The arithmetic of quadratic twists of elliptic curves

— In memory of John Henry Coates

Ye Tian

Academy of Mathematics and Systems Science

2022/07/13

The Congruent Number Problem

The Congruent Number Problem

Definition (Congruent number)

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

The Congruent Number Problem

Definition (Congruent number)

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

- 5, 6, 7 are congruent numbers (Fibonacci),

The Congruent Number Problem

Definition (Congruent number)

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

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

The Congruent Number Problem

Definition (Congruent number)

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

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

Example

The number 2022 is congruent with the "simplest" triangle having side lengths

$$\frac{51897851719}{88847070}, \quad \frac{359297551080}{51897851719}, \quad \frac{2693576182377580134961}{4610972064527613330}.$$

The Congruent Number Problem

Definition (Congruent number)

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

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

Example

The number 2022 is congruent with the "simplest" triangle having side lengths

$$\frac{51897851719}{88847070}, \quad \frac{359297551080}{51897851719}, \quad \frac{2693576182377580134961}{4610972064527613330}.$$

The Congruent Number Problem

The congruent number problem is to determine whether or not a given positive integer is congruent number.

Theorem (Heegner 1952)

Any prime or twice of prime congruent to $5, 6, 7 \mod 8$ *is a congruent number.*

Theorem (Heegner 1952)

Any prime or twice of prime congruent to $5, 6, 7 \mod 8$ *is a congruent number.*

Theorem (T 2012)

For any $k \geq 1$*, there are infinitely many congruent numbers among square-free integers* $\equiv 5 \mod 8$ *(resp.* $6 \mod 8$, $7 \mod 8$*) with exact* k *odd prime factors.*

Theorem (Heegner 1952)

Any prime or twice of prime congruent to $5, 6, 7 \mod 8$ *is a congruent number.*

Theorem (T 2012)

For any $k \geq 1$*, there are infinitely many congruent numbers among square-free integers* $\equiv 5 \mod 8$ *(resp.* $6 \mod 8$, $7 \mod 8$*) with exact* k *odd prime factors.*

Theorem (Smith, Yuan-Zhang-T 2014)

At least half of square-free positive integers $\equiv 5, 6, 7 \mod 8$ *are congruent numbers.*

Theorem (Heegner 1952)

Any prime or twice of prime congruent to $5, 6, 7 \mod 8$ *is a congruent number.*

Theorem (T 2012)

For any $k \geq 1$*, there are infinitely many congruent numbers among square-free integers* $\equiv 5 \mod 8$ *(resp.* $6 \mod 8$, $7 \mod 8$*) with exact* k *odd prime factors.*

Theorem (Smith, Yuan-Zhang-T 2014)

At least half of square-free positive integers $\equiv 5, 6, 7 \mod 8$ *are congruent numbers.*

Remark

Our generalization of Heegner's results by introduce an induction argument (on the number k of prime factors), which involves L-functions and Gross-Zagier and Waldspurger formulae.

Quadratic twists of elliptic curves over $\mathbb{Q}$

Quadratic twists of elliptic curves over $\mathbb{Q}$

Congruent number problem is essentially about the quadratic family $ny^2 = x^3 - x$.

Quadratic twists of elliptic curves over $\mathbb{Q}$

Congruent number problem is essentially about the quadratic family $ny^2 = x^3 - x$. In general, for an elliptic curve over $\mathbb{Q}$ given by: $y^2 = x^3 + ax + b$, let $\mathscr{A}$ denote the set of all isomorphism classes of its quadratic twists:

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

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

Quadratic twists of elliptic curves over $\mathbb{Q}$

Congruent number problem is essentially about the quadratic family $ny^2 = x^3 - x$. In general, for an elliptic curve over $\mathbb{Q}$ given by: $y^2 = x^3 + ax + b$, let $\mathscr{A}$ denote the set of all isomorphism classes of its quadratic twists:

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

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

- $\operatorname{rank} A(\mathbb{Q})$, $\#Ш(A/\mathbb{Q})[p^\infty]$, $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(A/\mathbb{Q})$, $\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/\mathbb{Q})$.

Quadratic twists of elliptic curves over $\mathbb{Q}$

Congruent number problem is essentially about the quadratic family $ny^2 = x^3 - x$. In general, for an elliptic curve over $\mathbb{Q}$ given by: $y^2 = x^3 + ax + b$, let $\mathscr{A}$ denote the set of all isomorphism classes of its quadratic twists:

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

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

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

Quadratic twists of elliptic curves over $\mathbb{Q}$

Congruent number problem is essentially about the quadratic family $ny^2 = x^3 - x$. In general, for an elliptic curve over $\mathbb{Q}$ given by: $y^2 = x^3 + ax + b$, let $\mathscr{A}$ denote the set of all isomorphism classes of its quadratic twists:

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

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

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

In this talk, we focus on the **L-function side**, although some of the discussions are related to Selmer groups.

Conjectures on Leading terms of L-series under Quadratic Twists

Conjectures on Leading terms of L-series under Quadratic Twists

Conjecture (Goldfeld)

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$. Then for $r \in \{0, 1\}$

$$\mathrm{Prob}\left(\mathrm{ord}_{s=1} L(A, s) = r \mid A \in \mathscr{A}, \epsilon(A) = (-1)^r\right) = 1.$$

We call the case with $r = 0$ (resp 1) the even (resp. odd) parity Goldfeld conjecture.

Conjectures on Leading terms of L-series under Quadratic Twists

Conjecture (Goldfeld)

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$. Then for $r \in \{0, 1\}$

$$\mathrm{Prob}\left(\mathrm{ord}_{s=1} L(A, s) = r \mid A \in \mathscr{A}, \epsilon(A) = (-1)^r\right) = 1.$$

We call the case with $r = 0$ (resp 1) the even (resp. odd) parity Goldfeld conjecture.

