



UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

On the Logarithmic Density of Rank ≥ 1 and Rank ≥ 2 Genus-2 Jacobians

and applications to hyperelliptic curve cryptography

George C. Țurcaș

Babeș-Bolyai University, Cluj-Napoca

joint work with Răzvan Bărbulescu, Mugurel Barcău & Vicențiu Pașol

Bucharest–Shenzhen International Mathematics Conference

Number Theory session · 30th of June 2026



The problem and the ordering

For a genus-2 curve $C/\mathbb{Q}$, the Mordell–Weil group decomposes as $\text{Jac}(C)(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$ with T finite; the invariant of interest is the rank $r = \text{rank } \text{Jac}(C)(\mathbb{Q})$.

Ordering by height. Following Booker et al., we enumerate integral Weierstrass models

$$C : y^2 + h(x)y = f(x), \quad \deg f \leq 6, \deg h \leq 3, h_i \in \{0, 1\},$$

by the naive height $H(C) = \max_i |a_i|$. (The simplified model $y^2 = f(x)$ is the case $h = 0$.) The box of such models of height $\leq X$ satisfies

$$\#S_1(X) = \#\{(f, h) : |a_i| \leq X, h_i \in \{0, 1\}\} \asymp X^7.$$

The difficulty. Curves of positive rank are expected to have *proportion zero*, so ordinary density is blind to them. We measure them on a logarithmic scale.

Logarithmic density and the main theorem

Definition

A set $S \subseteq S_1$ has *logarithmic density* $\alpha = \liminf_{X \rightarrow \infty} \frac{\log \#S(X)}{\log \#S_1(X)}$. Since $\#S_1(X) \asymp X^7$, this is the growth exponent of S divided by 7.

Theorem (Bărbulescu–Barcău–Paşol–Ț., 2026)

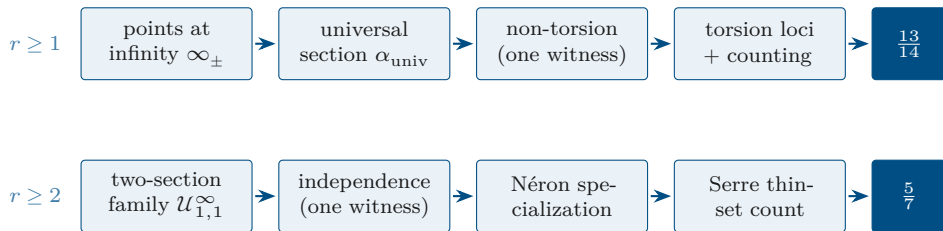
With respect to this height ordering, **unconditionally**:

$$\text{rank Jac}(C)(\mathbb{Q}) \geq 1 : \text{logarithmic density} \geq \frac{13}{14} \quad (\text{Corollary 2.7}),$$

$$\text{rank Jac}(C)(\mathbb{Q}) \geq 2 : \text{logarithmic density} \geq \frac{5}{7} \quad (\text{Corollary 2.11}).$$

Two parallel arguments

The proofs for the two lower bounds follow the *same* four-step pattern.



Both rest on a divisor class that is rational *for free*, a *single* explicit witness fixing the generic behaviour, and a count of the exceptional locus.

Part I

Rank ≥ 1 : logarithmic density $\frac{13}{14}$

A divisor class supported at infinity is, generically, non-torsion.

Rank ≥ 1 : the points at infinity

Complete the square on $y^2 + h(x)y = f(x)$:

$$g(x) = 4f(x) + h(x)^2, \quad c = \text{coeff}_{x^6}(g).$$

If $\deg g = 6$, the two points at infinity $\infty_{\pm}$ are defined over $\mathbb{Q}(\sqrt{c})$, and

$$\infty_+, \infty_- \in C(\mathbb{Q}) \iff c \in (\mathbb{Q}^\times)^2.$$

In that case we obtain a canonical rational class

$$\alpha = [\infty_+ - \infty_-] \in \text{Jac}(C)(\mathbb{Q}).$$

Observation

If α is *non-torsion*, then $\text{rank Jac}(C)(\mathbb{Q}) \geq 1$ — a rational *Jacobian point* (a divisor class), obtained for free from the model.

