

# ARITHMETIC OF QUADRATIC TWISTS OF ELLIPTIC CURVES

YE TIAN

(NOTES BY WENHAN DAI)

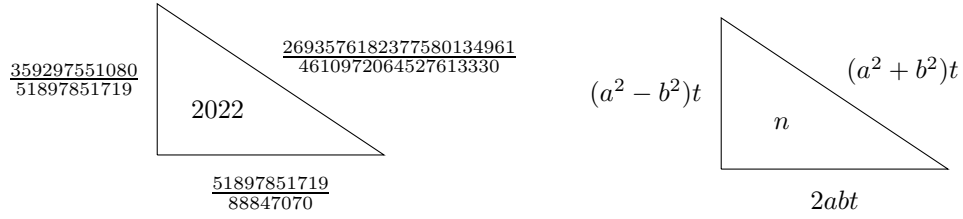
## 1. MOTIVATION: THE CONGRUENT NUMBER PROBLEM

**Definition 1.1** (Congruent number). A positive integer is called a **congruent number** if it is the area of a right angled triangle with rational side lengths.

For example,

- 5, 6, 7 are congruent numbers (Fibonacci),
- 1, 2, 3 are non-congruent numbers (Fermat).

**Example 1.2.** The number 2022 is congruent with the “simplest” triangle having side lengths



For the triangle on the right hand side, require that  $\gcd(a, b) = 1$ ,  $2 \nmid a + b$ , and  $t \in \mathbb{Q}_{>0}^\times$ . Plugging in with  $(a, b) = (5, 4), (2, 1), (16, 9)$  outputs the triple  $(5, 6, 7)$ .

**The Congruent Number Problem.** The congruent number problem is to determine whether or not a given positive integer is congruent number.

**Theorem 1.3** (Heegner 1952). *Any positive  $q \equiv 5, 6, 7 \pmod{8}$ , a prime or twice of a prime, is a congruent number.*

**Theorem 1.4** (Tian 2012). *Let  $n = qp_1 \cdots p_k$  with odd part  $n_0$ , with*

- $q$ : as in Heegner case;
- $p_i \equiv 1 \pmod{8}$  distinct primes

*such that  $\mathbb{Q}(\sqrt{-n_0})$  has no ideal class of order 4. Then  $n$  is a congruent number.*

**Theorem 1.5** (Smith, Yuan-Zhang-Tian 2014). *At least half of square-free positive integers  $\equiv 5, 6, 7 \pmod{8}$  are congruent numbers.*

Main ingredients:

- (1) Heegner points construction: complex multiplication;
- (2) Gross-Zagier and Waldspurger formulae: special  $L$ -values;
- (3) Positive density: imaginary quadratic fields with no order 4 ideal class;
- (4) Induction methods: relation among quadratic twist Heegner points.

---

Date: November 2, 2022.

**1.1. The  $\theta$ -congruent number problem.** Consider triangles with rational side lengths with an angle  $\theta$  fixed, called  $\theta$ -rational triangles. (Note that  $\cos \theta$  must be rational). The  $\theta$ -congruent number problem is stated as follows.

**Question 1.6.** *For which integers  $n$ ,  $n \sin \theta$  is the area of a  $\theta$ -rational triangle?*

It turns out that the problem is essentially to ask which quadratic twists

$$ny^2 = x(x-a)(x-b), \quad a, b \in \mathbb{Q}$$

have positive Mordell-Weil ranks. Here  $\cos \theta = \frac{a+b}{a-b}$  if  $ab < 0$  (we may always assume this). In particular, the congruent number problem is about the family

$$ny^2 = x^3 - x.$$

In general, an elliptic curve  $A$  over  $\mathbb{Q}$  is a smooth curve given by

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

The set of all the rational points (together with  $\infty$ ), denoted by  $A(\mathbb{Q})$ , has an abelian group structure: Theorem (Mordell 1921)

$$A(\mathbb{Q}) \cong A(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r, \quad r \geq 0.$$