The behavior for Ш^{an} is subtle. However, Kolyvagin proposed the following

Conjectures on Leading terms of L-series under Quadratic Twists

Conjecture (Goldfeld)

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$. Then for $r \in \{0, 1\}$

$$\mathrm{Prob}\left(\mathrm{ord}_{s=1} L(A, s) = r \mid A \in \mathscr{A}, \epsilon(A) = (-1)^r\right) = 1.$$

We call the case with $r = 0$ (resp 1) the even (resp. odd) parity Goldfeld conjecture.

The behavior for $Ш^{an}$ is subtle. However, Kolyvagin proposed the following

Conjecture (Kolyvagin)

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$ and p any prime. There exists $A \in \mathscr{A}$ such that

Conjectures on Leading terms of L-series under Quadratic Twists

Conjecture (Goldfeld)

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$. Then for $r \in \{0, 1\}$

$$\mathrm{Prob}\left(\mathrm{ord}_{s=1} L(A, s) = r \mid A \in \mathscr{A}, \epsilon(A) = (-1)^r\right) = 1.$$

We call the case with $r = 0$ (resp 1) the even (resp. odd) parity Goldfeld conjecture.

The behavior for $Ш^{an}$ is subtle. However, Kolyvagin proposed the following

Conjecture (Kolyvagin)

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$ and p any prime. There exists $A \in \mathscr{A}$ such that

- $\mathrm{ord}_{s=1} L(A, s) = 0$ *(resp. 1).*

Conjectures on Leading terms of L-series under Quadratic Twists

Conjecture (Goldfeld)

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$. Then for $r \in \{0, 1\}$

$$\operatorname{Prob}\left(\operatorname{ord}_{s=1} L(A, s) = r \mid A \in \mathscr{A}, \epsilon(A) = (-1)^r\right) = 1.$$

We call the case with $r = 0$ (resp 1) the even (resp. odd) parity Goldfeld conjecture.

The behavior for $Ш^{an}$ is subtle. However, Kolyvagin proposed the following

Conjecture (Kolyvagin)

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$ and p any prime. There exists $A \in \mathscr{A}$ such that

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

Goldfeld Conjecture for CM Families

Goldfeld Conjecture for CM Families

Theorem A

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 2 splits in the CM field.*

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

Goldfeld Conjecture for CM Families

Theorem A

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 2 splits in the CM field.*

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

The proof of the result consists of two parts.

Goldfeld Conjecture for CM Families

Theorem A

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 2 splits in the CM field.*

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

The proof of the result consists of two parts.

Theorem A1 (Burungale-T, Burungale-Castella-Skinner-T)

Let A be a CM elliptic curve over $\mathbb{Q}$, p a prime and $r = 0, 1$. Then the rank r p-converse holds:

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

provided that p is ordinary if $r = 1$.

Goldfeld Conjecture for CM Families

Theorem A

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 2 splits in the CM field.*

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

The proof of the result consists of two parts.

Theorem A1 (Burungale-T, Burungale-Castella-Skinner-T)

Let A be a CM elliptic curve over $\mathbb{Q}$, p a prime and $r = 0, 1$. Then the rank r p-converse holds:

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

provided that p is ordinary if $r = 1$.

Theorem A2 (Smith)

The 2^∞-Selmer analogue Goldfeld conjecture holds for families $\mathscr{A}$ over $\mathbb{Q}$ satisfying the following assumption S.

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

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

- $A(\mathbb{Q})[2] = 0$; or

Assumption S: There is $A \in \mathscr{A}$ 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 $A \to A_0$, $\mathbb{Q}(A_0[2]) \neq \mathbb{Q}, \mathbb{Q}(A[2])$; or

Assumption S: There is $A \in \mathscr{A}$ 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 $A \to A_0$, $\mathbb{Q}(A_0[2]) \neq \mathbb{Q}, \mathbb{Q}(A[2])$; or
- $A(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ and A has no cyclic degree 4 isogeny over $\mathbb{Q}$.

Assumption S: There is $A \in \mathscr{A}$ 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 $A \to A_0$, $\mathbb{Q}(A_0[2]) \neq \mathbb{Q}, \mathbb{Q}(A[2])$; 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^∞-Selmer groups in $\mathscr{A}$ follows the same principle in the BKLPR conjecture for $p = 2$.

Assumption S: There is $A \in \mathscr{A}$ 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 $A \to A_0$, $\mathbb{Q}(A_0[2]) \neq \mathbb{Q}, \mathbb{Q}(A[2])$; 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^∞-Selmer groups in $\mathscr{A}$ follows the same principle in the BKLPR conjecture for $p = 2$.

Conjecture (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,

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

Assumption S: There is $A \in \mathscr{A}$ 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 $A \to A_0$, $\mathbb{Q}(A_0[2]) \neq \mathbb{Q}, \mathbb{Q}(A[2])$; 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^∞-Selmer groups in $\mathscr{A}$ follows the same principle in the BKLPR conjecture for $p = 2$.

Conjecture (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,

$$\mathrm{Prob}\left(\mathrm{Sel}_{p^\infty}(A/F) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r \bigoplus G \;\middle|\; A \in \mathfrak{A}_F, \epsilon(A) = (-1)^r\right) = \frac{(\#G)^{1-r}}{\#\mathrm{Sp}(G)} \cdot \prod_{i \geq r}(1 - p^{1-2i}).$$

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

$$\mathrm{Prob}\left(\mathrm{rank}\, A(F) = r \;\middle|\; A \in \mathfrak{A}_F, \epsilon(A) = (-1)^r\right) = 1.$$

Equivalence relation for quadratic twist families

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.

