Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

LOGARITHMIC DENSITY OF RANK ≥ 1 AND RANK ≥ 2 GENUS-2 JACOBIANS AND APPLICATIONS TO HYPERELLIPTIC CURVE CRYPTOGRAPHY

RAZVAN BARBULESCU, MUGUREL BARCAU, VICENŢIU PAŞOL, AND GEORGE C. ŢURCAŞ

Abstract. In this work we study quantitative existence results for genus-2 curves over $\mathbb{Q}$ whose Jacobians have Mordell–Weil rank at least 1 or 2, ordering the curves by the naive height of their integral Weierstrass models. We use geometric techniques to show that asymptotically the Jacobians of almost all integral models with two rational points at infinity have rank $r \geq 1$. Since there are $\asymp X^{\frac{13}{2}}$ such models among the X^7 curves $y^2 = f(x)$ of height at most X, this yields a lower bound of logarithmic density 13/14 for the subset of such curves whose Jacobians have rank at least 1. We further present a large explicit subfamily of genus-2 curves, ordered by height as above, for which the Jacobians have rank $r \geq 2$, yielding an unconditional logarithmic density of at least 5/7. Independently, we give a construction of genus-2 curves with split Jacobian and rank at least 2, producing a subfamily of logarithmic density at least 2/21. Finally, we analyze quadratic and biquadratic twist families in the split-Jacobian setting, obtaining a positive proportion of rank-2 twists. These results have implications for Regev's quantum algorithm in hyperelliptic curve cryptography.

1. Introduction

The Mordell–Weil theorem implies that for any smooth projective curve C of genus $g \geq 1$ defined over $\mathbb{Q}$, the group of rational points on its Jacobian admits a decomposition $\mathrm{Jac}(C)(\mathbb{Q}) \simeq T \times \mathbb{Z}^r$, where T is a finite group and $r \geq 0$ is an integer called the (Mordell–Weil) rank of $\mathrm{Jac}(C)(\mathbb{Q})$. A fundamental problem in arithmetic geometry is to understand how these ranks are distributed in families of curves, and in particular among hyperelliptic curves of a fixed genus g.

To ask precise distribution questions and give quantitative answers, one must first choose an ordering of the family, a notion of arithmetic *size* $H(C)$ and then count curves C with $H(C) \leq X$ as $X \to \infty$. Common choices include ordering by conductor, discriminant, or by various height functions on coefficients of integral models. Since counting by conductor is notoriously difficult (see [13]), here we enumerate integral models by the height of the coefficients of their models.

This work was supported by the project "Group schemes, root systems, and related representations" funded by the European Union - NextGenerationEU through Romania's National Recovery and Resilience Plan (PNRR) call no. PNRR-III-C9-2023- I8, Project CF159/31.07.2023, and coordinated by the Ministry of Research, Innovation and Digitalization (MCID) of Romania. The first author was supported by Agence Nationale de la Recherche under grant ANR-22-PNCQ-0002.

In particular, for a model of the form $C : y^2 = \sum_{i=0}^{2g+2} f_i x^i$ with $f_i \in \mathbb{Z}$, we define the height by $H_1(C) = \max\{|f_i|\}$ as in [6]. This gives rise to the following box

$$\mathcal{C}_1^{(g)}(X) = \left\{ C : y^2 = \sum_{i=0}^{2g+2} f_i x^i \in \mathbb{Z}[x] \middle| H_1(C) \leq X \right\} \tag{1}$$

of cardinality $(\gamma_1 + o(1))X^{2g+3}$, for an explicit constant $\gamma_1 > 0$. This is the ordering used by Booker et al. in [9].

Another height function, considered in [5] for models of the form $C : y^2 = x^{2g+1} + \sum_{k=2}^{2g+1} c_k x^{2g+1-k}$ with $c_i \in \mathbb{Z}$, is given by $H_2(C) = \max\{|c_k|^{\frac{2g(2g+1)}{k}}\}$, which gives rise to the box

$$\mathcal{C}_2^{(g)}(X) = \left\{ C : y^2 = x^{2g+1} + \sum_{k=2}^{2g+1} c_k x^{2g+1-k} \in \mathbb{Z}[x] \middle| H_2(C) \leq X \right\}. \tag{2}$$

By [5, Theorem 44] the cardinality of $\mathcal{C}_2^{(g)}(X)$ is $(\gamma_2 + o(1))X^{\frac{2g+3}{4g+2}}$ for an explicit constant $\gamma_2 > 0$.

Let $\mathcal{C}^{(g)}(X)$ denote one of the families of genus-g curves defined above (i.e., $\mathcal{C}_1^{(g)}(X)$ or $\mathcal{C}_2^{(g)}(X)$). If S is any set of hyperelliptic curves, we define $S(X) := S \bigcap \mathcal{C}^{(g)}(X)$. We say that S has *proportion* $\delta \in [0, 1]$ (with respect to the family $\mathcal{C}^{(g)}(X)$) if $\lim_{X\to\infty} \frac{|S(X)|}{|\mathcal{C}^{(g)}(X)|} = \delta$, whenever the limit exists. In many arithmetic situations of interest, such as hyperelliptic curves whose Jacobian has large Mordell–Weil rank, one expects this proportion to be zero. To capture the asymptotic size of such thin subsets, we introduce a logarithmic notion of density.

Definition 1. *A set S of hyperelliptic curves of genus g has logarithmic density α with respect to $\mathcal{C}^{(g)}(X)$ if*

$$\liminf_{X\to\infty} \frac{\log |S(X)|}{\log |\mathcal{C}^{(g)}(X)|} = \alpha.$$

In what follows, all notions of proportion and density are taken with respect to the family $\mathcal{C}_1^{(g)}(X)$, unless otherwise specified.

The main results of this article, some summarized in the next theorem, focus on the genus-2 case. Accordingly, when referring specifically to genus-2 curves, we omit the superscript (g) and write $\mathcal{C}(X)$ in place of $\mathcal{C}^{(g)}(X)$.

Theorem 1 (see Corollaries 2.7, 2.11 and Prop. 2.14)**.**

1. *The subset of genus-2 curves with split Jacobian and rank $r \geq 2$ has logarithmic density at least $\frac{2}{21}$ with respect to $\mathcal{C}_1(X)$.*
2. *The subset of genus-2 curves with rank $r \geq 1$ has logarithmic density at least $\frac{13}{14}$ with respect to $\mathcal{C}_1(X)$.*
3. *The subset of genus-2 curves with rank $r \geq 2$ has logarithmic density at least $\frac{5}{7}$ with respect to $\mathcal{C}_1(X)$.*

For comparison, in the case of elliptic curves the random matrix model predicts that the set of curves of rank $r \geq 2$ has logarithmic density $\frac{19}{24}$ with respect to $\mathcal{C}_2^{(1)}(X)$ (see Theorem 7.3.3 in [44]). In genus 2, we prove unconditional lower bounds $\frac{13}{14}$ for rank $r \geq 1$ and $5/7$ for rank $r \geq 2$ with respect to $\mathcal{C}_1(X)$. If rank parities are equidistributed in the subfamily with two points at infinity, then the

same construction would suggest logarithmic density at least $\frac{13}{14} > \frac{19}{24}$ for rank $r \geq 2$ as well. This phenomenon is also consistent with existing numerical data: for $X \leq 2^{18}$, the percentage of curves of rank at least 2 is larger among the Jacobians of genus-2 curves than among elliptic curves (see [3]).

Our work toward Theorem 1 is partially motivated by [9, Remark A.1], where the authors observe that, for genus-2 curves of small discriminant with small coefficients, the divisor class $[\infty_+ - \infty_-]$ is rational and typically has infinite order. Indeed, small coefficients make it more likely that the leading coefficient of $g(x) = 4f(x) + h(x)^2$ is a square, which implies rationality of the two points at infinity in the sextic case. We turn this heuristic into a conceptual and quantitative statement by viewing $[\infty_+ - \infty_-]$ as a universal section of the universal Jacobian, proving that this section is not torsion, and showing that among the integral models for which the two points at infinity are rational, the proportion for which $[\infty_+ - \infty_-]$ is torsion tends to 0. We also produce in Corollary 2.11 an unconditional source of Jacobian rank at least 2 by constructing an explicit two-section subfamily and applying Néron specialization. This offers a partial explanation for the abundance of rank-2 examples in small-coefficient or small-discriminant databases.

Remark 1.1 (Brute-force search complexity)**.** *A naive brute-force search that draws curves uniformly at random from $\mathcal{C}_1(X)$ would succeed in finding a curve of rank $r \geq 1$ in time $|\mathcal{C}_1(X)|^{1-\alpha+o(1)}$, where α is the logarithmic density of such curves in $\mathcal{C}_1(X)$. A consequence of the second part of this theorem is that the complexity of this algorithm is at most $O(X^{\frac{1}{2}+o(1)})$. Similarly, if such an algorithm is used to find curves of rank $r \geq 2$ by sampling uniformly at random from $\mathcal{C}_1(X)$, the third part of the theorem implies that the algorithm succeeds after at most $O(X^{2+o(1)})$ trials.*

The twists of a given curve. Let $C : y^2 = f(x)$ be a fixed hyperelliptic curve defined over $\mathbb{Q}$. For each squarefree integer d, we denote by $C^{(d)}$ the quadratic twist of C given by $dy^2 = f(x)$. We now study rank distributions within the family of quadratic twists of this fixed hyperelliptic curve. We consider the set

$$D(X) = \{d \in \mathbb{Z} \mid 1 \leq d < X \text{ and } d \text{ is squarefree}\}. \tag{3}$$

In complete analogy with a definition above, for any set S of squarefree integers, we set $S(X) := S \cap D(X)$. We say that S has *proportion* $\delta \in \mathbb{R}_{\geq 0} \cup \{\infty\}$ if the limit $\lim\limits_{X\to\infty} \frac{|S(X)|}{|D(X)|} = \delta$ exists. To measure the asymptotic size of subsets that have proportion 0 within a fixed twist family, we introduce the following logarithmic notion of density.

Definition 2. *Let C be a hyperelliptic curve and $r \geq 0$ be an integer. The logarithmic density of the set of twists $C^{(d)}$ with* $\operatorname{rank}(\operatorname{Jac}(C^{(d)})) \geq r$ *is defined by*

$$\alpha(C, r) := \liminf_{X\to\infty} \frac{\log\left|\{d \in D(X) \mid \operatorname{rank}(\operatorname{Jac}(C^{(d)})(\mathbb{Q})) \geq r\}\right|}{\log |D(X)|}.$$

For example, in [55] it is proven under BSD that, for all elliptic curves E, the proportion of rank $r \geq 2$ twists of E is 0. The proportion of odd rank twists exists for all hyperelliptic curves (see [63]), but it can be zero. It has been conjectured in [61] that it has a logarithmic density $\alpha = \frac{3}{4}$ whereas the best proven result is that of [28], where the authors show that $\alpha \geq \frac{1}{2}$.

We prove a result on the twists of a genus-2 curve with split Jacobian.

Theorem 2 (simplified statement of Prop. 2.19 and Prop. 2.18)**.**

(1) *Let $E_1, E_2/\mathbb{Q}$ be elliptic curves with full rational 2-torsion, together with an ordering of their nonzero 2-torsion points. Assume that isomorphism $E_1[2] \simeq E_2[2]$ is not induced by a $\overline{\mathbb{Q}}$-isomorphism $E_1 \simeq E_2$. For squarefree integers d_1, d_2, let $C^{(d_1,d_2)}$ be the genus-2 curve obtained by gluing the quadratic twists $E_1^{(d_1)}$ and $E_2^{(d_2)}$ with the induced ordering of their 2-torsion. If the Birch–Swinnerton-Dyer conjecture holds for the quadratic twists of E_1 and E_2, then*

$$\lim_{X\to\infty} \frac{\left|\{(d_1,d_2) \in D(X)^2 : \operatorname{rank} \operatorname{Jac}(C^{(d_1,d_2)})(\mathbb{Q}) \geq 2\}\right|}{|D(X)|^2} = \frac{1}{4}.$$

(2) *Let $E/\mathbb{Q}$ be a semistable elliptic curve admitting a $\mathbb{Q}$-rational 3-isogeny, and let $C/\mathbb{Q}$ be a genus-2 curve such that $\operatorname{Jac}(C) \sim_{\mathbb{Q}} E^2$. Then, for every nonzero squarefree integer d,*

$$\operatorname{Jac}(C^{(d)}) \sim_{\mathbb{Q}} \left(E^{(d)}\right)^2,$$

and

$$\liminf_{X\to\infty} \frac{\#\{d \in D(X) : \operatorname{rank}_{\mathbb{Q}} \operatorname{Jac}(C^{(d)}) \geq 2\}}{|D(X)|} > 0.$$

The theoretical arguments are accompanied by explicit computational experiments; the scripts illustrating the results are publicly available in the GitHub repository [3].