There are two important objects to study the Mordell-Weil groups:

$$\boxed{\text{Selmer Groups}}, \quad \boxed{L\text{-functions}}.$$

## 2. SELMER GROUPS

**2.1. 2-Selmer groups.** Let  $A : y^2 = (x - c_1)(x - c_2)(x - c_3)$  be an elliptic curve over  $\mathbb{Q}$  with  $A[2] \subseteq A(\mathbb{Q})$ . For  $(x, y) \in A(\mathbb{Q})$ , write

$$x - c_i = m_i z_i^2, \quad \text{with } m_i \in \mathbb{Z} \text{ square-free and } z_i \in \mathbb{Q},$$

then  $m_1 m_2 m_3$  is a square. This motivates to consider double covers of  $A$ . For  $m = (m_1, m_2, m_3) \in (\mathbb{Q}^\times / \mathbb{Q}^{\times 2})^{\oplus 3, \text{Nm}=1}$ , define the double cover  $C_m \subset \mathbb{P}^3$  of  $A$ :

$$C_m : \quad m_i z_i^2 - m_j z_j^2 = (c_j - c_i) t^2, \quad \forall 1 \leq i < j \leq 3.$$

and 2-Selmer group  $\text{Sel}_2(A/\mathbb{Q})$  by

$$A(\mathbb{Q})/2A(\mathbb{Q}) \cong \{m \mid C_m(\mathbb{Q}) \neq \emptyset\} \subseteq \text{Sel}_2(A/\mathbb{Q}) := \{m \mid C_m(\mathbb{Q}_v) \neq \emptyset \text{ for all } v\}.$$

We obtain

- (1)  $\text{rank}_{\mathbb{Z}} A(\mathbb{Q}) \leq s(A) := \dim_{\mathbb{F}_2} \text{Sel}_2(A/\mathbb{Q})/A(\mathbb{Q})[2]$ .
- (2) if  $s(A) = 0$  then  $A(\mathbb{Q})$  is finite..
- (3) if  $s(A) = 1$ , then it is conjectured that  $\text{rank}_{\mathbb{Z}} A(\mathbb{Q}) = 1$ .

A basic arithmetic question is as follows.

**Question 2.1.** *Find the distribution of  $s(A)$  when  $A$  runs over a quadratic twist family  $\mathcal{A}$ .*

**2.2. General Selmer groups.** In general, if  $A/\mathbb{Q}$  is an elliptic curve and  $p$  is a prime, the  $p$ -Selmer group and  $p^\infty$ -Selmer group of  $A$  can be defined in term of cohomology

$$\begin{aligned} \text{Sel}_p(A/\mathbb{Q}) &= \text{Ker}(H^1(\mathbb{Q}, A[p]) \longrightarrow \prod_v H^1(\mathbb{Q}_v, A)/A(\mathbb{Q}_v)/pA(\mathbb{Q}_v)), \\ \text{Sel}_{p^\infty}(A/\mathbb{Q}) &= \text{Ker}(H^1(\mathbb{Q}, A[p^\infty]) \longrightarrow \prod_v H^1(\mathbb{Q}_v, A)/A(\mathbb{Q}_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p)). \end{aligned}$$

They fit into short exact sequences

$$0 \rightarrow A(\mathbb{Q})/pA(\mathbb{Q}) \rightarrow \text{Sel}_p(A/\mathbb{Q}) \rightarrow \text{III}(A/\mathbb{Q})[p] \rightarrow 0$$

and

$$0 \rightarrow A(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow \text{Sel}_p(A/\mathbb{Q}) \rightarrow \text{III}(A/\mathbb{Q})[p^\infty] \rightarrow 0.$$

**Conjecture 2.2.** *The Shafarevich-Tate group  $\text{III}(A/\mathbb{Q})$  is finite and*

$$\text{corank}_{\mathbb{Z}_p} \text{Sel}_p(A/\mathbb{Q}) = \text{rank}_{\mathbb{Z}} A(\mathbb{Q}).$$

A. Smith gives a method to study the distribution of  $2^\infty$ -Selmer groups  $\text{Sel}_{2^\infty}(A/\mathbb{Q})$  of  $A$  in a quadratic twist family  $\mathcal{A}$  starting from distribution of 2-Selmer groups.

