A Computational Comparison of Lang–Trotter and Hardy–Littlewood Constants for CM Elliptic Curves

Anish Ray

Department of Mathematics
University of Houston

April 25 2026

Elliptic Curves

An **elliptic curve over** $\mathbb{Q}$ is a nonsingular cubic curve of the form

$$E: \ y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Q},$$

with

$$4A^3 + 27B^2 \neq 0.$$

This condition means that the cubic has **no repeated roots**, so the curve has no singularities.

We also include one extra point O, called the **point at infinity**.

We write

$$E(\overline{\mathbb{Q}}) = \{(x, y) \in \overline{\mathbb{Q}}^2 : y^2 = x^3 + Ax + B\} \cup \{O\}.$$

for the set of algebraic points of E. Here $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$.

Group Law and Torsion Points

The set $E(\overline{\mathbb{Q}})$ carries an abelian group law with identity O.

For $m \geq 1$, define the multiplication map

$$[m] : E \to E, \qquad P \mapsto P + \cdots + P.$$

The m-torsion subgroup is

$$E[m] = \{P \in E(\overline{\mathbb{Q}}) : [m]P = O\}.$$

Over characteristic 0,

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

The coordinates of these points generate the **m-division field**

$$\mathbb{Q}(E[m]).$$

Galois Representations from Torsion

Let

$$G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

Since E is defined over $\mathbb{Q}$, every $\sigma \in G_{\mathbb{Q}}$ acts on $E[m]$.

Choosing a basis of

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2,$$

this action is represented by an invertible matrix modulo m.
Hence we obtain

$$\rho_{E,m} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

called the **mod-m Galois representation**.

These representations are the source of the Lang–Trotter constant.

Reduction Modulo Primes and Frobenius Trace

For all but finitely many primes p, reducing the equation of $E/\mathbb{Q}$ modulo p gives an elliptic curve

$$E_p/\mathbb{F}_p.$$

Such primes are called primes of **good reduction**.

We define

$$a_p(E) := p + 1 - \#E_p(\mathbb{F}_p).$$

Equivalently,

$$\#E_p(\mathbb{F}_p) = p + 1 - a_p(E).$$

By Hasse's bound,

$$|a_p(E)| \leq 2\sqrt{p}.$$

Thus $a_p(E)$ measures the fluctuation in the number of points modulo p.

Complex Multiplication

An endomorphism of an elliptic curve is an algebraic map

$$\varphi : E \to E$$

preserving the group law.

All multiplication maps

$$[n] : P \mapsto nP$$

are endomorphisms.

Over characteristic 0,

$$\mathrm{End}(E) = \mathbb{Z}$$

for most curves, but sometimes $\mathrm{End}(E)$ is an order in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. Then E is said to have **complex multiplication (CM)**.

Bad Reduction and the Conductor

A prime p is a prime of **bad reduction** if the reduced curve modulo p becomes singular.
Otherwise p is of good reduction.

The **conductor** of E, denoted N_E, is a positive integer whose prime divisors are exactly the bad primes.

Hence

$$p \nmid N_E$$

means that E has good reduction at p.

Only good primes are counted in the Lang–Trotter problem.

The Lang–Trotter Problem

Let $E/\mathbb{Q}$ be a CM elliptic curve and fix an integer $r \neq 0$.
Define

$$\pi_{E,r}(x) = \#\{p \leq x : \ a_p(E) = r, \ p \nmid N_E\}.$$

This counts primes of good reduction whose Frobenius trace equals r.

The Lang–Trotter conjecture predicts

$$\pi_{E,r}(x) \sim C_{E,r} \frac{\sqrt{x}}{\log x}.$$

Here $C_{E,r} \geq 0$ is the Lang–Trotter constant.

Imaginary Quadratic Fields

A CM elliptic curve is associated with an imaginary quadratic field

$$K = \mathbb{Q}(\sqrt{-D}), \qquad D > 0.$$

Its ring of integers is denoted

$$\mathcal{O}_K.$$

Example:

$$\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1}), \qquad \mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i].$$

The arithmetic of this field controls the Frobenius traces of CM curves.

How Primes Behave in K

A rational prime p can behave differently inside K.

It **splits** if

$$p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},$$

with two distinct prime ideals.

It is **inert** if

$$p\mathcal{O}_K$$

remains prime.

This distinction determines the Frobenius trace for CM elliptic curves.