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 $\mathscr{A}$ a quadratic twist family of elliptic curves over $\mathbb{Q}$, let Σ be a finite set of places

$$\Sigma \supseteq \{p \mid \text{any } A \in \mathscr{A} \text{ has bad reduction at } p\} \cup \{2, \infty\}.$$

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 $\mathscr{A}$ a quadratic twist family of elliptic curves over $\mathbb{Q}$, let Σ be a finite set of places

$$\Sigma \supseteq \{p \mid \text{any } A \in \mathscr{A} \text{ has bad reduction at } p\} \cup \{2, \infty\}.$$

Definition

Two elliptic curves in $\mathscr{A}$ are called Σ-equivalent if they are isomorphic over $\mathbb{Q}_v$ for all $v \in \Sigma$.

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 $\mathscr{A}$ a quadratic twist family of elliptic curves over $\mathbb{Q}$, let Σ be a finite set of places

$$\Sigma \supseteq \{p \mid \text{any } A \in \mathscr{A} \text{ has bad reduction at } p\} \cup \{2, \infty\}.$$

Definition

Two elliptic curves in $\mathscr{A}$ are called Σ-equivalent if they are isomorphic over $\mathbb{Q}_v$ for all $v \in \Sigma$.

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

Elliptic curves with full rational 2-torsion

Elliptic curves with full rational 2-torsion

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

Elliptic curves with full rational 2-torsion

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

(A) $\mathscr{A}$ does not have a rational cyclic 4-isogeny, e.g. the congruent number curves $ny^2 = x^3 - x$.

Elliptic curves with full rational 2-torsion

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

(A) $\mathscr{A}$ does not have a rational cyclic 4-isogeny, e.g. the congruent number curves $ny^2 = x^3 - x$.

(B) $\mathscr{A}$ has a rational cyclic 4-isogeny, and $A[4] \not\subset A(\mathbb{Q}(\sqrt{-1}))$ for any $A \in \mathscr{A}$, e.g. $ny^2 = x(x-3)(x+1)$.

Elliptic curves with full rational 2-torsion

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

(A) $\mathscr{A}$ does not have a rational cyclic 4-isogeny, e.g. the congruent number curves $ny^2 = x^3 - x$.

(B) $\mathscr{A}$ has a rational cyclic 4-isogeny, and $A[4] \not\subseteq A(\mathbb{Q}(\sqrt{-1}))$ for any $A \in \mathscr{A}$, e.g. $ny^2 = x(x-3)(x+1)$.

(C) $\mathscr{A}$ has a rational cyclic 4-isogeny, and $A[4] \subseteq A(\mathbb{Q}(\sqrt{-1}))$ for some $A \in \mathscr{A}$. e.g. $ny^2 = x(x-9)(x-25)$.

Elliptic curves with full rational 2-torsion

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

(A) $\mathscr{A}$ does not have a rational cyclic 4-isogeny, e.g. the congruent number curves $ny^2 = x^3 - x$.

(B) $\mathscr{A}$ has a rational cyclic 4-isogeny, and $A[4] \not\subseteq A(\mathbb{Q}(\sqrt{-1}))$ for any $A \in \mathscr{A}$, e.g. $ny^2 = x(x-3)(x+1)$.

(C) $\mathscr{A}$ has a rational cyclic 4-isogeny, and $A[4] \subseteq A(\mathbb{Q}(\sqrt{-1}))$ for some $A \in \mathscr{A}$. e.g. $ny^2 = x(x-9)(x-25)$.

We now discuss the distribution of 2-Selmer group $\mathrm{Sel}_2(A/\mathbb{Q})$.

Distribution of 2-Selmer groups for type (A)

Distribution of 2-Selmer groups for type (A)

For type (A), the distribution of 2^∞-Selmer groups is independent of equivalence classes $\mathfrak{X} \subset \mathscr{A}$.

Distribution of 2-Selmer groups for type (A)

For type (A), the distribution of 2^∞-Selmer groups is independent of equivalence classes $\mathfrak{X} \subset \mathscr{A}$.

Theorem (Heath-Brown, Swinnetron-Dyer, Kane)

Let $\mathscr{A}$ be a quadratic twist family of type (A) and $\mathfrak{X} \subset \mathscr{A}$ an equivalence class. Then for any $d \in \mathbb{Z}_{\geq 0}$ with $(-1)^d = \epsilon(\mathfrak{X})$,

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/\mathbb{Q})/A(\mathbb{Q})[2] = d \;\middle|\; A \in \mathfrak{X}\right) = 2\prod_{j=0}^{\infty}(1+2^{-j})^{-1}\prod_{i=1}^{d}\frac{2}{2^i-1}.$$

Distribution of 2-Selmer groups for type (A)

For type (A), the distribution of 2^∞-Selmer groups is independent of equivalence classes $\mathfrak{X} \subset \mathscr{A}$.

Theorem (Heath-Brown, Swinnetron-Dyer, Kane)

Let $\mathscr{A}$ be a quadratic twist family of type (A) and $\mathfrak{X} \subset \mathscr{A}$ an equivalence class. Then for any $d \in \mathbb{Z}_{\geq 0}$ with $(-1)^d = \epsilon(\mathfrak{X})$,

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/\mathbb{Q})/A(\mathbb{Q})[2] = d \;\middle|\; A \in \mathfrak{X}\right) = 2\prod_{j=0}^{\infty}(1+2^{-j})^{-1}\prod_{i=1}^{d}\frac{2}{2^i-1}.$$

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

Distribution of 2-Selmer groups for type (A)

For type (A), the distribution of 2^∞-Selmer groups is independent of equivalence classes $\mathfrak{X} \subset \mathscr{A}$.