### 3. L-FUNCTIONS

**Conjecture 3.1** (Birch and Swinnerton-Dyer).  *$A/\mathbb{Q}$  elliptic curve,  $r \geq 0$  integer,  $p$  prime. Then the following are equivalent:*

- (1)  $\text{ord}_{s=1} L(A, s) = r$ ;
- (2)  $\text{rank}_{\mathbb{Z}} A(\mathbb{Q}) = r$  and  $\Pi(A/\mathbb{Q})$  finite;
- (3)  $\text{corank}_{\mathbb{Z}_p} \text{Sel}_p \infty(A/\mathbb{Q}) = r$ .

*Under equivalent conditions, the BSD formula holds:*

$$\frac{L^{(r)}(A, 1)}{r! \cdot R \cdot \Omega} = \frac{\#\text{III}(A/\mathbb{Q}) \cdot \prod_\ell c_\ell(A)}{(\#A(\mathbb{Q})_{\text{tor}})^2}.$$

**Theorem 3.2** (Gross-Zagier, Kolyvagin). *Let  $A$  be an elliptic curve over  $\mathbb{Q}$  and  $\text{ord}_{s=1} L(A, s) \leq 1$ , then*

$$\text{ord}_{s=1} L(A, s) = \text{rank}_{\mathbb{Z}} A(\mathbb{Q}), \quad \#\Pi(A/\mathbb{Q}) < \infty.$$

**Theorem 3.3** (Tunnell 1983). *Let  $E$  be the elliptic curve  $y^2 = x^3 - x$ . Let  $n$  be a positive square-free integer,  $a = 1$  for  $n$  odd and  $a = 2$  for  $n$  even. Then*

$$\frac{L(E^{(n)}, 1)}{\Omega/\sqrt{n}} = \frac{a}{16} \left( \sum_{2ax^2+y^2+8z^2=\frac{n}{2}} (-1)^z \right)^2, \quad \Omega = \int_1^\infty \frac{dx}{\sqrt{x^3-x}}.$$

**3.1. Quadratic twists of elliptic curves over  $\mathbb{Q}$ .** In general, for an elliptic curve over  $\mathbb{Q}$  given by:  $y^2 = x^3 + ax + b$ , let  $\mathcal{A}$  denote the set of all isomorphism classes of its quadratic twists:

$$ny^2 = x^3 + ax + b, \quad n \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}.$$

As  $A \in \mathcal{A}$  varies, we are interested in the distribution of

- $\text{rank}_{\mathbb{Z}} A(\mathbb{Q})$ ,  $\#\text{III}(A/\mathbb{Q})[p^\infty]$ ,  $\dim_{\mathbb{F}_p} \text{Sel}_p(A/\mathbb{Q})$ , and  $\text{corank}_{\mathbb{Z}_p} \text{Sel}_p \infty(A/\mathbb{Q})$ .
- leading term of  $L(A, s)$ , i.e.  $\text{ord}_{s=1} L(A, s)$ , and  $\text{III}^{\text{an}}(A/\mathbb{Q})$ .

We now start with ***L*-function side**, some of the discussions are related to Selmer groups via the BSD conjecture.