Deuring's Lemma

Let $E/\mathbb{Q}$ have CM by $K = \mathbb{Q}(\sqrt{-D})$, and let $p \nmid N_E$.
Then:

$$p \text{ inert } \implies a_p(E) = 0.$$

If

$$p = \pi\overline{\pi}$$

splits in K, then

$$a_p(E) = \pi + \overline{\pi}.$$

So the trace $a_p(E)$ is governed by the factorization of p in the CM field.

From Deuring to Norm Forms

By Deuring's lemma, when p splits in

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

we may write

$$p = \pi\overline{\pi}.$$

If $D \equiv 1, 2 \pmod 4$, then

$$\pi = m + n\sqrt{-D}, \qquad m, n \in \mathbb{Z}.$$

Therefore

$$p = N(\pi) = m^2 + Dn^2.$$

Fixing the Frobenius Trace

In the same case $D \equiv 1, 2 \pmod 4$, we have

$$a_p(E) = \pi + \overline{\pi}.$$

Since

$$\pi = m + n\sqrt{-D},$$

we get

$$a_p(E) = 2m.$$

Thus the condition $a_p(E) = r$ forces

$$m = \frac{r}{2}.$$

So primes with trace r are related to primes of the form

$$p = \left(\frac{r}{2}\right)^2 + Dn^2.$$

The Hardy–Littlewood Conjecture

Let

$$f(m) = am^2 + bm + c, \qquad a, b, c \in \mathbb{Z}, \quad a > 0,$$

with

$$\gcd(a, b, c) = 1, \qquad b^2 - 4ac \text{ not a square.}$$

Assume also that $a + b$ and c are not both even.

Define

$$\pi_{a,b,c}(x) = \#\{p \leq x : \ p = am^2 + bm + c \text{ for some } m \in \mathbb{N}\}.$$

The Hardy–Littlewood Constant

The Hardy–Littlewood conjecture predicts

$$\pi_{a,b,c}(x) \sim C_{a,b,c} \frac{\sqrt{x}}{\log x},$$

where

$$C_{a,b,c} = \frac{\gcd(2, a+b)\delta}{\sqrt{a}\,\varphi(\delta)} \prod_{p \nmid 2a} \left(1 - \frac{\left(\frac{b^2-4ac}{p}\right)}{p-1}\right).$$

Here:

$$\delta = \text{odd part of } \gcd(a, b),$$

φ is Euler's totient function, and $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

Wan–Xi's Reformulation

Using Deuring's lemma, Wan and Xi related the Lang–Trotter problem for CM elliptic curves to primes represented by quadratic polynomials.

Assuming the Hardy–Littlewood conjecture for such polynomials, they proved

$$\pi_{E,r}(x) \sim \omega_{E,r} \frac{\sqrt{x}}{\log x}.$$

Here $\omega_{E,r} \geq 0$ is an explicit constant obtained using methods like orthogonality of Gauss sums from analytic number theory.

Thus the same counting function admits a second predicted constant:

$$C_{E,r} \qquad \text{and} \qquad \omega_{E,r}.$$

Wan–Xi Conjecture

For CM elliptic curves, Wan and Xi conjectured that

$$\boxed{\omega_{E,r} = C_{E,r}.}$$

That is, the constant coming from:

- Galois representations (Lang–Trotter), and
- quadratic polynomial prime counting (Hardy–Littlewood)

should be identical.

This is the central conjecture studied in my work.

Nathan Jones's Formula for $C_{E,r}$

Jones interprets the Lang–Trotter constant $C_{E,r}$ for CM elliptic curves as

$$C_{E,r} = \frac{m_E}{2\pi} \frac{|\mathrm{Gal}(K(E[m_E])/K)_r|}{|\mathrm{Gal}(K(E[m_E])/K)|} \prod_{\ell \nmid m_E} \frac{\ell \cdot |((\mathcal{O}/\ell\mathcal{O})^\times)_r|}{|(\mathcal{O}/\ell\mathcal{O})^\times|}.$$

Here:

- m_E is a positive integer depending on E,
- $\mathcal{O}$ is the CM order in the imaginary quadratic field K,
- the subscript r denotes the subset of elements with trace equal to r,
- the product runs over primes $\ell \nmid m_E$.

The infinite product is absolutely convergent.

Wan–Xi's Constant $\omega_{E,r}$

Wan and Xi give an explicit analytic constant $\omega_{E,r}$ by applying the Hardy–Littlewood conjecture to the quadratic polynomials arising from Deuring's lemma.