Theorem (Heath-Brown, Swinnetron-Dyer, Kane)

Let $\mathscr{A}$ be a quadratic twist family of type (A) and $\mathfrak{X} \subset \mathscr{A}$ an equivalence class. Then for any $d \in \mathbb{Z}_{\geq 0}$ with $(-1)^d = \epsilon(\mathfrak{X})$,

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/\mathbb{Q})/A(\mathbb{Q})[2] = d \,\middle|\, A \in \mathfrak{X}\right) = 2\prod_{j=0}^{\infty}(1+2^{-j})^{-1}\prod_{i=1}^{d}\frac{2}{2^i-1}.$$

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

Corollary

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

Distribution of 2-Selmer groups for type (B) and (C)

Distribution of 2-Selmer groups for type (B) and (C)

Theorem (Pan-T)

Let $\mathscr{A}$ be a family of type (B) or (C) and $\mathfrak{X} \subset \mathscr{A}$ an equivalence class. Then there is $t \in \mathbb{Z}$ for type (B), $t = (t_1, t_2) \in \mathbb{Z}^2$ for type (C), only dependent on $\mathfrak{X}$, with

$$(-1)^t = \epsilon(\mathfrak{X}) \text{ for type (B)}, \qquad (-1)^{t_i} = \epsilon(\mathfrak{X}),\ t_1 + t_2 \leq 0 \text{ for type (C)},$$

such that for any integer $d \geq 0$ with $(-1)^d = \epsilon(\mathfrak{X})$,

Distribution of 2-Selmer groups for type (B) and (C)

Theorem (Pan-T)

Let $\mathscr{A}$ be a family of type (B) or (C) and $\mathfrak{X} \subset \mathscr{A}$ an equivalence class. Then there is $t \in \mathbb{Z}$ for type (B), $t = (t_1, t_2) \in \mathbb{Z}^2$ for type (C), only dependent on $\mathfrak{X}$, with

$$(-1)^t = \epsilon(\mathfrak{X}) \text{ for type (B)}, \qquad (-1)^{t_i} = \epsilon(\mathfrak{X}),\ t_1 + t_2 \leq 0 \text{ for type (C)},$$

such that for any integer $d \geq 0$ with $(-1)^d = \epsilon(\mathfrak{X})$,

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/\mathbb{Q})/A[2] = d \,\middle|\, A \in \mathfrak{X}\right) = \alpha_{d,t} \prod_{i=1}^{\infty} (1 - 2^{-i}),$$

Distribution of 2-Selmer groups for type (B) and (C)

Theorem (Pan-T)

Let $\mathscr{A}$ be a family of type (B) or (C) and $\mathfrak{X} \subset \mathscr{A}$ an equivalence class. Then there is $t \in \mathbb{Z}$ for type (B), $t = (t_1, t_2) \in \mathbb{Z}^2$ for type (C), only dependent on $\mathfrak{X}$, with

$$(-1)^t = \epsilon(\mathfrak{X}) \text{ for type (B)}, \qquad (-1)^{t_i} = \epsilon(\mathfrak{X}),\ t_1 + t_2 \leq 0 \text{ for type (C)},$$

such that for any integer $d \geq 0$ with $(-1)^d = \epsilon(\mathfrak{X})$,

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/\mathbb{Q})/A[2] = d \,\middle|\, A \in \mathfrak{X}\right) = \alpha_{d,t} \prod_{i=1}^{\infty}(1 - 2^{-i}),$$

where $\alpha_{d,t} = 0$ if $d < t$ $(\max\{t_i\})$, otherwise $\alpha_{d,t} \in \mathbb{Q}_{>0}$ only dependent on d and t.

Distribution of 2-Selmer groups for type (B) and (C)

Theorem (Pan-T)

Let $\mathscr{A}$ be a family of type (B) or (C) and $\mathfrak{X} \subset \mathscr{A}$ an equivalence class. Then there is $t \in \mathbb{Z}$ for type (B), $t = (t_1, t_2) \in \mathbb{Z}^2$ for type (C), only dependent on $\mathfrak{X}$, with

$$(-1)^t = \epsilon(\mathfrak{X}) \text{ for type (B)}, \qquad (-1)^{t_i} = \epsilon(\mathfrak{X}),\ t_1 + t_2 \le 0 \text{ for type (C)},$$

such that for any integer $d \ge 0$ with $(-1)^d = \epsilon(\mathfrak{X})$,

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/\mathbb{Q})/A[2] = d \;\middle|\; A \in \mathfrak{X}\right) = \alpha_{d,t} \prod_{i=1}^{\infty} (1 - 2^{-i}),$$

where $\alpha_{d,t} = 0$ if $d < t$ $(\max\{t_i\})$, otherwise $\alpha_{d,t} \in \mathbb{Q}_{>0}$ only dependent on d and t. Moreover, if $\Sigma \subset \Sigma'$, then any Σ'-equivalence class $\mathfrak{X}' \subset \mathfrak{X}$ has the same t and $\alpha_{d,t}$.

Distribution of 2-Selmer groups for type (B) and (C)

Theorem (Pan-T)

Let $\mathscr{A}$ be a family of type (B) or (C) and $\mathfrak{X} \subset \mathscr{A}$ an equivalence class. Then there is $t \in \mathbb{Z}$ for type (B), $t = (t_1, t_2) \in \mathbb{Z}^2$ for type (C), only dependent on $\mathfrak{X}$, with

$$(-1)^t = \epsilon(\mathfrak{X}) \text{ for type (B)}, \qquad (-1)^{t_i} = \epsilon(\mathfrak{X}),\ t_1 + t_2 \leq 0 \text{ for type (C)},$$

such that for any integer $d \geq 0$ with $(-1)^d = \epsilon(\mathfrak{X})$,

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/\mathbb{Q})/A[2] = d \;\middle|\; A \in \mathfrak{X}\right) = \alpha_{d,t} \prod_{i=1}^{\infty} (1 - 2^{-i}),$$

where $\alpha_{d,t} = 0$ if $d < t$ $(\max\{t_i\})$, otherwise $\alpha_{d,t} \in \mathbb{Q}_{>0}$ only dependent on d and t. Moreover, if $\Sigma \subset \Sigma'$, then any Σ'-equivalence class $\mathfrak{X}' \subset \mathfrak{X}$ has the same t and $\alpha_{d,t}$.

