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 $\leq X$, this yields a lower bound of logarithmic density 13/14 for the subset of rank $r \geq 1$. We further present a large explicit subfamily where Jacobians have ranks $r \geq 2$, yielding an unconditional logarithmic density of at least 5/7. Independently, we give a construction of genus-2 curves with split Jacobian and rank 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 density 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 [14]), 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 $(\gamma + o(1))X^{2g+3}$, for an explicit constant $\gamma > 0$. This ordering was also used by Booker et al. in [10] for creating a database of genus-2 curves (see Section 3.1).

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 $(\gamma + o(1))X^{\frac{2g+3}{4g+2}}$ for an explicit constant γ. This ordering has been used as well in [10, Sec 3.1].

If S is a subset of $\bigcup_{X \geq 1} \mathcal{C}^{(g)}(X)$, where $\mathcal{C}^{(g)}(X)$ denotes one of the boxes defined above, we set $S(X) := S \bigcap \mathcal{C}^{(g)}(X)$. We say that S has proportion $\delta \in \mathbb{R}_{\geq 0} \bigcup \{\infty\}$ if $\lim_{X \to \infty} \frac{|S(X)|}{|\mathcal{C}^{(g)}(X)|} = \delta$. 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*

$$|S(X)| = |\mathcal{C}^{(g)}(X)|^{\alpha + o(1)},$$

or, equivalently,

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

For example, in the case of elliptic curves, in [42] it is proven that the random matrix model predicts that the set of curves of rank $r \geq 2$ has logarithmic density $\frac{19}{24}$ with respect to $\mathcal{C}_2^{(1)}(X)$.

The main results of this article 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. 2.15)**.**

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 elliptic curve case the conjectural logarithmic density is $\frac{19}{24}$ for rank $r \geq 2$ (see Th 7.3.3 in [42]). In genus 2, we only prove unconditional lower bounds $\frac{13}{14}$ for rank $r \geq 1$ and $5/7$ for rank $r \geq 2$ with respect to $\mathcal{C}_1(X)$. However, some heuristics predict rank parities to be equidistributed in the subfamily with two points at infinity, hence this would suggest logarithmic density at least $\frac{13}{14}$ for rank $r \geq 2$ as well (cf. Remark 2.12). This phenomenon is also consistent with existing numerical data. In particular, data available in the LMFDB indicates that, 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.

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 finding 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 by d. We now study rank distributions within the family of quadratic twists of this fixed hyperelliptic curve. We consider the set

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

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 $\lim_{X\to\infty} \frac{|S(X)|}{|D(X)|} = \delta$ 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 $\mathrm{rank}(\mathrm{Jac}(C^{(d)})) \geq r$ is defined by*

$$\alpha(C, r) := \lim_{X\to\infty} \frac{\log\big|\{d \in D(X) \mid \mathrm{rank}(\mathrm{Jac}(C^{(d)})(\mathbb{Q})) \geq r\}\big|}{\log|D(X)|},$$

whenever the limit exists.

For example, in [53] it is proven under the 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 [61]), but it can be zero. It has been conjectured in [59] that it has a logarithmic density $\alpha = \frac{3}{4}$ whereas the best proven result is that of [28], where the author shows 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. 2.22 and Prop. 2.21)**.**

(1) *Let E_1, E_2 and C be two elliptic curves and a genus-2 curve defined over $\mathbb{Q}$ such that $\mathrm{Jac}(C) \simeq E_1 \times E_2$. Then there exists a family of curves $C^{(d_1,d_2)}$*

defined over $\mathbb{Q}$ *which are isomorphic to* C *over* $\mathbb{Q}(\sqrt{d_1},\sqrt{d_2})$ *but not over* $\mathbb{Q}$ *and*

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

(2) *Let* E *and* C *be an elliptic curve and a hyperelliptic curve of genus-2 defined over* $\mathbb{Q}$ *such that* $\operatorname{Jac}(C)\simeq_{\mathbb{Q}} E\times E$. *Let* $y^2=f(x)$ *be the equation of* C. *For all nonzero integer* d *let* $C^{(d)}$ *be the curve of equation* $dy^2=f(x)$. *Then we have*

$$\lim_{X\to\infty}\frac{|\{d\in D(X) \mid \operatorname{rank}(\operatorname{Jac}(C^{(d)})(\mathbb{Q}))\geq 2\}|}{|D(X)|}\geq\frac{1}{2}.$$

In this article we are interested in the following two problems.

Problem 1 (THE HIGH RANK CURVE PROBLEM)**.** *Let* g *be an integer and let* S *be* $\mathcal{C}_1^{(g)}(X)$, $\mathcal{C}_2^{(g)}(X)$ *or their subsets of split Jacobian. Given a bound* X *and an integer* r, *sample, if it exists, a random curve* $C\in S(X)$ *such that* $\operatorname{rank}\operatorname{Jac}(C)=r$.

Problem 2 (THE HIGH RANK TWIST PROBLEM)**.** *For any hyperelliptic curve* $C:y^2=f(x)$, $C^{(d)}$ *denotes the twist of equation* $C^{(d)}:dy^2=f(x)$.

