A database of genus 3 curves over $\mathbb{Q}$

Andrew V. Sutherland
MIT

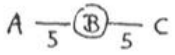
Rational Points, July 7, 2017

Joint with Raymond van Bommel, Andrew Booker, John Cremona, Tim Dokchitser, Francesc Fité, David Harvey, Kiran Kedlaya, Davide Lombardo, Elisa Lorenzo, Maike Massierer, Christian Neurohr, David Platt, Victor Rotger, Jeroen Sijsling, Michael Stoll, John Voight, Dan Yasaki (et al.)

Tables of elliptic curves over $\mathbb{Q}$ have a rich history...

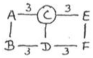
11 = 11

A	0	-1	1	0	0	-	1	I1	1	5	0
B	0	-1	1	-10	-20	-	5	I5	5	5	0
C	0	-1	1	-7820	-263580	-	1	I1	1	1	0



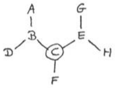
14 = 2.7

A	1	0	1	-1	0	-	2, 1	I2, I1	2, 1	6	0
B	1	0	1	-11	12	+	1, 2	I1, I2	1, 2	6	0
C	1	0	1	4	-6	-	6, 3	I6, I3	6, 3	6	0
D	1	0	1	-36	-70	+	3, 6	I3, I6	3, 6	6	0
E	1	0	1	-171	-874	-	18, 1	I18, I1	18, 1	2	0
F	1	0	1	-2731	-55146	+	9, 2	I9, I2	9, 2	2	0



15 = 3.5

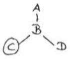
A	1	1	1	0	0	-	1, 1	I1, I1	1, 1	4	0
B	1	1	1	-5	2	+	2, 2	I2, I2	2, 2	8	0
C	1	1	1	-10	-10	+	4, 4	I4, I4	4, 4	8	0
D	1	1	1	-80	242	+	1, 1	I1, I1	1, 1	4	0
E	1	1	1	-135	-660	+	8, 2	I8, I2	8, 2	8	0
F	1	1	1	35	-28	-	2, 8	I2, I8	2, 8	4	0
G	1	1	1	-110	-880	-	16, 1	I16, I1	16, 1	2	0
H	1	1	1	-2160	-39540	+	4, 1	I4, I1	4, 1	2	0



28

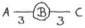
17 = 17

A	1	-1	1	-1	0	+	1	I1	1	4	0
B	1	-1	1	-6	-4	+	2	I2	2	4	0
C	1	-1	1	-1	-14	-	4	I4	4	4	0
D	1	-1	1	-91	-310	+	1	I1	1	2	0



19 = 19

A	0	1	1	1	0	-	1	I1	1	3	0
B	0	1	1	-9	-15	-	3	I3	3	3	0
C	0	1	1	-769	-8470	-	1	I1	1	1	0



20 = 2.2.5

The L-functions and modular forms database (LMFDB)

Elliptic Curve 234446.a1 (Cremona label 234446a1)

Introduction and more

Introduction · Features · Universe · Future Plans · News

L-functions

Degree: 1 2 3 4

ζ zeros

Modular Forms

GL(2): Classical · Maass · Hilbert

GL(3): Maass

Other: Siegel

Varieties

Curves: Elliptic: /Q · /NumberFields; Genus 2: /Q

Fields

Number fields: Global · Local

Representations

Characters: Dirichlet · Artin

Groups

Galois groups

Show commands for: Magma / SageMath / Pari/GP

This elliptic curve has smallest conductor amongst those of rank 4.

