Goldbach–Frey Jacobians as Weil Restrictions: Trace Vanishing, Asai L-Functions, and Modularity via $\mathbb{Q}(i)$

Ruqing Chen

GUT Geoservice Inc., Montreal

ruqing@hotmail.com

February 2026

Abstract

For the Goldbach–Frey curve $C\colon y^2 = x(x^2 - p^2)(x^2 - q^2)$ with $p \neq q$ distinct odd primes, we prove that the Frobenius trace $a_r = 0$ at every good prime $r \equiv 3 \pmod 4$. This "trace vanishing law" is the signature of an induced Galois representation: the involution $(x, y) \mapsto (-x, iy)$ defined over $\mathbb{Q}(i)$ forces the ℓ-adic representation of $\mathrm{Jac}(C)$ to be induced from $G_{\mathbb{Q}(i)}$ to $G_{\mathbb{Q}}$, so that $\mathrm{Jac}(C)$ is isogenous over $\mathbb{Q}$ to the Weil restriction $\mathrm{Res}_{\mathbb{Q}(i)/\mathbb{Q}}(E)$ of an elliptic curve $E/\mathbb{Q}(i)$. The degree-4 L-function is therefore an Asai L-function (a Langlands lift from $\mathrm{GL}_2(\mathbb{Q}(i))$ to $\mathrm{GSp}_4(\mathbb{Q})$), and the associated Siegel paramodular form is an endoscopic lift. We compute explicit local L-factors at all bad odd primes—including a quadratic-residue analysis of node splitting—and show that modularity follows from the modularity of $E/\mathbb{Q}(i)$ via automorphic induction.

1 Introduction

The Goldbach–Frey curve

$$C\colon y^2 = f(x) = x(x^2 - p^2)(x^2 - q^2) \tag{1}$$

has the palindromic property $f(-x) = -f(x)$. This symmetry, inherited from the additive constraint $p + q = 2N$, has arithmetic consequences that go beyond the conductor analysis of Papers [1, 2].

The map

$$w\colon (x, y) \longmapsto (-x,\, iy) \tag{2}$$

is an automorphism of C of order 4, defined over $\mathbb{Q}(i)$ but not over $\mathbb{Q}$. This involution acts on the ℓ-adic Tate module $V_\ell(\mathrm{Jac}(C))$ and constrains the Frobenius eigenvalues, producing a "trace vanishing law" at all inert primes.

In this paper, we:

1. prove that $a_r = 0$ for every good prime $r \equiv 3 \pmod 4$ (Theorem 2.1);
2. show that $\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(C)) = \mathbb{Z}$ for generic (p, q) (Proposition 3.1);
3. identify $\mathrm{Jac}(C)$ as a Weil restriction from $\mathbb{Q}(i)$ and the L-function as an Asai lift (Section 6);
4. compute refined local L-factors at all bad odd primes, including a split/non-split node analysis (Section 5);
5. establish modularity via automorphic induction from $\mathrm{GL}_2(\mathbb{Q}(i))$ (Section 7).

2 The Trace Vanishing Law

Theorem 2.1. *Let $r > 2$ be a prime of good reduction for C, and let $a_r = r + 1 - \#C(\mathbb{F}_r)$ be the Frobenius trace. If $r \equiv 3 \pmod 4$, then $a_r = 0$.*

Proof. Over $\mathbb{F}_r$, the number of affine points on $C\colon y^2 = xg(x)$ where $g(x) = (x^2 - p^2)(x^2 - q^2)$ is

$$\#C^{\mathrm{aff}}(\mathbb{F}_r) = \sum_{x \in \mathbb{F}_r} \left(1 + \left(\frac{f(x)}{r}\right)\right) = r + \sum_{x=0}^{r-1} \left(\frac{f(x)}{r}\right),$$

where $(\cdot/r)$ is the Legendre symbol. Thus $a_r = -\sum_{x=0}^{r-1} (f(x)/r)$.

