

Cubic-residue quadruplets: elliptic formulas and arithmetic fluctuations

Brice Pouly*

12 October 2026

Abstract

Let A_p count the monochromatic consecutive four-windows of a nontrivial cubic character modulo a prime $p \equiv 1 \pmod{3}$, with zero excluded and overlapping windows counted separately. We give an exact formula for A_p in terms of fixed elliptic traces and a finite boundary correction. Its complex-multiplication terms are related cubic twists. This produces two arithmetic fluctuation regimes: the first four moments of $(27A_p - p)/\sqrt{p}$ tend to $(0, 44, 0, 4224)$ when three is a cube and to $(0, 17, 0, 738)$ otherwise. Over all admissible primes they tend to $(0, 26, 0, 1900)$. The proof combines a four-position identity following from Greene’s hypergeometric formalism and Lennon’s trace formula with symmetric-power automorphy, cyclic base change and a finite collection of Rankin–Selberg prime number theorems; it uses no GRH. A direct geometric proof exposes the phases and exceptional points, with the genus-two and isogeny constructions of Freeman–Sato and Guillemin–Vergnaud explicitly credited. Point-order and Hasse certificates verify numerical examples without enumerating their billion-position character words. The conclusions concern fixed pattern length and four moments; no complete limiting distribution, constant-order centring of the raw count, or law for logarithmic-length maxima is proved.

Keywords. Cubic characters; Jacobi sums; elliptic curves; isogenies; complex multiplication; moments over primes; Rankin–Selberg functions; exact certificates.

1 The observable and the two main results

The number A_p of monochromatic cubic four-windows has leading scale $p/27$, but its fluctuations depend on a small arithmetic condition. After normalization by $\sqrt{p}$, the limiting variance is 44 when three is a cube modulo p , and 17 otherwise. The cause is not a change in the number of colours: two complex-multiplication traces in the exact count are related twists, and their relation depends on the cubic class of three. We count all overlapping consecutive windows of length four on the ordinary positions $1, \dots, p-1$. This observable differs from maximal-run starts and from a quadratic four-window count.

Questions about consecutive power residues and prescribed character patterns have a long history, including Lehmer–Lehmer [1], the computational theorem on cubic triples of Lehmer–Lehmer–Mills–Selfridge [2], and Graham’s result on first occurrences of quadruples [3]. Our observable counts all monochromatic four-windows in one period. The four-position identity used to compute it is a corollary of Greene [4] and Lennon [5], with an explicit fractional linear substitution given below. The associated genus-two family and isogeny were studied by Freeman–Sato [6] and Guillemin–Vergnaud [7]; the latter contains the short Weierstrass model used here. The contributions developed here are the assembled exact count with its boundary corrections, its certified evaluations, and the first four prime-averaged moments of that count. We retain a direct geometric proof to expose the phase and contributions at infinity; we do not claim a new general character-sum or isogeny identity.

*Prepared with artificial-intelligence assistance; see the declaration at the end.

Scope and relation to the atlas and certificates. The published atlas [10] studies a complete finite population of power-residue runs below 2^{32} , selected algebraic windows and separate sampled ternary diagnostics. These finite computations provide context for questions about arithmetic structure. The exact formula and the moment arguments below are self-contained apart from their cited mathematical inputs. Rabung certificates and recurrence-closed bounds [9] use finite run maxima and boundary conditions. Here the observable is instead a count of fixed four-windows, and its averaging population consists of primes. The finite atlas diagnostics and the prime-averaged moments below concern different populations. No theorem about logarithmic-length maxima or new van der Waerden bound is inferred from the four moments. When needed, $W(r, k)$ denotes r colours and progression length k ; the ordinary window convention is fixed explicitly below.

1.1 Windows, characters, and the prime population

Throughout, $p > 3$ is prime, $p \equiv 1 \pmod{3}$, and χ is a nontrivial cubic character of $\mathbb{F}_p^\times$. Write $\omega^2 + \omega + 1 = 0$ and regard its values as $1, \omega, \omega^2$. Extend χ by $\chi(0) = 0$. Because $3 \mid (p-1)/2$, we have $\chi(-1) = 1$. Conjugating χ does not change any equality of colours.

Define the cubic four-window count by

$$A_p = \#\{1 \leq x \leq p-4 : \chi(x) = \chi(x+1) = \chi(x+2) = \chi(x+3)\}. \quad (1)$$

All three nonzero colours are included. The four entries are consecutive integer residues, and overlapping windows are counted separately. This is a window statistic, not a count of maximal runs. The character order is part of its definition: a cubic four-window count is not reconstructed by relabelling a quadratic four-window count.

Put

$$I_2(p) = \mathbf{1}_{\chi(2)=1}, \quad I_{23}(p) = \mathbf{1}_{\chi(2)=\chi(3)=1}, \quad b_p = 26 + 18I_2(p) + 18I_{23}(p). \quad (2)$$

Thus $b_p \in \{26, 44, 62\}$. We use both normalizations

$$D_p = \frac{27A_p - p + b_p}{\sqrt{p}}, \quad Y_p = \frac{27A_p - p}{\sqrt{p}}. \quad (3)$$

The first retains the exact finite boundary correction; the second is the more immediate fluctuation around $p/27$.

Our population of varying primes is

$$\mathcal{P}(X) = \{p \text{ prime} : X \leq p < 2X, p \equiv 1 \pmod{3}\}.$$

Let $\mathcal{P}_0(X)$ consist of its primes for which three is a cube, and let $\mathcal{P}_*(X)$ be the complement. Each average below is uniform on the stated finite set and is divided by that set's own cardinality. There is no additional random origin in a character word, or additional random choice of the orientation of χ .

1.2 An exact elliptic formula

For an elliptic curve $E/\mathbb{F}_p$ write $t_E(p) = p + 1 - \#E(\mathbb{F}_p)$. Consider the fixed rational curves

$$\begin{aligned} E_1 : y^2 &= x^3 - 99x + 414, \\ E_2 : y^2 &= x^3 - 21x + 37, \\ E_3 : y^2 &= x^3 - 2835x + 58158, \end{aligned} \quad (4)$$

and the three curves with complex multiplication

$$C_0 : y^2 = x^3 - 27, \quad C_1 : y^2 = x^3 - 243, \quad C_2 : y^2 = x^3 - 2187. \quad (5)$$

All six have good reduction for $p > 3$. Write $t_i = t_{E_i}$, $c_j = t_{C_j}$, and $\beta_p = \chi(3) + \overline{\chi(3)} \in \{2, -1\}$.