Minimal Weierstrass equation

$y^2 + xy = x^3 - x^2 - 79x + 289$

Mordell-Weil group structure

$\mathbb{Z}^4$

Infinite order Mordell-Weil generators and heights

P	=	$(4,3)$	$(5,-2)$	$(6,-1)$	$(8,7)$
$\hat{h}(P)$	≈	1.17647633592	1.20262600414	0.9837083405	1.51275519856

Integral points

$(-10,7)$, $(-9,19)$, $(-8,23)$, $(-7,25)$, $(-4,25)$, $(0,17)$, $(1,14)$, $(3,7)$, $(4,3)$, $(5,-2)$, $(6,-1)$, $(7,3)$, $(8,7)$, $(12,25)$, $(13,30)$, $(22,83)$, $(27,118)$, $(29,133)$, $(38,207)$, $(60,427)$, $(70,543)$, $(91,815)$, $(123,1295)$, $(129,1393)$, $(176,2239)$, $(292,4835)$, $(992,30735)$, $(1140,37907)$, $(1656,66545)$, $(4532,302803)$, $(10583,1083382)$, $(19405,2693397)$

Note: only one of each pair $\pm P$ is listed.

Invariants

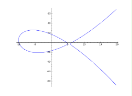
N	=	234446	=	$2 \cdot 117223$
Δ	=	468892	=	$2^2 \cdot 117223$
j	=	$\frac{54915331401}{468892}$	=	$2^{-2} \cdot 3^3 \cdot 7^3 \cdot 181^3 \cdot 117223^{-1}$
$\mathrm{End}(E)$	=	$\mathbb{Z}$		(no Complex Multiplication)
$\mathrm{ST}(E)$	=	SU(2)		

BSD invariants

r	=	4
Reg	≈	1.50434488828

Properties

Label	234446.a1



Conductor	234446
Discriminant	468892
j-invariant	$\frac{54915331401}{468892}$
CM	no
Rank	4
Torsion Structure	Trivial

Related objects

Isogeny class 234446.a
Minimal quadratic twist (itself) 234446.a1
All twists
L-function

Downloads

Download coefficients of q-expansion
Download all stored data
Download Magma code
Download Sage code
Download GP code

Learn more about

Completeness of the data
Source of the data
Elliptic Curve labels

www.lmfdb.org

A quick genus 2 update

Some (very recent) updates to the genus 2 database:

- Tamagawa numbers for 99.99 percent of curves (van Bommel).
- Proved Mordell-Weil ranks for 99 percent of curves (Stoll). Matches the analytic rank bound in each case.
- Explicit Mordell-Weil generators for 98 percent of curves (Stoll).
- Complete rational point data up to height bound 10^6.
- All rational points now known for 60 percent of the curves.
- Arithmetic conductors computed for 77 percent of the curves (Dokchitser–Doris 2017). All match analytic conductors.

We hope to add real periods and regulators in the near(ish) future.

Building a database of genus 1 curves over $\mathbb{Q}$

1. Prove modularity ✓
2. Enumerate weight 2 newforms with coefficients in $\mathbb{Z}$ by conductor ✓
3. Construct corresponding elliptic curves ✓
4. Walk the isogeny graph ✓
5. Compute L-functions ✓
6. Test BSD ✓ (well, mostly)
7. Find integer and rational points ✓ (in most cases)

Building a database of genus 2 curves over $\mathbb{Q}$

1. Prove modularity ×
2. Enumerate Siegel modular forms by conductor ×
3. Construct corresponding genus 2 curves ×
4. Walk the isogeny graph × (not yet, but some progress)
5. Compute L-functions ✓ (this is very feasible!)
6. Test BSD ✓ (this is feasible!)
7. Find integer and rational points ✓ (so is this, in many cases)

How do we organize curves if we can't enumerate them by conductor?

We need small conductors to compute L-functions.

Discriminants

Every hyperelliptic curve $X/\mathbb{Q}$ of genus g has a minimal Weierstrass model

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

with $\deg f \leq 2g+2$ and $\deg h \leq g+1$. The discriminant of X is then

$$\Delta(X) = 2^{4g}\,\mathrm{disc}_{2g+2}(f + h^2/4) \in \mathbb{Z}$$

The curve X has bad reduction at a prime p if and only if $p|\Delta(X)$.

This needn't apply to $\mathrm{Jac}(X)$, but if $p|N(\mathrm{Jac}(X)) =: N(X)$, then $p|\Delta(X)$.

In general, one expects $N(X)|\Delta(X)$; this is known for $g=2$ (Liu 1994), and for curves with a rational Weierstrass point (Srinivasan 2015).