1.1. **Cryptographic consequences.** Hyperelliptic curve cryptography (HECC) is the genus-2 analogue of elliptic curve cryptography (ECC): one works in the Jacobian group $\operatorname{Jac}(C)(\mathbb{F}_q)$ of a genus-2 curve $C/\mathbb{F}_q$. In the classical proposal of Köblitz [36], the curve is sampled from a large family of models $C : y^2 + h(x)y = f(x)$ over $\mathbb{F}_q$, so that security is tied to the average-case difficulty of the discrete logarithm problem in these Jacobian groups. For simplicity in this cryptographic discussion, we take q to be prime.

Shor's algorithm [53] already gives a polynomial-time quantum algorithm for discrete logarithms. The relevance of Regev's work is different: Regev's factoring algorithm [49], and its extensions to the discrete logarithm problem by Ekerå and Gärtner [18], provide a new quantum approach whose cost per run, i.e. the size of the quantum circuit, depends on an additional parameter. This approach was adapted to elliptic curves in [2] and to genus-2 Jacobians in [4].

In the curve setting, the Regev parameter can be supplied by rational Mordell–Weil generators on a lift or twist of the curve. Section 3.1 makes this precise: subject to the usual independence heuristic for the reduced Mordell–Weil points, a rank-r lift or compatible twist allows one to take the Regev parameter to be $d = r + 2$. This is the sense in which high Mordell–Weil rank is useful for the Regev-style cryptanalytic preprocessing step. Throughout the paper, when we say that a curve is suitable for Regev's algorithm, we mean suitable as an input to this attack or experimental preprocessing procedure, not suitable as a recommendation for secure HECC curve selection.

This leads first to the corresponding search problem for rational curves.

Problem 1 (THE HIGH RANK CURVE PROBLEM)**.** *Fix an integer $g \geq 1$, a target rank $r \geq 0$, and a height-ordered family $\mathcal{F}^{(g)}$ of genus-g hyperelliptic curves over $\mathbb{Q}$, for instance $\mathcal{C}_1^{(g)}$, $\mathcal{C}_2^{(g)}$, or a prescribed height-ordered subfamily such as the split-Jacobian locus. For $X \geq 1$, write $\mathcal{F}^{(g)}(X)$ for the curves in this family of height at most X. Given X, sample a curve from the finite set*

$$\left\{ C \in \mathcal{F}^{(g)}(X) : \operatorname{rank} \operatorname{Jac}(C)(\mathbb{Q}) \geq r \right\},$$

if this set is nonempty.

Theorem 1 gives unconditional logarithmic-density lower bounds for this search in our height ordering, and Remark 1.1 translates these bounds into upper bounds on the number of random trials needed to find curves of rank at least 1 or at least 2. The explicit high-rank curves collected in Appendix A serve a different purpose: they provide concrete inputs for experiments with the Regev-style algorithm, rather than evidence for the density theorems.

For cryptographic applications, however, the curve over $\mathbb{F}_q$ is often fixed in advance. In that case one cannot freely sample a new rational curve; one instead searches for a high-rank lift, twist, or related curve whose reduction is isomorphic to the original curve, or whose reduced Jacobian is isogenous to the original Jacobian with suitable kernel. This leads to the second search problem.

Problem 2 (THE HIGH RANK TWIST PROBLEM)**.** *Let C be a rational genus-2 curve and let r be a fixed nonnegative integer.*

(1) *If $\operatorname{Jac}(C)$ is simple, find, if it exists, a squarefree integer $d \in [1, X]$ such that*

$$\operatorname{rank} \operatorname{Jac}(C^{(d)})(\mathbb{Q}) = r.$$

(2) *If $\operatorname{Jac}(C) \sim_{\mathbb{Q}} E^2$ for an elliptic curve $E/\mathbb{Q}$, find, if it exists, a squarefree integer $d \in [1, X]$ such that*

$$2 \operatorname{rank}\big((E^{(d)})(\mathbb{Q})\big) = r,$$

equivalently, under the induced isogeny,

$$\operatorname{rank} \operatorname{Jac}(C^{(d)})(\mathbb{Q}) = r.$$

(3) *Let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be elliptic curves satisfying the same conditions as in part (1) of Theorem 2 above. Find, if they exist, squarefree integers $(d_1, d_2) \in [1, X]^2$ such that $C^{(d_1,d_2)}$ satisfies*

$$\operatorname{rank} \operatorname{Jac}(C^{(d_1,d_2)})(\mathbb{Q}) = \operatorname{rank} E_1^{(d_1)}(\mathbb{Q}) + \operatorname{rank} E_2^{(d_2)}(\mathbb{Q}) = r,$$

where $C^{(d_1,d_2)}$ is constructed as above.

The Poincaré complete reducibility theorem motivates the cases separated in Problem 2: after extending the base field, the Jacobian of a genus-2 curve is either simple, isogenous to a product $E_1 \times E_2$ of two non-isogenous elliptic curves, or isogenous to E^2 for an elliptic curve E. The split cases are especially amenable to analysis because the genus-2 rank problem reduces to rank questions for elliptic curves; the compatibility of twisting with these split constructions is made precise in Lemma 2.16 and Propositions 2.18 and 2.19. Theorem 2, under its stated hypotheses, asserts that the relevant split-Jacobian twist families contain a positive proportion of twists of Jacobian rank at least 2.

Several structured subclasses of genus-2 curves used in cryptography, including split-Jacobian and CM families, have been studied extensively [12, 14, 16, 34]. We are not aware of a discrete-logarithm algorithm prior to this work which is faster for these subclasses than for general genus-2 Jacobians. The distinction in the present paper is that these structures can make the high-rank preprocessing used by the Regev-style algorithm easier. For CM curves of the form $y^2 = x^5 + a$, one can exploit dedicated arithmetic methods such as those in [57] and [41]; for split Jacobians, the constructions of Section 2.3 reduce the search to quadratic twists of elliptic curves. The computations in Section 3.2 illustrate these two phenomena on curves appearing in the cryptographic literature.

Acknowledgments. We would like to thank Bill Allombert and Aurel Page for discussions about the implementation of L-functions of genus-2 curves and Hecke characters in PARI/GP. We also thank Alex Bartel for suggesting, in a personal discussion, that the rank distribution of twists of certain curves used in cryptography may be explained by the decomposition of their Jacobians. Finally, we are very grateful to the anonymous referees for their careful reading of the manuscript and for their detailed, thoughtful, and constructive reports, which led us to correct several mathematical points, clarify the exposition, and improve the organization of the paper.

2. Main results

2.1. **Number of curves whose Jacobian has positive rank.** Following [9, Section 2.1], every genus-2 curve defined over an integral domain of characteristic $\neq 2$ admits a Weierstrass model

$$C: \quad y^2 + h(x)y = f(x), \tag{4}$$

with $\deg f \leq 6$ and $\deg h \leq 3$.

Completing the square gives the simplified equation

$$(2y + h(x))^2 \;=\; 4f(x) + h(x)^2 \;=:\; g(x). \tag{5}$$

The discriminant of (4) is defined by

$$\Delta(f,h) := 2^{-12}\mathrm{disc}\big(4f + h^2\big),$$

and $\Delta(f,h) \neq 0$ is equivalent to (4) defining a smooth genus-2 curve.

In the search for genus-2 curves of bounded discriminant, Booker et al. [9, Section 3.1] enumerate integral models of the form (4). Although these models are more general than the ones in the boxes $\mathcal{C}_1(X)$ and $\mathcal{C}_2(X)$ (see (1) and (2)), one may reduce h modulo 2 without changing the isomorphism class of the curve. Indeed, for any $q(x) \in \mathbb{Z}[x]$ with $\deg q \leq 3$, the change of variables $Y = y + q(x)$ transforms $y^2 + h(x)y = f(x)$ into the isomorphic integral model

$$Y^2 + (h(x) - 2q(x))Y = f(x) + q(x)h(x) - q(x)^2.$$

Moreover, $4\big(f + qh - q^2\big) + (h - 2q)^2 = 4f + h^2$, so the completed-square polynomial, and hence the discriminant, is unchanged. Choosing q coefficientwise therefore allows us to take every coefficient of h to be 0 or 1, which explains the condition $h_i \in \{0,1\}$ in the boxes below.

For parameters $X, Y \geq 1$ the authors of [9] define the boxes

$$\begin{cases} S_1(X) := \{(f,h) : |a_i| \leq X,\ h_i \in \{0,1\}\} \\ S_2(X,Y) := \{(f,h) : |a_i| \leq X\,Y^{6-i},\ h_i \in \{0,1\}\}. \end{cases},$$

where $f = \sum_{i=0}^{6} a_i x^i$ and $h = \sum_{i=0}^{\deg h} h_i x^i$. Thus $S_1(X)$ decomposes as the disjoint union of the 16 fibers obtained by fixing $h \in \{0,1\}^4$; each fiber has the same coefficient bounds for f as $\mathcal{C}_1(X)$, but parametrizes the models

$$y^2 + h(x)y = f(x)$$

with that fixed choice of h.

This motivates the definition of the following parameter space $\mathcal{U}^\infty$.

The parameter space $\mathcal{U}^\infty$. Let $\mathcal{H}$ be the reduced finite $\mathbb{Q}$-scheme with $\mathcal{H}(\mathbb{Q}) = \{0,1\}^4$ parametrizing the 16 possible choices of h with coefficients in $\{0,1\}$. Let

$$\mathcal{X} \;:=\; \mathbb{A}^7_{\mathbb{Q}} \times \mathcal{H}$$

be the parameter space of pairs (f,h) with $\deg f \le 6$, $\deg h \le 3$, and $h_i \in \{0,1\}$. We use coordinates $\underline{a} = (a_6, \dots, a_0)$ on the $\mathbb{A}^7$-factor, so that

$$f_{\underline{a}}(x) = a_6x^6 + a_5x^5 + \cdots + a_0 \text{ and } h(x) = h_3x^3 + h_2x^2 + h_1x + h_0$$

with $h_i \in \{0,1\}$. Since $\mathcal{X}$ is a disjoint union of 16 copies of $\mathbb{A}^7_{\mathbb{Q}}$, all arguments below should be read after fixing one h; in particular, for any irreducible component $\mathcal{X}_h \simeq \mathbb{A}^7_{\mathbb{Q}}$ and we will simply write $\mathcal{X}$.

Consider the universal genus-2 curve $\mathfrak{C} \to \mathcal{X}$, defined as the projective closure of the affine equation

$$y^2 + h(x)y = f_{\underline{a}}(x) \tag{6}$$

inside the weighted projective space $\mathbb{P}(1,3,1)$. Let $\mathcal{U} \subset \mathcal{X}$ denote the open subset where the discriminant of this equation is non-vanishing. Over $\mathcal{U}$, the morphism $\mathcal{C} \to \mathcal{U}$ is smooth and proper of relative dimension 1, and its geometric fibers are curves of genus 2. In addition, the Jacobian of $\mathcal{C}$ is an abelian scheme $\mathcal{J}$ over $\mathcal{U}$.

The two points at infinity and the universal section. Write $g(x) := 4f_{\underline{a}}(x) + h(x)^2$ and set

$$c := \operatorname{coeff}_{x^6}(g) = 4a_6 + h_3^2 \in \Gamma(\mathcal{U}, \mathcal{O}_{\mathcal{U}}).$$

Let $\mathcal{U}_6 \subset \mathcal{U}$ be the open subset where $c \neq 0$ (equivalently, $\deg g = 6$). In general the two points at ∞ are only defined after adjoining a square root of c, so we form the finite étale double cover $\pi : \mathcal{U}^\infty \longrightarrow \mathcal{U}_6$, where $\mathcal{U}^\infty := \operatorname{Spec}\big(\mathcal{O}_{\mathcal{U}_6}[u]/(u^2 - c)\big)$. On the weighted projective closure of (6) over $\mathcal{U}^\infty$ the fiber at infinity consists of two sections $\infty_\pm = (1 : \pm u : 0)$

We then define

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

For any rational point $\underline{a} \in \mathcal{U}^\infty(\mathbb{Q})$ we write $\mathfrak{C}_{\underline{a}}$, $\mathcal{J}_{\underline{a}}$ and $\alpha_{\underline{a}}$ for the corresponding specializations.