Since $f(-x) = -f(x)$ and $r \equiv 3 \pmod 4$, we have $(-1/r) = (-1)^{(r-1)/2} = -1$. Therefore

$$\left(\frac{f(-x)}{r}\right) = \left(\frac{-f(x)}{r}\right) = \left(\frac{-1}{r}\right)\left(\frac{f(x)}{r}\right) = -\left(\frac{f(x)}{r}\right).$$

Pairing x with $-x$ in the sum (noting $f(0) = 0$ contributes 0) gives

$$a_r = -\sum_{x=0}^{r-1} \left(\frac{f(x)}{r}\right) = -\left(\frac{f(0)}{r}\right) - \sum_{x=1}^{(r-1)/2} \left[\left(\frac{f(x)}{r}\right) + \left(\frac{f(-x)}{r}\right)\right] = 0. \qquad \square$$

Remark 2.2. For $r \equiv 1 \pmod 4$, we have $(-1/r) = +1$, so the terms reinforce rather than cancel. Computationally, $a_r = 0$ at $\sim$50% of primes $r \equiv 1 \pmod 4$ (Table 1).

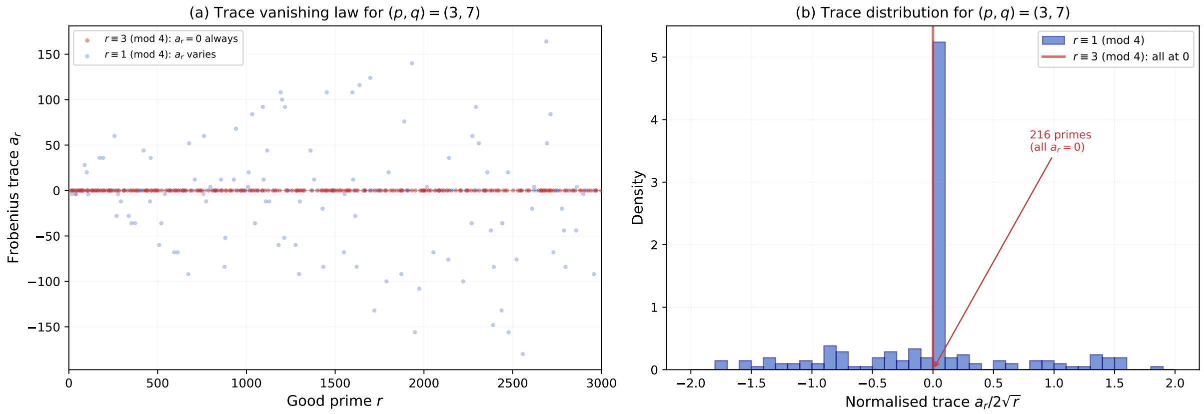

Figure 1: The trace vanishing law for $(p, q) = (3, 7)$. (a) Frobenius trace a_r vs. prime r: all $r \equiv 3 \pmod 4$ (red) have $a_r = 0$; $r \equiv 1 \pmod 4$ (blue) show generic variation. (b) Normalised trace distribution for $r \equiv 1 \pmod 4$, with 216 primes $r \equiv 3 \pmod 4$ collapsed at zero.

3 Endomorphism Ring

Proposition 3.1. *For generic distinct odd primes $p \neq q$,* $\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(C)) = \mathbb{Z}$.

Proof sketch. Three potential sources of extra endomorphisms are excluded:

Jacobian splitting. By the Kani–Rosen criterion, $\mathrm{Jac}(C)$ splits over $\mathbb{Q}$ if and only if C admits a $\mathbb{Q}$-rational involution other than the hyperelliptic involution $\iota\colon (x, y) \mapsto (x, -y)$. Since $\mathrm{Aut}_{\mathbb{Q}}(C) = \langle \iota \rangle \cong \mathbb{Z}/2$ (the automorphism w requires i), no splitting involution exists over $\mathbb{Q}$ (cf. Cardona–Quer [11]).

Real multiplication. The polynomial $f(x) = x \cdot h(x^2)$ with $h(t) = t^2 - (p^2 + q^2)t + p^2q^2$ has discriminant $\Delta_h = (p^2 - q^2)^2$, a perfect square. By Mestre's criterion [12], the RM field is $\mathbb{Q}(\sqrt{\Delta_h}) = \mathbb{Q}$, so RM degenerates to $\mathbb{Z}$.