Finding genus 2 curves of small discriminant

We searched for curves in boxes of various shapes, including

$$
\begin{aligned}
S_1(B) &= \{(f,h) : |f_i| \le B,\ h_i = 0,1\} && (\text{“flat”}) \\
S_2(a,b) &= \{(f,h) : |f_i| \le ab^{6-i},\ h_i = 0,1\} && (\text{“weighted”}) \\
S_3(b) &= \{(f,h) : |f_i| \le b^{4-|i-3|},\ h_i = 0,1\} && (\text{“crested”}) \\
S_4(b,d) &= \{(f,h) : \textstyle\sum_i \lceil \log_b(|f_i|+1) \rceil \le d,\ h_i = 0,1\} && (\text{“weird”})
\end{aligned}
$$

In the end we used

$$S_1(90) \cup S_2(2, 3.51) \cup S_3(7.14) \cup S_4(10, 10).$$

This includes more than 3×10^{17} (not necessarily minimal) equations of (not necessarily smooth) curves.

Many of these define isomorphic curves, so we also need an efficient way to reduce to isomorphism class representatives.

Monomial trees

For hyperelliptic curves of genus g, the discriminant polynomial $D(h_i, f_i)$ has $3g + 5$ (or $2g + 3$ variables for any fixed choice of h_i).

Suppose we want to evaluate a polynomial $p(x_1, \ldots, x_n)$ at every point in a box $A_1 \times \cdots \times A_n \subset \mathbb{Z}^n$. We use a monomial tree with

- nodes at level n (leaves): monomials in x_i of $p(x_1, \ldots, x_n)$.
- nodes at level $n-1$: monomials in x_i of $p(x_1, \ldots, x_{n-1}, a_n)$.
- ...
- nodes at level 1: monomials in x_1 of $p(x_1, a_2, \ldots, a_n) = p_1(x)$.

Nodes at level $m+1$ are connected to those at level m via an edge corresponding to the substitution $x_{m+1} = a_{m+1}$.

At level 1 we only need to evaluate a univariate polynomial in x_1.

For $g = 2$, with h_i fixed, $D(f_0, \ldots, f_6)$ has 246 terms and 703 nodes in its monomial tree. For $g = 3$, we have 5247 terms and 19916 nodes.

Computing 10^{17} discriminants

We enumerate values $(a_1, \ldots, a_n)$ in $A_1 \times \cdots \times A_n$ in reverse lexicographic order (so a_1 changes most frequently), updating the nodes at level i of the tree each time a_i changes.

The computation is dominated by the evaluation of at univariate polynomial along an arithmetic progression, to which very fast finite difference methods can be applied (as in Kedlaya-S 2008).

For genus 3 hyperelliptic curves the inner loop consists of 7 word size additions and takes only a few nanoseconds.

All arithmetic is performed modulo 2^{64}; provided our discriminant bound is substantially less than this, almost all discriminants that are “small" in $\mathbb{Z}/2^{64}\mathbb{Z}$ are small in $\mathbb{Z}$.

Smooth plane curves

The discriminant of a smooth plane curve $f(x, y, z) = 0$ of degree d is the resultant of the three partial derivatives f_x, f_y, f_z, with suitable powers of $p|d$ removed so that discriminants are integers and generate the unit ideal.
(divide by the GCD of the coefficients of the discriminant polynomial).

For $d = 4$ the discriminant can be computed as the determinant of a 15×15 matrix whose entries are homogeneous polynomials in 15 variables (corresponding to the 15 homogeneous monomials of degree 4).

The discriminant polynomial for $d = 4$ is a homogeneous polynomial of degree 27 in 15 variables with $50,767,957$ terms. With a suitable ordering of variables the monomial tree has $246,798,254$ nodes.

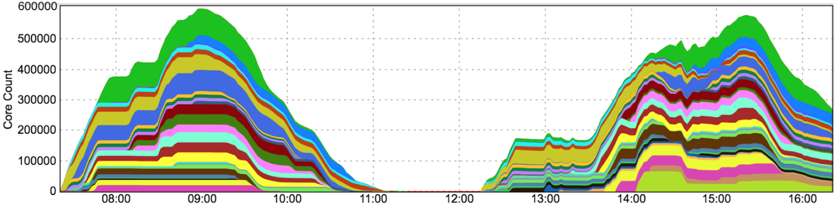
Remarkably, using a monomial tree is not only feasible, but dramatically faster than computing discriminants individually (for a big enough box).