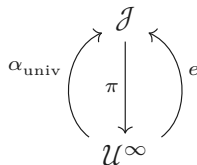
The universal section

Let (f, h) vary. Over the smooth (discriminant $\neq 0$) sextic locus, adjoin $\sqrt{c}$ to form the double cover

$$\mathcal{U}^\infty = \{u^2 = c\} \longrightarrow \{\deg g = 6\}.$$

There the Jacobian is an abelian scheme $\mathcal{J} \rightarrow \mathcal{U}^\infty$ carrying the *universal section*

$$\alpha_{\text{univ}} = [\infty_+ - \infty_-] \in \mathcal{J}(\mathcal{U}^\infty).$$



$\pi \circ \alpha_{\text{univ}} = \text{id}$, e the zero section.

Reduction

Each specialization at which α_{univ} stays non-torsion has $\text{rank Jac} \geq 1$. So the question becomes: **how often is α_{univ} torsion after specialization?** — which we now show is rare, in two steps.

Fact 1: a single witness suffices

To prove α_{univ} is non-torsion it is enough to exhibit *one* specialization where α has infinite order: a relation $n\alpha_{\text{univ}} = 0$ would specialize identically.

Witness (Tengely)

For

$$C : y^2 = x^6 + 18x^5 + 75x^4 + 120x^3 + 120x^2 + 72x + 28,$$

the Jacobian has rank $\text{Jac}(C)(\mathbb{Q}) = 1$, generated by $[\infty_+ - \infty_-]$.

Hence α_{univ} is non-torsion. (The parameter space splits into 16 sheets indexed by $h \in \{0, 1\}^4$; one LMFDB witness per sheet covers all of them.)

Fact 2a: only finitely many torsion loci can occur

The n -torsion locus

$$\mathcal{V}_n = \{ \underline{a} \in \mathcal{U}^\infty : n \alpha_{\text{univ}}(\underline{a}) = 0 \}$$

is a *proper* Zariski-closed subset, defined over $\mathbb{Q}$ (proper by Fact 1).

Uniform torsion bound

$$|\text{Jac}(C)(\mathbb{Q})_{\text{tors}}| \ll (\log H(C))^2 \quad (\text{Kieffer } \theta\text{-heights} + \text{Pazuki} + \text{Gaudron-Rémond}).$$

Hence a torsion $\alpha_{\underline{a}}$ has order $n \ll (\log X)^2$, so

$$T(X) \subseteq \bigcup_{n \ll (\log X)^2} \mathcal{V}_n \quad \text{— only get contribution from } O((\log X)^2) \text{ torsion}$$

Fact 2b: counting the torsion loci

Degree. For a symmetric, relatively very ample L ,

$$[n]^*L \simeq L^{\otimes n^2},$$

so in the induced projective coordinates $\mathcal{V}_n$ is cut out by equations of degree $O(n^2)$ — not n^4 .¹

Count & sum. A hypersurface estimate gives

$$\#(\mathcal{V}_n(\mathbb{Z}) \cap \{H \leq X\}) \ll n^2 X^6 \implies \#T(X) \ll X^6 \sum_{n \ll (\log X)^2} n^2 \ll X^6 (\log X)^6.$$

¹Multiplication by n on the abelian surface has degree $n^{2g} = n^4$; the input here is the *polarization scaling* $[n]^*L \simeq L^{\otimes n^2}$, which controls the degree in projective coordinates.