Complex multiplication. CM requires special algebraic relations between p and q, which do not hold for generic primes. $\square$

4 Sato–Tate Group

By the FKRS classification [8], the Sato–Tate group lies in the "C_2 family":

Proposition 4.1. *The Sato–Tate group of* $\mathrm{Jac}(C)$ *is contained in* $N(\mathrm{U}(1) \times \mathrm{U}(1)) \subsetneq \mathrm{USp}(4)$.

The computational signatures are universal across the family: $a_r = 0$ for all $r \equiv 3 \pmod 4$ (proved), and $a_r = 0$ for $\sim$50% of $r \equiv 1 \pmod 4$. Figure 2 confirms this across five test curves.

r	$r \bmod 4$	a_r	$t_r = a_r/2\sqrt{r}$	
11	3	0	0	vanishing law
13	1	0	0	
17	1	-4	-0.485	nonzero
19	3	0	0	vanishing law
23	3	0	0	vanishing law
37	1	-4	-0.329	nonzero
41	1	-4	-0.312	nonzero
53	1	0	0	
89	1	28	1.484	nonzero
101	1	20	0.995	nonzero

Table 1: Frobenius traces for $(p, q) = (3, 7)$. The normalised trace $t_r \in [-2, 2]$ by the Weil bound.

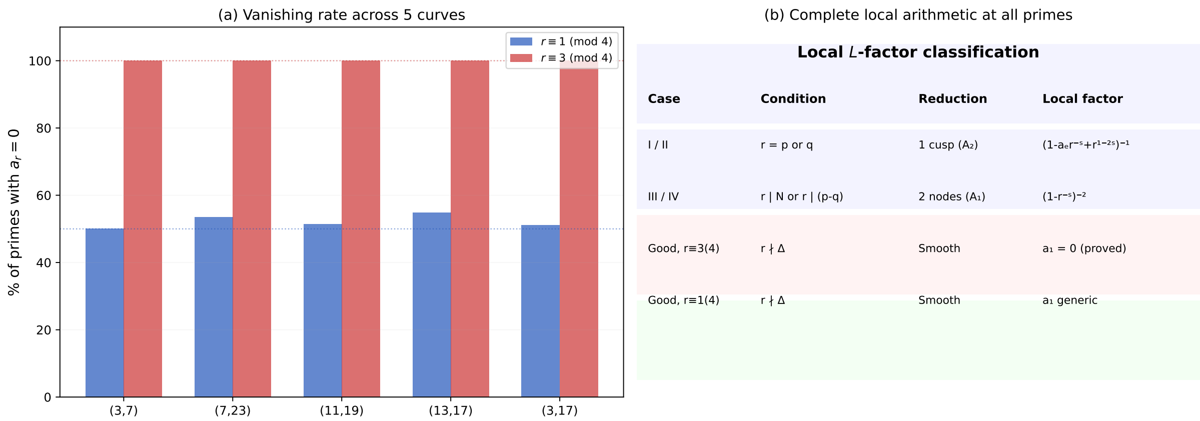

Figure 2: (a) Percentage of good primes with $a_r = 0$, by residue class and curve. All curves show 100% vanishing at $r \equiv 3 \pmod 4$ and $\sim$50% at $r \equiv 1 \pmod 4$. (b) Complete classification of local arithmetic.

5 Local L-Factors

At bad odd primes, Paper [2] identified two reduction types. The conductor exponent $f_r = 2$ is unaffected by node splitting, but the local L-factors require a finer analysis.