The inner loop boils down to 10 word-size additions.

Parallel computation

The computation was parallelized by dividing boxes into sub-boxes then run on Google's Cloud Platform. We spread the load across multiple data-centers in ten geographic zones.

For the smooth plane quartic search we used a total of approximately 19,000 pre-emptible 32-core compute instances. At peak usage we had 580,000 cores running at full load (a new record).



This 300 core-year computation took about 10 hours.

The boxes we searched and what we found therein

For genus 3 hyperelliptic curves $y^2 + h(x)y = f(x)$ we used a flat box with $h_i \in \{0, 1\}$ and $|f_i| \leq 31$, approximately 3×10^{17} equations, as in genus 2.

For smooth plane quartics $f(x, y, z) = 0$ we used a flat box with $|f_i| \leq 9$, more than 10^{19} equations, but after taking advantage of the 48 symmetries the number we considered was approximately 3×10^{17}.

In both cases we used a discriminant bound of 10^7 (versus 10^6 in genus 2). We found about two million hyperelliptic and ten million non-hyperelliptic equations meeting this bound.

Among the hyperelliptic curves we found 67,879 non-isomorphic curves in (at least) 67,830 isogeny classes of Jacobians.

Among the non-hyperelliptic curves we have at least 82,011 isogeny classes of Jacobians (isomorphism testing is still in progress).

Some hyperelliptic highlights

- 65,272 conductors, including 10 below 10,000, and 6992 primes.
- Smallest conductor found is 3993 for the Jacobian of the curve:

$$y^2 + (x^4 + x^2 + 1)y = x^7 + x^6 + x^5 + x^3 + x^2 + x$$

  which is isogenous (but not isomorphic) to $X_0(33)$.

- Analytic rank bounds (conditional on Selberg class assumption):

rank	count	proportion
0	7,700	11%
1	30,840	46%
2	25,486	37%
3	3,723	5%
4	8	0%

- Rank computations for 52 curves still in progress.

A few non-hyperelliptic highlights

- Smallest conductor is 2940, for the Jacobian of the curve

$$-x^3y + x^2y^2 + 5x^2yz - x^2z^2 + 4xy^3 + 5xy^2z + xyz^2 + 4xz^3 + 2y^4 + y^2z^2 + 3z^4 = 0$$

- 7056 prime conductors, smallest of which, 8233, arising for the curve

$$x^3z - x^2y^2 + 2x^2yz - x^2z^2 - xy^3 + 2xy^2z - yz^3.$$

  This is also the conductor of the Jacobian of the hyperelliptic curve

$$y^2 + (x^4 + x^3 + x^2 + 1)y = x^7 - 8x^5 - 4x^4 + 18x^3 - 3x^2 - 16x + 8.$$

  In fact, the two Jacobians are isogenous.

- Conductor computations and isomorphism testing still in progress, rank computations to follow.

The L-function of a curve

Let X be a nice (smooth, projective, geometrically integral) curve of genus g over $\mathbb{Q}$. The L-series of X is the Dirichlet series

$$L(X,s) = L(\mathrm{Jac}(X),s) := \sum_{n\geq 1} a_n n^{-s} := \prod_p L_p(p^{-s})^{-1}.$$

For primes p of good reduction for X we have the zeta function

$$Z(X_p;s) := \exp\left(\sum_{r\geq 1} \#X(\mathbb{F}_{p^r})\frac{T^r}{r}\right) = \frac{L_p(T)}{(1-T)(1-pT)},$$

and the L-polynomial $L_p \in \mathbb{Z}[T]$ in the numerator satisfies

$$L_p(T) = T^{2g}\chi_p(1/T) = 1 - a_p T + \cdots + p^g T^{2g}$$

where $\chi_p(T)$ is the charpoly of the Frobenius endomorphism of $\mathrm{Jac}(X_p)$.