Let C *be a genus-2 curve.*

(1) *if* $\operatorname{Jac}(C)$ *is simple find, if it exists, a random squarefree integer* $d\in[1,X]$ *such that* $\operatorname{rank}\operatorname{Jac}(C^{(d)})=r$;
(2) *if* $\operatorname{Jac}(C)\simeq E\times E$ *for an elliptic curve* E *find, if it exists, a squarefree integer* $d\in[1,X]$ *such that* $\operatorname{rank}(E^{(d)}\times E^{(d)})=r$;
(3) *if* $\operatorname{Jac}(C)\simeq E_1\times E_2$, *find, if they exist, random squarefree integers* $(d_1,d_2)\in[1,X]^2$ *such that* $\operatorname{rank}(E_1^{(d_1)}\times E_2^{(d_2)})=r$.

1.1. **Cryptographic consequences.** Hyperelliptic curve cryptography (HECC) is the genus-2 analogue of elliptic curve cryptography (ECC) with the difference that one works in the Jacobian group $\operatorname{Jac}(C)(\mathbb{F}_q)$ of a genus-2 curve $C/\mathbb{F}_q$. To ensure that the security of the desired cryptographic construction relies on the average case difficulty of the discrete logarithm problem, Köblitz [34] proposed to sample a random prime q and a random model $C:y^2+h(x)y=f(x)$, $f,h\in\mathbb{F}_q[X]$.

A recent algorithm of Regev [45] gives a quantum approach to the discrete logarithm problem. This was initially designed for integer factorization, but was extended in [4] to HECC. As explained in Section 3.1 the curves obtained by solving Problem 1 are suited for Regev's algorithm.

At a theoretical level, part (3) of Theorem 1 gives an unconditional lower bound on the density of rank-2 Jacobians in our height ordering, and hence an upper bound on the expected number of trials needed to solve Problem 1 with $r=2$. Part (1) tackles the case of curves with split Jacobian. At a practical level, one finds high rank curves using the examples in the literature. We estimate the Néron-Tate height of the generators of the Mordell-Weil group (see 3.2).

In cryptography one uses a fixed list of curves (see [4]). We tackle Problem 2 for a list of genus-2 curves used in cryptography. Recall that the Poincaré decomposition theorem states that for any genus-2 curve C, its $\operatorname{Jac}(C)$ is isogenous, after some extension of the base field, either to a simple variety, to a split variety of the form $E_1\times E_2$ for two non-isogenous curves E_1 and E_2 or of the form $E\times E$ for an elliptic curve E.

Genus-2 curves with split Jacobian or with complex multiplication form structured particular subclasses of curves within HECC. Although these special subclasses have received significant attention, we are not aware of any dedicated algorithmic treatment tailored to the present setting prior to this work. Remarkably, these two subclasses of genus-2 curves appear in several cryptographic works, e.g. [15], [13], [32] and [17].

At a theoretical level, Theorem 2 asserts that if $\mathrm{Jac}(C) \simeq E_1 \times E_2$ or $\mathrm{Jac}(C) \simeq E \times E$ one can find a twist of rank $r = 2$ in a constant number of trials. At a practical level, it is easier to find twists of high rank for the curves of split Jacobian (Section 3.4).

2. Main results

2.1. **Informal presentation of the results.** Let $C : \quad y^2 + h(x)y = f(x)$ be the Weierstrass model of a genus-2 hyperelliptic curve defined over a field k of characteristic $\neq 2$. We restrict to the case where f is sextic. We call ∞_+ and ∞_- the two points at infinity, which are potentially in a quadratic extension of k. We write $[D]$ for the class of a degree-zero divisor D in $\mathrm{Pic}^0(C) = \mathrm{Jac}(C)$. When $\infty_\pm$ are conjugate (possibly non-rational), the divisor $(\infty_+) + (\infty_-)$ is rational, so for $P \in C(k)$ the class $[2(P) - (\infty_+) - (\infty_-)]$ defines a k-rational point of $\mathrm{Jac}(C)$.

To see when ∞_+ and ∞_- are rational, one completes the square: $(2y + h(x))^2 = g(x) := 4f(x) + h(x)^2$. When $\deg g = 6$ and the leading coefficient of g is a square in k, the weighted projective closure of C has two k-rational points at infinity, which we denote by ∞_+ and ∞_-. The image of ∞_+ by the Abel-Jacobi map is a k-rational point

$$\alpha_C := [\infty_+ - \infty_-] \in \mathrm{Jac}(C)(k).$$

We study the density of genus-2 curves $C \in \mathcal{C}_1(X)$ where α_C is non-torsion. This theme goes back at least to a question of Serre: in a real-analytic family of *real* hyperelliptic curves with two real points at infinity, how frequently does the divisor class $[\infty_+ - \infty_-]$ become torsion? Lawrence [35] proved that the divisor is torsion when specialized at a *dense* set of parameters in the usual Euclidean topology. This is a useful motivating viewpoint, but it is important to stress that "dense over $\mathbb{R}$" is a statement of *analytic* nature, and it does not predict how often torsion occurs among curves defined over $\mathbb{Q}$ and ordered arithmetically (e.g. by the size of integral coefficients). A good mental model is that $\mathbb{Q}$ is dense in $\mathbb{R}$ but still has density 0 in any counting problem. Our results in this section are on the arithmetic side: we order curves by height in explicit boxes of integral models and show that, in this sense, torsion specializations of $[\infty_+ - \infty_-]$ are rare.