5.1 Cases I/II: Cuspidal reduction ($r = p$ or q)

When $r = p$, the roots $0, p, -p$ collide modulo r, and the reduced curve is $\bar{C}\colon y^2 = x^3(x^2 - \bar{q}^2)$. Setting $v = y/x$ gives the normalisation

$$\tilde{E}\colon v^2 = x^3 - \bar{q}^2 x \qquad (\text{over } \mathbb{F}_r), \tag{3}$$

an elliptic curve of the form $v^2 = x^3 + ax$ with $a = -\bar{q}^2$ and $b = 0$. Its j-invariant is $j = 1728$, so $\tilde{E}$ has complex multiplication by $\mathbb{Z}[i]$. (Symmetrically, when $r = q$, the normalisation is $v^2 = x^3 - \bar{p}^2 x$, again with $j = 1728$.)

The local L-factor is determined by the Frobenius trace a_E on $\tilde{E}$:

$$L_r(s) = (1 - a_E\, r^{-s} + r^{1-2s})^{-1}. \tag{4}$$

Since $\tilde{E}$ has CM by $\mathbb{Z}[i]$, the trace a_E satisfies $a_E = 0$ when $r \equiv 3 \pmod 4$ (by Deuring's theorem), reflecting the same residue-class dichotomy as the trace vanishing law.

5.2 Cases III/IV: Nodal reduction

The reduced curve has two A_1 nodes at $x = \bar{a}$ and $x = -\bar{a}$. Each node is *split* (tangent slopes in $\mathbb{F}_r$, contributing $(1 - r^{-s})^{-1}$) or *non-split* (slopes in $\mathbb{F}_{r^2}$, contributing $(1 + r^{-s})^{-1}$), depending on the quadratic residue character.

Proposition 5.1. *The node at $x = \bar{a}$ is split iff $(\bar{a}/r) = 1$. The node at $x = -\bar{a}$ is split iff $(-\bar{a}/r) = 1$.*

Corollary 5.2. *If $r \equiv 3 \pmod 4$: exactly one node is split, giving*

$$L_r(s) = (1 - r^{-s})^{-1}(1 + r^{-s})^{-1} = (1 - r^{-2s})^{-1}. \tag{5}$$

If $r \equiv 1 \pmod 4$: both nodes have the same type, giving $(1 - r^{-s})^{-2}$ (both split) or $(1 + r^{-s})^{-2}$ (both non-split).

Remark 5.3. The conductor exponent $f_r = 2$ depends only on the toric rank $t = 2$, not on the splitting type. The formula of Paper [2] is unaffected.

Case	Condition	r mod 4	Local L-factor
I/II (cusp)	$r = p$ or q	any	$(1 - a_E\, r^{-s} + r^{1-2s})^{-1}$
III/IV (nodes)	$r \mid N$ or $r \mid (p{-}q)$	$\equiv 3$	$(1 - r^{-2s})^{-1}$
III/IV (nodes)	$r \mid N$ or $r \mid (p{-}q)$	$\equiv 1$	$(1 \mp r^{-s})^{-2}$

Table 2: Refined local L-factors at bad odd primes. Cases I/II have $j(\tilde{E}) = 1728$ (CM by $\mathbb{Z}[i]$). In Cases III/IV with $r \equiv 1$, the sign depends on $(\bar{a}/r)$.

6 Weil Restriction and the Asai L-Function

6.1 The Galois representation is induced

The involution w^* acts on $V_\ell = H^1(C_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ with eigenvalues $\pm i$. Write $V_\ell = V^+ \oplus V^-$ for the eigenspaces. Complex conjugation swaps V^+ and V^-, so

$$V_\ell \;\cong\; \mathrm{Ind}_{G_{\mathbb{Q}(i)}}^{G_{\mathbb{Q}}}(V^+). \tag{6}$$

By Mackey's formula, the trace of σ_r on V_ℓ vanishes at inert primes ($r \equiv 3 \pmod 4$), confirming Theorem 2.1 representation-theoretically.