The Selberg class with polynomial Euler factors

The Selberg class S^{poly} consists of Dirichlet series $L(s) = \sum_{n\geq 1} a_n n^{-s}$:

1. $L(s)$ has an analytic continuation that is holomorphic at $s \neq 1$;
2. For some $\gamma(s) = Q^s \prod_{i=1}^r \Gamma(\lambda_i s + \mu_i)$ and ε, the completed L-function $\Lambda(s) := \gamma(s)L(s)$ satisfies the functional equation

$$\Lambda(s) = \varepsilon\overline{\Lambda(1-\bar{s})},$$

   where $Q > 0$, $\lambda_i > 0$, $\mathrm{Re}(\mu_i) \geq 0$, $|\varepsilon| = 1$. Define $\deg L := 2\sum_i^r \lambda_i$.
3. $a_1 = 1$ and $a_n = O(n^\varepsilon)$ for all $\varepsilon > 0$ (Ramanujan conjecture).
4. $L(s) = \prod_p L_p(p^{-s})^{-1}$ for some $L_p \in \mathbb{Z}[T]$ with $\deg L_p \leq \deg L$ (has an Euler product).

The Dirichlet series $L_{\text{an}}(s, X) := L(X, s + \frac{1}{2})$ satisfies (3) and (4), and conjecturally lies in S^{poly}; for $g = 1$ this is known (via modularity).

Strong multiplicity one

Theorem (Kaczorowski-Perelli 2001)

If $A(s) = \sum_{n\geq 1} a_n n^{-s}$ and $B(s) = \sum_{n\geq 1} b_n n^{-s}$ lie in S^{poly} and $a_p = b_p$ for all but finitely many primes p, then $A(s) = B(s)$.

Corollary

If $L_{\mathrm{an}}(s, X)$ lies in S^{poly} then it is completely determined by (any choice of) all but finitely many coefficients a_p.

Henceforth we assume that $L_{\mathrm{an}}(s, X) \in S^{\mathrm{poly}}$.

Let $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^s\Gamma(s)$ and define $\Lambda(X, s) := \Gamma_{\mathbb{C}}(s)^g L(X, s)$. Then

$$\Lambda(X, s) = \varepsilon N^{1-s}\Lambda(X, 2 - s).$$

where the analytic root number $\varepsilon = \pm 1$ and the analytic conductor $N \in \mathbb{Z}_{\geq 1}$ are determined by the a_p values (take these as definitions).

Testing the functional equation

Let $G(x)$ be the inverse Mellin transform of $\Gamma_{\mathbb{C}}(s)^g = \int_0^\infty G(x)x^{s-1}dx$, and define

$$S(x) := \frac{1}{x}\sum a_n G(n/x),$$

so that $\Lambda(X,s) = \int_0^\infty S(x)x^{-s}dx$, and for all $x > 0$ we have

$$S(x) = \varepsilon S(N/x).$$

The function $G(x)$ decays rapidly, and for sufficiently large c_0 we have

$$S(x) \approx S_0(x) := \frac{1}{x}\sum_{n\le c_0 x} a_n G(n/x),$$

with an explicit bound on the error $|S(x) - S_0(x)|$.

Effective strong multiplicity one

Fix a finite set of small primes $\mathcal{S}$ (e.g. $\mathcal{S} = \{2\}$) and an integer M that we know is a multiple of the conductor N (e.g. $M = \Delta(X)$).

There is a finite set of possibilities for $\varepsilon = \pm 1$, $N|M$, and the Euler factors $L_p \in \mathbb{Z}[T]$ for $p \in \mathcal{S}$ (the coefficients of $L_p(T)$ are bounded).

Suppose we can compute a_n for $n \leq c_1\sqrt{M}$ whenever $p \nmid n$ for $p \in \mathcal{S}$.

We now compute $\delta(x) := |S_0(x) - \varepsilon S_0(N/x)|$ with $x = c_1\sqrt{N}$) for every possible choice of ε, N, and $L_p(T)$ for $p \in \mathcal{S}$. If all but one choice makes $\delta(x)$ larger than our explicit error bound, we know the correct choice.