We now study the torsion loci of this universal section.

Algebraicity of torsion loci. For every integer $n \ge 1$ we define the *n-torsion locus* of α_{univ} by

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

Proposition 2.1. *For every positive integer n, $\mathcal{V}_n$ is a Zariski-closed subset of $\mathcal{U}^\infty$ and is defined over $\mathbb{Q}$.*

Proof. Recall $\mathcal{J} \to \mathcal{U}^\infty$ is an abelian scheme. Let $s : \mathcal{U}^\infty \to \mathcal{J}$ be the section corresponding to α_{univ}, $[n] : \mathcal{J} \to \mathcal{J}$ the multiplication-by-n morphism, and write $e : \mathcal{U}^\infty \to \mathcal{J}$ for the zero section.

By definition, $\underline{a} \in \mathcal{U}^\infty$ lies in $\mathcal{V}_n$ if and only if $[n](s(\underline{a})) = e(\underline{a})$ in the fiber $\mathcal{J}_{\underline{a}}$. Equivalently,

$$\mathcal{V}_n = \left\{ \underline{a} \in \mathcal{U}^\infty : ([n] \circ s, e)(\underline{a}) \in \Delta_{\mathcal{J}/\mathcal{U}^\infty} \right\},$$

where $([n] \circ s, e) : \mathcal{U}^\infty \to \mathcal{J} \times_{\mathcal{U}^\infty} \mathcal{J}$ is the product morphism and $\Delta_{\mathcal{J}/\mathcal{U}^\infty} \subset \mathcal{J} \times_{\mathcal{U}^\infty} \mathcal{J}$ is the relative diagonal.

Since $\mathcal{J} \to \mathcal{U}^\infty$ is an abelian scheme, it is proper and hence separated [31, Section 4], so its relative diagonal is closed [31, Corollary 4.2]. Taking preimages of closed subschemes under morphisms preserves closedness.

Finally, all maps and sections are defined over $\mathbb{Q}$, hence so is $\mathcal{V}_n$. □

The universal section is not torsion. We now prove that α_{univ} has infinite order in $\mathcal{J}(\mathcal{U}^\infty)$. For each of the 16 possible choices of $h(x)$, it suffices to find a single specialization $\underline{a} \in \mathcal{U}^\infty$ such that $\alpha_{\underline{a}}$ is non-torsion.

Take $h = 0$ and consider the curve

$$C : \quad Y^2 = X^6 + 18X^5 + 75X^4 + 120X^3 + 120X^2 + 72X + 28. \tag{7}$$

By [59, Section 4.2], we know that its Jacobian has rank 1 and is generated by the divisor class $[\infty_+ - \infty_-]$. This curve corresponds to $\underline{a} = (1, 18, 75, 120, 120, 72, 28) \in \mathcal{U}^\infty(\mathbb{Q})$ and hence $\alpha_{\underline{a}}$ has infinite order, from which we deduce that α_{univ} is non-torsion in $\mathcal{J}(\mathcal{U}^\infty)$.

Remark 2.2. *For the remaining* 15 *choices of* $h(x) \in \{0, 1\}^4$*, we ran an explicit search in the LMFDB. For each such* $h(x)$ *we found at least one specialization* $\underline{a} \in \mathcal{U}^\infty(\mathbb{Q})$ *for which the associated genus-*2 *curve has Jacobian of analytic rank* 1 *and trivial torsion subgroup. In all cases, the corresponding sextic satisfies the condition* $c = 4a_6 + h_3^2 \in (\mathbb{Q}^\times)^2$*, ensuring that the two points at infinity are* $\mathbb{Q}$*-rational. For brevity, we do not list these additional examples here but they are recorded in* [3, remark22_examples.md file].

We now turn the geometric input above into a quantitative statement for integral models of bounded height. The key point is that, for a curve $C/\mathbb{Q}$ given by an integral model (4), any torsion specialization $\alpha_a \in J_a(\mathbb{Q})$ has order bounded in terms of the height of the model. We need the following technical result.

Proposition 2.3. *Let* C *be a hyperelliptic curve with an integral model given by the equation* (4) *and let* $H(C) := \max_{0 \le i \le 6} |a_i|$*, be the naive height of* C*. Let* $\mathrm{Jac}(C)$ *be its Jacobian, equipped with its canonical principal polarization, and let* $h_F(\mathrm{Jac}(C))$ *be its normalized stable Faltings height (as defined in* [45, Definition 2.1]*). Then, for* $H(C)$ *large enough, we have*

$$h_F(\mathrm{Jac}(C)) \ll \log H(C)$$

where the implied constant is explicit and independent of C*.*

Proof. Kieffer used Thomae's formulae ([43, IIIa.8.1]) and height bounds for root differences of polynomials (see [35, Proposition 5.4]) to prove an explicit upper-bound for the level-4 θ-height (see [35, end of proof of Proposition 5.17]). This bound implies that, for $H(C) \ge 2$,

$$h_{\theta,4}(\mathrm{Jac}(C)) \ll \log H(C),$$

where the implied constant is explicit. Note that Kieffer uses a *naive* height for rational functions, which is $\ll \log H(C)$ (see Remark 3 after [35, Definition 5.1]).

We next use Pazuki's comparison theorem between θ-height and (stable) Faltings height h_F [45, Corollary 1.3(1)] with $g = 2$ and $r = 4$ which gives

$$\left|h_{\theta,4}(\mathrm{Jac}(C)) - \tfrac{1}{2}h_F(\mathrm{Jac}(C))\right| \ll \log(h_{\theta,4}(\mathrm{Jac}(C)) + 2),$$

with an effective implied constant which is independent of C.

Since $\log(h_{\theta,4}(\mathrm{Jac}(C)) + 2) \ll \log\log H(C)$ for large $H(C)$, the conclusion follows.

□

Theorem 1.2 of Gaudron–Rémond [27] (with $K = \mathbb{Q}$ and $g = 2$) implies that $|\mathrm{Jac}(C)(\mathbb{Q})_{tors}| \ll \max\{1, h_F(\mathrm{Jac}(C))\}^2$. Combining with Proposition 2.3, we obtain the following corollary.

Corollary 2.4. *Let $C/\mathbb{Q}$ be a smooth genus 2 curve with an integral model given by (4). Then for $H(C)$ sufficiently large,*

$$|\mathrm{Jac}(C)(\mathbb{Q})_{tors}| \ll (\log H(C))^2,$$

with an effective absolute implied constant which is independent of C.

Proposition 2.5. *Using the notations above, define*

$$T(X) := \Big\{\underline{a} \in \mathcal{U}^\infty(\mathbb{Z}) : H(\underline{a}) \le X,\ \alpha_{\underline{a}} \in \mathcal{J}_{\underline{a}}(\mathbb{Q}) \text{ is torsion}\Big\},$$

where $H(\underline{a}) := \max_{0\le i\le 6}|a_i|$. Then, for X sufficiently large, one has

$$\#T(X) \ll X^6(\log X)^6,$$

with an effective absolute implied constant independent of X. In particular,

$$\lim_{X\to\infty} \frac{\#T(X)}{\#\{\underline{a} \in \mathcal{U}^\infty(\mathbb{Z}) : H(\underline{a}) \le X\}} = 0.$$

Proof. Let $\underline{a} \in \mathcal{U}^\infty(\mathbb{Z})$ with $H(\underline{a}) \le X$ and assume that $\alpha_{\underline{a}}$ is torsion. By Corollary 2.4 (applied to the integral model parametrized by $\underline{a}$), we have

$$\left|\mathcal{J}_{\underline{a}}(\mathbb{Q})_{\mathrm{tors}}\right| \ll (\log H(C_{\underline{a}}))^2 \ll (\log X)^2,$$

for X sufficiently large. In particular,

$$\left|\mathcal{J}_{\underline{a}}(\mathbb{Q})_{\mathrm{tors}}\right| \le N(X), \qquad N(X) := \lceil \kappa(\log X)^2 \rceil$$

for some absolute constant $\kappa > 0$. Hence there exists an integer $1 \le n \le N(X)$ such that $[n]\alpha_{\underline{a}} = 0$, i.e. $\underline{a} \in \mathcal{V}_n$. Therefore

$$T(X) \subseteq \bigcup_{n=1}^{N(X)} \Big(\mathcal{V}_n(\mathbb{Z}) \cap \{\underline{a} \in \mathcal{U}^\infty(\mathbb{Z}) : H(\underline{a}) \le X\}\Big). \tag{8}$$

For each $n \ge 1$, Proposition 2.1 shows that $\mathcal{V}_n$ is Zariski-closed in $\mathcal{U}^\infty$ (and defined over $\mathbb{Q}$). Moreover, since α_{univ} is non-torsion in $\mathcal{J}(\mathcal{U}^\infty)$, the section $[n]\alpha_{\mathrm{univ}}$ is not identically zero, hence $\mathcal{V}_n \subsetneq \mathcal{U}^\infty$ is a *proper* closed subset.

We now bound integral points on $\mathcal{V}_n$ uniformly in terms of n. Since $\mathcal{U}^\infty$ is smooth over $\mathbb{Q}$ (hence normal and locally Noetherian), the abelian scheme $\mathcal{J} \to \mathcal{U}^\infty$ is projective (see for instance [23, Remarks 1.10(a)]) and admits a $\mathcal{U}^\infty$-ample line bundle. Fix such a line bundle $\mathcal{L}$, replace it by $\mathcal{L}\otimes[-1]^*\mathcal{L}$ to assume it is symmetric, and then replace $\mathcal{L}$ by a fixed tensor power so that it is relatively very ample and

induces a projectively normal embedding (Zariski-locally on $\mathcal{U}^\infty$) into $\mathbb{P}^N_{\mathcal{U}^\infty}$. For symmetric $\mathcal{L}$ one has

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

(cf. [40, Corollary 3.3]); by projective normality it follows that, in these projective coordinates, the morphism $[n] : \mathcal{J} \to \mathcal{J}$ is given by homogeneous polynomials of degree n^2. Composing with the section $s : \mathcal{U}^\infty \to \mathcal{J}$ corresponding to α_{univ} and comparing with the zero section, we obtain finitely many polynomial conditions on $\mathcal{U}^\infty$ of total degree $\ll n^2$ cutting out $\mathcal{V}_n$. Since $\mathcal{V}_n$ is proper, at least one of these conditions is nontrivial. Recall that, on one fixed h-component,

$$\mathcal{U}^\infty = \mathrm{Spec}\big(\mathcal{O}_{\mathcal{U}_6}[u]/(u^2 - c)\big), \qquad c = 4a_6 + h_3^2,$$

so u is the coordinate on the quadratic cover $\mathcal{U}^\infty \to \mathcal{U}_6 \subset \mathbb{A}^7$. Thus, viewing $\mathcal{U}^\infty$ as a finite cover of $\mathcal{U}_6 \subset \mathbb{A}^7$, we may eliminate u and obtain a nonzero polynomial $F_n \in \mathbb{Z}[a_6, \dots, a_0]$ with $\deg(F_n) \ll n^2$ such that every $\underline{a} \in \mathcal{V}_n$ satisfies $F_n(a_6, \dots, a_0) = 0$.