The formula is given case-by-case according to the CM field:

$$K = \mathbb{Q}(\sqrt{-D}), \qquad D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

The general shape is

$$\omega_{E,r} = \text{finite correction factor depending on } (E, r) \prod_{p \nmid 2r} \left(1 - \frac{\left(\frac{-D}{p}\right)}{p-1}\right).$$

Here $\left(\frac{-D}{p}\right)$ is the Legendre symbol. Thus $\omega_{E,r}$ is built from Hardy–Littlewood local densities rather than Galois representations.

The Constant $\omega_{E,r}$ for $K = \mathbb{Q}(i)$

Let $E/\mathbb{Q}$ have CM by

$$K = \mathbb{Q}(\sqrt{-1}).$$

Wan–Xi consider curves of the form

$$E: \ y^2 = x^3 - gx,$$

where

$$g = (-1)^{\delta} 2^{\lambda} g_1, \qquad \delta \in \{0, 1\}, \quad \lambda \in \mathbb{Z}_{\geq 0}, \quad g_1 \in \mathbb{N} \text{ odd}.$$

For $j \in \{2, 4\}$, define

$$\Omega_j(1; g_1; r) := \prod_{\substack{p^{\nu} \| g_1,\ p \nmid r \\ j \nmid \nu}} \frac{-1}{p - 1 - \left(\frac{-1}{p}\right)}.$$

Here $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol.

The Correction Factor $\kappa(g, r)$ (contd.)

If $4 \mid r$, then

$$\kappa(g,r) = 1 - (-1)^{\lambda r/4}\Omega_2 + (-1)^{\frac{r}{4}\left(\delta+\frac{g_1-1}{2}\right)}\left(1-(-1)^{r/4}\right)\mathrm{Re}\left(i^{1+\lambda r/4}\right)\Omega_4.$$

If $2\|r$ and $2 \mid \lambda$, then

$$\kappa(g,r) = 1 + \Omega_2 + (-1)^{\frac{r-2}{4}+\frac{g_1^2-1}{8}}\left(1-(-1)^{\delta+\lambda+\frac{g_1-1}{2}}\right)\Omega_4.$$

The Correction Factor $\kappa(g, r)$ (contd.)

If

$$2 \| r \qquad \text{and} \qquad 2 \nmid \lambda,$$

then the finite correction factor is simply

$$\kappa(g, r) = 1.$$

Thus, in this case,

$$\omega_{E,r} = \frac{1}{4} \prod_{p \nmid 2r} \left(1 - \frac{\left(\frac{-1}{p}\right)}{p-1} \right).$$

Computational Goal

The formulas for $C_{E,r}$ and $\omega_{E,r}$ are explicit, but highly nontrivial to evaluate in practice.

The main goal of this work was to compute both constants independently for CM elliptic curves over $\mathbb{Q}$, and compare them numerically.

More precisely:

1. Compute $\omega_{E,r}$ using the case-by-case formulas of Wan–Xi.
2. Compute $C_{E,r}$ using Jones's formula.
3. Use recent results on CM Galois images to determine the required local data.
4. Test whether

$$\omega_{E,r} = C_{E,r}.$$

What Must Be Computed

To evaluate Jones's constant, the difficult term is

$$\frac{|\mathrm{Gal}(K(E[m_E])/K)_r|}{|\mathrm{Gal}(K(E[m_E])/K)|}.$$

Thus we need two pieces of information:

1. the integer m_E,
2. the explicit matrix group

$$\mathrm{Gal}(K(E[m_E])/K) \subseteq \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}).$$

Once this group is known, the finite factor is obtained by counting matrices with trace r.

Input from Lozano–Robledo: Local Galois Images

Let $E/\mathbb{Q}(j_{K,f})$ have CM by an order $\mathcal{O}$ of conductor f in an imaginary quadratic field K.

For each prime p, Lozano–Robledo describes the image of the p-adic representation

$$\rho_{E,p^\infty} : G_{\mathbb{Q}(j_{K,f})} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_p).$$

The image is described, up to conjugation, inside the normalizer of a Cartan subgroup

$$N_{\delta,\phi}(p^\infty) \subseteq \mathrm{GL}_2(\mathbb{Z}_p).$$

This gives explicit control of the local Galois images at each prime p.

Why Lozano–Robledo Is Needed

Jones's formula requires the finite group

$$\mathrm{Gal}(K(E[m_E])/K).$$

To compute it, one must understand the images of the representations modulo prime powers dividing m_E.

