank one and with non-trivial Shafarevich-Tate group. In fact, the associated Heegner point (x, y) has coordinates

$$x = \frac{2456153549914721493968975459422696932728951498371630131453}{295850118285420757194446868756192006468120535851 0529},$$

$$y = \frac{121725780668263596873618123810557983972375660184180439465365335709906181098721585260100}{16091910960547986287175324647321077268221974568783910945697471178779686889 2833}.$$

One can then show $E^{(p)}(\mathbb{Q})$ modulo torsion has a generator

$$\left[\frac{1674371133}{744769}, -\frac{51224214734700}{642735647} \right].$$

Then the result in Theorem 6.1 shows that $Ш(E^{(p)}/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2$.

To describe the reason behind it, we introduce some notations. Let $f = \sum_n a_n q^n \in S_2(\Gamma_0(N))$ be a newform of weight 2 and level $\Gamma_0(N)$. Let $\mathbb{Q}(f) \subset \mathbb{C}$ be the total real field generated over $\mathbb{Q}$ by Hecke eigenvalues of f. Let A be the abelian variety over $\mathbb{Q}$ associated to f. Then A has the complex L-function

$$L(s, A) = \prod_{\sigma : \mathbb{Q}(f) \to \mathbb{C}} L(s, f^\sigma),$$

where σ runs over all embeddings of $\mathbb{Q}(f)$ into $\mathbb{C}$. Moreover, $A(\mathbb{Q})_\mathbb{Q} := A(\mathbb{Q}) \otimes_\mathbb{Z} \mathbb{Q}$ is a finite dimensional $\mathbb{Q}(f)$ vector space.

Assume that f has complex multiplication by an imaginary quadratic field K and let F_0 denote the minimal finite abelian extension of K such that the base change of A to F_0 is isogenous to a power of an elliptic curve (with complex multiplication by K).

Theorem 6.2. *Let p be a prime split in K, unramified in F_0, and $p \nmid [F_0 : \mathbb{Q}]$.*

(i) Assume that $L(s,f)$ has a simple zero at $s=1$. Then $\dim_{\mathbb{Q}(f)} A(\mathbb{Q})_{\mathbb{Q}} = 1$ and $Ш(A/\mathbb{Q})$ is finite. Moreover the order of $Ш(A/\mathbb{Q})(p)$ is as predicted by the conjecture of Birch and Swinnerton-Dyer.

(ii) If $\dim_{\mathbb{Q}(f)} A(\mathbb{Q})_{\mathbb{Q}} = 1$ and $Ш(A/\mathbb{Q})(p)$ is finite, then $L(f,s)$ has a simple zero at $s=1$.

As a special case of the above theorem, we have

Corollary 6.3. *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication. Let p be any potentially good ordinary odd prime for E.*

(i) Assume that $L(s,E)$ has a simple zero at $s=1$. Then $E(\mathbb{Q})$ has rank one and $Ш(E/\mathbb{Q})$ is finite. Moreover the order of $Ш(E/\mathbb{Q})(p)$ is as predicted by the conjecture of Birch and Swinnerton-Dyer.

(ii) If $E(\mathbb{Q})$ has rank one and $Ш(E/\mathbb{Q})(p)$ is finite, then $L(E,s)$ has a simple zero at $s=1$.

Remark. The first part of (i) in Theorem 6.2 is the results of Gross-Zagier and Kolyvagin. The remaining part is due to Perrin-Riou for good ordinary primes. We deal with odd bad primes which are potentially ordinary.

Proof of Theorem 6.1. An induction argument (see [31] and also [32]) shows the Heegner point associated to E and $\mathbb{Q}(\sqrt{-n})$ is of infinite order. In fact, together with the Gross-Zagier formula [5], the 2-part of full BSD for $E^{(n)} : y^2 = x^3 - n^2 x$ is also verified. Therefore, both the analytic rank and Mordell-Weil rank of $E^{(n)}$ are one.

By Perrion-Riou [24] and Kobayashi [18], we know that the p-part of full BSD holds for all primes $p \nmid 2n$. By Theorem 6.2, the p-part of BSD also holds for all primes $p \mid n$, since all primes p with $p \equiv 1 \mod 4$ are potentially good ordinary primes for $E^{(n)}$. □

References

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

[2] B. J. Birch, *Elliptic curves and modular functions*, Symposia Mathematica, Indam Rome 1968/1969, vol. 4, pp. 27–32. London: Academic Press (1970).