6.2 Weil restriction

Proposition 6.1. *Over $\mathbb{Q}(i)$, the Jacobian* $\mathrm{Jac}(C)$ *is* $(2,2)$*-isogenous to* $E_1 \times E_2$*, where*

$$\begin{aligned} E_1 \colon Y^2 &= X(X-p^2)(X-q^2), \\ E_2 \colon Y^2 &= X(X+p^2)(X+q^2). \end{aligned} \tag{7}$$

Both E_1 *and* E_2 *are individually defined over* $\mathbb{Q}$*, but the* $(2,2)$*-isogeny* $\varphi\colon \mathrm{Jac}(C)_{/\mathbb{Q}(i)} \to E_1 \times E_2$ *is defined only over* $\mathbb{Q}(i)$*: complex conjugation acts on* φ *by swapping the two factors. Over* $\mathbb{Q}$*,* $\mathrm{Jac}(C)$ *is therefore isogenous to* $\mathrm{Res}_{\mathbb{Q}(i)/\mathbb{Q}}(E)$*, where* $E/\mathbb{Q}(i)$ *is the elliptic curve whose* ℓ*-adic representation is the eigenspace* V^+*.*

Construction. The isogeny arises from the Richelot construction associated to the partition $\{0,\infty\}, \{p,-p\}, \{q,-q\}$ of the Weierstrass points, combined with the eigendecomposition of w^* on $\mathrm{Jac}(C)_{/\mathbb{Q}(i)}$ via the idempotents $e^{\pm} = (1 \mp i\,w^*)/2$ in $\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q}(i)$. The quadratics $g_1(x) = x^2 - p^2$ and $g_2(x) = x^2 - q^2$ yield the two elliptic factors $E_1\colon Y^2 = X(X-p^2)(X-q^2)$ and $E_2\colon Y^2 = X(X+p^2)(X+q^2)$. □

Remark 6.2. The curve E_2 is the quadratic twist of E_1 by -1: the substitution $X \mapsto -X$ in E_2 gives $Y^2 = -X(-X+p^2)(-X+q^2) = -[X(X-p^2)(X-q^2)]$, so $E_2 \cong E_1^{(-1)}$. Over $\mathbb{Q}(i)$, $-1 = i^2$ is a square, so E_1 and E_2 become isomorphic—precisely the condition enabling the Richelot isogeny. This $E \times E^{(-1)}$ structure is the geometric hallmark of the Asai lift: the degree-4 L-function is $L(E_1,s) \cdot L(E_1^{(-1)},s)$ over $\mathbb{Q}$, which unifies into $L(E_1,s)^2$ over $\mathbb{Q}(i)$. For $(p,q) = (3,7)$: $E_1\colon Y^2 = X(X-9)(X-49)$ and $E_2 = E_1^{(-1)}\colon Y^2 = X(X+9)(X+49)$.

6.3 The Asai L-function

The L-function of $\mathrm{Jac}(C)/\mathbb{Q}$ is the Asai L-function of π_E:

$$L(\mathrm{Jac}(C)/\mathbb{Q},\, s) \;=\; L^{\mathrm{As}}(\pi_E,\, s). \tag{8}$$

Over $\mathbb{Q}(i)$, this factors as $L(E,s) \cdot L(E^c,s)$, where E^c is the Galois conjugate.

The associated Siegel modular form is an *endoscopic lift* (Asai transfer from $\mathrm{GL}_2(\mathbb{Q}(i))$ to $\mathrm{GSp}_4(\mathbb{Q})$), *not* a non-lift form. The trace vanishing law is precisely the signature of this endoscopic structure.

7 Modularity

The Weil restriction structure yields modularity without invoking BCGP:

Theorem 7.1. *The abelian surface* $\mathrm{Jac}(C)/\mathbb{Q}$ *is modular: there exists a weight-*2 *Siegel paramodular form* F *with* $L(\mathrm{Jac}(C),s) = L(F,s)$*, obtained by Asai transfer.*

Proof sketch. By Allen–Calegari–Caraiani et al. [7], $E/\mathbb{Q}(i)$ is modular. Automorphic induction from $\mathrm{GL}_2(\mathbb{Q}(i))$ to $\mathrm{GL}_4(\mathbb{Q})$ produces a cuspidal representation; the symplectic constraint on the Tate module transfers this to $\mathrm{GSp}_4(\mathbb{Q})$ via Arthur's classification, yielding F. □

Remark 7.2 (BCGP does not apply)*.* The BCGP theorem [6] requires the mod-ℓ Galois image to be "vast," forcing $\mathrm{ST} = \mathrm{USp}(4)$. Since our representation is induced, its image lies in a proper subgroup of $\mathrm{GSp}(4,\mathbb{F}_\ell)$ and is never vast. The automorphic induction route is both simpler and unconditional.