### 3.2. conjectures on leading terms of *L*-series under quadratic twists.

**Conjecture 3.4** (Goldfeld). *Let  $\mathcal{A}$  be a quadratic twist family of elliptic curves over  $\mathbb{Q}$ . Then*

- (*Even parity*)  $\text{Prob}(\text{ord}_{s=1} L(A, s) = 0 \mid A \in \mathcal{A}, \epsilon(A) = +1) = 1.$
- (*Odd parity*)  $\text{Prob}(\text{ord}_{s=1} L(A, s) = 1 \mid A \in \mathcal{A}, \epsilon(A) = -1) = 1.$

The behavior for analytic Sha is subtle. However, Kolyvagin proposed the following:

**Conjecture 3.5** (Kolyvagin). *Let  $\mathcal{A}$  be a quadratic twist family of elliptic curves over  $\mathbb{Q}$  and  $p$  any prime. There exists  $A \in \mathcal{A}$  such that*

- $\text{ord}_{s=1} L(A, s) = 0$  (resp. 1), and
- $p \nmid \text{III}^{\text{an}}(A/\mathbb{Q}).$

### 3.3. Goldfeld conjecture for CM families.

**Theorem 3.6.** *For quadratic twist families of CM elliptic curves over  $\mathbb{Q}$ , we have the following*

- (1) *the even parity Goldfeld conjecture holds if the CM field is not  $\mathbb{Q}(\sqrt{-2})$ ;*
- (2) *the odd parity Goldfeld conjecture holds if  $p = 2$  is an ordinary prime.*

*Thus the Goldfeld conjecture holds for the family containing the conductor 49 curve.*

The proof of the result consists of two parts.

**Theorem 3.7** (Burungale-Tian, Burungale-Castella-Skinner-Tian). *Let  $A$  be a CM elliptic curve over  $\mathbb{Q}$ ,  $p$  a prime and  $r = 0, 1$ . Then the rank  $r$   $p$ -converse holds:*

$$\text{corank}_{\mathbb{Z}_p} \text{Sel}_p(A/\mathbb{Q}) = r \implies \text{ord}_{s=1} L(A, s) = r,$$

*provided that  $p$  is ordinary for  $r = 1$ .*

**Theorem 3.8** (Smith). *The  $2^\infty$ -Selmer analogue Goldfeld conjecture holds for families  $\mathcal{A}$  over  $\mathbb{Q}$  satisfying the following assumption  $S$ .*

**Assumption S:** There is  $A \in \mathcal{A}$  such that one of the following holds:

- $A(\mathbb{Q})[2] = 0$ ; or
- $A(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$  and for the unique  $\mathbb{Q}$ -degree 2 isogeny  $A \rightarrow A_0$ ,  $\mathbb{Q}(A_0[2]) \neq \mathbb{Q}, \mathbb{Q}(A[2])$ ; or
- $A(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$  and  $A$  has no cyclic degree 4 isogeny over  $\mathbb{Q}$ .

Actually, in many cases Smith proved the Selmer analogue Goldfeld conjecture via establishing that the distribution of  $2^\infty$ -Selmer groups in  $\mathcal{A}$  follows the same principle in the BKLPR conjecture for  $p = 2$ .

**Conjecture 3.9** (Bhargava-Kane-Lenstra-Poonen-Rains). *Let  $\mathfrak{A}_F$  be the set of all isomorphism classes of elliptic curves over a fixed number field  $F$ , ordered by height. For  $r = 0, 1$  and any  $G$  finite symplectic  $p$ -group,*

$$\text{Prob}(\text{Sel}_{p^\infty}(A/F) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus G \mid A \in \mathfrak{A}_F, \epsilon(A) = (-1)^r) = \frac{(\#G)^{1-r}}{\#\text{Sp}(G)} \cdot \prod_{i \geq r} (1 - p^{1-2i}).$$

In particular, the average of  $\#\text{Sel}_2(A/F)$  is 3 and

$$\text{Prob}(\text{rank}_{\mathbb{Z}} A(F) = r \mid A \in \mathfrak{A}_F, \epsilon(A) = (-1)^r) = 1.$$

#### 4. ON QUADRATIC TWIST FAMILIES

**4.1. Equivalence relation for quadratic twist families.** For general quadratic twist families of elliptic curves over  $\mathbb{Q}$ , the distribution of Selmer groups does not follow the BKLPR's principle.

