ANTS XVII — Groningen, July 7th 2026

Logarithmic density of rank ≥ 1 and rank ≥ 2 genus-2 Jacobians and applications to hyperelliptic curve cryptography

Razvan Barbulescu, Mugurel Barcau, Vicențiu Pașol and George Țurcaș

CNRS, Institut de mathémathiques de Bordeaux

Background on hyperelliptic curves

Hyperelliptic curves of genus g over a field K

- An algebraic curve C is hyperelliptic if it has an equation

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

  with $\deg f \in \{2g+1, 2g+2\}$ and $\deg h \leq g+1$.
  One has: $\text{genus}(C) = g$.
- For any field $L \geq K$, the L-rational points of C, denoted $C(L)$ are the solutions of the equation in $\mathbb{P}^2(L)$.

Jacobian variety $\mathrm{Jac}(C)(L)$ for a field $L \geq K$

- when $L = \overline{K}$
  - divisor group of degree zero:
    $I = \{\sum_{P \in C(\overline{K})} n_P P : |\{P, n_P \neq 0\}| < \infty \text{ and } \sum_P n_P = 0\}$
  - principal subgroup: $P = \{\sum_{P \in C(\overline{K})} \mathrm{val}_P(f) P : f \in \overline{K}(C)\}$
  - $\mathrm{Jac}(C)(\overline{K}) := I/P$ is an abelian variety
- when $L \neq \overline{K}$, $\mathrm{Jac}(C)(L) = \mathrm{Jac}(C)(\overline{K})^{\mathrm{Gal}(\overline{K}/L)}$

Examples of problems

Curves over $\mathbb{Q}$

By the Mordell-Weil theorem,

$$\mathrm{Jac}_{\mathbb{Q}}(C) \simeq T \times \mathbb{Z}^r$$

with $|T| < \infty$ and $r \in \mathbb{N}$.

For a given genus, study the distribution of ranks.

Genus-2 curves over $\mathbb{F}_q$

Discrete logarithm problem (DLP):

given two elements $g, h = [x]g \in \mathrm{Jac}_{\mathbb{F}_q}(C)$, find x.

When $|\mathrm{Jac}_{\mathbb{F}_q}(C)|$ is an n-bit integer,

- the best classical DLP algorithm has a cost $2^{n/2}$
- there are two quantum DLP algorithms of cost $\mathrm{poly}(n)$: Shor and Regev.

Implement and compare the quantum DLP algorithms

The problem in study

No algorithm is known to list curves of discriminant $\leq X$

Instead, Bhagava et al. used the following set for their proofs.

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

In the computations recorded in LMFDB one uses the same set (see Booker et al.).

Problem (THE HIGH RANK CURVE PROBLEM)

Given

- *an integer* $g \geq 1$,
- *a target rank* $r \geq 0$,
- *a height bound* X,
- *a family* $\mathcal{F} \subset \bigcup_{X>0} \mathcal{C}^{(g)}(X)$ *(e.g. CM)*

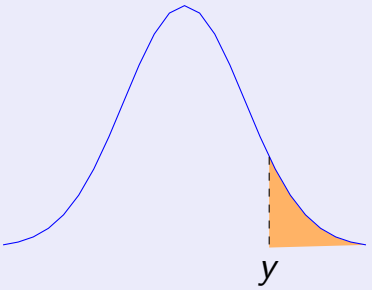
sample a curve from the finite set

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

if this set is nonempty.