More concretely, the authors of [10] observed in their search for genus-2 curves of small discriminant that *small coefficients make it more likely* that $g(x) = 4f(x) + h(x)^2$ has square leading coefficient, in which case $\infty_\pm$ are $\mathbb{Q}$-rational. Moreover, the divisor class $[\infty_+ - \infty_-]$ "typically has infinite order" [10, Remark A.1]. Our first goal is to turn this heuristic into a conceptual and quantitative statement. We do this by working over a universal parameter space and viewing $[\infty_+ - \infty_-]$ as a universal section α_{univ} of the universal Jacobian. We show: (i) for each $n \geq 1$, the locus where $n\alpha_{\mathrm{univ}} = 0$ is Zariski closed; (ii) α_{univ} is not torsion (by exhibiting a single specialization of infinite order); and (iii) using torsion bounds for Jacobians in terms of the height of the model, we show that torsion specializations of α_{univ} contribute negligibly in the relevant boxes. A box-counting argument then shows

that among the many integral models for which the two points at infinity are $\mathbb{Q}$-rational, the proportion for which $[\infty_+ - \infty_-]$ is torsion tends to 0. Equivalently, "most" such curves have $\operatorname{rank} \mathrm{Jac}(C)(\mathbb{Q}) \geq 1$. We also produce an unconditional source of rank $r \geq 2$ by constructing an explicit two-section subfamily and applying Néron specialisation (Corollary 2.11). This offers a partial explanation for the abundance of rank-2 examples in databases built from small-coefficient or small-discriminant searches (such as the current genus-2 data in the LMFDB).

Finally, we study a different, more rigid source of extra rank: curves whose Jacobian splits up to isogeny as a product of elliptic curves. For curves of the form $C : y^2 = f(x)$, the condition $\mathrm{Jac}(C) \simeq E_1 \times E_2$ can be related to writing f as a product of two cubics, and we reduce the relevant counting problem to counting suitable pairs of elliptic curves with full rational 2-torsion. This provides a second family of explicit rank phenomena in genus-2 and leads to the bounds proved in Section 2.3.

We complement the theoretical arguments above with explicit computational experiments supporting the rank phenomena discussed in this and in the next section. For transparency and reproducibility, the scripts used in these computations are publicly available on our GitHub Repository [3].

2.2. **Number of curves whose Jacobian has positive rank.** Following [10, Section 2.1], every genus-2 curve defined over an integral domain of characteristic $\neq 2$ admits a Weierstrass model

$$C : \quad y^2 + h(x)y = f(x), \tag{3}$$

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

Completing the square gives the simplified equation

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

The discriminant of (3) is defined by

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

and $\Delta(f,h) \neq 0$ is equivalent to (3) defining a smooth genus-2 curve.

In the search for genus-2 curves of bounded discriminant, Booker et al. [10, Section 3.1] enumerate integral models of the form (3). 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)), the authors noted that one can subtract from h a polynomial in $2\mathbb{Z}[x]$.

For parameters $X, Y \geq 1$ they 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 $h = \sum_{i=0}^{\deg h} h_i x^i$. Note that $S_1(X)$ is the disjoint union of 16 copies of $\mathcal{C}_1(X)$. The sets S_2 and $\mathcal{C}_2(X)$ are defined using the same height but note that the degrees of the polynomials f in the two cases are not the same.

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

$$y^2 + h(x)y = f_{\underline{a}}(x) \tag{5}$$

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 $\mathfrak{C} \to \mathcal{U}$ is smooth and proper of relative dimension 1, with geometric fibers curves of genus-2. In addition, the Jacobian of $\mathfrak{C}$ 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 (5) 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 prove some results that can be regarded as a more conceptual explanation of the "typically infinite order" comment in [10, Remark A.1] described in the previous part.

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,

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

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 [29, Section 4], so its relative diagonal is closed [29, 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 $\underline{a} \in U^\infty$ such that $\alpha_{\underline{a}}$ is non-torsion.

Take $h = 0$ and consider the curve

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

By [57, 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.*

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 (3), 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* (3) *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* [43, 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 ([41, IIIa.8.1]) and height bounds for root differences of polynomials (see [33, Proposition 5.4]) to prove an explicit upper-bound for the level-4 θ-height (see [33, 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 [33, Definition 5.1]).

We next use Pazuki's comparison theorem between θ-height and (stable) Faltings height h_F [43, 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 (3). 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

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

for X sufficiently large. In particular,

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

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

$$T(X) \subseteq \bigcup_{n=1}^{N(X)} \Big(\mathcal{V}_n(\mathbb{Z}) \cap \{\underline{a} \in \mathcal{U}^\infty(\mathbb{Z}) : H(\underline{a}) \le X\}\Big). \tag{7}$$

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. [37, 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; 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 $F_n(a_6, \dots, a_0) = 0$.

One can count that

$$\#\big(\mathcal{V}_n(\mathbb{Z})\cap\{H \le X\}\big) \ \ll \ \#\big(\{F_n = 0\}(\mathbb{Z})\cap[-X, X]^7\big) \ \ll \ (\deg(F_n))\, X^6 \ \ll \ n^2X^6,$$

with absolute implied constants (independent of n). Combining with (7) 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

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

Hence

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

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 $X \to \infty$.