For  $\mathcal{A}$  a quadratic twist family of elliptic curves over  $\mathbb{Q}$ , let  $\Sigma$  be a finite set of places  $\Sigma \supseteq \{p \mid \text{any } A \in \mathcal{A} \text{ has bad reduction at } p\} \cup \{2, \infty\}$ .

**Definition 4.1.**  $A_1, A_2 \in \mathcal{A}$  are called  $\Sigma$ -equivalent if  $A_1 \cong A_2$  over  $\mathbb{Q}_v$  for any  $v \in \Sigma$ .

The root numbers of elliptic curves in a fixed class  $\mathfrak{X}$  are the same, denoted by  $\epsilon(\mathfrak{X})$ .

**4.2. Elliptic curves with full rational 2-torsion.** Recall that we have seen that  $\theta$ -congruent number problem is essentially about quadratic twist families of elliptic curves over  $\mathbb{Q}$  with full rational 2-torsions.

Families  $\mathcal{A}$  over  $\mathbb{Q}$  with full rational 2-torsion points are divided into three types:

- (A)  $\mathcal{A}$  does not have a rational cyclic 4-isogeny, e.g. the congruent number curves  $ny^2 = x^3 - x$ .
- (B)  $\mathcal{A}$  has a rational cyclic 4-isogeny, and  $A[4] \not\subseteq A(\mathbb{Q}(\sqrt{-1}))$  for any  $A \in \mathcal{A}$ , e.g. the tiling number curves  $ny^2 = x(x-3)(x+1)$ .
- (C)  $\mathcal{A}$  has a rational cyclic 4-isogeny, and  $A[4] \subseteq A(\mathbb{Q}(\sqrt{-1}))$  for some  $A \in \mathcal{A}$ . e.g.  $ny^2 = x(x-9)(x-25)$ .

We now discuss the distribution of  $s(A) := \dim_{\mathbb{F}_2} \text{Sel}_2(A/\mathbb{Q})/A(\mathbb{Q})[2]$ .

**4.3. Distribution of 2-Selmer groups for type (A).** For type (A), the distribution of  $2^\infty$ -Selmer groups is independent of equivalence classes  $\mathfrak{X} \subset \mathcal{A}$ .

**Theorem 4.2** (Heath-Brown, Swinnerton-Dyer, Kane). *Let  $\mathcal{A}$  be a quadratic twist family of type (A) and  $\mathfrak{X} \subset \mathcal{A}$  an equivalence class. Let  $t \in \{0, 1\}$  with  $(-1)^t = \epsilon(\mathfrak{X})$ . Then for any  $d \in \mathbb{Z}_{\geq 0}$ ,*

$$\text{Prob}(s(A) = d \mid A \in \mathfrak{X}) = \lim_{k \rightarrow \infty} P_{k;t}^{\text{Alt}}(d),$$

where  $P_{k;t}^{\text{Alt}}(d)$  is the ratio of corank  $d$  matrices in alternating  $(2k+t) \times (2k+t)$  matrices of coefficient  $\mathbb{F}_2$ .

The above result is the starting point of Smith's work on  $2^\infty$ -Selmer groups.

**Corollary 4.3.** *The average of  $\#\text{Sel}_2(A/\mathbb{Q})/A(\mathbb{Q})[2]$  for  $A \in \mathfrak{X}$  of type (A) is always 3.*

**4.4. Distribution of 2-Selmer groups for type (B) and (C).** To describe the distribution of 2-Selmer groups for type (B) and (C), we introduce the following model of alternating matrices.

Let  $t \in \{0, 1\}$ ,  $s \in \{0, 1, 2\}$ ,  $\vec{t} = (t_1, \dots, t_s) \in \mathbb{Z}^s$  such that  $t_i \equiv t \pmod{2}$  for all  $i$ . When  $s = 2$  we require that  $t_1 + t_2 \leq 0$ .