A type of exhaustive search algorithms

Graphical representation



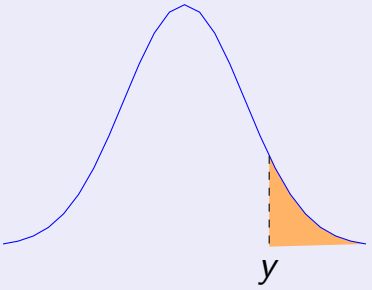
1. subfamily with good distribution
2. ranking function to rapidly eliminate bad candidates
3. estimate the distribution

Example of polynomial selection in NFS

1. Kleinjung 2006 and 2008 proposed families of polynomials
2. Murphy 1999 proposed a criterion called α
3. B. and Lachand 2017 studied the average of α

A type of exhaustive search algorithms

Graphical representation



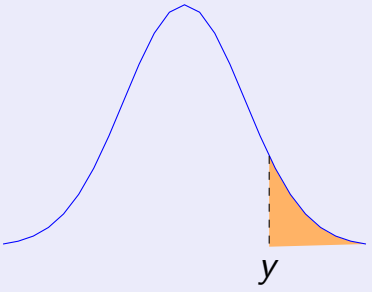
1. subfamily with good distribution
2. ranking function to rapidly eliminate bad candidates
3. estimate the distribution

Example of the high rank twist problem for elliptic curves

1. Mestre 1992 proposed a family of twists of rank $r \geq 2$
2. Mestre 1982 used the criterion of Mestre-Nagao sums
3. The Goldfeld-Smith theorem (proved in 2025 under the BSD) estimates the proportion of twists of rank $r = 0$ and $r = 1$ are $1/2$ each.

A type of exhaustive search algorithms

Graphical representation



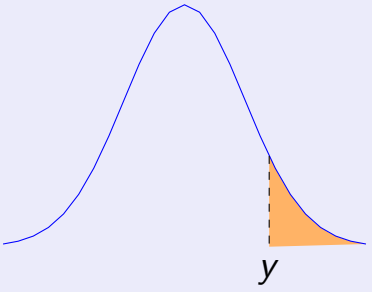
1. subfamily with good distribution
2. ranking function to rapidly eliminate bad candidates
3. estimate the distribution

Example of the high rank twist problem for genus-2 curves

1. the family of genus-2 curves defined over $\mathbb{Q}(u)$ by $y^2 = \sum_{i=0}^{6} f_i x^i$ with $f_0 \in (\mathbb{Q}^*)^2$ has positive rank and simple Jacobian
2. B. and Bisson 2024 used as criterion the number of points on the curve up to a given height
3. this work prove a lower bound on the number of rank-2 genus-2 curves

A type of exhaustive search algorithms

Graphical representation



1. subfamily with good distribution
2. ranking function to rapidly eliminate bad candidates
3. estimate the distribution

Example of the high rank twist problem for genus-2 curves

1. the family of genus-2 curves defined over $\mathbb{Q}(u)$ by $y^2 = \sum_{i=0}^{6} f_i x^i$ with $f_0 \in (\mathbb{Q}^*)^2$ has positive rank and simple Jacobian
2. B. and Bisson 2024 used as criterion the number of points on the curve up to a given height
3. this work prove a lower bound on the number of rank-2 genus-2 curves

What are the "densities" of curves rank $\geq 1, 2$ for genus 2?

Main result

Definition

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

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

Theorem (1)

The subset of genus-2 curves with rank $r \geq 2$ has logarithmic density at least $\frac{5}{7}$ with respect to $\mathcal{C}^{(2)}(X) = \{C : y^2 = \sum_{i=0}^{6} f_i x^i \in \mathbb{Z}[x] \mid \max(|f_i|) \leq X\}$.

Sketch of the proof of Theorem 1 (1/3)

The Abel-Jacobi map with two points at infinity

- $C : y^2 + h(x)y = f(x)$ with $\deg h \leq g+1$ and $\deg f \leq 2g+2$

  $(2y + h(x))^2 = 4f(x) + h(x)^2$

  $y'^2 = g(x)$ with $c(x) = 4f(x) + h(x)^2$

  The points at infinity $(x : y' : z) = (1 : \pm\sqrt{c_{2g}} : 0)$, called ∞_+ and ∞_-.
- When C is defined over a field k (including the case when $\sqrt{c_{2g}} \in \overline{k}\backslash k$), one has the Abel-Jacobi map $\begin{cases} \iota : & C(k) & \to & \mathrm{Jac}_k(C) \\ & P & \mapsto & [2P - \infty_+ - \infty_-] \end{cases}$