For a suitable choice of c_1 this is guaranteed to happen.[1] One can explicitly determine a set of $O(N^\varepsilon)$ candidate values of c_1, one of which is guaranteed to work; in practice the first one usually works.

[1] Subject to our assumptions; if it does not happen then we have found an explicit counterexample to the conjectured Langlands correspondence.

Algorithms to compute zeta functions

Given $X/\mathbb{Q}$ of genus g, we want to compute $L_p(T)$ for all good $p \le B$.

	complexity per prime (ignoring factors of $O(\log\log p)$)		
algorithm	$g = 1$	$g = 2$	$g = 3$
point enumeration	$p \log p$	$p^2 \log p$	$p^3 (\log p)^2$
group computation	$p^{1/4} \log p$	$p^{3/4} \log p$	$p (\log p)^2$
p-adic cohomology	$p^{1/2} (\log p)^2$	$p^{1/2} (\log p)^2$	$p^{1/2} (\log p)^2$
CRT (Schoof-Pila)	$(\log p)^5$	$(\log p)^8$	$(\log p)^{12?}$
average poly-time	$(\log p)^4$	$(\log p)^4$	$(\log p)^4$

For $L(X, s) = \sum a_n n^{-s}$, we only need a_{p^2} for $p^2 \le B$, and a_{p^3} for $p^3 \le B$. For $1 < r \le g$ we can compute all a_{p^r} with $p^r \le B$ in time $O(B \log B)$.

The bottom line: it boils down to efficiently computing lots of a_p's.

Genus 3 curves

The canonical embedding of a genus 3 curve into $\mathbb{P}^2$ is either

1. a degree-2 cover of a smooth conic (hyperelliptic case)
   - conic has a rational point (rationally hyperelliptic);
   - conic has no rational points (only geometrically hyperelliptic).
2. a smooth plane quartic (generic case).

Average polynomial-time implementations are available for the first case:

- rational hyperelliptic model [Harvey-S 2014];
- no rational hyperelliptic model [Harvey-Massierer-S 2016].

And now for the second case as well:

- smooth plane quartics [Harvey-S 2017].

Prior work has all been based on p-adic cohomology:

[Lauder 2004], [Castryck-Denef-Vercauteren 2006], [Abott-Kedlaya-Roe 2006], [Harvey 2010], [Tuitman-Pancrantz 2013], [Tuitman 2015], [Costa 2015], [Tuitman-Castryck 2016], [Shieh 2016]

Cumulative timings for genus 3 curves

Time to compute $L_p(T) \bmod p$ for all good $p \leq B$.

B	spq-Costa-AKR	spq-HS	ghyp-MHS	hyp-HS	hyp-Harvey
2^{12}	18	1.4	0.3	0.1	1.3
2^{13}	49	2.4	0.7	0.2	2.6
2^{14}	142	4.6	1.7	0.5	5.4
2^{15}	475	9.4	4.6	1.0	12
2^{16}	1,670	21	11	2.1	29
2^{17}	5,880	47	27	5.3	74
2^{18}	22,300	112	62	14	192
2^{19}	78,100	241	153	37	532
2^{20}	297,000	551	370	97	1,480
2^{21}	1,130,000	1,240	891	244	4,170
2^{22}	4,280,000	2,980	2,190	617	12,200
2^{23}	16,800,000	6,330	5,110	1,500	36,800
2^{24}	66,800,000	14,200	11,750	3,520	113,000
2^{25}	244,000,000	31,900	28,200	8,220	395,000
2^{26}	972,000,000	83,300	62,700	19,700	1,060,000

(Intel Xeon E7-8867v3 3.3 GHz CPU seconds).