Theorem 1.1 (Exact four-window formula). *For every admissible prime,*

$$27A_p = p - b_p - 2c_0(p) - 2c_1(p) - 2t_1(p) - 2t_2(p) - \beta_p t_3(p). \quad (6)$$

Equivalently, if $J_p = J(\chi, \chi)$,

$$27A_p = p - b_p + 4 \operatorname{Re}\{J_p(\overline{\chi(2)} + \overline{\chi(6)})\} - 2t_1(p) - 2t_2(p) - \beta_p t_3(p). \quad (7)$$

The CM traces satisfy

$$\begin{cases} c_0 = c_1 = c_2, & \chi(3) = 1, \\ c_0 + c_1 + c_2 = 0, & \chi(3) \neq 1. \end{cases} \quad (8)$$

Sections 2–4 prove these formulas. The finite corrections in (6) matter for an exact count: the character expansion on all of $\mathbb{F}_p$ is not the desired count until the four excluded residues have been removed.

1.3 Four moments over primes

Theorem 1.2 (Moments over the actual primes). *As $X \rightarrow \infty$, the relative cardinalities of $\mathcal{P}_0(X)$ and $\mathcal{P}_*(X)$ inside $\mathcal{P}(X)$ tend to $1/3$ and $2/3$. For $r = 1, 2, 3, 4$, the limits of the averages of D_p^r are*

population	$r = 1$	$r = 2$	$r = 3$	$r = 4$
$\mathcal{P}_0(X)$	0	44	0	4224
$\mathcal{P}_*(X)$	0	17	0	738
$\mathcal{P}(X)$	0	26	0	1900

The same statements hold with Y_p in place of D_p .

The constants can be read from the trace combination before the analytic proof. Write $x_i = t_i/\sqrt{p}$ and $v_j = c_j/\sqrt{p}$. Equations (6) and (8) give

$$D_p = \begin{cases} -4v_0 - 2x_1 - 2x_2 - 2x_3, & \chi(3) = 1, \\ 2v_2 - 2x_1 - 2x_2 + x_3, & \chi(3) \neq 1. \end{cases}$$

The low-degree averaging rule proved below assigns second moment 2 to the CM coordinate and 1 to each non-CM coordinate, with vanishing mixed terms in the required range. Thus

$$44 = 4^2 \cdot 2 + 2^2 + 2^2 + 2^2, \quad 17 = 2^2 \cdot 2 + 2^2 + 2^2 + 1.$$

Proving this averaging rule under the finite cubic conditioning is the analytic task. It provides the needed mixed moments through total degree four and does not posit an independent joint law in every degree.

The analytic proof in Sections 5–7 uses fixed automorphic objects. It establishes the mixed moments needed up to total degree four, without postulating complete joint equidistribution of the six curves. The displayed limits have $o(1)$ errors; we do not extract a numerical error bound applicable near 2^{32} .

2 A four-position identity from Greene and Lennon

2.1 The phase and the elliptic curve

Take distinct $a, b, c, d \in \mathbb{F}_p$ and set

$$\rho = \frac{c-d}{a-b}, \quad A = \frac{4(ab+cd) - 2(a+b)(c+d)}{(a-b)(c-d)}. \quad (9)$$

Define

$$E_A : Y^2 = X^3 - (6A + 15)X + (A^2 + 14A + 22), \quad t_A(p) = p + 1 - \#E_A(\mathbb{F}_p). \quad (10)$$

The identities

$$A - 2 = \frac{4(a-d)(b-c)}{(a-b)(c-d)}, \quad A + 2 = \frac{4(a-c)(b-d)}{(a-b)(c-d)}$$

give $A \neq \pm 2$. Direct substitution in the Weierstrass discriminant gives

$$\Delta(E_A) = -432(A-2)^3(A+2) \neq 0. \quad (11)$$

Thus none of the curves occurring in the identity is singular.

Corollary 2.1 (Four-position correlation; Greene–Lennon). *With the conventions above,*

$$1 + \sum_{z \in \mathbb{F}_p} \chi((z+a)(z+b)(z+c)^2(z+d)^2) = -\overline{\chi(\rho)} t_A(p). \quad (12)$$

Moreover $t_A(p) = t_{-A}(p)$. If $\beta_p(u) = \chi(u) + \overline{\chi(u)}$, the conjugate pair of sums is therefore

$$S_e(p) + S_{-e}(p) = -2 - \beta_p(\rho) t_A(p). \quad (13)$$

The explicit phase is part of the formula. Isomorphism over an algebraic closure alone would not recover it.

2.2 The hypergeometric derivation and its normalization

Extend the trivial character ε by $\varepsilon(0) = 0$, as in Greene. Put

$$s = \frac{2-A}{4} = \frac{(a-d)(c-b)}{(a-b)(c-d)}, \quad u = \frac{a-b}{a-d} \frac{z+d}{z+b}.$$

The distinct-position assumption gives $s \neq 0, 1$. This projective change of variable sends $-d, -a, -c, -b$ to $0, 1, 1/s, \infty$, and

$$\frac{(z+a)(z+b)}{(z+c)(z+d)} = \rho^{-1} \frac{1-u}{u(1-su)}.$$

Define Greene’s normalized function, here specialized to cubic characters, by its character sum:

$$F(s) = {}_2F_1 \left(\begin{matrix} \chi, & \overline{\chi} \\ \varepsilon \end{matrix}; s \right)_p = \frac{1}{p} \sum_{u \in \mathbb{F}_p} \overline{\chi}(u) \chi(1-u) \overline{\chi}(1-su). \quad (14)$$

This is Definition 3.5 of [4, p. 82], since $\chi(-1) = 1$ and $\varepsilon(s) = 1$. The poles and zeros contribute zero; the source point $z = \infty$ contributes one. Therefore the left side of (12) is $\overline{\chi}(\rho) pF(s)$, including its cubic phase and the extra one.

In (10) the substitution $X = x + 3$, $Y = y - 3x + A - 2$ gives

$$y^2 - 6xy + 2(A-2)y = x^3.$$

Lennon’s Theorem 1.1 [5], with $a_1 = -6$, $a_3 = 2(A-2)$, and $27a_3/a_1^3 = s$, gives $t_A(p) = -pF(s)$. A residue value of A can be lifted to an integer; $p > 3$ and $A \neq \pm 2$ give the required good reduction and $p \nmid a_1$. This also covers $A = 0$. Greene’s transformation [4, Theorem 4.4(i), p. 88] specializes to $F(s) = F(1-s)$, so $t_A = t_{-A}$. Conjugation gives (13). This proves the corollary using the published identities.

2.3 Direct geometric proof: a degree-two rational map

Let $R(z) = (z + a)(z + b)/((z + c)(z + d))$. Its character equals that of the polynomial in (12) wherever the quotient is defined, because the two differ by a cube. Its poles contribute zero, while $R(\infty) = 1$. If S_e denotes the affine polynomial sum, the character sum on this projective source is $S_e + 1$.