Counting gives $\frac{13}{14}$

On the subfamily $S_1^\square(X)$ where $\infty_\pm$ are rational (c a square):

$$\#S_1^\square(X) \asymp \underbrace{X^{1/2}}_{c=\square} \cdot \underbrace{X^6}_{a_5, \dots, a_0} = X^{13/2}, \quad \#T(X) \ll X^6 (\log X)^6 = o(X^{13/2}).$$

Thus all but a negligible subset have α non-torsion, hence $\text{rank Jac}(C)(\mathbb{Q}) \geq 1$.
Inside the box $\#S_1(X) \asymp X^7$, the logarithmic density is

$$\frac{13/2}{7} = \frac{13}{14}.$$

Corollary 2.7 (unconditional)

$$\liminf_{X \rightarrow \infty} \frac{\log \#\{(f, h) \in S_1(X) : \text{rank Jac}(C)(\mathbb{Q}) \geq 1\}}{\log \#S_1(X)} \geq \frac{13}{14}.$$

Part II

Rank ≥ 2 : logarithmic density $\frac{5}{7}$

Same machine — now we need two independent sections.

Rank ≥ 2 : a two-section family

We need a second independent class, so restrict to the 5-parameter family ($h = 0$, $a_6 = a_0 = 1$):

$$C_{\underline{a}} : y^2 = x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1.$$

- $a_6 = 1 \Rightarrow c = 4$ is a square, so $\infty_{\pm}$ are rational;
- $a_0 = 1 \Rightarrow P = (0, -1) \in C_{\underline{a}}(\mathbb{Q})$.

This yields *two* universal sections on $\mathcal{U}_{1,1}^{\infty}$:

$$\alpha_{\text{univ}} = [\infty_+ - \infty_-], \quad \beta_{\text{univ}} = [P - \infty_+].$$

Observation

If the *specialized* classes $\alpha_{\underline{a}}, \beta_{\underline{a}}$ are $\mathbb{Z}$ -independent, then $\text{rank Jac}(C_{\underline{a}})(\mathbb{Q}) \geq 2$.

Generic independence of the sections is not enough by itself — the next two slides upgrade it to almost every specialization.

Independence from one witness

Again a single specialization controls the generic fibre.

Witness (LMFDB 15625.a.15625.1)

For $C_0 : y^2 = x^6 + 8x^5 + 10x^4 + 10x^3 + 5x^2 + 2x + 1$, one has $\text{Jac}(C_0)(\mathbb{Q}) \simeq \mathbb{Z}^2$, with generators G_1, G_2 satisfying

$$G_2 = \beta_{\text{univ}}, \quad G_1 - 2G_2 = \alpha_{\text{univ}}.$$

Hence α_{univ} and β_{univ} generate a rank-2 subgroup at $\underline{a}_0$, so they are $\mathbb{Z}$ -independent in $\mathcal{J}(\mathcal{U}_{1,1}^\infty)$.

Néron specialization and Serre's count

Néron specialization. The map

$$\mathrm{sp}_{\underline{a}} : \Gamma = \langle \alpha_{\mathrm{univ}}, \beta_{\mathrm{univ}} \rangle \longrightarrow \mathrm{Jac}(C_{\underline{a}})(\mathbb{Q})$$

is **injective** for all $\underline{a}$ outside a *thin* set $\Omega \subset \mathcal{U}_{1,1}^{\infty}(\mathbb{Q})$;
for $\underline{a} \notin \Omega$, $\mathrm{rank} \mathrm{Jac}(C_{\underline{a}})(\mathbb{Q}) \geq 2$.

Serre's estimate for affine thin sets
($n = 5$, $d = 1$):

$$\#(\Omega \cap [-X, X]^5) \ll X^{9/2}(\log X)^{\gamma}.$$

The exceptional locus is a vanishing fraction of the $\asymp X^5$ family.

exponent comparison

family $\asymp X^5$

bad set $\Omega \ll X^{9/2+o(1)}$

ratio $\ll X^{-1/2+o(1)} \rightarrow 0$

Counting gives $\frac{5}{7}$

Exactly as in the rank-1 count, with the five free coefficients $a_1, \dots, a_5$:

$$\#\mathcal{U}_{1,1}^\infty(\mathbb{Z}; X) \asymp X^5, \quad \#\{\text{rank} < 2\} \ll X^{9/2}(\log X)^\gamma = o(X^5).$$

All but a negligible subset have $\text{rank Jac}(C_{\underline{a}})(\mathbb{Q}) \geq 2$. This X^5 family sits inside the box $\#S_1(X) \asymp X^7$, giving logarithmic density $\frac{5}{7}$.