A straightforward counting argument shows that $S_1^{\square}(X)$, the subset of $S_1(X)$ defined by the first 3 conditions in the corollary above is $\#S_1^{\square}(X) \asymp X^{13/2}$ and hence, as $X \to \infty$, the proportion of $(f,h) \in S_1^{\square}(X)$ for which the divisor $[\infty_+ - \infty_-]$ is torsion on the Jacobian of $y^2 + h(x)y = f(x)$ is $O(X^{-1/2}(\log X)^6)$. This proves part (2) of Theorem 1.

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

$$\frac{\#\{(f,h) \in S_1^{\square}(X) \mid \mathrm{rank}\left(\mathcal{J}_{(f,h)}(\mathbb{Q})\right) \geq 1\}}{\#S_1^{\square}(X)} = 1 - O(X^{-1/2}(\log X)^6).$$

In particular,

$$\liminf_{X\to\infty} \frac{\log|\{(f,h) \in S_1(X) \mid \mathrm{rank}\left(\mathcal{J}_{(f,h)}(\mathbb{Q})\right) \geq 1\}|}{\log|S_1(X)|} \geq \frac{13}{14}.$$

Proof. The last part of the corollary holds because $S_1^{\square}(X)$ is a subset of $S_1(X)$. The former has cardinality $X^{\frac{13}{2}}$ for 6 arbitrary coefficients and a leading coefficient which can be any square less than X. The cardinality of $S_1(X)$ is X^7, corresponding to 7 arbitrary coefficients, which leads to a logarithmic density of $\frac{13}{14}$. □

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

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

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 [36]). 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. □

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 [49, §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 [49, §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*

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

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

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

In particular,

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

Proof. Let Ω be as in Proposition 2.9. Since Ω is thin in $\mathbb{A}^5(\mathbb{Q})$, Serre's quantitative estimate for affine thin sets [49, §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 claimed proportion follows. □

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

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

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 make precise, in an arithmetic ordering by height, the phenomenon noted in [10, Remark A.1]: 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 $C_1(X)$).

Remark 2.12. *If one expects rank parities to be equidistributed in $S_1^{\square}(X)$, then among the Jacobians of rank ≥ 1 one should see a positive proportion of even ranks; in particular one would expect rank ≥ 2 to occur with the logarithmic density* 13/14*, as in Corollary 2.7.*

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

$$\frac{\#\{(f,h) \in S_2^{\square}(X,Y) \mid \operatorname{rank}\big(\mathcal{J}_{(f,h)}(\mathbb{Q})\big) \geq 1\}}{\#S_2^{\square}(X,Y)} = 1 - O_Y(X^{-1/2}(\log X)^6).$$

Remark 2.14. *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 type of ideas in higher genus.*

2.3. **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 2.15. *Let* $\mathcal{N}_2(X) = \{f \in \mathcal{C}_1(X) \mid \operatorname{rank} \operatorname{Jac}(C_f) \geq 2\}$. *Then*

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

Following Gajović-Park [26], let $d, m \neq 0$ be squarefree integers and consider the genus-2 curve

$$C_{d,m}: \quad y^2 = d^3x^6 + m^3$$

together with the elliptic curves

$$E_d : y^2 = x^3 + d^3 \text{ and } E_m : y^2 = x^3 + m^3.$$

The Jacobian of $C_{d,m}$ splits as follows.

Lemma 2.16 (see [26, Section 2.2])**.** *There is a* $\mathbb{Q}$*-isogeny*

$$\operatorname{Jac}(C_{d,m}) \sim_{\mathbb{Q}} E_d \times E_m.$$

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

To ensure that both elliptic factors have positive rank, we use the following result due to Frey, as cited and used in [26] (proof of Theorem 2.5).

Lemma 2.17. *Let* $p > 3$ *be prime. Then*

$$\operatorname{rank} E_p(\mathbb{Q}) = \begin{cases} 0 & \text{if } p \equiv 5 (\mathrm{mod} 12), \\ 1 & \text{if } p \equiv 3 (\mathrm{mod} 4). \end{cases}$$

We are now ready to prove the above proposition.

Proof of Proposition 2.15 . 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 Lemmas 2.16 and 2.17,

$$\operatorname{rank} \operatorname{Jac}(C_{d,m})(\mathbb{Q}) = \operatorname{rank} E_d(\mathbb{Q}) + \operatorname{rank} E_m(\mathbb{Q}) = 2.$$

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 $\frac{9}{4} \frac{X^{2/3}}{(\log X)^2}$. □

2.4. **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 [31], 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 $F_{\bar{K}} \to G_{\bar{K}}$. 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 it is isomorphic to the Jacobian of a genus-2 curve defined over K.

Proposition 2.18 (Prop. 4 in [31])**.** *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 $C\colon y^2 = \operatorname{glue}(f,g)(x)$. Then

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

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 2.19. *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 $\operatorname{Jac}(C) \simeq F \times G$ 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 representation (see [30] 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 2.20. *Let K be a number field, and let $F\colon y^2 = f(x)$ and $G\colon y^2 = g(x)$ be elliptic curves such that*

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

for some $\lambda_1, \lambda_2 \in K$. Let C be the genus-2 curve given by the equation $y^2 = \mathrm{glue}(f,g)$. For each nonzero integer d, consider the quadratic twist $C^{(d)}$ of C given by $dy^2 = \mathrm{glue}(f,g)$. Then the set of integers d for which $\operatorname{rank}\mathrm{Jac}(C^{(d)}) \geq 2$ has logarithmic density $\geq \frac{1}{6}$.