When $\sqrt{c_{2g}} \in k$ one has $\iota(\infty_+) = [\infty_+ - \infty_-] \in \mathrm{Jac}_k(C)$

Booker et al. (ANTS 2016): the divisor class $[\infty_+ - \infty_-]$ "typically has infinite order"

Sketch of the proof of Theorem 1 (1/3)

The Abel-Jacobi map with two points at infinity

- $C : y^2 + h(x)y = f(x)$ with $\deg h \leq g+1$ and $\deg f \leq 2g+2$
  $(2y + h(x))^2 = 4f(x) + h(x)^2$
  $y'^2 = g(x)$ with $c(x) = 4f(x) + h(x)^2$
  The points at infinity $(x : y' : z) = (1 : \pm\sqrt{c_{2g}} : 0)$, called ∞_+ and ∞_-.
- When C is defined over a field k (including the case when $\sqrt{c_{2g}} \in \overline{k}\backslash k$), one has the Abel-Jacobi map $\begin{cases} \iota : & C(k) & \to & \mathrm{Jac}_k(C) \\ & P & \mapsto & [2P - \infty_+ - \infty_-] \end{cases}$

When $\sqrt{c_{2g}} \in k$ one has $\iota(\infty_+) = [\infty_+ - \infty_-] \in \mathrm{Jac}_k(C)$

Booker et al. (ANTS 2016): the divisor class $[\infty_+ - \infty_-]$ "typically has infinite order"

Proof idea

- count the number of pairs (f, h) for which the leading coeff. of $4f + h^2$ is square
- the number of pairs which have torsion (not necessarily $[\infty_+ - \infty_-]$) is negligible

Heuristic behind the idea

- the Torsion conjecture (see Cadoret and Tamagawa) states that the torsion is uniformly bounded (e.g. Mazur's theorem for $g = 1$)
- for $n = 2, 3$ and 5 the n-torsion genus-2 curves have zero density

Sketch of the proof of Theorem 1 (2/3)

Let C be a genus-2 curve over $\mathbb{Q}$. Denote by h_F the Faltings height.

- Gaudron and Rémond 2025: $\mathrm{Jac}_{\mathbb{Q}}(C)_{\mathrm{tors}} \ll \max(1, (\log H_F(C)))^2$
- Kieffer 2022 and Pazuki 2012: $\max(1, (\log H_F(C)))^2 \ll (\log H(C))^2 \ll (\log X)^2$
- (informal) we show: $|\{\text{genus-2 curves where } n[\infty_+ - \infty_-] = 0\}| \ll n^2 X^6$
- (informal) When combining, the proportion of genus-2 curves with rational points at infinity which are torsion is

$$\text{probability that } [\alpha_+ - \alpha_-] \text{ is torsion}) \ll \frac{(\log X)^6}{X}.$$

Sketch of the proof of Theorem 1 (3/3)

Notations

- $h = \sum_{i=0}^{3} h_i x^i$ is fixed
- $f_{\underline{a}} = \sum_{i=0}^{6} f_i x^i$
- $\mathcal{X} = \mathbb{A}^7_{\mathbb{Q}} \times \{0,1\}^4$
- $\mathfrak{C}$ is universal curve $y^2 + h(x)y = f(x)$ inside the projective plane $\mathbb{P}(1,3,1)$
- $\mathcal{U} = \{\underline{a} \in \mathcal{X} \mid \Delta(4f_{\underline{a}} + h_{\underline{a}}^2) \neq 0\}$
- $\mathcal{J}_{\underline{a}} = \mathrm{Jac}(\mathfrak{C}_{\underline{a}})$
- $c = 4f_6 + h_3^2 \in \Gamma(\mathcal{U}, \mathcal{O}_{\mathcal{U}})$
- $\mathcal{U}_6 = \{\underline{a} \in \mathcal{U} \mid c \neq 0\}$
- $\mathcal{U}^\infty = \mathrm{Spec}(\mathcal{O}_{\mathcal{U}_6}[u]/(u^2 - c))$
- $\alpha_{\mathrm{univ}} = [(1:c:0) - (1:-c:0)] \in \mathcal{J}_{\underline{a}}$
- $\mathcal{V}_n = \{\underline{a} \in \mathcal{U}^\infty \mid n\alpha_{\mathrm{univ}} = 0\}$