Let $S_X = [-X, X] \cap \mathbb{Z}$. We use the hypersurface estimate

$$\#\{\mathbf{z} \in S_X^m : F(\mathbf{z}) = 0\} \le (\deg F)|S_X|^{m-1}$$

for every nonzero $F \in \mathbb{Z}[x_1, \dots, x_m]$. Indeed, if F has degree e in one variable, then the fibers over points where the leading coefficient is nonzero contribute at most $e|S_X|^{m-1}$, while the fibers where the leading coefficient vanishes are bounded inductively by $(\deg F - e)|S_X|^{m-1}$. Applying this with $m = 7$ and $F = F_n$, and using that $U^\infty \to U_6$ is given by $u^2 = c$, so each coefficient tuple has at most two lifts to $U^\infty(\mathbb{Z})$, gives

$$\#\big(V_n(\mathbb{Z}) \cap \{H \le X\}\big) \le 2\,\#\{\mathbf{a} \in S_X^7 : F_n(\mathbf{a}) = 0\} \ll (\deg F_n)X^6 \ll n^2 X^6,$$

with absolute implied constants independent of n and X. Combining with (8) yields

$$\#T(X) \;\ll\; X^6 \sum_{n=1}^{N(X)} n^2 \;\ll\; X^6\, N(X)^3 \;\ll\; X^6 (\log X)^6.$$

Finally, since $\mathcal{U}^\infty \to \mathcal{U}_6 \subset \mathbb{A}^7$ is finite of degree 2, we can count that

$$\#\{\underline{a} \in \mathcal{U}^\infty(\mathbb{Z}) : H(\underline{a}) \le X\} \;\asymp\; X^6\sqrt{X} \;=\; X^{13/2}.$$

Hence

$$\frac{\#T(X)}{\#\{\underline{a} \in \mathcal{U}^\infty(\mathbb{Z}) : H(\underline{a}) \le X\}} \;\ll\; \frac{X^6(\log X)^6}{X^{13/2}} \;=\; X^{-1/2}(\log X)^6 \;\xrightarrow[X\to\infty]{}\; 0,$$

as claimed. □

As a consequence of Proposition 2.5 we obtain the following immediate corollaries.

Corollary 2.6. *The number of pairs $(f, h) \in S_1(X)$ for which*

$$\begin{cases} \deg(f) = 6, \\ \Delta(f, h) \neq 0, \\ \mathrm{coeff}_{x^6}(4f(x) + h(x)^2) \text{ is a square, and} \\ \text{the divisor } [\infty_+ - \infty_-] \text{ is torsion on the Jacobian of } y^2 + h(x)y = f(x) \end{cases}$$

is of the order $O(X^6(\log X)^6)$, as $X \to \infty$.

Let $S_1^{\square}(X)$ be the subset of $S_1(X)$ defined by the first three conditions in Corollary 2.6. We claim that $\#S_1^{\square}(X) \asymp X^{13/2}$. Indeed, fix $h \in \{0,1\}^4$ and write $c = \mathrm{coeff}_{x^6}(4f+h^2) = 4a_6+h_3^2$. The condition that c is a square gives $\asymp X^{1/2}$ possible leading coefficients a_6 with $|a_6| \le X$ and $a_6 \neq 0$: if $h_3 = 0$, then $a_6 = t^2$ with $1 \le t^2 \le X$, while if $h_3 = 1$, then $a_6 = t(t+1)$ with $1 \le t(t+1) \le X$. For each such a_6, the remaining six coefficients $a_5, \dots, a_0$ have $(2X+1)^6$ possible values before imposing smoothness. For fixed h and a_6, the discriminant condition $\Delta(f,h) = 0$ is a nonzero polynomial condition in $a_5, \dots, a_0$: indeed, the lower coefficients of $4f + h^2$ are affine coordinates over $\mathbb{Q}$, and there exist separable sextics with any prescribed nonzero leading coefficient. Thus the elementary hypersurface estimate used above shows that the singular choices contribute $O(X^5)$ for each admissible a_6, hence $O(X^{11/2})$ choices in total after summing over a_6 and over the finitely many choices of h. Therefore

$$\#S_1^{\square}(X) \asymp X^{1/2} \cdot X^6 = X^{13/2}.$$

Together with Corollary 2.6, this shows that the proportion of $(f,h) \in S_1^{\square}(X)$ for which $[\infty_+ - \infty_-]$ is torsion on $\mathrm{Jac}(y^2 + h(x)y = f(x))$ is

$$O\big(X^{-1/2}(\log X)^6\big).$$

This allows us to prove part (2) of Theorem 1.

Corollary 2.7. *For $(f,h) \in S_1^{\square}(X)$, write $J_{(f,h)}$ for the Jacobian of $y^2 + h(x)y = f(x)$. Then, as $X \to \infty$,*

$$1 - O\big(X^{-1/2}(\log X)^6\big) \le \frac{\#\{(f,h) \in S_1^{\square}(X) : \mathrm{rank}\, J_{(f,h)}(\mathbb{Q}) \ge 1\}}{\#S_1^{\square}(X)} \le 1.$$

In particular,

$$\liminf_{X\to\infty} \frac{\log\big|\{(f,h) \in S_1(X) : \mathrm{rank}\, J_{(f,h)}(\mathbb{Q}) \ge 1\}\big|}{\log|S_1(X)|} \ge \frac{13}{14}.$$

Proof. Let $E_1(X) \subset S_1^{\square}(X)$ be the subset for which $\alpha_{(f,h)} = [\infty_+ - \infty_-] \in J_{(f,h)}(\mathbb{Q})$ is torsion. By Corollary 2.6 and the count of $S_1^{\square}(X)$ above,

$$\frac{\#E_1(X)}{\#S_1^{\square}(X)} = O\big(X^{-1/2}(\log X)^6\big).$$

If $J_{(f,h)}(\mathbb{Q})$ has rank 0, then every rational point of $J_{(f,h)}(\mathbb{Q})$ is torsion; in particular $\alpha_{(f,h)}$ is torsion. Thus

$$S_1^{\square}(X) \setminus E_1(X) \subseteq \{(f,h) \in S_1^{\square}(X) : \mathrm{rank}\, J_{(f,h)}(\mathbb{Q}) \ge 1\}.$$

This gives the displayed lower bound, while the upper bound is trivial. Since $\#S_1^{\square}(X) \asymp X^{13/2}$ and $\#S_1(X) \asymp X^7$, the claimed logarithmic density lower bound of $\frac{13}{14}$ also follows. □

Proposition 2.8. *Assume $h(x) = 0$. Define the subvariety*

$$\mathcal{U}_{1,1}^{\infty} := \big\{\underline{a} = (a_6, \dots, a_0) \in \mathcal{U}^{\infty} \ : \ a_6 = 1,\ a_0 = 1\big\}.$$

For $\underline{a} \in \mathcal{U}_{1,1}^{\infty}$ we write

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

and we denote by $\infty_\pm$ the two points at infinity. Let $\mathcal{J} \to \mathcal{U}_{1,1}^\infty$ be the restriction of the universal Jacobian, and let

$$P_{\mathrm{univ}} = (0,-1) \in \mathcal{C}(\mathcal{U}_{1,1}^\infty) \qquad \text{and} \qquad \beta_{\mathrm{univ}} := [P_{\mathrm{univ}} - \infty_+] \in \mathcal{J}(\mathcal{U}_{1,1}^\infty).$$

Then the two sections $\alpha_{\mathrm{univ}}|_{\mathcal{U}_{1,1}^\infty}$ and β_{univ} are $\mathbb{Z}$–linearly independent in $\mathcal{J}(\mathcal{U}_{1,1}^\infty)$.

Proof. Consider the specialization at

$$C_0 : \quad y^2 = x^6 + 8x^5 + 10x^4 + 10x^3 + 5x^2 + 2x + 1,$$

corresponding to $\underline{a}_0 = (1,8,10,10,5,2,1) \in \mathcal{U}_{1,1}^\infty(\mathbb{Z})$. The LMFDB entry for C_0 (see LMFDB:15625.a.15625.1) states that $\mathrm{Jac}(C_0)(\mathbb{Q}) \simeq \mathbb{Z}^2$ and has trivial torsion, and it lists generators on the (simplified) model as

$$G_1 = 2(0:-1:1) - (1:-1:0) - (1:1:0), \qquad G_2 = (0:-1:1) - (1:1:0)$$

(see [39]). With our notation $\infty_+ = (1:1:0)$, $\infty_- = (1:-1:0)$ and $P = (0:-1:1)$, we have $G_2 = \beta_{\underline{a}_0}$ and

$$G_1 - 2G_2 = (1:1:0) - (1:-1:0) = \alpha_{\underline{a}_0}.$$

Hence $\alpha_{\underline{a}_0}$ and $\beta_{\underline{a}_0}$ generate a rank-2 subgroup of $\mathrm{Jac}(C_0)(\mathbb{Q})$, so in particular they are $\mathbb{Z}$–linearly independent. If there were a nontrivial relation $m\alpha_{\mathrm{univ}} + n\beta_{\mathrm{univ}} = 0$ in $\mathcal{J}(\mathcal{U}_{1,1}^\infty)$, it would specialize to the same relation at $\underline{a}_0$, a contradiction. □

On this locus we have that $u^2 = 4$ and $\mathcal{U}_{1,1}^\infty$ is the disjoint union of the two components $u = 2$ and $u = -2$. To avoid introducing new notation, for the next two results, we apply the argument on each component and take the union of the two resulting thin exceptional sets.

Proposition 2.9. *Let $\Gamma \subset \mathcal{J}(\mathcal{U}_{1,1}^\infty)$ be the subgroup generated by $\alpha_{\mathrm{univ}}|_{\mathcal{U}_{1,1}^\infty}$ and β_{univ}. There exists a thin subset $\Omega \subset \mathcal{U}_{1,1}^\infty(\mathbb{Q})$ (in the sense of [51, §9.1]) such that for every $\underline{a} \in \mathcal{U}_{1,1}^\infty(\mathbb{Q}) \setminus \Omega$, the specialization map*

$$\mathrm{sp}_{\underline{a}} : \Gamma \longrightarrow \mathrm{Jac}(C_{\underline{a}})(\mathbb{Q})$$

is injective. In particular, for such $\underline{a}$ the points $\alpha_{\underline{a}}$ and $\beta_{\underline{a}}$ are $\mathbb{Z}$–linearly independent and

$$\mathrm{rank}\,\mathrm{Jac}(C_{\underline{a}})(\mathbb{Q}) \;\geq\; 2.$$

Proof. Since $\mathcal{U}_{1,1}^\infty$ is a Zariski open subset of an affine 5–space, its function field is a purely transcendental extension $K = \mathbb{Q}(a_1, \ldots, a_5)$. Let A/K be the generic fiber of the abelian scheme $\mathcal{J} \to \mathcal{U}_{1,1}^\infty$. By Proposition 2.8, the subgroup $\Gamma \subset A(K)$ has rank 2. Néron's specialization theorem (as stated in [51, §11.1]) asserts that the set of $\underline{a} \in \mathcal{U}_{1,1}^\infty(\mathbb{Q})$ for which the specialization homomorphism $A(K) \to \mathrm{Jac}(C_{\underline{a}})(\mathbb{Q})$ fails to be injective is thin. Taking Ω to be this thin set gives the claim. □

Corollary 2.10. *Define*

$$\mathcal{U}_{1,1}^\infty(\mathbb{Z}; X) := \{a \in \mathcal{U}_{1,1}^\infty(\mathbb{Z}) : H(a) \leq X\}, \qquad H(a) = \max_{0 \leq i \leq 6} |a_i|.$$

Then there exists $\gamma > 0$ such that, for X sufficiently large,

$$\#\{a \in \mathcal{U}_{1,1}^\infty(\mathbb{Z}; X) : \mathrm{rank}\,\mathrm{Jac}(C_a)(\mathbb{Q}) < 2\} \ll X^{9/2}(\log X)^\gamma.$$

Consequently,

$$1 - O\big(X^{-1/2}(\log X)^\gamma\big) \leq \frac{\#\{a \in \mathcal{U}_{1,1}^\infty(\mathbb{Z}; X) : \mathrm{rank}\,\mathrm{Jac}(C_a)(\mathbb{Q}) \geq 2\}}{\#\mathcal{U}_{1,1}^\infty(\mathbb{Z}; X)} \leq 1.$$

Proof. Let Ω be as in Proposition 2.9. For every $a \in \mathcal{U}_{1,1}^{\infty}(\mathbb{Q}) \setminus \Omega$, the specialization map is injective on the subgroup generated by α_{univ} and β_{univ}. Hence α_a and β_a are $\mathbb{Z}$-linearly independent in $\mathrm{Jac}(C_a)(\mathbb{Q})$, and therefore

$$\operatorname{rank} \mathrm{Jac}(C_a)(\mathbb{Q}) \geq 2.$$

Thus

$$\{a \in \mathcal{U}_{1,1}^{\infty}(\mathbb{Z}; X) : \operatorname{rank} \mathrm{Jac}(C_a)(\mathbb{Q}) < 2\} \subseteq \Omega \cap [-X, X]^5.$$