Lozano–Robledo provides:

- the Cartan subgroup $C_{\delta,\phi}(N)$,
- its normalizer $N_{\delta,\phi}(N)$,
- the role of complex conjugation,
- special descriptions at bad primes and at $p = 2$.

Thus his results identify the possible Galois images needed for the finite factor in $C_{E,r}$.

Input from Campagna–Pengo: Entanglement

Even if we understand each prime-power division field

$$K(E[p^\infty]),$$

we still need to understand how these fields intersect each other.

Campagna–Pengo study the natural map

$$\mathrm{Gal}(K(E_{\mathrm{tors}})/K) \longrightarrow \prod_p \mathrm{Gal}(K(E[p^\infty])/K).$$

Their results determine when the family of division fields is linearly disjoint over K, and when there is entanglement.

This is essential for decomposing groups such as

$$\mathrm{Gal}(K(E[m_E])/K)$$

into prime-power pieces.

How These Inputs Enter the Computation

The computation of $C_{E,r}$ has two parts.

$$C_{E,r} = \frac{m_E}{2\pi} \cdot \frac{|\mathrm{Gal}(K(E[m_E])/K)_r|}{|\mathrm{Gal}(K(E[m_E])/K)|} \cdot \text{Euler product.}$$

- Lozano–Robledo gives the local Galois images modulo prime powers.
- Campagna–Pengo tells us when the corresponding division fields can be combined as a direct product.
- Together, they make the finite ratio

$$\frac{|\mathrm{Gal}(K(E[m_E])/K)_r|}{|\mathrm{Gal}(K(E[m_E])/K)|}$$

computable.

Example: The Curve E_1^*

Consider

$$E_1^* : \ y^2 = x^3 - 11x + 14.$$

This curve has CM by the order

$$\mathcal{O} = \mathbb{Z}[\sqrt{-4}]$$

inside

$$K = \mathbb{Q}(\sqrt{-1}).$$

For this curve one obtains

$$m_{E_1^*} = 4.$$

Hence the finite Galois group needed in Jones's formula is

$$\mathrm{Gal}(K(E_1^*[4])/K).$$

Lozano–Robledo Input for E_1^*

Lozano–Robledo's results determine the image of the relevant Galois representation.

For E_1^*, one has

$$\mathrm{Gal}(K(E_1^*[4])/K) \cong (\mathcal{O}/4\mathcal{O})^\times/\{\pm 1\}.$$

Moreover,

$$\mathrm{Gal}(K(E_1^*[4])/K) \leq (\mathcal{O}/4\mathcal{O})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Thus the image has order 4, and it is an index-two subgroup of $(\mathcal{O}/4\mathcal{O})^\times$.

The Explicit Galois Image for E_1^*

The full group $(\mathcal{O}/4\mathcal{O})^\times$ is

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 0 & 3 \end{pmatrix} \right\}.$$

Using Lozano–Robledo's classification, the Galois image is

$$\mathrm{Gal}(K(E_1^*[4])/K) = \left\langle \begin{pmatrix} 3 & 3 \\ 0 & 3 \end{pmatrix} \right\rangle.$$

Trace Count for E_1^*

From the explicit Galois image,

$$\mathrm{Gal}(K(E_1^*[4])/K) = \left\langle \begin{pmatrix} 3 & 3 \\ 0 & 3 \end{pmatrix} \right\rangle,$$

one computes the trace condition modulo 4.

The result is

$$|\mathrm{Gal}(K(E_1^*[4])/K)_r| = \begin{cases} |\mathrm{Gal}(K(E_1^*[4])/K)|, & r \equiv 2 \pmod 4, \\ 0, & \text{otherwise.} \end{cases}$$

This determines the finite Galois factor in $C_{E_1^*,r}$.

Where Campagna–Pengo Enters

For the second example,

$$E_2^* : \ y^2 = x^3 - 15x + 22,$$

one has CM by

$$\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$$

inside

$$K = \mathbb{Q}(\sqrt{-3}).$$

Here

$$m_{E_2^*} = 12.$$

Therefore Jones's formula requires the composite-level group

$$\mathrm{Gal}(K(E_2^*[12])/K).$$

Campagna–Pengo Decomposition

Campagna–Pengo's entanglement results allow us to decompose the composite-level group:

$$\mathrm{Gal}(K(E_2^*[12])/K) \cong \mathrm{Gal}(K(E_2^*[4])/K) \times \mathrm{Gal}(K(E_2^*[3])/K).$$

Thus the 12-torsion calculation reduces to two smaller calculations:

$$\text{4-torsion} \qquad \text{and} \qquad \text{3-torsion}.$$

This is the precise role of the entanglement theory in the computation.