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

Distribution of 2-Selmer groups for type (B) and (C)

Theorem (Pan-T)

Let $\mathscr{A}$ be a family of type (B) or (C) and $\mathfrak{X} \subset \mathscr{A}$ an equivalence class. Then there is $t \in \mathbb{Z}$ for type (B), $t = (t_1, t_2) \in \mathbb{Z}^2$ for type (C), only dependent on $\mathfrak{X}$, with

$$(-1)^t = \epsilon(\mathfrak{X}) \text{ for type (B)}, \qquad (-1)^{t_i} = \epsilon(\mathfrak{X}),\ t_1 + t_2 \leq 0 \text{ for type (C)},$$

such that for any integer $d \geq 0$ with $(-1)^d = \epsilon(\mathfrak{X})$,

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_2} \mathrm{Sel}_2(A/\mathbb{Q})/A[2] = d \;\middle|\; A \in \mathfrak{X}\right) = \alpha_{d,t} \prod_{i=1}^{\infty} (1 - 2^{-i}),$$

where $\alpha_{d,t} = 0$ if $d < t$ ($\max\{t_i\}$), otherwise $\alpha_{d,t} \in \mathbb{Q}_{>0}$ only dependent on d and t. Moreover, if $\Sigma \subset \Sigma'$, then any Σ'-equivalence class $\mathfrak{X}' \subset \mathfrak{X}$ has the same t and $\alpha_{d,t}$.

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

Corollary

The average of $\# \mathrm{Sel}_2(A/\mathbb{Q})/A[2]$ for $A \in \mathfrak{X}$ is equal to $3 + 2^t$ for type (B) and $3 + 2^{t_1} + 2^{t_2}$ for type (C).

Kolyvagin's Question

Kolyvagin's Question

Now we are in the situation that

Kolyvagin's Question

Now we are in the situation that

- Kolyvagin's conjecture predicts that for $r = 0, 1$,

$$\min_{A \in \mathscr{A}, \mathrm{sign}(A) = (-1)^r} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A)/A[2] = r.$$

Kolyvagin's Question

Now we are in the situation that

- Kolyvagin's conjecture predicts that for $r = 0, 1$,

$$\min_{A \in \mathscr{A}, \mathrm{sign}(A) = (-1)^r} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A)/A[2] = r.$$

- distribution has nicer behavior when restricted in equivalence classes, but for some classes $\mathfrak{X}$, $\min_{A \in \mathfrak{X}} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A)/A[2]$ may not reach minimal (i.e. 0 or 1 according to sign).

Kolyvagin's Question

Now we are in the situation that

- Kolyvagin's conjecture predicts that for $r = 0, 1$,

$$\min_{A \in \mathscr{A}, \mathrm{sign}(A) = (-1)^r} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A)/A[2] = r.$$

- distribution has nicer behavior when restricted in equivalence classes, but for some classes $\mathfrak{X}$, $\min_{A \in \mathfrak{X}} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A)/A[2]$ may not reach minimal (i.e. 0 or 1 according to sign).

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

Kolyvagin's Question

Now we are in the situation that

- Kolyvagin's conjecture predicts that for $r = 0, 1$,

$$\min_{A \in \mathscr{A}, \mathrm{sign}(A) = (-1)^r} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A)/A[2] = r.$$

- distribution has nicer behavior when restricted in equivalence classes, but for some classes $\mathfrak{X}$, $\min_{A \in \mathfrak{X}} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A)/A[2]$ may not reach minimal (i.e. 0 or 1 according to sign).

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

Question

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

$$\min_{A \in \mathfrak{X}, r_A = r} \mathrm{ord}_p \text{Ш}^{an}(A), \qquad \textit{as } \mathfrak{X} \subseteq \mathscr{A} \textit{ varies?}$$

Kolyvagin's Question

Now we are in the situation that

- Kolyvagin's conjecture predicts that for $r = 0, 1$,

$$\min_{A \in \mathscr{A}, \mathrm{sign}(A) = (-1)^r} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A)/A[2] = r.$$

- distribution has nicer behavior when restricted in equivalence classes, but for some classes $\mathfrak{X}$, $\min_{A \in \mathfrak{X}} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(A)/A[2]$ may not reach minimal (i.e. 0 or 1 according to sign).

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

Question

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

$$\min_{A \in \mathfrak{X}, r_A = r} \mathrm{ord}_p \text{Ш}^{an}(A), \qquad \text{as } \mathfrak{X} \subseteq \mathscr{A} \text{ varies?}$$

Suitable constructed (arithmetic) theta series on $\widetilde{\mathrm{SL}_2}$ have Fourier coefficients basically $\text{Ш}^{an}(A)$ exactly for $A \in \mathfrak{X}$ with $r_A \in \{0, 1\}$ and $(-1)^{r_A} = \epsilon(\mathfrak{X})$.

Modularity of Heegner cycles

Modularity of Heegner cycles

the classical theta lifting.