Let  $P_{k;t,\vec{t}}^{\text{Alt}}(d)$  be the ratio of corank  $d$  matrices in alternating  $(2k+t) \times (2k+t)$  matrices of coefficient  $\mathbb{F}_2$  of form

$$\begin{pmatrix} 0 & B_{12} & \cdots & B_{1,s+1} \\ B_{21} & \ddots & \ddots & \vdots \\ \vdots & \ddots & 0 & B_{s,s+1} \\ B_{s+1,1} & \cdots & B_{s+1,s} & B_{s+1,s+1} \end{pmatrix}$$

such that for  $1 \leq i \leq s, 1 \leq j \leq s$ , the  $B_{ij}$  is of size

$$(k + \frac{t_i + t}{2}) \times (k + \frac{t_j + t}{2}).$$

**Theorem 4.4** (Pan-Tian). *Let  $\mathcal{A}$  be a family of type (B) or (C) and  $\mathfrak{X} \subset \mathcal{A}$  an equivalence class. Then there exists  $\vec{t} \in \mathbb{Z}^s$  only dependent on  $\mathfrak{X}$ , with  $s = 1$  for type (B),  $s = 2$  for type (C), such that for any  $d \in \mathbb{Z}_{\geq 0}$ ,*

$$\text{Prob}(s(A) = d \mid A \in \mathfrak{X}) = \lim_{k \rightarrow \infty} P_{k;t,\vec{t}}^{\text{Alt}}(d),$$

*in particular, it is positive if and only if  $d \geq \max_i t_i$  and  $d \equiv t \pmod{2}$ . Moreover, if  $\Sigma \subset \Sigma'$ , then any  $\Sigma'$ -equivalence class  $\mathfrak{X}' \subset \mathfrak{X}$  has the same  $\vec{t}$ .*

We expect to establish the distribution of  $2^\infty$ -Selmer groups starting from this result.

**Corollary 4.5.** *The average of  $\#\text{Sel}_2(A/\mathbb{Q})/A[2]$  for  $A \in \mathfrak{X}$  is equal to  $3 + \sum_i 2^{t_i}$ .*

**Corollary 4.6.** *Let  $A_0 \in \mathfrak{X}$  be any curve which has a bad prime outside  $\Sigma$ . Then*

$$\text{Prob}(s(A) = s(A_0) \mid A \in \mathfrak{X}) > 0.$$

**4.5. Kolyvagin's Question.** Kolyvagin's conjecture is displayed as

$$\min_{A \in \mathcal{A}, \text{sign}(A) = (-1)} \dim_{\mathbb{F}_2} \text{Sel}_2(A)/A[2] = r, \quad r = 0, 1.$$

*Note:* Distribution has nicer behavior when restricted in equivalence classes.

**Conjecture 4.7.** *Given  $\mathcal{A}$ , exists equivalent class  $\mathfrak{X}$  such that  $\vec{t} \leq \begin{cases} \vec{0}, & \text{if } \epsilon(\mathfrak{X}) = +1; \\ \vec{1}, & \text{if } \epsilon(\mathfrak{X}) = -1. \end{cases}$*

For some classes  $\mathfrak{X}$ ,  $\min_{A \in \mathfrak{X}} \dim_{\mathbb{F}_2} \text{Sel}_2(A)/A[2]$  may not reach minimal.

It seems natural to consider the following variation of Kolyvagin's problem:

**Question 4.8.** *For an equivalence class  $\mathfrak{X}$  of quadratic twists of elliptic curves over  $\mathbb{Q}$  and a prime  $p$ , let  $r \in \{0, 1\}$  with  $(-1)^r = \epsilon(\mathfrak{X})$ , what is the behavior of*

$$\min_{A \in \mathfrak{X}, r_A = r} \text{ord}_p \text{III}^{\text{an}}(A),$$

*as  $\mathfrak{X} \subseteq \mathcal{A}$  varies?*

Suitable constructed (arithmetic) theta series on  $\widetilde{\text{SL}}_2$  have Fourier coefficients basically  $W^{\text{an}}(A)$  exactly for  $A \in \mathfrak{X}$ .