For $v \in \mathbb{F}_p$, the homogeneous equation $R(z) = v$ has $1 + \lambda(D(v))$ distinct rational roots, where λ is the quadratic character and

$$D(v) = (c - d)^2 v^2 + [4(ab + cd) - 2(a + b)(c + d)]v + (a - b)^2.$$

This root count includes infinity when the affine leading coefficient vanishes. The equation is never identically zero: its numerator and denominator have four distinct roots. Since $\sum_v \chi(v) = 0$, changing variables by $w = \rho v$ gives

$$S_e + 1 = \overline{\chi(\rho)} B_A, \quad B_A = \sum_{w \in \mathbb{F}_p} \chi(w) \lambda(w^2 + Aw + 1). \quad (15)$$

Inversion $w \mapsto w^{-1}$, with the zero term treated separately, shows that $B_A = \overline{B_A}$. Since it belongs to $\mathbb{Z}[\omega]$, it is an integer. We will identify it with $-t_A$.

2.4 The genus-two curve and its elliptic quotients

Let C_A be the smooth completion of $y^2 = x^6 + Ax^3 + 1$. The polynomial is squarefree because $A^2 \neq 4$, and the leading coefficient gives two rational points at infinity. This is the $b = 1$ specialization of the family in Freeman–Sato [6, Proposition 4.2]. The short model (10) and its degree-three isogeny also appear in Guillemin–Vergnaud [7, Section 3.1, p. 241]. We give the maps and an elementary point count for this specialization. The number of cube roots of w is $1 + \chi(w) + \overline{\chi(w)}$, including the value one at zero. Using $\sum_w \lambda(w^2 + Aw + 1) = -1$ gives

$$\sum_x \lambda(x^6 + Ax^3 + 1) = -1 + 2B_A, \quad \#C_A(\mathbb{F}_p) = p + 1 + 2B_A.$$

Thus its genus-two trace, defined as $p + 1 - \#C_A(\mathbb{F}_p)$, is $-2B_A$.

The two quotient curves are

$$E_+ : v^2 = (u + 2)(u^3 - 3u + A), \quad E_- : v^2 = (u - 2)(u^3 - 3u + A).$$

On suitable affine opens the maps are $u = x + x^{-1}$ and $v = y(x \pm 1)/x^2$. We keep track of the traces by an elementary count, rather than requiring a decomposition theorem for the Jacobian. For each u ,

$$\sum_{\substack{x \neq 0 \\ x + x^{-1} = u}} \lambda(x) = \lambda(u + 2) + \lambda(u - 2). \quad (16)$$

Indeed, away from $u = \pm 2$, the two roots have the same quadratic character, and $(x \pm 1)^2/x = u \pm 2$. A nonsplit fibre has zero on both sides in aggregate. At $u = \pm 2$ the formula is checked with the single root $x = \pm 1$. Now $x^6 + Ax^3 + 1 = x^3(u^3 - 3u + A)$ for $x \neq 0$. Equation (16), the term $x = 0$, and the two infinities on each quartic yield

$$t(C_A) = t(E_+) + t(E_-). \quad (17)$$

The substitutions

$$w = (u + 2)^{-1}, \quad v' = vw^2, \quad X = (A - 2)w + 3, \quad Y = (A - 2)v'$$

transform E_+ to (10). Birational maps between their smooth projective completions preserve the point count, including the points outside this open. The change $u \mapsto -u$ identifies E_- with the corresponding quartic for $-A$, hence with E_{-A} .

2.5 The degree-three isogeny and the square twist

The point $Q = (3, A - 2)$ on E_A has order exactly three. Its tangent has slope -3 , and the group law gives $2Q = -Q$. With $h = X - 3$, put

$$T = -12(A - 2), \quad V = 4(A - 2)^2, \quad r(X) = X + \frac{T}{h} + \frac{V}{h^2}.$$

The map $(X, Y) \mapsto (r(X), r'(X)Y)$ is the Vélú isogeny with kernel $\{O, Q, -Q\}$, whose target is

$$Y^2 = X^3 + (54A - 135)X - 27A^2 + 378A - 594. \quad (18)$$

The rational identity defining this map can also be verified directly over $\mathbb{Z}[A, X]$ after multiplication by h^6 ; the supplied verifier does this formal calculation. Since $p > 3$ the isogeny is separable and extends across its kernel to the smooth projective curves.

The target coefficients are those of the quadratic twist of E_{-A} by -3 : they are nine times its linear coefficient and -27 times its constant coefficient. A primitive cubic root $\zeta \in \mathbb{F}_p$ satisfies $(2\zeta + 1)^2 = -3$. Consequently this twist is isomorphic to E_{-A} over $\mathbb{F}_p$. Curves isogenous over a finite field have the same trace. For this direction, an isogeny commutes with Frobenius minus the identity; taking degrees and cancelling its degree proves equality of the degrees of Frobenius minus the identity, which are the point counts.

We have proved $t(E_+) = t(E_-) = t_A(p)$. Combining this with (17) gives $-2B_A = 2t_A(p)$. Equation (15) proves (12), and conjugation proves (13). This completes the direct proof of Corollary 2.1. The two elliptic quotients need not be isomorphic to each other; their equality of traces here follows from the isogeny and the square twist.

3 Derivation of the consecutive quadruplet formula

3.1 The pair and triple sectors

Away from the four zeros, the equality indicator has the expansion

$$27 \mathbf{1}_{\chi(z)=\dots=\chi(z+3)} = \sum_{\substack{e \in \{0,1,2\}^4 \\ \sum e_i = 0}} \prod_{i: e_i \neq 0} \chi(z+i)^{e_i}. \quad (19)$$

An empty product is one. This convention for zero exponents is retained at the excluded residues when the polynomial expansion is summed over $\mathbb{F}_p$. There are 27 terms: the constant, 12 of support two, eight of support three, and six of support four.

Every support-two sum is -1 . For example, the quotient $(z+a)/(z+b)$ parametrizes $\mathbb{F}_p \setminus \{1\}$ as z runs away from its pole, and has the same cubic character as $(z+a)(z+b)^2$. Its full sum is therefore -1 .

For distinct $i < j < l$, set $\delta = (j-i)(l-i)(l-j)$. We claim the exact triple identity

$$1 + \sum_{z \in \mathbb{F}_p} \chi((z+i)(z+j)(z+l)) = J_p \overline{\chi(\delta)}. \quad (20)$$

To see the missing constant explicitly, let $t = (l-j)(z+i)/((l-i)(z+j))$. It sends the three roots to $0, \infty, 1$ and satisfies

$$(z+i)(z+j)(z+l) = \delta^{-1}((l-i)(z+j))^3 t(1-t).$$

The value of t omitted by finite z is $t_\infty = (l-j)/(l-i)$. Since $\chi(t_\infty(1-t_\infty)) = \chi(\delta)$, the Jacobi sum loses exactly one after multiplication by $\chi(\delta)$. The pole at $z = -j$ contributes zero. This proves (20) with its orientation and its constant.