Since Ω is thin in $\mathbb{A}^5(\mathbb{Q})$, Serre's quantitative estimate for affine thin sets [51, §13.1, Theorem 1] (with $K = \mathbb{Q}$, $n = 5$, $d = 1$) gives

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

Moreover $\#\mathcal{U}_{1,1}^{\infty}(\mathbb{Z}; X) \asymp X^5$ (the complement of $\mathcal{U}_{1,1}^{\infty}$ is Zariski closed of codimension ≥ 1, hence contributes $O(X^4)$ points). The two components $u = \pm 2$, mentioned before Proposition 2.9 only change the leading constant. This proves the bound for the rank smaller than 2 locus and hence the displayed lower bound for the proportion of Jacobians of rank greater than or equal to 2. □

Corollary 2.11 (part (3) of Theorem 1)**.** *One has*

$$\liminf_{X \to \infty} \frac{\log \big|\{(f,h) \in S_1(X) : \operatorname{rank}\big(J_{(f,h)}(\mathbb{Q})\big) \geq 2\}\big|}{\log |S_1(X)|} \ \geq \ \frac{5}{7}.$$

Proof. For $X \geq 1$, the family $\mathcal{U}_{1,1}^{\infty}(\mathbb{Z}; X)$ parametrizes a subset of $\mathcal{C}_1(X)$ of cardinality $\asymp X^5$ (five freely varying coefficients, with $a_6 = a_0 = 1$ fixed). By Corollary 2.10, all but $O(X^{9/2}(\log X)^{\gamma})$ of these model curves have Jacobian rank at least 2. Since $|S_1(X)| \asymp X^7$, the stated logarithmic density follows. □

Corollaries 2.7 and 2.11 show that, in an arithmetic ordering by height, imposing the condition that the two points at infinity are $\mathbb{Q}$-rational produces a distinguished rational class $\alpha_C = [\infty_+ - \infty_-] \in \mathrm{Jac}(C)(\mathbb{Q})$, which is non-torsion for all but a negligible subset of models.

Moreover, Corollary 2.11 gives an unconditional source of *two* independent rational classes on a large explicit subfamily: on the 5-parameter family $U_{\infty}^{1,1}(\mathbb{Z}; X)$ (of logarithmic density $\frac{5}{7}$ inside $C_1(X)$).

Completely analogously to $S_1^{\square}(X)$, write $S_2^{\square}(X, Y)$ for the subset of $S_2(X, Y)$ defined by the same conditions. For a fixed $Y \geq 1$, one has $\#S_2^{\square}(X, Y) \asymp_Y X^{13/2}$ when $X \to \infty$. Then, we have the following corollary.

Corollary 2.12. *For any fixed positive integer Y, when $X \to \infty$ we have*

$$1 - O_Y\big(X^{-1/2}(\log X)^6\big) \leq \frac{\#\{(f,h) \in S_2^{\square}(X, Y) : \operatorname{rank} J_{(f,h)}(\mathbb{Q}) \geq 1\}}{\#S_2^{\square}(X, Y)} \leq 1.$$

Remark 2.13. *The arguments of this subsection extend to hyperelliptic curves of genus $g \geq 1$: imposing a condition that guarantees the existence of two points at infinity produces a subfamily of size $\asymp X^{2g+2}\sqrt{X}$ inside the box of size $\asymp X^{2g+3}$, so one obtains rank $r \geq 1$ for a set of logarithmic density at least $\frac{4g+5}{4g+6}$. For rank $r \geq 2$ one would need a second section and to prove it is generically $\mathbb{Z}$-independent from $[\infty_+ - \infty_-]$; without an explicit specialization witnessing independence, proving this would require other ideas in higher genus.*

2.2. **A lower bound for the number of genus-2 curves with split Jacobian and rank at least 2.** In this subsection we give an explicit construction of *many* models for genus-2 curves whose Jacobians have Mordell–Weil rank at least 2. The family we consider here has split Jacobian, so the rank computation reduces to a rank computation on the two elliptic curves factors. We follow the construction of Gajović–Park in [26].

Proposition 2.14. *Let* $\mathcal{N}_2(X) = \{f \in \mathcal{C}_1(X) \mid \operatorname{rank} \operatorname{Jac}(C_f) \geq 2\}$. *Then*

$$|\mathcal{N}_2(X)| \gg \frac{X^{2/3}}{(\log X)^2}.$$

We prove the proposition using two auxiliary inputs recorded in Gajović–Park. For squarefree integers $d, m \neq 0$, let

$$C_{d,m}:\ y^2 = d^3x^6 + m^3, \qquad E_d:\ y^2 = x^3 + d^3, \qquad E_m:\ y^2 = x^3 + m^3.$$

The split-Jacobian construction in [26, Section 2.2] gives $\operatorname{Jac}(C_{d,m}) \sim_{\mathbb{Q}} E_d \times E_m$, hence

$$\operatorname{rank} \operatorname{Jac}(C_{d,m})(\mathbb{Q}) = \operatorname{rank} E_d(\mathbb{Q}) + \operatorname{rank} E_m(\mathbb{Q}).$$

We also use the needed case of Frey's rank computation, as cited in [26, proof of Theorem 2.5]: if $p > 3$ is prime, $p \equiv 3 \pmod 4$, then $\operatorname{rank} E_p(\mathbb{Q}) = 1$.

Proof of Proposition 2.14 . Fix $X \geq 1$. Consider all pairs of primes (d, m) with

$$d \leq X^{1/3}, \quad m \leq X^{1/3}, \quad d \equiv m \equiv 3 \pmod 4, \quad d, m > 3.$$

For each such pair, define the polynomial $f_{d,m}(x) = d^3x^6 + m^3$. By construction, $|f_{d,m}| = \max\left\{\left|d^3\right|, \left|m^3\right|\right\} \leq X$ so $C_{d,m}$ is a smooth hyperelliptic curve lying in $\mathcal{C}_1(X)$.

By the cited isogeny and Frey's rank computation, both E_d and E_m have rank 1, and hence $\operatorname{rank} \operatorname{Jac}(C_{d,m})(\mathbb{Q}) = 2$.

Using the Prime Number Theorem for primes in arithmetic progressions, we have

$$\left|\left\{p \leq X^{1/3} : p \text{ prime}, p \equiv 3 \bmod 4\right\}\right| \sim \frac{3}{2}\frac{X^{1/3}}{\log X}$$

hence the number of pairs (d, m) as above is asymptotically $\frac{9}{4}\frac{X^{2/3}}{(\log X)^2}$. □

2.3. **Finding high rank twists of genus-2 curves with split Jacobian.** The aim of this section is to explain how to construct twists of genus-2 curves with split Jacobians whose Mordell—Weil rank is high. We will follow the presentation of [33], recalling the main constructions and results relevant for our purposes and adapting them to our specific setting.

Let K be a field of characteristic zero, and let $\bar{K}$ be an algebraic closure of K. Let F and G be elliptic curves over K given by the equations $y^2 = f(x)$ and $y^2 = g(x)$, respectively, where f and g are separable monic cubic polynomials in $K[x]$, with discriminants $\operatorname{disc}(f)$ and $\operatorname{disc}(g)$. Suppose that

$$\psi\colon F[2](\bar{K}) \longrightarrow G[2](\bar{K})$$

is an isomorphism of Galois modules that does not arise from an isomorphism $F_{\bar{K}} \to G_{\bar{K}}$. In the situation of Proposition 2.15, since both curves have full K-rational 2-torsion, the isomorphism ψ is given by a bijection between the sets $\{(\alpha_i, 0)\}$ and $\{(\beta_i, 0)\}$, identifying the 2-torsion points corresponding to the roots of f and g.

Then one can *glue* F and G along ψ as follows. Let $H \subset F \times G$ be the graph of ψ, viewed as a finite subgroup scheme. The quotient $(F \times G)/H$ is an abelian surface defined over K, and, as explained below, it is isomorphic to the Jacobian of a genus-2 curve defined over K.

A precise justification of this construction is given in [33, Section 3.2]. More precisely, the quotient $(F \times G)/H$ carries a natural principal polarization induced by the product polarization on $F \times G$, and it follows from [33, Proposition 3 and Section 3.2] that this principally polarized abelian surface is isomorphic over K to the Jacobian of a genus-2 curve.

Proposition 2.15 (Prop. 4 in [33])**.** *Let $F\colon y^2 = f(x)$ and $G\colon y^2 = g(x)$ be elliptic curves over K with full K-rational 2-torsion. Let $\alpha_1, \alpha_2, \alpha_3$ (resp. $\beta_1, \beta_2, \beta_3$) be the roots of f (resp. g), indexed cyclically modulo 3. Define*

$$a_1 = \sum_{i=1}^{3} \frac{(\alpha_{i+2} - \alpha_{i+1})^2}{\beta_{i+2} - \beta_{i+1}}, \qquad b_1 = \sum_{i=1}^{3} \frac{(\beta_{i+2} - \beta_{i+1})^2}{\alpha_{i+2} - \alpha_{i+1}},$$

$$a_2 = \sum_{i=1}^{3} \alpha_i(\beta_{i+2} - \beta_{i+1}), \qquad b_2 = \sum_{i=1}^{3} \beta_i(\alpha_{i+2} - \alpha_{i+1}),$$

and set

$$A = \operatorname{disc}(g)\frac{a_1}{a_2}, \qquad B = \operatorname{disc}(f)\frac{b_1}{b_2}.$$

Define

$$\operatorname{glue}(f,g) = -\prod_{i=1}^{3}\big(A(\alpha_{i+1} - \alpha_i)(\alpha_i - \alpha_{i-1})x^2 + B(\beta_{i+1} - \beta_i)(\beta_i - \beta_{i+2})\big),$$

where all indices are taken modulo 3. Then $\operatorname{glue}(f,g)$ is a separable sextic polynomial in $K[x]$. Let $C\colon y^2 = \operatorname{glue}(f,g)(x)$. Let $H \subset F \times G$ be the graph of the isomorphism

$$(\alpha_i, 0) \longmapsto (\beta_i, 0), \qquad i = 1, 2, 3.$$

Then

$$\operatorname{Jac}(C) \simeq_K (F \times G)/H.$$

In particular,

$$\operatorname{Jac}(C) \sim_K F \times G.$$

For any nonzero integer d, let $F^{(d)}$ (resp. $G^{(d)}$) denote the quadratic twist of F (resp. G), given by the equation $y^2 = f^{(d)}(x)$ (resp. $y^2 = g^{(d)}(x)$), where $f^{(d)}(x) = d^3 f(x/d)$ (resp. $g^{(d)}(x) = d^3 g(x/d)$).

Lemma 2.16. *Let $F\colon y^2 = f(x)$ and $G\colon y^2 = g(x)$ be elliptic curves over K with full 2-torsion, and let $C\colon y^2 = \operatorname{glue}(f,g)$. For any nonzero integer d, the curve*

$$C^{(d)}\colon dy^2 = \operatorname{glue}(f,g)$$

is isomorphic to the curve

$$y^2 = \operatorname{glue}\big(f^{(d)}, g^{(d)}\big).$$

Proof. A direct calculation shows that the roots of $f^{(d)}$ (resp. $g^{(d)}$) are $d\alpha_i$ (resp. $d\beta_i$). Moreover,

$$\operatorname{disc}\big(f^{(d)}\big) = d^6\operatorname{disc}(f), \qquad \operatorname{disc}\big(g^{(d)}\big) = d^6\operatorname{disc}(g),$$

and

$$\operatorname{glue}\big(f^{(d)}, g^{(d)}\big) = d^{21} \operatorname{glue}(f, g).$$

The change of variables $y \mapsto d^{11}y$ transforms the equation $y^2 = \operatorname{glue}\big(f^{(d)}, g^{(d)}\big)$ into $dy^2 = \operatorname{glue}(f, g)$, as claimed. □

The lemma suggests a manner to find high rank quadratic twists of a genus-2 curve C such that $\operatorname{Jac}(C)$ is isogenous to $F \times G$ for two elliptic curves F and G with full rational 2-torsion: one finds integers d such that both $F^{(d)}$ and $G^{(d)}$ have high rank. Ralph Greenberg proposed a study in terms of Galois representations (see [32] for a review and recent results).