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;
- B: a quaternion algebra over $\mathbb{Q}$ and $V = B^{\mathrm{tr}=0}$;

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;
- B: a quaternion algebra over $\mathbb{Q}$ and $V = B^{\mathrm{tr}=0}$;
- $H = PB^\times$ and $\mathbb{G} = \widetilde{\mathrm{SL}_2(\mathbb{A})}$;

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;
- B: a quaternion algebra over $\mathbb{Q}$ and $V = B^{\mathrm{tr}=0}$;
- $H = PB^\times$ and $\mathbb{G} = \widetilde{\mathrm{SL}_2(\mathbb{A})}$;
- $\mathscr{S}(V_\mathbb{A})$: the Weil representation $\omega = \omega_\psi$ of $H_\mathbb{A} \times \mathbb{G}$.

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;
- B: a quaternion algebra over $\mathbb{Q}$ and $V = B^{\mathrm{tr}=0}$;
- $H = PB^\times$ and $\mathbb{G} = \widetilde{\mathrm{SL}_2(\mathbb{A})}$;
- $\mathscr{S}(V_\mathbb{A})$: the Weil representation $\omega = \omega_\psi$ of $H_\mathbb{A} \times \mathbb{G}$.

For an automorphic $\pi \subset \mathscr{A}(H_\mathbb{A})$, the theta kernels $\theta_\phi := \sum_{x \in V(\mathbb{Q})} \omega(g, h)\phi(x)$ define its lifting $\theta(\pi) \subset \mathscr{A}(\mathbb{G})$.

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;
- B: a quaternion algebra over $\mathbb{Q}$ and $V = B^{\mathrm{tr}=0}$;
- $H = PB^\times$ and $\mathbb{G} = \widetilde{\mathrm{SL}_2(\mathbb{A})}$;
- $\mathscr{S}(V_\mathbb{A})$: the Weil representation $\omega = \omega_\psi$ of $H_\mathbb{A} \times \mathbb{G}$.

For an automorphic $\pi \subset \mathscr{A}(H_\mathbb{A})$, the theta kernels $\theta_\phi := \sum_{x \in V(\mathbb{Q})} \omega(g, h)\phi(x)$ define its lifting $\theta(\pi) \subset \mathscr{A}(\mathbb{G})$.

the arithmetic theta lifting:

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;
- B: a quaternion algebra over $\mathbb{Q}$ and $V = B^{\mathrm{tr}=0}$;
- $H = PB^\times$ and $\mathbb{G} = \widetilde{\mathrm{SL}_2(\mathbb{A})}$;
- $\mathscr{S}(V_\mathbb{A})$: the Weil representation $\omega = \omega_\psi$ of $H_\mathbb{A} \times \mathbb{G}$.

For an automorphic $\pi \subset \mathscr{A}(H_\mathbb{A})$, the theta kernels $\theta_\phi := \sum_{x\in V(\mathbb{Q})} \omega(g,h)\phi(x)$ define its lifting $\theta(\pi) \subset \mathscr{A}(\mathbb{G})$.

the arithmetic theta lifting:

- $\mathbb{B}$: an incoherent definite quaternion algebra over $\mathbb{A}$ and $\mathbb{V} = \mathbb{B}^{\mathrm{tr}=0}$.

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;
- B: a quaternion algebra over $\mathbb{Q}$ and $V = B^{\mathrm{tr}=0}$;
- $H = PB^\times$ and $\mathbb{G} = \widetilde{\mathrm{SL}_2(\mathbb{A})}$;
- $\mathscr{S}(V_\mathbb{A})$: the Weil representation $\omega = \omega_\psi$ of $H_\mathbb{A} \times \mathbb{G}$.

For an automorphic $\pi \subset \mathscr{A}(H_\mathbb{A})$, the theta kernels $\theta_\phi := \sum_{x \in V(\mathbb{Q})} \omega(g, h)\phi(x)$ define its lifting $\theta(\pi) \subset \mathscr{A}(\mathbb{G})$.

the arithmetic theta lifting:

- $\mathbb{B}$: an incoherent definite quaternion algebra over $\mathbb{A}$ and $\mathbb{V} = \mathbb{B}^{\mathrm{tr}=0}$.
- $\mathscr{S}(\mathbb{V})$: the Weil representation of $\mathbb{H} \times \mathbb{G}$, $\mathbb{H} = \mathbb{A}^\times\backslash\mathbb{B}^\times$.

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;
- B: a quaternion algebra over $\mathbb{Q}$ and $V = B^{\mathrm{tr}=0}$;
- $H = PB^\times$ and $\mathbb{G} = \widetilde{\mathrm{SL}_2(\mathbb{A})}$;
- $\mathscr{S}(V_\mathbb{A})$: the Weil representation $\omega = \omega_\psi$ of $H_\mathbb{A} \times \mathbb{G}$.

For an automorphic $\pi \subset \mathscr{A}(H_\mathbb{A})$, the theta kernels $\theta_\phi := \sum_{x\in V(\mathbb{Q})} \omega(g,h)\phi(x)$ define its lifting $\theta(\pi) \subset \mathscr{A}(\mathbb{G})$.

the arithmetic theta lifting:

- $\mathbb{B}$: an incoherent definite quaternion algebra over $\mathbb{A}$ and $\mathbb{V} = \mathbb{B}^{\mathrm{tr}=0}$.
- $\mathscr{S}(\mathbb{V})$: the Weil representation of $\mathbb{H} \times \mathbb{G}$, $\mathbb{H} = \mathbb{A}^\times\backslash\mathbb{B}^\times$.
- $X = \varprojlim_U X_U$: the Shimura curve over $\mathbb{Q}$ for $\mathbb{H}$, and J its Jacobian.