The four triples of $\{0, 1, 2, 3\}$ have difference products $2, 6, 6, 2$. Adding their conjugates gives the nonconstant contribution $4 \operatorname{Re}\{J_p(\overline{\chi(2)} + \overline{\chi(6)})\} - 8$.

3.2 The four-support sector and all four exclusions

For the three unoriented partitions of $\{0, 1, 2, 3\}$, the parameters (A, ρ) in (9) are

$$(14, 1), \quad (-1, 1), \quad (-10/3, 1/3).$$

Their conjugate sums contribute $-6 - 2t_{14} - 2t_1 - \beta_p t_{10/3}$. The equalities of opposite-parameter traces have been proved, and $\beta_p(1/3) = \beta_p(3)$. The first two positive parameters give E_1, E_2 in (4). The map $(X, Y) \mapsto (x, y) = (9X, 27Y)$ sends $E_{10/3}$, whose constant coefficient is $718/9$, to E_3 . It is an isomorphism for every $p > 3$. Together with the constant and pair sectors, the complete sum over $\mathbb{F}_p$ has main term $p - 26$.

We must remove $z = -r$, $r = 0, 1, 2, 3$. Terms with an active exponent at r are already zero. The remaining terms sum to nine if the other three values are equal, and to zero otherwise. At $r = 0, 3$ the equality condition is $\chi(2) = \chi(3) = 1$; at $r = 1, 2$ it is $\chi(2) = 1$, using $\chi(-1) = 1$. Thus the exclusions subtract exactly $18I_2 + 18I_{23}$, including their share of the constant term. The remaining residues are precisely $z = 1, \dots, p-4$, and (7) follows. This calculation accounts for all zero terms and avoids an error of four from treating the full field as the nonzero interval.

4 Complex multiplication and the exact conditional form

4.1 Fermat curves and Jacobi traces

For $a \in \mathbb{F}_p^\times$, the smooth projective Fermat cubic $u^3 + v^3 = aw^3$ has three rational points at infinity. Counting cube fibres in the affine chart gives

$$\#F_a(\mathbb{F}_p) = p + 1 + J_p \overline{\chi(a)} + \overline{J_p} \chi(a). \quad (21)$$

Indeed the two mixed character terms each equal -1 ; the remaining nonconstant pair is the two Jacobi terms. The affine count is $p - 2$ plus that pair, and the three infinities add three. This proves the sign in (21) directly.

On $u + v \neq 0$, the change

$$X = \frac{12a}{u+v}, \quad Y = \frac{36a(u-v)}{u+v}$$

gives $Y^2 = X^3 - 432a^2$. Conversely $u+v = 12a/X$ and $u-v = Y/(3X)$. These birational maps identify the smooth projective curves, so the exceptional points do not alter the point count. For $a = 2, 6, 18$, scaling $(X, Y) = (4x, 8y)$ gives the three curves in (5). Hence

$$c_j(p) = -2 \operatorname{Re}\{J_p \overline{\chi(2 \cdot 3^j)}\}, \quad j = 0, 1, 2. \quad (22)$$

Substitution proves (6). If $\eta = \chi(3)$ is one, the three traces coincide. Otherwise $1 + \eta + \eta^2 = 0$ proves their zero sum. This also proves (8).

4.2 Two arithmetic fluctuation regimes

Put $x_i = t_i/\sqrt{p}$ and $v_j = c_j/\sqrt{p}$. Equations (6) and (8) give

$$D_p = \begin{cases} -4v_0 - 2x_1 - 2x_2 - 2x_3, & 3 \text{ a cube,} \\ 2v_2 - 2x_1 - 2x_2 + x_3, & 3 \text{ not a cube.} \end{cases} \quad (23)$$

Hasse gives $|v_j|, |x_i| \leq 2$. Thus $|D_p| \leq 20$ in the first class and $|D_p| \leq 14$ in the second. Since $|D_p - Y_p| \leq 62/\sqrt{X}$ on $[X, 2X)$, the limits of every fixed moment agree for these two normalizations whenever either limit is established.

The two CM terms in the original exact formula are related twists. Treating them as independent would give the wrong second and fourth moments. Their dependence also persists when their unconditional covariance happens to vanish.

5 Arithmetic qualification of the non-CM factors

5.1 Non-CM and good reduction

The j -invariants of E_1, E_2, E_3 are, respectively, $-35937/4$, 790272 , and $-3472875/4$. The first and third are not algebraic integers, which already excludes complex multiplication for them. A uniform alternative for all three curves uses two good ordinary reductions with different Frobenius fields:

Curve	p	t_p	Frobenius field	p	t_p	Frobenius field
E_1	5	-3	$\mathbb{Q}(\sqrt{-11})$	7	-4	$\mathbb{Q}(\sqrt{-3})$
E_2	5	3	$\mathbb{Q}(\sqrt{-11})$	7	-1	$\mathbb{Q}(\sqrt{-3})$
E_3	7	-1	$\mathbb{Q}(\sqrt{-3})$	19	5	$\mathbb{Q}(\sqrt{-51})$

In each entry $p \nmid t_p$, so the reduction is ordinary. The specialization of endomorphisms is injective at good reduction [17]. For an ordinary reduction, the geometric endomorphism algebra is the imaginary quadratic field $\mathbb{Q}(\sqrt{t_p^2 - 4p})$ [16]. This remains the same on finite extensions: the two Frobenius roots have different p -adic valuations, so their ratio is not a root of unity and no power of Frobenius becomes rational. A characteristic-zero CM field would therefore inject into each of the two different fields in its row, which is impossible.

The Weierstrass discriminants are $-2^{14}3^6$, 2^43^4 , and $-2^{14}3^{11}$. Thus all primes under consideration are good. The trace witnesses and these elementary invariants are recomputed in the finite verifier.

5.2 Symmetric powers and quadratic base change

Let π_i denote the unitary-normalized modular representation attached to $E_i/\mathbb{Q}$. Its central character is trivial and it is self-contragredient. Modularity and Newton–Thorne’s Theorem A [12] provide cuspidal $\text{Sym}^m \pi_i$ on $\text{GL}_{m+1}/\mathbb{Q}$ for $1 \leq m \leq 4$. Set $K = \mathbb{Q}(\omega)$. The cyclic base-change criterion recalled in [13, Proposition 2.3.1(5), p. 54] says that a cuspidal representation remains cuspidal in this quadratic extension unless it has the corresponding quadratic self-twist.