Note that all elliptic curves $E : y^2 = f(x)$ with full rational 2-torsion have a quadratic twist $E^{(d)} : dy^2 = f(x)$ which can be put in Legendre form $y^2 = x(x-1)(x-\lambda)$, with λ in its coefficient field. If F and G are two elliptic curves with full rational 2-torsion and if there exists a twist d_0 such that both $F^{(d_0)}$ and $G^{(d_0)}$ are in Legendre form the following result (see [1, Lemma 4.1]) asserts the existence of twists where both curves have positive rank.

Proposition 2.17. *Assume the abc-conjecture. Let $F\colon y^2 = f(x)$ and $G\colon y^2 = g(x)$ be two non-isomorphic elliptic curves over $\mathbb{Q}$ such that*

$$f(x) = x(x-1)(x-\lambda_1), \qquad g(x) = x(x-1)(x-\lambda_2),$$

for some distinct $\lambda_1, \lambda_2 \in \mathbb{Q}$. Let C be the genus-2 curve given by the equation $y^2 = \operatorname{glue}(f, g)$. For each nonzero integer d, consider the quadratic twist $C^{(d)}$ of C given by $dy^2 = \operatorname{glue}(f, g)$. Then the set of squarefree integers d such that

$$\operatorname{rank}_{\mathbb{Q}} \operatorname{Jac}(C^{(d)}) \geq 2$$

has logarithmic density at least $\frac{1}{6}$.

Proof. Replacing λ_i by an equivalent Legendre parameter if necessary, we may assume that

$$0 < \lambda_1 < \lambda_2 < 1.$$

Set

$$D(u) = (\lambda_1 - \lambda_2)(u^2 - 1)\big(1 - \lambda_2 + (\lambda_1 - 1)u^2\big)\big(\lambda_1 u^2 - \lambda_2\big).$$

Since the leading coefficient of $D(u)$ is

$$(\lambda_1 - \lambda_2)(\lambda_1 - 1)\lambda_1 > 0,$$

we have $D(u) > 0$ for all sufficiently large u. By [1, Lemma 4.1], the simultaneous twists $F^{(D(u))}$ and $G^{(D(u))}$ have positive rank over $\mathbb{Q}(u)$. By the Néron–Silverman specialization theorem [54, Chapter III, Theorem 11.4], for all but finitely many $u_0 \in \mathbb{Q}$, the specialized twists $F^{(D(u_0))}$ and $G^{(D(u_0))}$ have positive rank over $\mathbb{Q}$.

For such a specialization, let d be the squarefree representative of the class of $D(u_0)$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Then $F^{(D(u_0))} \simeq_{\mathbb{Q}} F^{(d)}$ and $G^{(D(u_0))} \simeq_{\mathbb{Q}} G^{(d)}$. Moreover, by Lemma 2.16 and Proposition 2.15,

$$\operatorname{Jac}(C^{(d)}) \sim_{\mathbb{Q}} F^{(d)} \times G^{(d)}.$$

Hence, since Mordell–Weil rank is invariant under isogeny,

$$\operatorname{rank}_{\mathbb{Q}} \operatorname{Jac}(C^{(d)}) = \operatorname{rank}_{\mathbb{Q}} F^{(d)} + \operatorname{rank}_{\mathbb{Q}} G^{(d)} \geq 2.$$

Since $D(u)$ is a squarefree polynomial of degree 6, Theorem 3.5 of [48], whose proof relies on the *abc*-conjecture, implies that the number of squarefree representatives in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ represented by the values $D(u)$ with $1 \le u \le B$ is $\gg B$. Choose $a > 0$ such that $D(u) \le X$ whenever

$$1 \le u \le aX^{1/6}$$

and X is sufficiently large. For each such value of u, let d be the positive squarefree representative of the class of $D(u)$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Then there exists a constant $C > 0$, depending only on λ_1 and λ_2, such that

$$d \le CD(u).$$

Hence $d \le CX$, and therefore the number of positive squarefree integers $d \le X$ obtained in this way is $\gg X^{1/6}$. Removing the finitely many exceptional specializations does not affect this lower bound.

Since $|D(X)| \asymp X$, it follows that

$$\liminf_{X\to\infty} \frac{\log\bigl|\{d \in D(X) : \operatorname{rank}_{\mathbb{Q}} \operatorname{Jac}(C^{(d)}) \ge 2\}\bigr|}{\log|D(X)|} \ge \frac{1}{6}.$$

This proves the claimed logarithmic density lower bound. □

We next describe the distribution of ranks in families of quadratic twists of genus-2 Jacobians that are isogenous to the square of an elliptic curve admitting a rational 3-isogeny.

We fix a hyperelliptic model $C : y^2 = h(x)$ over K. For $d \in K^\times$, we denote by $C^{(d)} : dy^2 = h(x)$ the quadratic twist relative to this model. Over $K(\sqrt{d})$, the curves C and $C^{(d)}$ are isomorphic via $(x, y) \mapsto (x, \sqrt{d}\, y)$. The associated descent cocycle is given by the hyperelliptic involution $(x, y) \mapsto (x, -y)$, which induces multiplication by -1 on $\operatorname{Jac}(C)$. It follows that $\operatorname{Jac}(C^{(d)})$ is the quadratic twist of $\operatorname{Jac}(C)$ by $[-1]$.

Proposition 2.18. *Let $E/\mathbb{Q}$ be a semistable elliptic curve admitting a $\mathbb{Q}$-rational 3-isogeny, and let $C/\mathbb{Q}$ be a genus-2 curve such that $\operatorname{Jac}(C) \sim_{\mathbb{Q}} E^2$. With $D(X)$ as in (3), one has*

$$\liminf_{X\to\infty} \frac{\#\{d \in D(X) : \operatorname{rank}_{\mathbb{Q}} \operatorname{Jac}(C^{(d)}) = 2\}}{|D(X)|} > 0.$$

Proof. Let $\mathcal{D}(X) = \{\Delta > 0 : \Delta < X,\ \Delta \text{ is a fundamental discriminant}\}$. Since E is semistable and admits a $\mathbb{Q}$-rational 3-isogeny, [38, Proposition 9.7] gives

$$\#\{\Delta \in \mathcal{D}(X) : \operatorname{ord}_{s=1} L(E^{(\Delta)}, s) = 1\} \gg_E X.$$

From the works of Gross–Zagier [30] and Kolyvagin [37] it follows that analytic rank 1 implies Mordell–Weil rank 1, hence $\#\{\Delta \in \mathcal{D}(X) : \operatorname{rank}_{\mathbb{Q}} E^{(\Delta)} = 1\} \gg_E X$.

We now pass from positive fundamental discriminants to positive squarefree twist parameters. For $\Delta \in \mathcal{D}(X)$, define

$$\operatorname{sf}(\Delta) = \begin{cases} \Delta, & \Delta \equiv 1 \pmod 4, \\ \Delta/4, & \Delta \equiv 0 \pmod 4. \end{cases}$$

Then $\operatorname{sf}(\Delta) \in D(X)$, the map $\Delta \mapsto \operatorname{sf}(\Delta)$ is injective, and $\Delta/\operatorname{sf}(\Delta) \in \mathbb{Q}^{\times 2}$. Therefore $E^{(\Delta)} \simeq_{\mathbb{Q}} E^{(\operatorname{sf}(\Delta))}$. Moreover, it is known (see for instance [24, page 467]) that

$|D(X)| \sim \frac{6}{\pi^2}X$ and $|\mathcal{D}(X)| \sim \frac{3}{\pi^2}X$, so $|\mathcal{D}(X)|/|D(X)| \to 1/2$. It follows that

$$\#\{d \in D(X) : \operatorname{rank}_{\mathbb{Q}} E^{(d)} = 1\} \gg_E X,$$

and hence this set has positive lower proportion inside $D(X)$. For each such d,

$$\operatorname{rank}_{\mathbb{Q}} \operatorname{Jac}(C^{(d)}) = 2 \operatorname{rank}_{\mathbb{Q}} E^{(d)} = 2,$$

and the conclusion follows. □

The next result describes the distribution of the Mordell–Weil ranks of Jacobians in the family of double quadratic twists of genus-2 curves with split Jacobian.

Proposition 2.19. *Let $E_i : y^2 = f_i(x)$, $i = 1, 2$, be elliptic curves over $\mathbb{Q}$, where f_i are monic separable cubic polynomials split over $\mathbb{Q}$. Choose orderings of the roots of f_1 and f_2, and assume that the resulting identification $E_1[2] \simeq E_2[2]$ does not arise from an isomorphism $E_{1,\overline{\mathbb{Q}}} \simeq E_{2,\overline{\mathbb{Q}}}$. Let $C : y^2 = \operatorname{glue}(f_1, f_2)$ be the corresponding genus-2 curve. Assume that the Birch and Swinnerton-Dyer conjecture holds for the quadratic twist families of E_1 and E_2.*

For nonzero squarefree integers d_1, d_2, let $E_i^{(d_i)} : y^2 = f_i^{(d_i)}(x)$, where $f_i^{(d_i)}(x) = d_i^3 f_i(x/d_i)$, and let $C^{(d_1,d_2)}$ be the genus-2 curve obtained by applying the same gluing construction to $E_1^{(d_1)}$ and $E_2^{(d_2)}$.

With $D(X)$ as in (3), one has

$$\lim_{X\to\infty} \frac{\left|\{(d_1, d_2) \in D(X)^2 : \operatorname{rank} \operatorname{Jac}(C^{(d_1,d_2)}) = r\}\right|}{|D(X)|^2} = \begin{cases} \frac{1}{4}, & r = 0, \\ \frac{1}{2}, & r = 1, \\ \frac{1}{4}, & r = 2, \\ 0, & r \geq 3. \end{cases}$$

Proof. By construction, $E_1^{(d_1)}$ (resp. $E_2^{(d_2)}$) is isomorphic to E_1 (resp. E_2) over $\mathbb{Q}(\sqrt{d_1})$ (resp. $\mathbb{Q}(\sqrt{d_2})$). Over $L = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, the maps

$$(x, y) \mapsto (x/d_i,\ y/d_i^{3/2})$$

identify $E_i^{(d_i)}$ with E_i and carry the ordered set of nontrivial 2-torsion points of $E_i^{(d_i)}$ to that of E_i. Hence they identify the graph used in the gluing of $E_1^{(d_1)}$ and $E_2^{(d_2)}$ with the graph used in the gluing of E_1 and E_2. Therefore the corresponding principally polarized quotients are isomorphic over L, and $C^{(d_1,d_2)}$ and C are isomorphic over L.

It follows that

$$\operatorname{Jac}(C^{(d_1,d_2)}) \sim_{\mathbb{Q}} E_1^{(d_1)} \times E_2^{(d_2)}.$$

By [55, Corollary 1.2], under BSD, the quadratic twists of E_i have rank 0 and 1 with proportions 1/2 each, while the twists of rank at least 2 have proportion 0. Since

$$\operatorname{rank} \operatorname{Jac}(C^{(d_1,d_2)}) = \operatorname{rank} E_1^{(d_1)} + \operatorname{rank} E_2^{(d_2)},$$

the claimed distribution of ranks follows. □

3. Cryptographic motivation: Regev's quantum algorithm

In this section we develop the cryptographic discussion from Section 1.1 and recall the features of Regev's DLP algorithm that are used below. Let $(G,+)$ be the group in which the DLP is posed, for us an elliptic curve group or the Jacobian of a genus-2 curve over $\mathbb{F}_q$, and let $h=[x]g$ be the target relation. Let n be the binary size of G. The step that dominates the gate complexity of Regev's algorithm requires $d+\frac{n}{d}$ additions and doublings in G, while the gate complexity per run of Shor's algorithm is n additions and doublings. Hence the asymptotic advantage of Regev's algorithm with respect to Shor's algorithm is $\min(d,\frac{n}{d})$. When G is the multiplicative group of a finite field, one can take $d=\sqrt{n}(\log n)^{O(1)}$ (see [46]). For elliptic curves and genus-2 Jacobians, the largest value currently obtained for d is $(\log n)^{\frac{1}{2}}$ (see [2]). In curve applications, increasing d amounts to finding suitable rational Mordell–Weil generators, as recalled next.