Proof. By [1, Lemma 4.1], for all integers d of the form

$$d = d(u) = (\lambda_1 - \lambda_2)(u^2-1)\big(1 - \lambda_2 + (\lambda_1 - 1)u^2\big)\big(\lambda_1 u^2 - \lambda_2\big),$$

the quadratic twists $F^{(d)}$ and $G^{(d)}$ both have positive rank.

Since $d(u)$ is a sextic polynomial in u, the set of integers represented by $d(u)$ has logarithmic density $\frac{1}{6}$. For such d, both $F^{(d)}$ and $G^{(d)}$ have positive rank, and hence

$$\operatorname{rank}\mathrm{Jac}(C^{(d)}) \geq \operatorname{rank} F^{(d)} + \operatorname{rank} G^{(d)} \geq 2,$$

as claimed. □

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.

Proposition 2.21. *Let K be a totally real number field, and let C be a genus-2 curve over K such that $\mathrm{Jac}(C) \simeq_K E^2$ for some elliptic curve E over K. Assume that E admits a K-rational 3-isogeny. Then there exists a constant δ with $-1 < \delta \leq 1$ such that, as d varies over quadratic twists,*

$$\operatorname{rank}_K\big(\mathrm{Jac}(C^{(d)})\big) \equiv \begin{cases} 0 \pmod 4, & \text{with proportion } \frac{1+\delta}{2}, \\ 2 \pmod 4, & \text{with proportion } \frac{1-\delta}{2}. \end{cases}$$

If E is defined over $\mathbb{Q}$, then $\delta \neq 1$.

Proof. By [61, Theorem 1], there exists a constant δ with $-1 \leq \delta \leq 1$ such that, as d varies over quadratic twists,

$$\operatorname{rank}_K\big(E^{(d)}\big) \text{ is } \begin{cases} \text{even}, & \text{with proportion } \frac{1+\delta}{2}, \\ \text{odd}, & \text{with proportion } \frac{1-\delta}{2}. \end{cases}$$

By [7, Theorem 2.5], one has $\delta \neq -1$. If E is defined over $\mathbb{Q}$, then [53, Corollary 1.2] implies that $\delta \neq 1$.

Moreover, by Lemma 2.19, we have $\mathrm{Jac}(C^{(d)}) \simeq_K \big(E^{(d)}\big)^2$ for all d, and hence

$$\operatorname{rank}_K\big(\mathrm{Jac}(C^{(d)})\big) = 2\operatorname{rank}_K\big(E^{(d)}\big).$$

The claim 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 2.22. *Let $E_1\colon y^2 = f_1(x)$ and $E_2\colon y^2 = f_2(x)$ be elliptic curves over $\mathbb{Q}$. Assume either that both curves have full rational 2-torsion and no rational point of order 4, or that the Birch–Swinnerton-Dyer conjecture holds for the quadratic twists of E_1 and E_2.*

For any nonzero integers d_1 and d_2, the curve $C^{(d_1,d_2)}\colon y^2 = \operatorname{glue}\bigl(f_1^{(d_1)}, f_2^{(d_2)}\bigr)$, which is isomorphic to the curve $C\colon y^2 = \operatorname{glue}(f_1, f_2)$ over $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$.

If $D(X) = \{\, d \in \mathbf{Z} : 1 \le d \le X,\ d \text{ squarefree} \,\}$, then

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

Proof. By [52, Corollary 1.3] and [53, Theorem 1.1], the pairs (d_1, d_2) of squarefree integers are equidistributed among the four possibilities

$$\bigl(\operatorname{rank} E_1^{(d_1)}, \operatorname{rank} E_2^{(d_2)}\bigr) \in \{0,1\}^2,$$

each occurring with proportion $\frac{1}{4}$. □

A practical improvement. A heuristic strategy to solve Problem 2 for a curve C is to generate families of twists d such that $C^{(d)}$ has rank $\ge r_0$. A heuristic, due to Fermigier [24], states that the density of curves with rank $r_0 + r$ inside the family of rank $\ge r_0$ is the density of curves without restriction which have rank r.

Let us summarize the results in the literature. Consider an elliptic curve E with full rational 2-torsion and let E' be a twist of the form $y^2 = x(x-1)(x-\lambda)$ for a rational λ. We call λ the Legendre parameter of the curve.

Lemma 2.23 ([38],Cor. 3.3 and Th. 4.1 in [48],Th. 3.6 in [47])**.**

(1) *Any elliptic curve E having a rational point of order 2 admits an element $d(t) \in \mathbb{Q}(t)$ such that $E^{(d(t))}$ has rank 2 over $\mathbb{Q}(t)$.*
(2) *Let E be an elliptic curve in Legendre form $y^2 = x(x-1)(x-\lambda)$. If the Legendre parameter is of the form $\lambda = (1-a^2)/(a^2+2)$ or $\lambda = a(a-2)/(a^2+1)$, then there exists $d(t) \in \mathbb{Q}(t)$ such that $\operatorname{rank}_{\mathbb{Q}(t)} E^{(d(t))} \ge 3$.*
(3) *For elliptic curve E in Legendre form which admits a Weierstrass model of the form $y^2 = x(x-1)(x-\lambda)$ with $\lambda = -2a^2$ for some $a \in \mathbb{Q}^*$ there exist infinitely many $d \in \mathbb{Q}$ such that $\operatorname{rank}_{\mathbb{Q}} E^{(d)} \ge 4$. Those rationals d are parametrized by the x coordinates of the rational points of an elliptic curve of rank 1.*

3. Cryptographic motivation: Regev's quantum algorithm

In this section we develop the arguments in Section 1.1. We recall the mathematical assumptions which support the security of the hyperelliptic curve cryptography. We first recall Regev's recent algorithm. By solving Problem 1 we produce hyperelliptic curves on which the algorithm is particularly fast. In practice HECC is implemented on a very small list of curves. We explain why the security of each

curve relies on the difficulty to find twists of high rank. This is an application of Problem 2.