This exceptional self-twist is excluded by a single inert prime for each curve and every needed m . Define $B_0 = 1$, $B_1 = t$, and $B_m = tB_{m-1} - pB_{m-2}$. The normalized symmetric-power trace is $B_m/p^{m/2}$. At the following inert primes, none is zero:

Curve	p	B_1	B_2	B_3	B_4
E_1	5	-3	4	3	-29
E_2	5	3	4	-3	-29
E_3	11	-6	25	-84	229

A self-twist by the quadratic character of $K/\mathbb{Q}$ would negate each such trace, forcing it to be zero. Write Π_i for the base change of π_i to K . The representations $\text{Sym}^m \Pi_i$ are consequently cuspidal, unitary, and self-contragredient, with trivial central character. In particular Π_i is nondihedral, because a dihedral GL_2 representation has a noncuspidal symmetric square.

5.3 Twist exclusions and the tensor products

At either place of K above the split prime 31 the traces are

$$(t_1, t_2, t_3) = (-4, 5, -7). \quad (24)$$

If two Π_i were character twists of each other, their trivial central characters would force the twisting character to have square one. Both local representations are unramified at 31, so that

character is unramified there and the absolute values of their traces would agree. The three distinct values in (24) exclude this. Ramakrishnan's tensor-product theorem [13, Theorem M] therefore gives cuspidal, self-contragredient $\Pi_i \boxtimes \Pi_j$ on GL_4/K for $i \neq j$. Here we use both nondihedrality and the twist exclusion.

The normalized symmetric-square traces at 31 are

$$-15/31, \quad -6/31, \quad 18/31. \quad (25)$$

Their absolute values are also distinct. In the moment proof all Hecke twists are unramified at 31 and unitary. Consequently (24) and (25) exclude the equal-rank collisions even after an arbitrary imaginary power of the norm is included: such a twist still multiplies a trace at 31 by a number of modulus one. This local argument deals with the norm twists appearing in the prime number theorem as well as the finite cubic characters. We do not infer independence just from different equations or different j -invariants.

6 A twisted averaging lemma through degree four

6.1 The CM Hecke character and the finite prescription

CM Hecke theory [15, Theorem 3.6 in arXiv v1] associates to C_0 a unitary Hecke character γ of K with nonzero angular infinity type. At a good prime ideal $\mathfrak{p}$, its normalized trace is $\gamma(\mathfrak{p}) + \gamma(\mathfrak{p})^{-1}$. The field $K(\sqrt[3]{3})/K$ is cyclic of degree three. Indeed the valuation of three at the place above three is two, not a multiple of three. Let η denote its nontrivial cubic Hecke character. At a degree-one place it records the cubic class of three, with conjugation coherent with the character orientation.

The three CM twists may be labelled so that

$$\begin{aligned} v_0 &= \gamma + \gamma^{-1}, \\ v_1 &= \gamma\eta^{-1} + \gamma^{-1}\eta, \\ v_2 &= \gamma\eta + \gamma^{-1}\eta^{-1}. \end{aligned} \quad (26)$$

Indeed, if $v^3 = 3$, the maps $(x, y) \mapsto (v^{2j}x, v^{3j}y)$ identify C_0 with C_j over $K(v)$ for $j = 1, 2$. Their descent characters are the two nontrivial powers of η , giving (26) after choosing an orientation. Conditioning the CM angle on a finite Galois class is an established method; see Fité–Sutherland [8, Propositions 3.6 and 3.10]. The particular six-curve observable still requires the mixed products below. Reversing the reciprocity convention conjugates both characters and leaves the class-conditioned moments unchanged. Their conductors have support only above two and three, so all twists here are unramified at 31.

At any good place of K with residue cardinality q , let x_i be the trace of E_i divided by $\sqrt{q}$. Define $P_0(x) = 1$, $P_1(x) = x$, $P_m(x) = xP_{m-1}(x) - P_{m-2}(x)$. Then $P_m(x_i)$ is the local trace of $\mathrm{Sym}^m \Pi_i$.

Lemma 6.1 (Fixed-object twisted averages). *For $h \in \mathbb{Z}$, $u \in \{0, 1, 2\}$, and nonnegative m_1, m_2, m_3 with $|h| + m_1 + m_2 + m_3 \leq 4$, the average over good prime ideals $\mathfrak{p}$ of K with $X \leq N\mathfrak{p} < 2X$ of*

$$\gamma(\mathfrak{p})^h \eta(\mathfrak{p})^u \prod_{i=1}^3 P_{m_i}(x_i(\mathfrak{p})) \quad (27)$$

tends to zero unless $h = m_1 = m_2 = m_3 = u = 0$. In that constant case the average is one.

6.2 The finite list of analytic products

Let $\theta = \gamma^h \eta^u$. Gillespie–Ji's Theorem 1.1 in arXiv v1 [14] applies over the fixed Galois field K to two unitary cuspidal factors when at least one is self-contragredient. Its possible main term

comes from equivalence of the factors up to an imaginary norm twist. We use the contragredient on the second factor when converting the notation to a product of the desired local traces.

The required products are exhausted by the following list. The regrouping of the degree pattern $(2, 1, 1)$ into ranks $(3, 4)$ uses the same tensor-product strategy as Ramakrishnan [13, Theorem 4.2.1, pp. 93–94]; the finite enumeration below checks its applicability to our specific moment expansion, rather than introducing that strategy. The indices i, j, l are distinct whenever they occur together.

Positive m_i	Allowed pattern	Factors for the prime number theorem
None	θ alone	θ and the trivial GL_1 character
One	$1 \leq m_i \leq 4$	$\mathrm{Sym}^{m_i} \Pi_i$ and θ
Two	$m_i + m_j \leq 4$	$\mathrm{Sym}^{m_i} \Pi_i$ and $\mathrm{Sym}^{m_j} \Pi_j \otimes \theta$
Three	$(1, 1, 1), h \leq 1$	$\Pi_1 \boxtimes \Pi_2$ and $\Pi_3 \otimes \theta$
Three	Permutation of $(2, 1, 1)$, $h = 0$	$\mathrm{Sym}^2 \Pi_i$ and $(\Pi_j \boxtimes \Pi_l) \otimes \eta^u$

Every listed first factor, except for the first row where the trivial factor can be used, is cuspidal and self-contragredient by Section 5. If the two ranks differ, equivalence is impossible. The two three-index rows have ranks $(4, 2)$ and $(3, 4)$, respectively. In the two-index row the only equal-rank patterns are $(1, 1)$ and $(2, 2)$. Equations (24) and (25) exclude both after every twist under consideration, including the imaginary norm twist. The one-index row has ranks $m_i + 1$ and one.

In the first row θ can equal an imaginary norm power only when $h = 0$, by its angular infinity type. Then its order-three part is nontrivial unless $u = 0$. In the constant case the usual prime ideal theorem provides the main term. Thus every nonconstant case has no main term.