3.1. Regev's algorithm in a nutshell.

For the chosen parameter d, the algorithm uses $d-2$ auxiliary elements of G, denoted $g_1,\dots,g_{d-2}$, and sets $g_{d-1}=h$ and $g_d=g$. It considers the lattice

$$L=\left\{(z_1,\dots,z_d)\in\mathbb{Z}^d \mid \sum_{i=1}^{d}[z_i]g_i=0\right\}. \tag{9}$$

One computes in superposition all the sums $\sum_{i=1}^{d}[z_i]g_i$, called multi-scalar product, where $z_1,\dots,z_d$ are non-negative $\frac{n}{d}$-bit integers. Next, a quantum procedure computes a basis of the lattice L. Finally, one solves a linear system to find a vector of L of the form $(0,\dots,0,-1,*)$. The last coordinate of this vector is $\log_g h$.

To obtain the stated complexity, one needs a classical algorithm that computes arbitrary multi-scalar products with coefficients of $\frac{n}{d}$ bits. This can be done using Pippenger's algorithm [47], provided one can store a table of all multi-scalar products with coefficients in $\{0,1\}$. In the quantum setting such large lookup tables are not available. To overcome this obstacle, Regev [49] chooses the auxiliary elements $g_1,\dots,g_{d-2}$ so that they can be represented using few bits.

As anticipated in Section 1.1, the parameter d is supplied, for curves, by reducing Mordell–Weil generators from a rational lift. Let $C_0/\mathbb{F}_q$ be the finite-field curve on which the DLP is posed, and let $\widetilde{C}/\mathbb{Q}$ be a curve with good reduction at q whose reduction is isomorphic to C_0. This is the setting used in [2, Section 3.3] and [4, Section 5.1]. If $J=\mathrm{Jac}(\widetilde{C})$, good reduction gives a specialization homomorphism $\rho_q: J(\mathbb{Q})\longrightarrow \mathrm{Jac}(C_0)(\mathbb{F}_q)$. Choose points $P_1,\dots,P_r\in J(\mathbb{Q})$ which are independent modulo torsion, and write $\overline{P}_i=\rho_q(P_i)$. These reduced points are used as the auxiliary elements in the lattice construction, namely

$$g_i=\overline{P}_i \quad (1\le i\le r), \quad g_{r+1}=h, \quad g_{r+2}=g,$$

where h is the DLP input and g is the base point. Thus $d-2=r$, so a rank-r lift allows one to take

$$d=r+2,$$

provided that the reduced points satisfy the usual independence heuristic which makes the lattice L in (9) behave as in Assumption 1 of [18]. This heuristic fails in degenerate cases such as the one described in [18, Example preceding Assumption 1], while the numerical experiments in [2, Section 3.2] support it when the chosen auxiliary elements behave independently.

Solving Problem 1 produces curves on which Regev's algorithm can be run with a large parameter d (see Appendix A); these are useful for experiments and comparisons with Shor's algorithm, but they do not by themselves give a curve compatible with a fixed HECC instance.

For a fixed curve $C/\mathbb{F}_q$, Problem 2 asks for a high-rank rational lift, twist, or related curve whose reduction is compatible with C. If the twisting parameter d, or the two parameters (d_1, d_2), are squares modulo q, then the corresponding twist has reduction isomorphic to C. More generally, if ψ is an isogeny, in particular an isomorphism, between two algebraic varieties of order $|G|$, with kernel of order coprime to $|G|$, then

$$\log_g h = \log_{\psi(g)} \psi(h).$$

Thus the DLP can be transported through this map. In this sense, solving Problem 2 for a rational lift $\widetilde{C}$ of C supplies a compatible curve on which Regev's algorithm can be run with a larger parameter.

3.2. **High rank twists of certain curves used in cryptography.** Problem 2 is solved on a list of HECC genus 1 (resp. genus 2) curves in [2] (resp. [4]). The empirical observation which motivated this work is that a naive enumeration offers better results in the case of two types of genus-2 curves: CM curves of simple Jacobian and the curves which are twists of a split Jacobian. In the rest of this section we obtain a justification for this phenomenon.

3.2.1. The curves $C_a : y^2 = x^5 + a$. The Buhler–Koblitz curve 4GLV127-BK (see [4]) has equation $y^2 = x^5 + 17$ and is a twist of $y^2 + y = x^5$ (see [14]). The curve is one of the most important in HECC, e.g. it was considered along the curve *Generic1271* in [10]. It has CM and simple Jacobian (see LMFDB:4096.b.65536.1). One of its twists, the curve $y^2 = x^5 + 8$, is used in [12].

Problem 2 was solved for $y^2 = x^5 + 17$ in [4]: an early-abort search enumerated the twists $y^2 = x^5 + 17\delta$ for $1 \leq \delta \leq 128 \cdot 10^4$ in 448 960 core-seconds, about 125 core-hours, and found twists up to rank 7. For the compatible finite-field instance used there, a rank-6 twist gives Regev parameter 8 and an eightfold speedup over Shor; thus the search is worthwhile as offline preprocessing in that example.

In an experiment, we used a modified search which uses the particular properties of the simple CM curves. Among the curves $y^2 = x^5 + a$ with $a \leq 10^5$ one has:

- 60794 are squarefree (this is close to $\zeta(2)^{-1}$, the theoretical proportion of squarefree positive integers, see [29] or [24, page 467]);
- 3559 of them have at least 3 rational points of height ≤ 500 on C_a (this is implemented in Magma, see [42]). Heuristically, when embedded in the Jacobian $J_a = \mathrm{Jac}(C_a)$ they are not torsion with high probability and we expect $\operatorname{rank} J_a \geq 3$.
- ≥ 1663 of them have a root number of opposite parity with respect to the lower bound obtained above, so the rank is larger than the previous bound. The root number can be computed by a closed formula proven in [7].
- For these curves one computes in Magma a basis of the Mordell–Weil group. This is implemented in Magma [11] V2.27-6 and PARI/GP [60] version 2.18 only for genus 1 and 2. We find $15, 11, 2, 2$ twists of ranks $5, 6, 7, 8$, respectively. If compatible with a finite-field target, a rank-8 example would give Regev parameter 10; this enumeration was not recorded as a timed

benchmark. For comparison, the similarly sized data set of [9] contains no genus-2 curve of rank ≥ 5.

Remark 3.1. *As an alternative to computing a basis of the Mordell–Weil group, one can compute the analytic rank. The method is interesting because the curves C_a are CM and in the genus* 1 *analogue, twists of high rank of the CM curve $y^2 = x^3 - x$ have been found by computing the analytic rank (see e.g.* [21]*).*

To extend their idea to genus 2, note that Stoll [57] *identified the Hecke character η_a such that $L(J_a) = L(\eta_a)$ (see also* [58]*). The computation of the Hecke grossen characters has an implementation in PARI/GP since version 2.15 using the algorithms in* [41]*. We are indebted to Aurel Page for the program that we used to compute the L-function of J_a (see* [3]*). However, with the current implementation, the computation of the L-function of J_a using the Hecke character is more than* 20 *times slower than the general method to compute L-functions of genus 2 curves, which is implemented in PARI/GP since version 2.10. It is approximately* 70 *times slower than the optimized implementation of Bill Allombert. Note however that, contrary to the elliptic curves analogue, in the case of genus 2 curves the Hecke grossen characters have relatively new implementations and the numerical results in this work were obtained without this alternative.*

3.2.2. *Curves whose Jacobians become isogenous to $E \times E$.* Freeman and Satoh defined two families of curves C whose Jacobian is the square of an elliptic curve:

Lemma 3.2 (Prop. 4.1 and 4.2 in [25])**.** *Let K be a perfect field and let C be a hyperelliptic curve defined over K which is defined by Equation* (10) *(resp.* (11)*).*

$$C : y^2 = x^5 + ax^3 + bx \tag{10}$$

$$C : y^2 = x^6 + ax^3 + b. \tag{11}$$

Let $m = 4$ (resp. $m = 3$). Set $c = a/\sqrt{b} \in \overline{K}$ and ζ_m a primitive m-th root of unity. Then $\mathrm{Jac}(C)$ *is isogenous over $K(b^{\frac{1}{2m}}, \zeta_m)$ to $E \times E$ where E is defined by Equation* (12) *(resp.* (13)*):*

$$E(c) : y^2 = (c+2)x^3 - (3c-10)x^2 + (3c-10)x - (c+2) \tag{12}$$

$$E(c) : y^2 = (c+2)x^3 - (3c-30)x^2 + (3c+30)x - (c-2). \tag{13}$$

The curves $y^2 = x^5 + bx$.

They occur in cryptography e.g. $b = 21$ in [16, Ex 20] and $b = 3$ in [34]. Note that the curves are twists over $\mathbb{Q}(b^{\frac{1}{5}})$ of $y^2 = x^5 + x$, which is of the form (10) with $a = 0$ and $b = 1$. By Lemma 3.2 we have

$$\mathrm{Jac}(C_1) \sim_{\mathbb{Q}(i)} E \times E \text{ with } E : y^2 = x^3 + 10x^2 - 20x - 8.$$

(see LMFDB:256.a2). We found the twist $d = 110814$ of rank 4.

Drylo's pairing-friendly curves with split Jacobian. Drylo [16] proposed a list of curves as in the statement of Lemma 3.2 with $K = \mathbb{Q}$. A priori, the parameter b is not required to be a square, but the second part of Example 19 in that article is a rational square.

Indeed, Drylo considered the 1/10-twist of $C : y^2 = x^6 + ax^3 + b$ with $a = 4/25$ and $b = (8/125)^2$; here $c = \frac{a}{\sqrt{b}} \in \mathbb{Q}$. By Lemma 3.2, $\mathrm{Jac}(C) \sim_{\mathbb{Q}(\zeta_3)} E \times E$ where $E = E(\frac{5}{2})$ as in Equation (11). The quadratic twist of $d = 1046$ of the curve

$y^2 = x^3 + \frac{5}{2}x^2 - \frac{45}{4}x - \frac{81}{4}$ has rank 4, so the corresponding twist of C has rank 8 over $\mathbb{Q}(\zeta_3)$.

Thus, in both split examples, a rank-4 elliptic twist gives genus-2 rank 8 over the splitting field, hence Regev parameter 10 and dominant-operation gain $n/(10+n/10)$; these twists are examples rather than timed search benchmarks.

Appendix A. List of hyperelliptic curves suited for an implementation of Regev's algorithm

An implementation of Regev's algorithm for hyperelliptic curves benefits from explicit curves for which the parameter d can be taken as large as possible. We collect a short list of small-coefficient, high-rank examples for Problem 1; they are not evidence for Theorem 1, but inputs for experiments with the Regev-style algorithm discussed in Section 3.

A.1. **Genus-2 curves with simple Jacobian and high rank.** *A curve of small height.* Booker et al. [9] found 66158 $\mathbb{Q}$-isomorphic classes of curves of absolute discriminant less than 10^6. They are available in the LMFDB. The largest rank in that list is 4, e.g. the curve

$$y^2 + (x^3 + x + 1)y = x^5 - x^4 - 5x^3 + 9x + 6$$

(see LMFDB:440509.a.440509.1) has a Jacobian of rank 4. Booker and Sutherland [8] have announced work in progress on a larger genus-2 database.

Curves of high rank. We summarize a list of record curves in the literature. Here $\widehat{h}$ denotes the base-2 logarithm of the maximum canonical height among the basis elements.

curve	ref.	rank	$\widehat{h}$
$y^2 = 1306881x^6 + 18610236x^5 - 46135758x^4$ $- 1536521592x^3 - 2095359287x^2 + 32447351356x + 89852477764$	[56]	≥ 16	8.41
$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3$ $+ 567207969x^2 - 985905640x + 247747600$	[42]	≥ 22	14.73
$y^2 = 4037229x^6 + 34187102x^5 - 724533076x^4 - 4944866082x^3$ $+ 57659086152x^2 + 241518308040x + 313383220164$	[15]	≥ 25	28.55
$y^2 = 80878009x^6 - 236558406x^5 - 1018244179x^4$ $+ 4436648480x^3 + 6445563464x^2 - 13620761544x + 68406^2$	[22]	≥ 26	32.14
$y^2 = 60516x^6 + 1680225324x^5 + 200663873413x^4 - 1021197439562x^3$ $- 290505889943111x^2 + 316071770416320x + 123355813282790400$	[20]	≥ 27	39.57

A.2. **Highest known ranks for genus-2 curves with split Jacobian.** By Proposition 2.15, gluing elliptic curves with full rational 2-torsion gives split genus-2 Jacobians, and for $J = \mathrm{Jac}(C) \sim_K E_1 \times E_2$ the Mordell–Weil rank is $\mathrm{rank}\, E_1(K) + \mathrm{rank}\, E_2(K)$; in the diagonal case this is $2\,\mathrm{rank}\, E$. Thus the congruent-number curve $E : y^2 = x^3 - x$ (LMFDB:32.a3) and $C : y^2 = 6x^6 - 9x^4 - 9x^2 + 6$, with $\mathrm{Jac}(C) \sim_{\mathbb{Q}} E \times E$, give genus-2 twists of rank $2s$ from rank-s twists of E; see Rogers [50] and Watkins [62, Table 2] for $s = 2, \ldots, 7$. Over $\mathbb{Q}(t)$, Shioda [52] found a rank-14 split example, and combining Elkies's $E_1(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}^{15}$ curve [19] with the rank-5 full-2-torsion curve from [17, Example 19] gives a rank-20 genus-2 Jacobian $(2,2)$-isogenous to $E_1 \times E_2$; the resulting sextic model has coefficients in $\mathbb{Q}(t)$ of degree 756 and binary size 1761.