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;
- B: a quaternion algebra over $\mathbb{Q}$ and $V = B^{\mathrm{tr}=0}$;
- $H = PB^\times$ and $\mathbb{G} = \widetilde{\mathrm{SL}_2(\mathbb{A})}$;
- $\mathscr{S}(V_\mathbb{A})$: the Weil representation $\omega = \omega_\psi$ of $H_\mathbb{A} \times \mathbb{G}$.

For an automorphic $\pi \subset \mathscr{A}(H_\mathbb{A})$, the theta kernels $\theta_\phi := \sum_{x \in V(\mathbb{Q})} \omega(g, h)\phi(x)$ define its lifting $\theta(\pi) \subset \mathscr{A}(\mathbb{G})$.

the arithmetic theta lifting:

- $\mathbb{B}$: an incoherent definite quaternion algebra over $\mathbb{A}$ and $\mathbb{V} = \mathbb{B}^{\mathrm{tr}=0}$.
- $\mathscr{S}(\mathbb{V})$: the Weil representation of $\mathbb{H} \times \mathbb{G}$, $\mathbb{H} = \mathbb{A}^\times\backslash\mathbb{B}^\times$.
- $X = \varprojlim_U X_U$: the Shimura curve over $\mathbb{Q}$ for $\mathbb{H}$, and J its Jacobian.
- $\pi_A := \mathrm{Hom}(J, A)_\mathbb{Q}$, where $A/\mathbb{Q}$ is an e.c. with sign -1 parameterized by X.

Modularity of Heegner cycles

the classical theta lifting.

- $\psi : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$: a fixed non-trivial additive character;
- B: a quaternion algebra over $\mathbb{Q}$ and $V = B^{\mathrm{tr}=0}$;
- $H = PB^\times$ and $\mathbb{G} = \widetilde{\mathrm{SL}_2(\mathbb{A})}$;
- $\mathscr{S}(V_\mathbb{A})$: the Weil representation $\omega = \omega_\psi$ of $H_\mathbb{A} \times \mathbb{G}$.

For an automorphic $\pi \subset \mathscr{A}(H_\mathbb{A})$, the theta kernels $\theta_\phi := \sum_{x\in V(\mathbb{Q})} \omega(g,h)\phi(x)$ define its lifting $\theta(\pi) \subset \mathscr{A}(\mathbb{G})$.

the arithmetic theta lifting:

- $\mathbb{B}$: an incoherent definite quaternion algebra over $\mathbb{A}$ and $\mathbb{V} = \mathbb{B}^{\mathrm{tr}=0}$.
- $\mathscr{S}(\mathbb{V})$: the Weil representation of $\mathbb{H} \times \mathbb{G}$, $\mathbb{H} = \mathbb{A}^\times\backslash\mathbb{B}^\times$.
- $X = \varprojlim_U X_U$: the Shimura curve over $\mathbb{Q}$ for $\mathbb{H}$, and J its Jacobian.
- $\pi_A := \mathrm{Hom}(J, A)_\mathbb{Q}$, where $A/\mathbb{Q}$ is an e.c. with sign -1 parameterized by X.

Definition (Yuan-Zhang-Zhang, Arithmatic theta lifting)

There is the theta kernel ϑ_ϕ (using CM points) such that the arithmetic theta lifting of π_A:

$$\vartheta(\pi_A) := \{\vartheta_\phi^f = f \circ \vartheta_\phi \mid f \in \pi_A, \phi \in \mathscr{S}(\mathbb{V})\} \subset \mathscr{A}(\mathbb{G}) \otimes_\mathbb{Q} A(\mathbb{Q})_\mathbb{Q},$$

is a representation of $\mathbb{G}$ with the pairing $(\ ,\ )_{NT}$ given by the Néron -Tate height.

Arithmetic Rallis inner product formula

Arithmetic Rallis inner product formula

Fix $\mathbb{H}_v$-invariant pairings $(\ ,\ )_v$ on π_v such that for any pure tensors $f_i = (f_{i,U})_U$,

$$\prod_v (f_{1,v}, f_{2,v})_v \doteq f_{1,U} \circ f_{2,U}^{\vee} \qquad (\text{fixed} \quad \pi_{A,\mathbb{C}} \cong \otimes \pi_v).$$

Arithmetic Rallis inner product formula

Fix $\mathbb{H}_v$-invariant pairings $(\ ,\ )_v$ on π_v such that for any pure tensors $f_i = (f_{i,U})_U$,

$$\prod_v (f_{1,v}, f_{2,v})_v \doteq f_{1,U} \circ f_{2,U}^\vee \qquad (\text{fixed} \quad \pi_{A,\mathbb{C}} \cong \otimes \pi_v).$$

Theorem C1 (He-Xiong-T)

For pure tensors $f_1, f_2 \in \pi_A$ and $\phi_1, \phi_2 \in \mathscr{S}(\mathbb{V})$, the following equality holds (with standard measures):

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

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

Arithmetic Rallis inner product formula

Fix $\mathbb{H}_v$-invariant pairings $(\ ,\ )_v$ on π_v such that for any pure tensors $f_i = (f_{i,U})_U$,

$$\prod_v (f_{1,v}, f_{2,v})_v \doteq f_{1,U} \circ f_{2,U}^{\vee} \qquad (\text{fixed} \quad \pi_{A,\mathbb{C}} \cong \otimes \pi_v).$$

Theorem C1 (He-Xiong-T)

For pure tensors $f_1, f_2 \in \pi_A$ and $\phi_1, \phi_2 \in \mathscr{S}(\mathbb{V})$, the following equality holds (with standard measures):

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

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

Remark

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 Whittaker periods and (ii) Gross-Zagier formula of Yuan-Zhang-Zhang.