6.3 Prime powers, ramified places, and unweighted averages

The cited theorem initially controls coefficients of a logarithmic derivative, with norm logarithms as weights. We spell out the passage to prime ideals used here. At every good place, normalized elliptic eigenvalues have modulus one. Symmetric powers and the two-factor tensor products retain that property; the Hecke characters are also unitary. Their traces at prime powers are therefore bounded by a constant depending only on the fixed ranks. The contribution from powers of order at least two up to norm $2X$ is $O(\sqrt{X}(\log X)^2)$.

There are finitely many bad places. Their factors here come from the local parameters of elliptic curves and CM characters, followed by the same fixed tensor and symmetric-power operations. In unitary normalization their local parameters in the Euler factors have modulus at most one. More explicitly, an elliptic unitary Weil–Deligne parameter is tempered: its special blocks have the form $U \otimes \mathrm{Sp}(r)$ with unitary U . On inertia invariants in the kernel of monodromy, the eigenvalues from such a block have modulus $q^{-(r-1)/2} \leq 1$. The fixed symmetric powers and tensor products here decompose into blocks of this same form; the unitary CM characters have $r = 1$. Thus this bound applies to the actual ramified Rankin–Selberg Euler factors, not just to the good places. Their higher-power contribution is consequently $O(\log X)$ after summing over the fixed bad places. Equivalently these factors may be removed before applying the prime number theorem and their finite Euler corrections restored afterwards.

The nonconstant logarithmically weighted sum is $o(X)$; the constant sum is $X + o(X)$. Partial summation on $[X, 2X)$ removes the logarithmic weight and gives $o(X/\log X)$ in the nonconstant cases, against $X/\log X + o(X/\log X)$ for the prime count. This proves Lemma 6.1. We have paid for prime powers directly using known tempered parameters. No general Ramanujan conjecture, Hypothesis H, or growing-conductor uniformity is being imported from a more general statement.

7 Conditioning and the integer moment calculations

7.1 From prime ideals to rational primes

Prime ideals of residue degree at least two and norm at most $2X$ lie over rational primes at most $\sqrt{2X}$. There are $O(\sqrt{X})$ of them in this quadratic field. All observables needed here are bounded, so their contribution is negligible in the prime ideal averages. Each split rational prime $p \equiv 1 \pmod{3}$ has exactly two conjugate degree-one places of norm p . The actual count, the trace combination D_p , and the events $\eta = 1$ and $\eta \neq 1$ are invariant under conjugation. Averaging them over the two places is therefore exactly the rational-prime average in Theorem 1.2.

The class indicators are

$$\mathbf{1}_{\eta=1} = \frac{1 + \eta + \eta^2}{3}, \quad \mathbf{1}_{\eta \neq 1} = \frac{2 - \eta - \eta^2}{3}. \quad (28)$$

Lemma 6.1 gives relative densities $1/3$ and $2/3$. Dividing the corresponding weighted averages by those densities gives the class-conditioned moments, not moments divided by the total population.

7.2 The mixed functional only through degree four

For nonnegative r_0, r_1, r_2, r_3 of total degree at most four, the conditional averages of $v_0^{r_0} \prod_i x_i^{r_i}$ in the cube class, and of $v_2^{r_0} \prod_i x_i^{r_i}$ in the noncube class, factor as

$$M_{\text{CM}}(r_0) \prod_{i=1}^3 M_{\text{ST}}(r_i). \quad (29)$$

Here, for orders zero through four,

$$M_{\text{CM}} = (1, 0, 2, 0, 6), \quad M_{\text{ST}} = (1, 0, 1, 0, 2).$$

To prove this formula, expand (26) in powers of γ and η , use

$$x^2 = P_2(x) + 1, \quad x^3 = P_3(x) + 2P_1(x), \quad x^4 = P_4(x) + 3P_2(x) + 2,$$

and multiply by (28). Every nonconstant term vanishes by Lemma 6.1. The surviving constant coefficients are $\binom{2r}{r}$ for a CM even power $2r$ and the Catalan number $\binom{2r}{r}/(r+1)$ for each non-CM factor. Odd powers have no constant coefficient. The factors of η in v_2 cancel in its constant term, so the same functional applies in the noncube class.

This factorization is proved only in the degree range just specified. It does not assert that the four variables have an independent joint law in all degrees.

7.3 Second and fourth moments

In the cube class, (23) has coefficient vector $(-4, -2, -2, -2)$. The CM contribution has variance $16 \cdot 2 = 32$, and the other three have variance four each. Thus the variance is 44. In the noncube class, the coefficient vector is $(2, -2, -2, 1)$: its variance is $4 \cdot 2 + 4 + 4 + 1 = 17$. The first and third moments vanish by (29).

Only the single-variable fourth powers and products of two squares survive in the fourth moment. They give

$$\begin{aligned} 4224 &= 4^4 \cdot 6 + 3 \cdot 2^4 \cdot 2 + 6\{3(32 \cdot 4) + 3(4 \cdot 4)\}, \\ 738 &= 2^4 \cdot 6 + (2^4 + 2^4 + 1) \cdot 2 + 6\{8 \cdot 9 + (4 \cdot 4 + 4 \cdot 1 + 4 \cdot 1)\}. \end{aligned}$$

Finally

$$\frac{44 + 2 \cdot 17}{3} = 26, \quad \frac{4224 + 2 \cdot 738}{3} = 1900.$$

The uniform bounds following (23) justify replacing D_p by Y_p . This completes the proof of Theorem 1.2. For the unmultiplied fluctuation $(A_p - p/27)/\sqrt{p}$, the second and fourth moments are 26/729 and 1900/531441.

7.4 The covariance of the original CM pair

The same lemma applied to (26) gives

$$\lim \mathbb{E} \left[\begin{pmatrix} v_0^2 & v_0 v_1 \\ v_0 v_1 & v_1^2 \end{pmatrix} \middle| 3 \text{ a cube} \right] = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix},$$

and in the noncube class the matrix is $\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$. The unconditional covariance is zero, although the exact twist relations remain. The arithmetic contrast concerns the cubic class of *three*. Replacing this stratum by the cube/noncube class of *two* would change the prime-averaging question.

8 Exact certificates and reproducibility

8.1 Point orders determine the trace

For a nonsingular short Weierstrass curve over $\mathbb{F}_p$, a trace certificate contains a point P , its claimed order r with complete prime factorization, and a claimed group order N . The verifier checks

$$[r]P = O, \quad [r/q]P \neq O \quad \text{for each prime } q \mid r,$$

and

$$r > 2\lfloor 2\sqrt{p} \rfloor, \quad |N - p - 1| \leq \lfloor 2\sqrt{p} \rfloor, \quad r \mid N. \quad (30)$$

The scalar checks and the complete prime factorization prove the exact point order. Lagrange then makes r a divisor of the true group order. Hasse puts that order in an integer interval of width $2\lfloor 2\sqrt{p} \rfloor < r$. There can be only one multiple of r in it, namely N . Thus $p + 1 - N$ is the certified trace.