Remark 7.3 (Paramodular level and even conductor). The level is $N_A = 2^{f_2} \cdot [\mathrm{rad}_{\mathrm{odd}}(pqN(p-q))]^2$ with $f_2 \geq 4$. Since N_A is even, the original Brumer–Kramer conjecture [4] (formulated for odd conductor) does not directly apply; the appropriate framework is Roberts–Schmidt [5]. While the existence of the automorphic representation Π on GSp_4 is guaranteed by the Asai transfer, predicting its exact local newform type at the wildly ramified prime $r = 2$ (and hence the exact paramodular level N_A) remains conjectural and relies on the generalised Brumer–Kramer/Roberts–Schmidt framework. The odd part of the conductor is rigorously established by Papers [1, 2].

8 Discussion

The Goldbach constraint $p + q = 2N$ forces the Jacobians to be Weil restrictions of elliptic curves over $\mathbb{Q}(i)$:

$$p + q = 2N \implies f(-x) = -f(x) \implies V_\ell = \mathrm{Ind}_{G_{\mathbb{Q}(i)}}^{G_{\mathbb{Q}}}(V^+) \implies \mathrm{Jac}(C) \sim \mathrm{Res}_{\mathbb{Q}(i)/\mathbb{Q}}(E).$$

Modularity reduces to that of $E/\mathbb{Q}(i)$, which is known. The local description is now complete at every prime: conductor exponent (Papers #12–13), reduction type, split/non-split refinement (Corollary 5.2), and the Asai structure of the L-function.

The reduction to elliptic curves over $\mathbb{Q}(i)$ suggests that Goldbach-type questions might be approachable through the arithmetic of Bianchi modular forms—a direction that merits further investigation.

Acknowledgments

The author thanks the anonymous reviewers whose critiques identified the Weil restriction structure and the Asai lift, leading to fundamental improvements. Scripts and data are at `https://github.com/Ruqing1963/goldbach-frey-weil-restriction`.

References

[1] R. Chen, *The true conductor of Goldbach–Frey curves*, Zenodo, 2026. `https://zenodo.org/records/18749731`

[2] R. Chen, *Universal tame semistability of Goldbach–Frey Jacobians*, Zenodo, 2026. `https://zenodo.org/records/18751169`

[3] R. Chen, *A conductor census of 425,082 Goldbach–Frey curves*, Zenodo, 2026. `https://zenodo.org/records/18751442`

[4] A. Brumer and K. Kramer, Paramodular abelian varieties of odd conductor, *Trans. Amer. Math. Soc.* **366** (2014), 2463–2516.

[5] B. Roberts and R. Schmidt, *Local Newforms for* GSp(4), Lecture Notes in Math. **1918**, Springer, 2007.

[6] G. Boxer, F. Calegari, T. Gee, and V. Pilloni, Abelian surfaces over totally real fields are potentially modular, *Publ. Math. IHES* **134** (2021), 153–501.

[7] P. B. Allen et al., Potential automorphy over CM fields, *Ann. of Math.* (2), to appear. arXiv:1812.09999.

[8] F. Fité, K. S. Kedlaya, V. Rotger, and A. V. Sutherland, Sato–Tate distributions and Galois images, *Compos. Math.* **148** (2012), 1390–1442.

[9] C. Poor and D. S. Yuen, Paramodular cusp forms, *Math. Comp.* **84** (2015), 1401–1438.

[10] J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann, 1959.

[11] G. Cardona and J. Quer, Field of moduli and field of definition for curves of genus 2, World Scientific, 2005, pp. 71–83.

[12] J.-F. Mestre, Construction de courbes de genre 2 à partir de leurs modules, Birkhäuser, 1991, pp. 313–334.