The discrete logarithm problem (DLP) plays a key role in cryptography. Let $(G,+)$ be a group, e.g. an elliptic curve or the Jacobian of a genus-2 curve. If g and h are two elements of G such that $h=[x]g$, the discrete logarithm of h in base g, denoted $\log_g h$, is x. Elliptic curve cryptography (ECC) and hyperelliptic curve cryptography (HECC) rely on the difficulty to compute discrete logarithms (see [4]).

The quantum algorithms offer a new paradigm: Shor's algorithm [51] can compute discrete logarithms in polynomial time, which compromises the security of ECC and HECC. Recently Regev [45] proposed a quantum algorithm for the DLP which has a parameter d. The step which dominates its gate complexity of Regev's algorithm consists of $d+\frac{n}{d}$ additions and doublings in the group G. We recall that the gate complexity of Shor's algorithm is n additions and doublings in G. Hence, from an asymptotic point of view, the advantage of Regev's algorithm with respect to Shor's algorithm is $\min(d,\frac{n}{d})$.

3.1. **Regev's algorithm in a nutshell.** One uses $d-2$ elements of G, $g_1,\dots,g_{d-2}$ and sets $g_{d-1}=h$ and $g_d=g$.

In Regev's algorithm one considers the lattice

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

One computes in superposition all the sums $\sum_{i=1}^{d}[z_i]g_i$, called multi-scalar multiplications, where $z_1,\dots,z_d$ are non-negative $\frac{n}{d}$-bit integers. 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 best complexity of the algorithm, one must have a classical algorithm which computes any scalar product with coefficients of $\frac{n}{d}$ bits. This can be done using Pippenger's algorithm [44] if one can store a table with all the multi-scalar multiplications with coefficients 0 and 1. In the paradigm of quantum algorithms one cannot store large tables and Regev [45] proposed to select the elements $g_1,\dots,g_{d-2}$ which can be represented on few bits.

If C is a hyperelliptic curve defined over a finite field $\mathbb{F}_q$, the method proposed in [2] and extended in [4] consists of using a curve $\overline{C}$ defined over $\mathbb{Q}$ whose reduction modulo q is isomorphic to C. A set of generators of $\mathrm{Jac}_{\mathbb{Q}}(\overline{C})$ modulo its torsion allows to produce points on $\mathrm{Jac}_{\mathbb{F}_q}(C)$ by reduction modulo q. These are used in the role of $g_1,\dots,g_{d-2}$ in Regev's algorithm.

By solving Problem 1 one finds curves on which Regev's algorithm can be run with a large parameter d.

Consider now the case of a curve C which has only lifts of small rank. Assume that one found an integer d or a pair of integers (d_1,d_2) which are squares modulo q, one can use any curve C' defined over $\mathbb{Q}$ which is isomorphic to C over $\mathbb{Q}(\sqrt{d})$ or $\mathbb{Q}(\sqrt{d_1},\sqrt{d_2})$. Hence, by solving Problem 2 one can run Regev's algorithm on the curve C.

3.2. **Genus-2 curves with simple Jacobian and high rank.** *A curve of small height.* Booker et al. [10] 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 generated by the following elements in Mumford representation

$$(1, x^2), (x + 1, 0), (x + 2, -x^3 - 4), (x^2 - 2, 1).$$

Note also that Booker and Sutherland [9] announced a work in progress to assemble a large database of genus-2 curves. It is interesting to search for curves of rank larger than 4.

Curves of high rank. We summarize a list of record curves in the literature. Here $\mathrm{Hyp}(f, h)$ is the hyperelliptic curves associated to the polynomials f and h. Whenever h is missing, it is assumed to be 0. Here $\widehat{h}$ denotes the 2-adic logarithm of the max of the canonical height over the elements of a basis of the Jacobian in question.

curve	ref.	rank	$\widehat{h}$
$\mathrm{Hyp}\left(\begin{smallmatrix}1306881x^6 + 18610236x^5 - 46135758x^4 - \\ 1536521592x^3 - 2095359287x^2 + 32447351356x + 89852477764\end{smallmatrix}\right)$	[54]	≥ 16	8.41
$\mathrm{Hyp}\left(\begin{smallmatrix}82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 \\ +567207969x^2 - 985905640x + 247747600\end{smallmatrix}\right)$	[40]	≥ 22	14.73
$\mathrm{Hyp}\left(\begin{smallmatrix}4037229x^6 + 34187102x^5 - 724533076x^4 - 4944866082x^3 \\ +57659086152x^2 + 241518308040x + 313383220164\end{smallmatrix}\right)$	[16]	≥ 25	28.55
$\mathrm{Hyp}\left(\begin{smallmatrix}80878009x^6 - 236558406x^5 - 1018244179x^4 \\ +4436648480x^3 + 6445563464x^2 - 13620761544x + 68406^2\end{smallmatrix}\right)$	[22]	≥ 26	32.14
$\mathrm{Hyp}\left(\begin{smallmatrix}60516x^6 + 1680225324x^5 + 200663873413x^4 - 1021197439562x^3 \\ -290505889943111x^2 + 316071770416320x + 123355813282790400\end{smallmatrix}\right)$	[20]	≥ 27	39.57