Lozano–Robledo Inputs for E_2^*

For the 4-division part, one obtains

$$\mathrm{Gal}(K(E_2^*[4])/K) = (\mathcal{O}/4\mathcal{O})^\times.$$

Explicitly,

$$(\mathcal{O}/4\mathcal{O})^\times = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}/4\mathbb{Z},\ a^2 - b^2 \equiv 1 \text{ or } 3 \pmod 4 \right\}.$$

For the 3-division part,

$$(\mathcal{O}/3\mathcal{O})^\times = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \{1,2\},\ b \in \{0,1,2\} \right\}.$$

The 3-Division Image for E_2^*

The group

$$\mathrm{Gal}(K(E_2^*[3])/K)$$

has index 2 in $(\mathcal{O}/3\mathcal{O})^\times$.

Computing the squares in $(\mathcal{O}/3\mathcal{O})^\times$ gives the subgroup

$$\mathrm{Gal}(K(E_2^*[3])/K) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Together with the 4-division image, this determines

$$\mathrm{Gal}(K(E_2^*[12])/K).$$

Trace Count for E_2^*

Using the Chinese remainder isomorphism

$$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/12\mathbb{Z}),$$

we compute traces in

$$\mathrm{Gal}(K(E_2^*[12])/K).$$

The result is

$$|\mathrm{Gal}(K(E_2^*[12])/K)_r| = \begin{cases} \frac{1}{2}\left|\mathrm{Gal}(K(E_2^*[12])/K)\right|, & r \equiv 2, 8 \pmod{12}, \\ 0, & \text{otherwise.} \end{cases}$$

The Computed Lang–Trotter Constants

For

$$E_1^* : \ y^2 = x^3 - 11x + 14, \qquad K = \mathbb{Q}(i),$$

we obtain

$$C_{E_1^*,r} = \begin{cases} \dfrac{2}{\pi} \displaystyle\prod_{\substack{p \nmid 2 \\ p \mid r}} \frac{p}{p - \left(\frac{-1}{p}\right)} \prod_{\substack{p \nmid 2 \\ p \nmid r}} \left(1 - \frac{\left(\frac{-1}{p}\right)}{(p-1)\left(p - \left(\frac{-1}{p}\right)\right)}\right), & r \equiv 2 \pmod{} \\ 0, & \text{otherwise.} \end{cases}$$

Why We Compute E_1^* Instead of E_1

Let

$$E_1 : \ y^2 = x^3 + 4x, \qquad E_1^* : \ y^2 = x^3 - 11x + 14.$$

These curves are isogenous over $\mathbb{Q}$.

For primes of good reduction, isogenous elliptic curves over $\mathbb{Q}$ have the same number of points over $\mathbb{F}_p$.

Therefore

$$\#E_{1,p}(\mathbb{F}_p) = \#E_{1,p}^*(\mathbb{F}_p),$$

and hence

$$a_p(E_1) = a_p(E_1^*).$$

Thus $\pi_{E_1,r}(x) = \pi_{E_1^*,r}(x)$, so we may compute the Lang–Trotter constant using E_1^*. Since E_1 and E_1^* are isogenous, $C_{E_1,r} = C_{E_1^*,r}$.

Comparison for E_1: Congruence Obstruction

From the computations,

$$C_{E_1^*,r} = 0 \qquad \text{if } r \not\equiv 2 \pmod 4,$$

and from Wan–Xi's formula,

$$\omega_{E_1,r} = 0 \qquad \text{if } r \not\equiv 2 \pmod 4.$$

Therefore,

$$C_{E_1^*,r} = \omega_{E_1,r}$$

outside the congruence class

$$r \equiv 2 \pmod 4.$$

It remains to verify the equality when $r \equiv 2 \pmod 4$.

Comparison for E_1: The Main Computation

Assume

$$r \equiv 2 \pmod 4.$$

Then

$$C_{E_1^*,r} = \frac{2}{\pi} \prod_{\substack{p \nmid 2 \\ p \mid r}} \frac{p}{p - \left(\frac{-1}{p}\right)} \prod_{\substack{p \nmid 2 \\ p \nmid r}} \left(1 - \frac{\left(\frac{-1}{p}\right)}{(p-1)\left(p - \left(\frac{-1}{p}\right)\right)}\right).$$

Let $\chi_4(p) = \left(\frac{-1}{p}\right)$, the non-principal character modulo 4.