Bounding $|\mathcal{V}_n|$

- the abelian scheme $\mathcal{J} \to \mathcal{U}^\infty$ is projective, so there is a $\mathcal{U}^\infty$-simple line bundle $\mathcal{L}$
- by replacing $\mathcal{L}$ with a power of $\mathcal{L} \otimes [-1]^*\mathcal{L}$ one can assume
  - it is symmetric
  - it is reatively very ample
  - it induces a projectively normal embedding into $\mathbb{P}^N_{\mathcal{U}^\infty}$
- since $[n]^*\mathcal{L} \simeq \mathcal{L}^{\otimes n^2}$, by projective normality the morphism $[n] : \mathcal{J} \to \mathcal{J}$ is defined by polynomial homogenous equations of degree n^2 and at least one is non-trivial
- the cardinality of a subset given by a homogenous polynomial of degree n^2 is at most $n^2 X^6$.

Background on twists of genus-two curves

Gluing

Given two elliptic curves over $F : y^2 = f(x)$ and $G : y^2 = g(x)$ defined over K having full K-rational 2-torsion, there exists a polynomial

$$h(x) = \mathrm{glue}(f(x), g(x))$$

and a genus-2 curve defined over K by $y^2 = h(x)$ such that $\mathrm{Jac}_K(C) \sim_K F \times G$.

Twist of a curve

- definition: C_1/K and C_2/K are twists of each other if $C_1 \not\simeq_K C_2$ and $C_1 \simeq_{\overline{K}} C_2$
- example 1: $C : y^2 = f(x)$ and $C^{(\delta)} : y^2 = f^{(\delta)}(x)$ with $f^{(\delta)} = \delta^{\deg f} f(x/\delta)$ when $\deg f$ is odd
- example 2: $C : y^2 = x^{2g+1} + a$ and $C_\delta : y^2 = x^{2g+1} + a\delta^{2g+1}$
- example 3: $C : y^2 = \mathrm{glue}(f_1(x), f_2(x))$ and $C^{(\delta_1,\delta_2)} : y^2 = \mathrm{glue}(f_1^{(\delta_1)}(x), f_2^{(\delta_2)}(x))$ with $f_i^{(\delta_i)} = \delta_i^{\deg f_i} f_i(x/\delta_i)$ when $\deg f_i$ is odd

The second problem in study

Poincaré decomposition

Every abelian variety has a unique decomposition into irreducible varieties. If C is a genus-2 curve one has one of the three cases:

- $\mathrm{Jac}(C)$ is simple
- $\mathrm{Jac}(C) \sim E \times E$
- $\mathrm{Jac}(C) \sim E_1 \times E_2$ with $E_1 \not\sim E_2$

THE HIGH RANK TWIST PROBLEM

Given $r \in \mathbb{N}$ and

- given a genus-2 curve $C : y^2 = f(x)$ with simple Jacobian, find $\delta \in \mathbb{Z}^*$ such that $\mathrm{rank}(C^{(\delta)}) \geq r$
- given $E : y^2 = f(x)$ with full $\mathbb{Q}$-rational 2-torsion, find $\delta \in \mathbb{Z}^*$ such that $\mathrm{rank}(y^2 = \mathrm{glue}(f^{(\delta)}(x), f^{(\delta)}(x))) \geq r$
- given $E_1 : y^2 = f_1(x)$ and $E_2 : y^2 = f_2(x)$ with full $\mathbb{Q}$-rational 2-torsion, find $\delta_1, \delta_2 \in \mathbb{Z}^*$ such that $\mathrm{rank}(y^2 = \mathrm{glue}(f_1^{(\delta_1)}(x), f_2^{(\delta_2)}(x)) \geq r$