3.3. **Highest known ranks for the genus-2 curves with split Jacobian.** By Proposition 2.18, for any elliptic curve E, there exists a genus-2 curve C such that

$$\mathrm{rank}_{\mathbb{Q}(E[2])}(\mathrm{Jac}(C)) = 2\,\mathrm{rank}_{\mathbb{Q}(E[2])}(E) \geq 2\,\mathrm{rank}_{\mathbb{Q}}(E).$$

In this section we present pairs of elliptic curves with full rational 2-torsion.

Shioda [50] proposed a genus-2 curve over $\mathbb{Q}(t)$ whose Jacobian has rank 14, which is the current record. This was done by gluing together two elliptic curves over $\mathbb{Q}(t)$ which have high rank. Indeed, the following result is a direct consequence of gluing.

The congruent number curve. Let $E : y^2 = x^3 - x$ be the curve (see LMFDB: 32.a3). The genus-2 curve of equation $y^2 = 6x^6 - 9x^4 - 9x^2 + 6$ has Jacobian $J \simeq_{\mathbb{Q}} E \times E$. The first record computations were found by Rogers [46]. See [60, Table 2] for some twists d of E which attain ranks from 2 to 7.

Moderate rank curves of small height. We list below elliptic curves with full rational 2-torsion and high rank, which are listed in LMFDB. They can be glues (see Prop. 2.18) to any elliptic curve with full rational 2-torsion, including to themselves.

torsion	E	$\mathrm{rank}(E \times E)$	$\widehat{h}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$[1, -1, 1, -41, 96]$	2	0.51
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$[1, -1, 1, -356, 2126]$	4	1.64
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$[0, 0, 0, -13251, 474370]$	6	2.20

3.3.1. *High rank genus-2 curves over* $\mathbb{Q}(t)$. The results in the literature offer directly examples of genus-2 curves with split Jacobian.

Lemma 3.1. *There is a genus-2 curve defined over $\mathbb{Q}(t)$ whose rank is ≥ 20. It is $(2,2)$-isogenous over $\mathbb{Q}(t)$ to $E_1 \times E_2$ where E_1 is defined over $\mathbb{Q}$ and E_2 is defined over $\mathbb{Q}(t)$ by coefficients of degree xx and binary size yy.*

Proof. By [19] there exists an elliptic curve E_1 defined over $\mathbb{Q}$ such that $E_1(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}^{15}$.

By Proposition 2.18 there exists an explicit genus-2 curve $C : y^2 = h(x)$ such that $\mathrm{Jac}(C) \simeq E_1 \times E_2$. Note that $\operatorname{rank} \mathrm{Jac}(C) = 20$ and a direct computation which can be done with a computer program verifies that h is a sextic polynomial whose coefficients are fractions in $\mathbb{Q}(t)$ of degree 756 and binary size of the coefficients 1761. □

We note that a family of rank 20 can be obtained with a family of elliptic curves such that $E(\mathbb{Q}(t)) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}^5$ (see [18] for a curve attributed to Elkies).

Recall that in Regev's algorithm, when $\mathrm{Jac}(C) \simeq E_1 \times E_2$ one sums the points of E_1 (resp. E_2) on E_1 (resp. E_2). Hence, instead of comparing the canonical height on $\mathrm{Jac}(C)$ we compare the canonical height on the elliptic curves.

3.4. **High rank twists of certain curves used in cryptography.**

3.4.1. 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 [15]). The curve is one of the most important in HECC, e.g. it was considered along the curve *Generic1271* in [11]. It has CM and simple Jacobian (see LMFDB:4096.b.65536.1). One of its twists, the curve $x^5 + 8$, is used in [13].

In an experiment, among the curves $y^2 = x^5 + a$ with $a \leq 10^5$ one has:

- 60794 are squarefree (close to a theoretical proportion of $\zeta(2)^{-1}$);
- 3559 of them have at least 3 rational points of height ≤ 500 on C_a (this is implemented in Magma, see [40]). 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 [8].
- For all the above curves one computes in Magma a basis of the Mordell-Weil group. This is implemented in Magma [12] and PARI/GP [58] only for genus 1 and 2. We find 15,11,2 and respectively 2 twists of rank 5,6,7 and respectively 8. For comparison, among approximately the same number of curves in [10] there are none of rank ≥ 5, which suggests that the curves $x^5 + a$ have different logarithmic densities than the twists of a generic genus-2 curve.