References

[1] Mohamed Alaa and Mohammad Sadek, *High rank quadratic twists of pairs of elliptic curves*, Journal of Number Theory **174** (2017), 436–444.

[2] Razvan Barbulescu, Mugurel Barcau, and Vicenţiu Paşol, *Extending Regev's quantum algorithm to elliptic curves*, Progress in Cryptology – LATINCRYPT 2025, 2025, pp. 234 – 266.

[3] Razvan Barbulescu, Mugurel Barcau, Vicenţiu Pasşol, and George Ţurcas, *Online complement to "Logarithmic Density of Rank ≥ 1 and Rank ≥ 2 Genus-2 Jacobians and Applications to Hyperelliptic Curve Cryptography"*, 2026. Available online at https://github.com/BarbulescuR/Logarithmic-density-of-positive-rank-genus-2-Jacobians/.

[4] Razvan Barbulescu and Gaetan Bisson, *Regev's attack on hyperelliptic cryptosystems*, 2024. Available online at https://eprint.iacr.org/2024/2004.

[5] M. Bhargava and B. H. Gross., *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point.*, In automorphic representations and L-functions, 2013, pp. 23–91.

[6] Manjul Bhargava, Benedict Gross, and Xiaoheng Wang, *A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension*, Journal of the American Mathematical Society **30** (2017), no. 2, 451–493.

[7] Matthew Bisatt, *Root number of the Jacobian of $y^2 = x^p + a$*, Journal de théorie des nombres de Bordeaux **34** (2022), no. 2, 575–582.

[8] Andrew Booker and Andrew Sutherland, *Genus 2 curves over $\mathbb{Q}$ of small conductor*, 2026. In preparation, preliminary version available online at https://math.mit.edu/~drew/cavaret.pdf.

[9] Andrew R Booker, Jeroen Sijsling, Andrew V Sutherland, John Voight, and Dan Yasaki, *A database of genus-2 curves over the rational numbers*, LMS Journal of Computation and Mathematics **19** (2016), no. A, 235–254.

[10] Joppe W Bos, Craig Costello, and Andrea Miele, *Elliptic and hyperelliptic curves: A practical security analysis*, International workshop on public key cryptography, 2014, pp. 203–220.

[11] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). MR1484478

[12] Ezra Brown, Bruce T Myers, and Jerome A Solinas, *Hyperelliptic curves with compact parameters*, Designs, Codes and Cryptography **36** (2005), no. 3, 245–261.

[13] Armand Brumer, *The average rank of elliptic curves I*, Inventiones mathematicae **109** (1992), no. 1, 445–472.

[14] Joe Buhler and Neal Koblitz, *Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems*, Bulletin of the Australian Mathematical Society **58** (1998), no. 1, 147–154.

[15] Roland Dreier, *Examples of genus 2 curves over $\mathbb{Q}$ with Jacobians of high Mordell–Weil rank*, International Mathematics Research Notices **1997** (1997), no. 18, 875–880.

[16] Robert Dryło, *Constructing pairing-friendly genus 2 curves with split Jacobian*, Progress in cryptology – indocrypt 2012, 2012, pp. 431–453.

[17] Andrej Dujella and Juan Carlos Peral, *High rank elliptic curves induced by rational Diophantine triples*, Glasnik matematički **55** (2020), no. 2, 237–252.

[18] Martin Ekerå and Joel Gärtner, *Extending Regev's factoring algorithm to compute discrete logarithms*, International conference on post-quantum cryptography, 2024, pp. 211–242.

[19] Noam Elkies, *Elliptic curve with Mordell–weil group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^{15}$*, 2009. Announcement to the Number Theory list server. Available online at https://web.math.pmf.unizg.hr/~duje/tors/z2z2.html.

[20] ———, *Simple genus-2 Jacobian of rank at least 29*, 2015. Announcement to the Number Theory list. Available online at https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1501&L=NMBRTHRY&P=R2.

[21] Noam D Elkies, *Curves $dy^2 = x^3 - x$ of odd analytic rank*, International algorithmic number theory symposium, 2002, pp. 244–251.

[22] ———, *Curves of genus 2 with many rational points via K3 surfaces*, ACM Communications in Computer Algebra **42** (2008), no. 1-2, 53–55.

[23] Gerd Faltings and Ching-Li Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, vol. 22, Springer-Verlag, Berlin, Heidelberg, 1990.

[24] Étienne Fouvry and Jürgen Klüners, *On the* 4*-rank of class groups of quadratic number fields*, Inventiones Mathematicae **167** (2007), no. 3, 455–513.
[25] David Mandell Freeman and Takakazu Satoh, *Constructing pairing-friendly hyperelliptic curves using weil restriction*, Journal of Number Theory **131** (2011), no. 5, 959–983.
[26] Stevan Gajović and Sun Woo Park, *Infinitely many genus two and three curves of small fixed positive rank*, arXiv preprint arXiv:2505.22470 (2025).
[27] Éric Gaudron and Gaël Rémond, *Nombre de petits points sur une variété abélienne*, Journal of the Institute of Mathematics of Jussieu **24** (2025), no. 3, 705–761.
[28] Fernando Gouvêa and Barry Mazur, *The square-free sieve and the rank of elliptic curves*, Journal of the American Mathematical Society **4** (1991), no. 1, 1–23.
[29] SW Graham, *The distribution of squarefree numbers*, Journal of the London Mathematical Society **2** (1981), no. 1, 54–64.
[30] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Inventiones Mathematicae **84** (1986), no. 2, 225–320.
[31] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.
[32] Jeffrey Hatley, *Rank parity for congruent supersingular elliptic curves*, Proceedings of the American Mathematical Society **145** (2017), no. 9, 3775–3786.
[33] Everett W Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Mathematicum **12** (2000), 315–364.
[34] Mitsuru Kawazoe and Tetsuya Takahashi, *Pairing-friendly hyperelliptic curves with ordinary jacobians of type* $y^2 = x^5 + ax$, International conference on pairing-based cryptography, 2008, pp. 164–177.
[35] Jean Kieffer, *Degree and height estimates for modular equations on PEL Shimura varieties*, Journal of the London Mathematical Society **105** (2022), 1314–1361.
[36] Neal Koblitz, *Hyperelliptic cryptosystems*, Journal of Cryptology **1** (1989), 139–150.
[37] V. A. Kolyvagin, *Finiteness of* $E(\mathbf{Q})$ *and* $\mathrm{Sha}(E, \mathbf{Q})$ *for a subclass of weil curves*, Mathematics of the USSR-Izvestiya **32** (1989), no. 3, 523–541. Russian original: Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), no. 3, 522–540.
[38] Daniel Kriz and Chao Li, *Goldfeld's conjecture and congruences between Heegner points*, Forum of Mathematics, Sigma **7** (2019), e15, 80 pp.
[39] The LMFDB Collaboration, *The L-functions and modular forms database*, 2026. [Online; accessed 15 January 2026].
[40] Davide Lombardo, *Abelian varieties*, 2018. Lecture notes, Luxembourg Summer School on Galois representations, July 3–7, 2018.
[41] Pascal Molin and Aurel Page, *Computing groups of Hecke characters*, Research in Number Theory **8** (2022), no. 4, 91.
[42] Jan Müller and Michael Stoll, *Canonical heights on genus-2 Jacobians*, Algebra & Number Theory **10** (2016), no. 10, 2153–2234. Record curve available online at `https://www.mathe2.uni-bayreuth.de/stoll/recordcurve.html`.
[43] David Mumford, *Tata lectures on theta. II*, Birkhäuser, Boston, 1984.
[44] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, Journal of the European Mathematical Society **21** (2019), no. 9.
[45] Fabien Pazuki, *Theta height and Faltings height*, Bulletin de la Société Mathématique de France **140** (2012), no. 1, 19–49.
[46] Cédric Pilatte, *Unconditional correctness of recent quantum algorithms for factoring and computing discrete logarithms*, Forum of mathematics, pi, 2026, pp. e5.
[47] Nicholas Pippenger, *On the evaluation of powers and monomials*, SIAM Journal on Computing **9** (1980), no. 2, 230–250.
[48] Bjorn Poonen, *Squarefree values of multivariable polynomials*, Duke Mathematical Journal **118** (2003), no. 2, 353–373.
[49] Oded Regev, *An efficient quantum factoring algorithm*, Journal of the ACM **72** (2025), no. 1, 1–13.
[50] Nicholas F Rogers, *Rank computations for the congruent number elliptic curves*, Experiment. Math. **9** (2000), no. 3, 591–594.

[51] Jean-Pierre Serre, *Lectures on the Mordell–Weil Theorem*, 3rd ed., Aspects of Mathematics, vol. E15, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated and edited by Martin Brown from French notes by Michel Waldschmidt.
[52] Tetsuji Shioda, *Genus two curves over $\mathbb{Q}(t)$ with high rank*, Commentarii mathematici Universitatis Sancti Pauli **46** (1997), no. 1, 15–21.
[53] Peter W Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings 35th annual symposium on foundations of computer science–SFCS'94, 1994, pp. 124–134.
[54] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994.
[55] Alexander Smith, *The Birch and Swinnerton-Dyer conjecture implies Goldfeld's conjecture*, arXiv preprint arXiv:2503.17619 (2025).
[56] Colin Stahlke, *Algebraic curves over $\mathbb{Q}$ with many rational points and minimal automorphism group*, International Mathematics Research Notices **1997** (1997), no. 1.
[57] Michael Stoll, *On the arithmetic of the curves $y^2 = x^\ell + a$, II*, Journal of Number Theory **93** (2002), no. 2, 183–206.
[58] Michael Stoll and Tonghai Yang, *On the L-function of the curves $y^2 = x^5 + a$*, Journal of the London Mathematical Society **68** (2003), no. 2, 273–287.
[59] Szabolcs Tengely, *Effective Methods for Diophantine Equations*, Ph.D. Thesis, 2005.
[60] The PARI Group, *PARI/GP version 2.18.1*, Univ. Bordeaux, 2025. available from http://pari.math.u-bordeaux.fr/.
[61] Mark Watkins, *Some heuristics about elliptic curves*, Experimental Mathematics **17** (2008), no. 1, 105–125.
[62] Mark Watkins, Stephen Donnelly, Noam D Elkies, Tom Fisher, Andrew Granville, and Nicholas F Rogers, *Ranks of quadratic twists of elliptic curves*, Publications matheématiques de Besançon. Algèbre et théorie des nombres **2** (2014), 63–98.
[63] Myungjun Yu, *The distribution of Selmer ranks of quadratic twists of Jacobians of hyperelliptic curves*, Mathematical Research Letters **26** (2019), no. 4, 1217–1250.

Institut de mathématiques de Bordeaux (Bordeaux INP, CNRS, Univ. Bordeaux) and Inria Bordeaux
Email address: razvan.barbulescu@u-bordeaux.fr

Institute of Mathematics of the Romanian Academy and CertSIGN, Bucharest
Email address: mugurel.barcau@imar.ro; vicentiu.pasol@imar.ro

Babeş-Bolyai University, Cluj-Napoca and certSIGN, Bucharest
Email address: george.turcas@ubbcluj.ro