**4.6. Arithmetic Rallis inner product formula.** Fix  $\mathbb{H}_v$ -invariant pairings  $(\ , \ )_v$  on  $\pi_v$  such that for any pure tensors  $f_i = (f_{i,U})_U$ ,

$$\Pi_v(f_{1,v}, f_{2,v})_v \doteq f_{1,u} \circ f_{2,U}^N \quad (\text{fixed } \pi_{A,C} \cong \otimes \pi_v).$$

**Theorem 4.9** (He-Xiong-Tian). *For pure tensors  $f_1, f_2 \in \pi_A$  and  $\phi_1, \phi_2 \in \mathcal{S}(\mathbb{V})$ , the following equality holds (with standard measures):*

$$(\vartheta_{\phi_1}^{f_1}, \vartheta_{\phi_2}^{f_2})_{NT} = \frac{L'(1/2, \pi_A)}{L(2, 1_Q)} \cdot \prod_v Z_v(\phi_{1,v}, \phi_{2,v}, f_{1,v}, f_{2,v}),$$

where

$$Z_v(\phi_{1,v}, \phi_{2,v}, f_{1,v}, f_{2,v}) = \frac{L(2, 1_v)}{L(1/2, \pi_v)} \cdot \int_{\mathbb{H}_v} (h\phi_{1,v}, \phi_{2,v})_v (hf_{1,v}, f_{2,v})_v dh.$$

*Remark 4.10.* (1) Previous work on RI were established by (arith.) Siegel-Weil formula and doubling method. Our approach does not involve doubling method, but

- (i) a decomposition formula of Fourier-Whittaker periods, and
  - (ii) Gross-Zagier formula of Yuan-Zhang-Zhang.
- (2) Certain form of ARI was first conjectured by Kudla, and proved by Kudla-Rapoport-Yang et al via an arithmetic Siegel-Weil over  $\mathbb{Q}$  in certain case.
- (3) In the rank 0 case, we have the parallel results and proofs. Our results have application to Kolyvagin's problem.

**4.7. Tunnell Type result.** As a byproduct of the rank 0 case Fourier-Whittaker period formula, we have:

**Theorem 4.11.** *Tunnell Type result holds for general quadratic twist family of elliptic curves over  $\mathbb{Q}$ .*

*Remark 4.12.* (1) For CN curves  $E^{(n)} : ny^2 = x^3 - x$ , we get new formula: For  $n > 0$  square-free

$$\sum_{x^2+2y^2+8z^2=n} (-1)^z = \pm \sum_{x^2+8y^2+16z^2=n} (-1)^{y+z}, \quad 0 < n \equiv 1 \pmod{8},$$

whose square is essentially  $L(E^{(n)}, 1)$ . Similar for other congruent class.

- (2) In general, there may be local obstructions due to Atkin-Lehner involutions: Consider  $A = X_0(14) : y^2 + xy + y = x^3 + 4x - 6$  and  $\mathfrak{X}$  the class of negative fundamental discriminants  $n \equiv -3 \pmod{56}$ . Let

$$Q(x, y, z) = (x + 14y + 4z)^2 + (x - 14y - 2z)^2 + x^2,$$

for each  $n \in \mathfrak{X}$ ,

$$\frac{L(A^{(n)}, 1)}{\Omega(A^{(-1)})/\sqrt{|n|}} = 2 \left( \sum_{\substack{Q(x,y,z)=|n|, \\ 3x+2z \equiv 3 \pmod{4}, \\ 3x+2z \equiv 3 \pmod{7}}} 1 - \sum_{\substack{Q(x,y,z)=|n|, \\ 3x+2z \equiv 3 \pmod{4}, \\ 3x+2z \equiv -3 \pmod{7}}} 1 \right)^2.$$