Remark 3.2. *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 [55] identified the Hecke character η_a such that $L(J_a) = L(\eta_a)$ (see also [56]). The computation of the Hecke grossen characters is implemented in PARI/GP using the algorithms in [39]. We are indebted to Aurel Page for the program that we used to compute the L-function of J_a. 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. It is approximately* 70 *times slower than the optimized implementation of Bill Allomber.*

3.4.2. *The curves C such that* $\mathrm{Jac}(C) \simeq_{\overline{\mathbb{Q}}} E \times E$ *for an elliptic curve E.* Freeman and Satoh defined two families of curves C whose Jacobian is the square of an elliptic curve:

Lemma 3.3 (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* (8) *(resp.* (9)*).*

$$C : y^2 = x^5 + ax^3 + bx \tag{8}$$

$$C : y^2 = x^6 + ax^3 + b. \tag{9}$$

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* (10) *(resp.* (11)*):*

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

$$E(c) : y^2 = (c+2)x^3 - (3c-30)x^2 + (3c+30)x - (c-2). \tag{11}$$

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

They occur in cryptography e.g. $b = 21$ in [17, Ex 20] and $b = 3$ in [32]. Note that the curves are twists over $\mathbb{Q}(b^{\frac{1}{5}})$ of $y^2 = x^5 + x$, which is of the form (8) with $a = 0$ and $b = 1$. By Lemma 3.3 we have

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

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

Drylo's pairing-friendly curves with split Jacobian. Drylo [17] proposed a list of curves as in the statement of Lemma 3.3 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 3.3, $\mathrm{Jac}(C) \simeq_{\mathbb{Q}(\zeta_3)} E \times E$ where $E = E(\frac{5}{2})$ as in Equation (9). 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 $\mathbb{Q}(\zeta_3)$.

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] Manjul Bhargava, Zev Klagsbrun, Robert J Lemke Oliver, and Ari Shnidman, *3-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field*, Duke Mathematical Journal **168** (2019), no. 15, 2951–2989.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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

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

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

[15] 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.

[16] 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.

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

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

[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] Stéfane Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur $\mathbb{Q}$*, Experimental Mathematics **5** (1996), no. 2, 119–130.

[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] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.

[30] Jeffrey Hatley, *Rank parity for congruent supersingular elliptic curves*, Proceedings of the American Mathematical Society **145** (2017), no. 9, 3775–3786.

[31] Everett W Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Mathematicum **3** (2000).
[32] 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.
[33] Jean Kieffer, *Degree and height estimates for modular equations on PEL shimura varieties*, Journal of the London Mathematical Society **105** (2022), 1314–1361.
[34] Neal Koblitz, *Hyperelliptic cryptosystems*, Journal of Cryptology **1** (1989), 139–150.
[35] Brian Lawrence, *A density result for real hyperelliptic curves*, Comptes Rendus Mathematique **354** (2016), no. 12, 1219–1224.
[36] The LMFDB Collaboration, *The L-functions and modular forms database*, 2026. [Online; accessed 15 January 2026].
[37] Davide Lombardo, *Abelian varieties*, 2018. Lecture notes, Luxembourg Summer School on Galois representations, July 3–7, 2018.
[38] Jean-François Mestre, *Rang de certaines familles de courbes elliptiques d'invariant donné*, Comptes Rendus de l'Académie des Sciences-Series I-Mathematics **327** (1998), no. 8, 763–764.
[39] Pascal Molin and Aurel Page, *Computing groups of Hecke characters*, Research in Number Theory **8** (2022), no. 4, 91.
[40] 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`.
[41] David Mumford, *Tata lectures on theta. II*, Birkhäuser, Boston, 1984.
[42] 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.
[43] Fabien Pazuki, *Theta height and Faltings height*, Bulletin de la Société Mathématique de France **140** (2012), no. 1, 19–49.
[44] Nicholas Pippenger, *On the evaluation of powers and monomials*, SIAM Journal on Computing **9** (1980), no. 2, 230–250.
[45] Oded Regev, *An efficient quantum factoring algorithm*, Journal of the ACM **72** (2025), no. 1, 1–13.
[46] Nicholas F Rogers, *Rank computations for the congruent number elliptic curves*, Experiment. Math. **9** (2000), no. 3, 591–594.
[47] K Rubin and A Silverberg, *Twists of elliptic curves of rank at least four*, London Mathematical Society Lecture Note Series **341** (2007), 177.
[48] Karl Rubin and Alice Silverberg, *Mod 2 representations of elliptic curves*, Proceedings of the American Mathematical Society (2001), 53–57.
[49] 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.
[50] Tetsuji Shioda, *Genus two curves over* $\mathbb{Q}(t)$ *with high rank*, Commentarii mathematici Universitatis Sancti Pauli **46** (1997), no. 1, 15–21.
[51] 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.
[52] Alexander Smith, 2^∞*-Selmer groups,* 2^∞*-class groups, and Goldfeld's conjecture*, 2017.
[53] ———, *The Birch and Swinnerton-Dyer conjecture implies Goldfeld's conjecture*, arXiv preprint arXiv:2503.17619 (2025).
[54] Colin Stahlke, *Algebraic curves over* $\mathbb{Q}$ *with many rational points and minimal automorphism group*, International Mathematics Research Notices **1997** (1997), no. 1.
[55] Michael Stoll, *On the arithmetic of the curves* $y^2 = x^\ell + a$*, II*, Journal of Number Theory **93** (2002), no. 2, 183–206.
[56] 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.
[57] Szabolcs Tengely, *Effective Methods for Diophantine Equations*, Ph.D. Thesis, 2005.
[58] The PARI Group, *PARI/GP version* `2.18.1`, Univ. Bordeaux, 2025. available from `http://pari.math.u-bordeaux.fr/`.

[59] Mark Watkins, *Some heuristics about elliptic curves*, Experimental Mathematics **17** (2008), no. 1, 105–125.
[60] 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.
[61] 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