[3] B. J. Birch and H. P. Swinnerton-Dyer, *Notes in Eeliptic curves (II)*, J. Reine Angew. Math. 218 (1965), 79–108.

[4] Daniel Bump, *Automorphic Forms and Representations*, Cambridge Studies in Advanced Mathematics 55, 1998.

[5] Li Cai, Jie Shu, and Ye Tian, *Explicit Gross-Zagier and Waldspurger formulae*, Algebra Number Theory 8(10) (2014), 2523–2572.

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

[7] John Coates and Andrew Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 233–251.

[8] H. Cohen and J. C. Lagarias, *On the existence of fields governing the 2-invariants of the class group $\mathbb{Q}(\sqrt{dp})$ as p varies*, Mathematics of computation 41, 1983, no. 164.

[9] Arian Diaconu and Ye Tian, *Twisted Fermat Curves over Totally Real Fields*, Annals of Math. 162, 2005.

[10] L. E. Dickson, *History of the Theory of Numbers* Volume II. Chapter XVI, Chelsea, New York, 1971.

[11] T. Dokchitser and V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Annals of Math. 172, (2010), 567–596.

[12] Keqin Feng, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arithmetica, LXXV. 1 (1996).

[13] B. Gross, *Kolyvagin's work on modular elliptic curves*, in: L-function and Arithmetic (ed. J. Coates and M. J. Talyor) Cambridge University Press (1991).

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

[15] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in Number theory, Carbondale 1979, M. B. Nathanson, ed., Lecture Notes in Math. 751, Springer, Berlin, 1979, 108–118.

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

[17] Nicholas M. Katz and Peter Sarnak, *Zeros of zeta functions and symmetry*, Bull. Amer. Math. Soc. (N.S.) 36(1) (1999), 1–26.

[18] Kobayashi, Shinichi, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*. Invent. Math. 191(3) (2013), 527–629.

[19] V. A. Kolyvagain, *Euler system*, The Grothendieck Festschrift. Prog. in Ath., Boston, Birkhauser (1990).

[20] V. A. Kolyvagain, *Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a subclass of Weil curves*, Math. USSR Izvestiya, Vol. 32 (1989), No. 3.

[21] Delang Li and Ye Tian, *On the Birch-Swinnerton-Dyer Conjecture of Elliptic Curves $E_D : y^2 = x^3 - D^2 x$*, Acta Mathematica Sinca, English Series 2000, April, Vol. 16, No. 2, pp. 229–236.

[22] D. Milovic, *On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv 1 \pmod 4$*, arxive(2015).

[23] P. Monsky, *Mock Heegner Points and Congruent Numbers*, Math. Z. 204 (1990), 45–68.

[24] B. Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math. 89(3) (1987), 455–510.

[25] G. Shimura *Introduction to the arithmetic theory of automorphic functions*. Princeton University Press (1971).

[26] J. H. Silverman. *The Arithmetic of Elliptic Curves*, 2nd ed. Graduate Texts in Mathematics 106. Springer, New York, 2009.

[27] A. Smith, *An approach to the full BSD conjecture at two in quadratic twist families of elliptic curves*, undergraduate thesis at Princeton.

[28] A. Smith, *Governing fields and statistics for 4-Selmer groups and 8-class groups.*

[29] A. Smith, *2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture.*

[30] N. M. Stephens, *Congruence properties of congruent numbers*, Bull. Lond. Math. Soc. 7 (1975), 182–184.

[31] Ye Tian, *Congruent Numbers and Heegner Points*, Cambridge Journal of Mathematics 2(1) (2014), 117–161.
[32] Ye Tian, Xinyi Yuan, and Shouwu Zhang, *Genus periods, Genus Points, and Congruent Number Problem*. Preprint.
[33] J. B. Tunnell, *A classical diophantine problem and modular forms*, Invent. Math. 72 (1983), 323–334.
[34] Z. J. Wang, *Congruent elliptic curves with non-trivial Shafarevich-Tate groups*, Sci. China Math. 59(11) (2016), 2145–2166.
[35] Z. J. Wang, *Congruent elliptic curves with non-trivial Shafarevich-Tate groups: Distribution part*, Sci. China Math. 60(4) (2017), 593–612.
[36] X. Yuan, S. Zhang, and W. Zhang *Gross-Zagier formula of Shimura Curves*, Annals of Mathematics Studies Number 184, 2012.