Arithmetic Rallis inner product formula

Fix $\mathbb{H}_v$-invariant pairings $(\ ,\ )_v$ on π_v such that for any pure tensors $f_i = (f_{i,U})_U$,

$$\prod_v (f_{1,v}, f_{2,v})_v \doteq f_{1,U} \circ f_{2,U}^{\vee} \qquad (\text{fixed} \quad \pi_{A,\mathbb{C}} \cong \otimes \pi_v).$$

Theorem C1 (He-Xiong-T)

For pure tensors $f_1, f_2 \in \pi_A$ and $\phi_1, \phi_2 \in \mathscr{S}(\mathbb{V})$, the following equality holds (with standard measures):

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

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

Remark

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 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 etal via an arithmetic Siegel-Weil over $\mathbb{Q}$ in certain case.

Application to Kolyvagin's Problem

Application to Kolyvagin's Problem

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$.

Application to Kolyvagin's Problem

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$.

- $(\mathfrak{X}_1, \mathfrak{X}_2, A)$: $\epsilon(\mathfrak{X}_1) = -1,\ \epsilon(\mathfrak{X}_2) = +1$ s.t $D_1 D_2 < 0$ for $A^{(D_i)} \in \mathfrak{X}_i$;

Application to Kolyvagin's Problem

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$.

- $(\mathfrak{X}_1, \mathfrak{X}_2, A)$: $\epsilon(\mathfrak{X}_1) = -1,\ \epsilon(\mathfrak{X}_2) = +1$ s.t $D_1 D_2 < 0$ for $A^{(D_i)} \in \mathfrak{X}_i$;
- π_A on $\mathbb{H}^\times$ and $\mathbb{V} = \mathbb{B}^{tr=0}$,

Application to Kolyvagin's Problem

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$.

- $(\mathfrak{X}_1, \mathfrak{X}_2, A)$: $\epsilon(\mathfrak{X}_1) = -1$, $\epsilon(\mathfrak{X}_2) = +1$ s.t $D_1 D_2 < 0$ for $A^{(D_i)} \in \mathfrak{X}_i$;
- π_A on $\mathbb{H}^\times$ and $\mathbb{V} = \mathbb{B}^{tr=0}$,
- $(f \in \pi_A, \phi \in \mathscr{S}(\mathbb{V}))$ sutible test vector, (f_{D_1}, ϕ_{D_1}) its twist.

Application to Kolyvagin's Problem

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$.

- $(\mathfrak{X}_1, \mathfrak{X}_2, A)$: $\epsilon(\mathfrak{X}_1) = -1,\ \epsilon(\mathfrak{X}_2) = +1$ s.t $D_1 D_2 < 0$ for $A^{(D_i)} \in \mathfrak{X}_i$;
- π_A on $\mathbb{H}^\times$ and $\mathbb{V} = \mathbb{B}^{tr=0}$,
- $(f \in \pi_A, \phi \in \mathscr{S}(\mathbb{V}))$ sutible test vector, (f_{D_1}, ϕ_{D_1}) its twist.

Consider the integral structure

$$\vartheta_{\phi_{D_1}}^{f_{D_1}} = p^{u_{D_1}} \cdot \vartheta_{D_1,0}, \qquad u_{D_1} \doteq \frac{1}{2} \min_{D_2} \sum_i \operatorname{ord}_p Ш^{an}(A^{(D_i)}),$$

and $\vartheta_{D_1,0}$ primitive.

Application to Kolyvagin's Problem

Let $\mathscr{A}$ be a quadratic twist family of elliptic curves over $\mathbb{Q}$.

- $(\mathfrak{X}_1, \mathfrak{X}_2, A)$: $\epsilon(\mathfrak{X}_1) = -1$, $\epsilon(\mathfrak{X}_2) = +1$ s.t $D_1 D_2 < 0$ for $A^{(D_i)} \in \mathfrak{X}_i$;
- π_A on $\mathbb{H}^\times$ and $\mathbb{V} = \mathbb{B}^{tr=0}$,
- $(f \in \pi_A, \phi \in \mathscr{S}(\mathbb{V}))$ sutible test vector, (f_{D_1}, ϕ_{D_1}) its twist.

Consider the integral structure

$$\vartheta_{\phi_{D_1}}^{f_{D_1}} = p^{u_{D_1}} \cdot \vartheta_{D_1,0}, \qquad u_{D_1} \doteq \frac{1}{2} \min_{D_2} \sum_i \mathrm{ord}_p\, Ш^{an}(A^{(D_i)}),$$

and $\vartheta_{D_1,0}$ primitive. It follows from ARI and certain arithmetic Whittaker period formula that

$$\min_{A^{(D_1)} \in \mathfrak{X}_1} \mathrm{ord}_p \frac{L'(A^{(D_1)}, 1)}{R_{A^{(D_1)}} \Omega_A^{\epsilon_1} / \sqrt{D_1}} - \min_{A^{(D_2)} \in \mathfrak{X}_2} \mathrm{ord}_p \frac{L(A^{(D_2)}, 1)}{\Omega_A^{\epsilon_2} / \sqrt{D_2}},$$

where $\epsilon_i = \mathrm{sign} D_i$, is equal to

$$(\mathrm{I}) + \mathrm{ord}_p(f, f) \cdot \frac{\Omega_{\pi_A}^+ \Omega_{\pi_A}^-}{2L(1, \pi_A, ad)} + 2 \min_{A^{(D_1)} \in \mathfrak{X}_1} \mathrm{ord}_p \frac{(\vartheta_{\phi_{D_1}}^{f_{D_1}}, \vartheta_{D_1,0})_{\mathrm{NT}}}{(f_{D_1}, f_{D_1}) R_{A^{(D_1)}} \Omega_{\pi_A}^{\epsilon_1}},$$

where (I) involves local integrals with test vectors, which can be made explicit.

Thank You !