The generator uses baby-step/giant-step in the Hasse interval and searches at most 256 candidate abscissas. Failure to find a sufficiently large point order is a refusal, not a presumed trace. The portable program uses exact trial primality and a declared modulus range $p < 10^{10}$. This numerical domain restricts the software, not the mathematical identities or prime limits. The verifier checks the point orders without repeating their search.

8.2 Three illustrative primes

The archived exact counts and traces include:

p	t_1	t_2	t_3	A_p
1 000 033	119	227	-1069	36 876
4 294 967 197	-34978	-101713	-19969	159 072 704
4 294 967 311	-52264	-46204	-7891	159 072 584

Their CM triples are, in the same order, $(-670, 1967, -1297)$, $(43250, 85529, -128779)$, and $(124244, -25963, -98281)$. All three are in the noncube class of three. Their exact corrected fluctuation numerators are -4355, -4145, and -7517.

The first count is also checked against a direct independent walk through its 1 000 032 character values. The two billion-scale examples are obtained from certificates; their full character words are not constructed. These examples check identities and are not a statistical confirmation sample for the moment limits.

8.3 What the finite programs establish

The elliptic verifier checks the formal Vélú map, its discriminant, the quotient change of variables, and small-prime sums. It rechecks 2625 large point-order certificates for the fixed-support applications, as well as the nine non-CM certificates for the three quadruplet examples.

The moment verifier checks 207 admissible primes below 3000, including both classes of three. It performs 1242 point counts by two methods, 621 CM–Jacobi comparisons, 621 Fermat–fibre comparisons, and 207 direct four-window checks. It verifies nine additional CM point-order certificates at the three illustrative primes. Arithmetic qualification is checked at the small primes specified above. Two separate integer computations, by multinomials and Laurent constant terms, reproduce the four moments. All 70 joint monomials through degree four and all 315 index cases of Lemma 6.1 are enumerated. Altered certificates and requests outside the stated degree range are rejected.

The 315 cases verify the completeness of the finite routing table. They do not prove automorphy or a prime number theorem. The output moment constants are exact evaluations of the functional justified in the proof, not empirical moments fitted to the 207 primes.

From the repository root, the exact six-curve oracle can be invoked as

```
python3 -B scripts/cubic_quadruplets.py 4294967197
```

It checks all six required curve identities and certificates and evaluates (6), without using a fast Jacobi evaluator. A missing stored certificate set is reported as such. The explicit option `-generate` requests a bounded new six-curve certificate search and may refuse. The two finite certificate replay commands are

```
python3 -B reproducibility/cubic_quadruplets/elliptic/src/verify.py
python3 -B reproducibility/cubic_quadruplets/moments/src/verify.py
```

They use standard Python only. These commands check the supplied finite identities and certificates without a network connection or GPU; they do not establish the external analytic theorems by computation.

9 Consequences and scope

9.1 A non-Gaussian moment signature

The ratio of the conditional variances is 44/17. Globally the standardized fourth-moment ratio is

$$\frac{1900}{26^2} = \frac{475}{169}.$$

A centred Gaussian of variance 26 has fourth moment 2028, not 1900. Uniform boundedness makes moment convergence necessary under weak convergence, so D_p and Y_p cannot converge in law to that Gaussian. This conclusion does not establish existence of a different complete limiting distribution. Compactness only assures subsequential limits, all sharing the four displayed moments.

9.2 A candidate distribution, not a theorem

Full joint equidistribution, if proved, would suggest the mixture

$$\begin{aligned} & \frac{1}{3} \mathcal{L}(8 \cos \Theta + 2T_1 + 2T_2 + 2T_3) \\ & + \frac{2}{3} \mathcal{L}(4 \cos \Theta + 2T_1 + 2T_2 + T_3), \end{aligned}$$

where Θ is uniform and the T_i have semicircle density $(2\pi)^{-1}\sqrt{4-t^2}$ on $[-2, 2]$, independently in this candidate model. Symmetry makes the signs immaterial. Theorem 1.2 verifies its moments through degree four by a separate analytic argument. It does not prove this distributional limit. For example, the degree-six product $P_2(x_1)P_2(x_2)P_2(x_3)$ is outside the finite routing table established here. Results about one or two curves are not silently extended to three.

9.3 Normalized centring and critical maxima

The bounded correction b_p vanishes after division by $\sqrt{p}$. Vanishing averages of normalized traces do not imply

$$\mathbb{E}(A_p - p/27) = -\mathbb{E}b_p/27 + o(1).$$

That would require substantially stronger cancellation of the raw trace sums. No constant-order raw-centering formula is asserted.

Likewise, a four-window count of order p , with fluctuations of order $\sqrt{p}$, does not determine the rare occurrence count at length $k \sim \log_3 p$ or its probability of being zero. The fixed-support application in the appendix retains exact signs, but makes no uniform claim about a family whose number and parameters grow with k . The global maximum problem remains separate from the theorems here.

9.4 Manuscript status

The analytic inputs are the cited literature theorems. Their required cuspidality, base-change and twist-exclusion conditions are verified for the fixed representations used here. Finite programs check the arithmetic identities and the routing of the low-degree calculations, rather than the external analytic theorems themselves. Specialist review is a validation task, not an additional mathematical hypothesis or a GRH assumption.

Artificial-intelligence tools assisted with proof development, computation, literature retrieval, and English writing and revision. Brice Pouly is the human author and assumes responsibility for the proof, programs, data, references and conclusions. Author-controlled checks do not constitute independent external replication or peer review. The accompanying article archive contains its numerical certificates and bounded reproduction commands.

A The signed support-four sector of a longer start count

For $k+1 < p$ define the predecessor-indexed starts

$$J_{p,z}^{(k)} = \mathbf{1}_{\chi(z) \neq \chi(z+1) = \dots = \chi(z+k)}, \quad 1 \leq z \leq p-k-1, \quad Z_{p,k} = \sum_z J_{p,z}^{(k)}.$$

The neutral prefix has no predecessor in this interval. At each admissible z , subtracting the $(k+1)$ -colour equality indicator from the last- k equality indicator gives

$$J_{p,z}^{(k)} = 3^{-k} \sum_{\substack{e \in \{0,1,2\}^{k+1} \\ \sum e_j = 0 \text{ (3)}}} (3\mathbf{1}_{e_0=0} - 1) \prod_{j:e_j \neq 0} \chi(z+j)^{e_j}. \quad (31)$$

For a support S of cardinality four, the six active exponent patterns have two ones and two twos. They form three conjugate pairs, with common coefficient $c(S) = -1$ if $0 \in S$, and $c(S) = 2$ otherwise. Apply Corollary 2.1 to the three unoriented partitions of each support. For integer indices compute A, ρ rationally first and then reduce modulo p . Grouping A and $-A$ is legitimate because their traces are equal, as proved above.