Corollary 2.11 (unconditional)

$$\liminf_{X \rightarrow \infty} \frac{\log \#\{(f, h) \in S_1(X) : \text{rank Jac}(C)(\mathbb{Q}) \geq 2\}}{\log \#S_1(X)} \geq \frac{5}{7}.$$

Context: comparison with elliptic curves

Family / rank	log. density	status
Elliptic curves, $r \geq 2$	$\frac{19}{24} \approx 0.79$	heuristic (random matrix)
Genus 2, $r \geq 1$	$\frac{13}{14} \approx 0.93$	unconditional
Genus 2, $r \geq 2$	$\frac{5}{7} \approx 0.71$	unconditional

Orientation only: the elliptic-curve entry is heuristic (random-matrix) and uses a *different* (H_2 , Bhargava–Gross) height ordering — not a theorem-to-theorem comparison. The genus-2 bounds are unconditional.

Heuristic. If rank *parities* equidistribute in the two-points-at-infinity subfamily, the same construction would suggest $\frac{13}{14}$ for $r \geq 2$ as well — but this is only heuristic.

An independent route: split Jacobians

When the Jacobian splits, the rank problem reduces to elliptic curves:

$$\mathrm{Jac}(C) \xrightarrow{\sim} E_1 \times E_2 \quad \implies \quad \mathrm{rank} \mathrm{Jac}(C) = \mathrm{rank} E_1 + \mathrm{rank} E_2.$$

- **Unconditional family.** For primes $d \equiv m \equiv 3 \pmod{4}$, the curve $y^2 = d^3x^6 + m^3$ has $\mathrm{Jac} \sim E_d \times E_m$ of rank 2, giving logarithmic density $\geq \frac{2}{21}$.
- **Twist families** (several variants): *conditional* on BSD (double twists) or on abc (a $\frac{1}{6}$ log-density bound), plus one *unconditional* positive proportion when $\mathrm{Jac} \sim E^2$ with a rational 3-isogeny.

Context only — the headline bounds $\frac{13}{14}, \frac{5}{7}$ do not rely on any of this.

Motivation: Regev's quantum DLP algorithm

For HECC the discrete log lives in $G = \text{Jac}(C)(\mathbb{F}_q)$, with $n = \log_2 |G|$.

- Regev / Ekerå–Gärtner: dominant cost $\approx d + \frac{n}{d}$ per run (vs. Shor's $\approx n$); advantage $\min(d, \frac{n}{d})$.
- In the curve setting, a rank- r lift or compatible twist supplies $d = r + 2$, under the usual independence heuristic on the reduced generators.

Consequence

The density bounds show high-rank lifts are *abundant* in the height-ordered rational family — so the preprocessing input is easy to find.

Motivation, not the theorem. For a curve fixed over $\mathbb{F}_q$ one still needs a compatible lift/twist whose reduction matches; this concerns attack/preprocessing inputs, not secure curve selection.

Summary

- Rank ≥ 1 : logarithmic density $\frac{13}{14}$ — via the free class $[\infty_+ - \infty_-]$ and counting of torsion loci.
- Rank ≥ 2 : logarithmic density $\frac{5}{7}$ — via the two-section family and Néron–Serre specialization.
- **Consequence:** high-rank genus-2 Jacobians are abundant in the height ordering — useful for Regev-style preprocessing experiments ($d = r + 2$).

Thank you!

Joint with Răzvan Bărbulescu, Mugurel Barcău & Vicențiu Pașol. · arXiv:2601.17142