Sketch of the proof of Theorem 2

Theorem (2)

Let E_1, E_2 and C be s.t. $\mathrm{Jac}(C) \sim E_1 \times E_2$.
Let $C^{'d_1,d_2)}$ denote the gluing of the quadratic twists $E^{(d_1)}$ and $E^{(d_2)}$. Then, one has

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

- Smith 2025: Goldfeld's conjecture holds under BSD, i.e. for any elliptic curve E,

$$\lim_{X\to\infty} \frac{\left|\{d \in D(X) : \mathrm{rank}(E^{(d)}) = r\}\right|}{|D(X)|^2} = \begin{cases} \frac{1}{2}, & r = 0, \\ \frac{1}{2}, & r = 1, \\ 0, & r \geq 2, \end{cases}$$

  where $D(X)$ is the set of squarefree positive integers less than X.

- Howe et al. 2000: any two elliptic curves with full rational 2-torsion can be glued
- since E_1 has full 2-torsion, any twist $E_1^{(d_1)}$ also does, so it can be glued to any twist of E_2
- since $\mathrm{Jac}(C^{(d_1,d_2)} \sim E_1^{(d_1)} \times E_2^{(d_2)}$ the Mordell-Weil ranks add.

Cryptographic application

Regev's quantum algorithm 2023

- To compute logarithms on $\mathrm{Jac}_{\mathbb{F}_q}(C)$ one must find elements in the group which can be written on a small number of bits.
- B., Barcau and Pasol 2025 and B. Bisson 2024 proposed to use a curve C' isogenous to C, in particular twists C_δ.

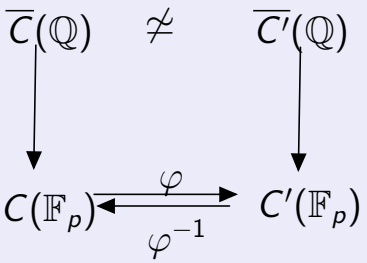


Figure: Here q is a prime and $\delta \in \mathbb{Z}$ which is a square in $\mathbb{F}_q$ but not in $\mathbb{Z}$. The figure illustrates the relations between a curve C over $\mathbb{F}_q$, a lift of C to $\mathbb{Q}$ denoted $\overline{C}$, the isogenous curve C' (which is ususally a twist C_δ) and its $\overline{C'}$ which is usually a twist $\overline{C}_\delta$ of $\overline{C}$. Here φ is an isogeny.

Solutions of the high rank twist problem for certain curves

- $g = 1$: Curve **secp256k1** has a twist of rank $r = 4$
- $g = 2$: Curve **4GLV127-BK** has a twist if rank $r = 7$

Cryptographic application

Regev's quantum algorithm 2023

- To compute logarithms on $\mathrm{Jac}_{\mathbb{F}_q}(C)$ one must find elements in the group which can be written on a small number of bits.
- B., Barcau and Pasol 2025 and B. Bisson 2024 proposed to use a curve C' isogenous to C, in particular twists C_δ.

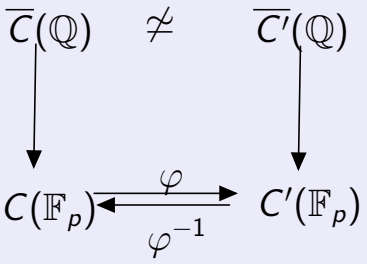


Figure: Here q is a prime and $\delta \in \mathbb{Z}$ which is a square in $\mathbb{F}_q$ but not in $\mathbb{Z}$. The figure illustrates the relations between a curve C over $\mathbb{F}_q$, a lift of C to $\mathbb{Q}$ denoted $\overline{C}$, the isogenous curve C' (which is ususally a twist C_δ) and its $\overline{C'}$ which is usually a twist $\overline{C}_\delta$ of $\overline{C}$. Here φ is an isogeny.