Set

$$C_k = 3 \left(2 \binom{k}{4} - \binom{k}{3} \right), \quad \mathcal{E}_{p,k}^{[4]} = \sum_{S, \{a,b\} | \{c,d\}} c(S) \beta_p(\rho) t_A(p).$$

The excluded residues are $z = -r$ for $0 \leq r \leq k$. The active roots already contribute zero; the others produce the finite correction

$$H_{p,k}^{[4]} = \sum_{S, \{a,b\}|\{c,d\}} c(S) \sum_{r \in \{0, \dots, k\} \setminus S} \beta_p \left(\frac{(a-r)(b-r)}{(c-r)(d-r)} \right).$$

Both the phase weights and this correction use only small character values of differences. The exact support-four contribution to $Z_{p,k}$ is

$$\mathcal{L}_{p,k}^{[4]} = -\frac{2C_k + \mathcal{E}_{p,k}^{[4]} + H_{p,k}^{[4]}}{3^k}. \quad (32)$$

This is a signed identity in the actual count, not an absolute-value upper bound or a substitute for the rest of the expansion.

At $k = 21$ there are 43890 monomials, 21945 conjugate pairs, and 1169 rational absolute parameters $|A|$. Zero aggregated weights can be removed before trace evaluation. The certified applications are

p	k	$\mathcal{E}_{p,k}^{[4]}$	$\mathcal{L}_{p,k}^{[4]}$
1 000 033	13	438273	$-148373/531441$
4 294 967 197	21	-108879048	$36273779/3486784401$
4 294 967 311	21	130803933	$-43623131/3486784401$

The corresponding H values are -18 , -6129 , and 1620 . This sector is expressed in units of the full count $Z_{p,k}$. The reduction does not estimate all higher supports collectively, and the four prime-averaged moments for the six fixed curves provide no uniform moment theorem for these growing parameter lists.

References

- [1] D. H. Lehmer and E. Lehmer, On runs of residues, *Proc. Amer. Math. Soc.* 13 (1962), 102–106. [doi:10.1090/S0002-9939-1962-0138582-6](https://doi.org/10.1090/S0002-9939-1962-0138582-6).
- [2] D. H. Lehmer, E. Lehmer, W. H. Mills and J. L. Selfridge, Machine proof of a theorem on cubic residues, *Math. Comp.* 16 (1962), 407–415.
- [3] R. L. Graham, On quadruples of consecutive k th power residues, *Proc. Amer. Math. Soc.* 15 (1964), 196–197.
- [4] J. Greene, Hypergeometric functions over finite fields, *Trans. Amer. Math. Soc.* 301 (1987), 77–101. [doi:10.1090/S0002-9947-1987-0879564-8](https://doi.org/10.1090/S0002-9947-1987-0879564-8).
- [5] C. Lennon, Trace formulas for Hecke operators, Gaussian hypergeometric functions, and the modularity of a threefold, *J. Number Theory* 131 (2011), 2320–2351. [doi:10.1016/j.jnt.2011.05.005](https://doi.org/10.1016/j.jnt.2011.05.005). Theorem 1.1 is cited from arXiv:1003.1157v2 (27 December 2010), *A Trace Formula for Certain Hecke Operators and Gaussian Hypergeometric Functions*. <https://arxiv.org/abs/1003.1157v2>.
- [6] D. M. Freeman and T. Satoh, Constructing pairing-friendly hyperelliptic curves using Weil restriction, *J. Number Theory* 131 (2011), 959–983. [doi:10.1016/j.jnt.2010.06.003](https://doi.org/10.1016/j.jnt.2010.06.003).
- [7] A. Guillevic and D. Vergnaud, Genus 2 hyperelliptic curve families with explicit Jacobian order evaluation and pairing-friendly constructions, *Pairing-Based Cryptography–Pairing 2012*, LNCS 7708 (2013), 234–253. [doi:10.1007/978-3-642-36334-4_16](https://doi.org/10.1007/978-3-642-36334-4_16).

- [8] F. Fité and A. V. Sutherland, Sato–Tate distributions of twists of $y^2 = x^5 - x$ and $y^2 = x^6 + 1$, *Algebra Number Theory* 8 (2014), 543–585. doi:10.2140/ant.2014.8.543.
- [9] B. Pouly, *Succinct Rabung certificates and recurrence-closed lower bounds for van der Waerden numbers*, published edition v2.0, 2026. doi:10.5281/zenodo.23337824.
- [10] B. Pouly, *Arithmetic structure in a complete atlas of power-residue runs below 2^{32} : Rabung profiles, Kummer densities, norm dependencies, and local codes*, published edition v1.0, 2026. doi:10.5281/zenodo.23339668.
- [11] J. Vélú, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A–B* 273 (1971), A238–A241.
- [12] J. Newton and J. A. Thorne, Symmetric power functoriality for holomorphic modular forms, II, *Publ. Math. IHÉS* 134 (2021), 117–152. <https://arxiv.org/abs/2009.07180>.
- [13] D. Ramakrishnan, Modularity of the Rankin–Selberg L -series, and multiplicity one for $SL(2)$, *Ann. of Math.* 152 (2000), 45–111. <https://arxiv.org/abs/math/0007203>.
- [14] T. Gillespie and G. Ji, Prime number theorems for Rankin–Selberg L -functions over number fields, *Sci. China Math.* 54 (2011), 35–46. doi:10.1007/s11425-010-4137-x. Theorem numbering follows arXiv:0910.3660v1 (19 October 2009), *A Prime number theorem for Rankin–Selberg L -functions over number fields*. <https://arxiv.org/abs/0910.3660v1>.
- [15] Q. Chen and E. Shen, Effective Sato–Tate distributions for surfaces arising from products of elliptic curves, *Res. Math. Sci.* 11 (2024), article 69. doi:10.1007/s40687-024-00470-x. Section 3.3 and Theorem 3.6 refer to arXiv:2309.08848v1 (16 September 2023), whose title starts *On Effective Sato–Tate distributions*. <https://arxiv.org/abs/2309.08848v1>.
- [16] A. V. Sutherland, *18.783 Elliptic Curves*, MIT lecture notes 13 (2023). <https://math.mit.edu/classes/18.783/2023/LectureNotes13.pdf>.
- [17] A. V. Sutherland, *18.783 Elliptic Curves*, MIT lecture notes 21 (2023), Section 21.5. <https://math.mit.edu/classes/18.783/2023/LectureNotes21.pdf>.