Comparison for E_1: Rewriting the Product

Using

$$L(1,\chi_4) = \prod_p \left(1 - \frac{\chi_4(p)}{p}\right)^{-1},$$

we rewrite

$$C_{E_1^*,r} = \frac{2}{\pi} L(1,\chi_4) \prod_{\substack{p\nmid 2 \\ p\nmid r}} \frac{p - \left(\frac{-1}{p}\right)}{p}$$

$$\times \prod_{\substack{p\nmid 2 \\ p\nmid r}} \left(1 - \frac{\left(\frac{-1}{p}\right)}{(p-1)\left(p - \left(\frac{-1}{p}\right)\right)}\right).$$

Comparison for E_1: Simplification

The two products combine as

$$\prod_{\substack{p\nmid 2\\ p\nmid r}} \frac{p-\left(\frac{-1}{p}\right)}{p}\left(1-\frac{\left(\frac{-1}{p}\right)}{(p-1)\left(p-\left(\frac{-1}{p}\right)\right)}\right)$$

$$=\prod_{p\nmid 2r}\left(1-\frac{\left(\frac{-1}{p}\right)}{p-1}\right).$$

Therefore,

$$C_{E_1^*,r}=\frac{2}{\pi}L(1,\chi_4)\prod_{p\nmid 2r}\left(1-\frac{\left(\frac{-1}{p}\right)}{p-1}\right).$$

Comparison for E_1: Identifying $\omega_{E_1,r}$

From Wan–Xi's formula,

$$\omega_{E_1,r} = \frac{1}{2} \prod_{p \nmid 2r} \left(1 - \frac{\left(\frac{-1}{p}\right)}{p-1}\right)$$

for $r \equiv 2 \pmod 4$.

Hence

$$\prod_{p \nmid 2r} \left(1 - \frac{\left(\frac{-1}{p}\right)}{p-1}\right) = 2\omega_{E_1,r}.$$

Thus

$$C_{E_1^*,r} = \frac{2}{\pi} L(1, \chi_4) \cdot 2\omega_{E_1,r}.$$

Comparison for E_1: Final Equality

We use the classical value

$$L(1, \chi_4) = \frac{\pi}{4}.$$

Therefore,

$$C_{E_1^*,r} = \frac{2}{\pi} \cdot \frac{\pi}{4} \cdot 2\omega_{E_1,r}.$$

Hence

$$C_{E_1^*,r} = \omega_{E_1,r}.$$

Since E_1 and E_1^* are isogenous,

$$a_p(E_1) = a_p(E_1^*)$$

for primes of good reduction, and so

$$C_{E_1,r} = \omega_{E_1,r}.$$

Final Result

We verified the equality

$$\omega_{E,r} = C_{E,r}$$

for a collection of 24 CM elliptic curves over $\mathbb{Q}$.

These curves span all 13 rational CM j-invariants.

Equivalently, they test the Wan–Xi conjecture across the rational CM family of elliptic curves over $\mathbb{Q}$.

Verified CM Fields

The curves considered have CM by orders in the fields

$$\mathbb{Q}(i), \qquad \mathbb{Q}(\sqrt{-3}), \qquad \mathbb{Q}(\sqrt{-7}), \qquad \mathbb{Q}(\sqrt{-11}),$$

$$\mathbb{Q}(\sqrt{-19}), \qquad \mathbb{Q}(\sqrt{-43}), \qquad \mathbb{Q}(\sqrt{-67}), \qquad \mathbb{Q}(\sqrt{-163}).$$

They are organized into 8 isogeny classes and include representatives for all 13 rational CM j-invariants.

Conclusion

For these 24 curves, the Lang–Trotter constant and the Hardy–Littlewood constant agree:

$$\boxed{C_{E,r} = \omega_{E,r}.}$$

Thus two very different viewpoints lead to the same asymptotic constant:

$$\text{Galois representations} \quad \Longleftrightarrow \quad \text{Quadratic prime values.}$$

Since every CM elliptic curve over $\mathbb{Q}$ with rational j-invariant is a quadratic twist of one of these representatives, this gives strong new evidence for the Wan–Xi conjecture across the full rational CM family.

Thank you.