Solutions of the high rank twist problem for certain curves

- $g = 1$: Curve **secp256k1** has a twist of rank $r = 4$
- $g = 2$: Curve **4GLV127-BK** has a twist if rank $r = 7$

Why is it easier to find high rank twists for genus-2 curves in cryptography ?

Numerical density of rank-2 elliptic curves and genus-2 curves

Recall the definition of logarithmic density

Consider the set of genus-g curves of height $\leq X$ and rank 2. One writes $\alpha(g, X)$ for the real number such that

$$|\{(f, h) \in \mathcal{C}^{(g)}(X) \mid \operatorname{rank}(y^2 + h(x)y = f(x)) = 2\}| = |\mathcal{C}^{(g)}(X)|^{\alpha(g,X)}.$$

Data from LMFDB

$\log_2 X$	$\alpha(g = 1, X)$	$\alpha(g = 2, X)$
15	0.773	0.778
16	0.802	0.828
17	0.825	0.859
18	0.841	0.878
19	0.854	
theory	$\geq 1/2 = 0.5$	$\geq 5/7 \approx 0.71$
heuristic	$19/24 \approx 0.79$	$\geq 13/14 \approx 0.93$

There is a slight advantage for genus 2, as predicted by Theorem 1, which proves a larger logarithmic density than the heuristic value for elliptic curves (see Watkins 2014).

Numerical density of rank-2 elliptic curves and genus-2 curves

Recall the definition of logarithmic density

Consider the set of genus-g curves of height $\leq X$ and rank 2. One writes $\alpha(g, X)$ for the real number such that

$$|\{(f, h) \in \mathcal{C}^{(g)}(X) \mid \mathrm{rank}(y^2 + h(x)y = f(x)) = 2\}| = |\mathcal{C}^{(g)}(X)|^{\alpha(g,X)}.$$

Data from LMFDB

$\log_2 X$	$\alpha(g = 1, X)$	$\alpha(g = 2, X)$
15	0.773	0.778
16	0.802	0.828
17	0.825	0.859
18	0.841	0.878
19	0.854	
theory	$\geq 1/2 = 0.5$	$\geq 5/7 \approx 0.71$
heuristic	$19/24 \approx 0.79$	$\geq 13/14 \approx 0.93$

There is a slight advantage for genus 2, as predicted by Theorem 1, which proves a larger logarithmic density than the heuristic value for elliptic curves (see Watkins 2014).

A. Bartel: the genus-2 curves in cryptography are not random.

The twist problem for CM curves $y^2 = x^5 + a$

The case of elliptic curves

- The curve $y^2 = x(x-1)(x+1)$ is CM and can compute its rank faster than for a geneural elliptic curve.
- Elkies improved the computation of the rank for CM curves and obtained the best results of the hight twist problem.

Use the Hecke characters in genus 2

1. Stoll and Yang 2003: found a Hecke character η s.t. $L(C) = L(\eta)$
2. Molin and Page 2022: new algorithms and implementation of Hecke characters.

The twist problem for curves of split Jacobian

Many pairing-friendly curves have split Jacobian

Kawazoe and Takahashi 2008 proposed to use the pairing-friendly curves $y^2 = x^5 + bx$ with $b = 1$, 3 and $b = 21$.

An algorithm to solve the high rank twist problem for certain genus-2 curves

When $C : y^2 = y^5 + x$

1. we found that, $C \sim E \times E$
2. we found twists of rank 4.

Conclusion and future work

- We lower bounded the logarithmic density of genus-2 rank-2 curves.
- This gives a theoretical explanation for numerical experiments done to prepare the implementation of Regev's quantum algorithm to compute discrete logarithms on certain curves used in cryptography.
- More work is required to propose quantum circuits for Regev's algorithm in genus-2 curves.
- The choice of CM curves $y^2 = x^5 + a$ and with split Jacobian are particularly suited for Regev's quantum algorithm.