Computing endomorphism rings and algebras

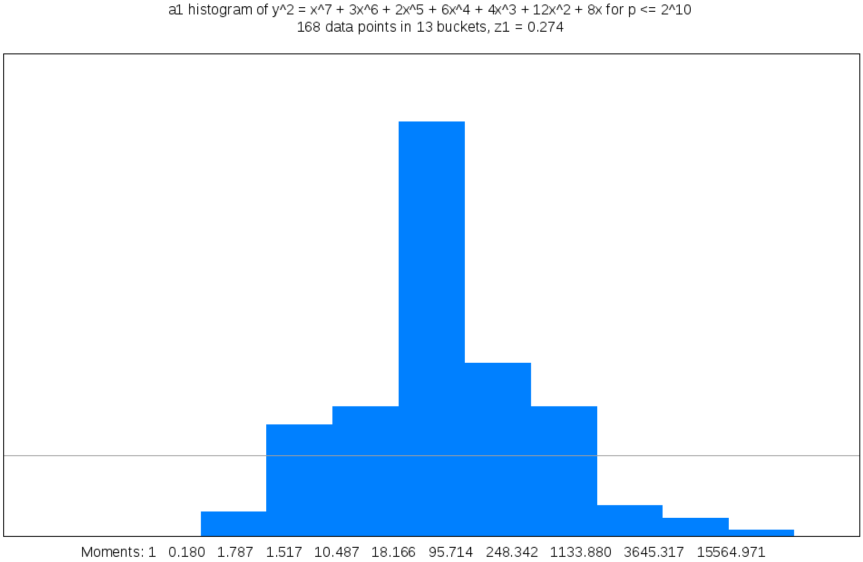
Given a curve $X/\mathbb{Q}$ one can explicitly compute $\mathrm{End}(\mathrm{Jac}(X)_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$, $\mathrm{End}(\mathrm{Jac}(X)_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$, and even the endomorphism ring $\mathrm{End}(\mathrm{Jac}(X))$:

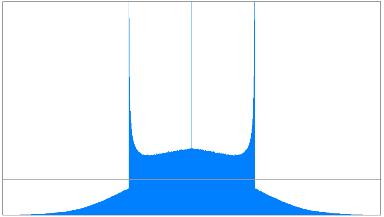
- Choose a symplectic basis $\gamma_1, \ldots, \gamma_{2g}$ of $H_1(X, \mathbb{Z})$ and a basis $\omega_1, \ldots, \omega_g$ of $H^0(X, \omega_X)$ over $\mathbb{Q}$;
- Realize $\mathrm{Jac}(X)(\mathbb{C})$ as a complex torus $\mathbb{C}^g/\Lambda$ by computing the period matrix $\Pi = (\int_{\gamma_j} \omega_i)_{i,j}$;
- Use LLL to determine a basis of the $\mathbb{Z}$-module of matrices $R \in M_{2g}(\mathbb{Z})$ such that $\Lambda R = R$;
- Determine the matrices $M \in M_2(\overline{\mathbb{Q}})$ in the equality $M\Pi = \Pi R$ to obtain the representation of $\mathrm{End}(\mathrm{Jac}(X)_{\overline{\mathbb{Q}}})$ on the tangent space at 0 of $\mathrm{Jac}(X)_{\overline{\mathbb{Q}}}$.

This can be made entirely rigorous (Costa-Mascot-Sijsling-Voight 2017).

Real endomorphism algebras of abelian threefolds

abelian threefold	**End$(A_K)_{\mathbb{R}}$**	**ST$(A)^0$**
cube of a CM elliptic curve	$\mathrm{M}_3(\mathbb{C})$	$\mathrm{U}(1)_3$
cube of a non-CM elliptic curve	$\mathrm{M}_3(\mathbb{R})$	$\mathrm{SU}(2)_3$
product of CM elliptic curve and square of CM elliptic curve	$\mathbb{C} \times \mathrm{M}_2(\mathbb{C})$	$\mathrm{U}(1) \times \mathrm{U}(1)_2$
• product of CM elliptic curve and QM abelian surface • product of CM elliptic curve and square of non-CM elliptic curve	$\mathbb{C} \times \mathrm{M}_2(\mathbb{R})$	$\mathrm{U}(1) \times \mathrm{SU}(2)_2$
product of non-CM elliptic curve and square of CM elliptic curve	$\mathbb{R} \times \mathrm{M}_2(\mathbb{C})$	$\mathrm{SU}(2) \times \mathrm{U}(1)_2$
• product of non-CM elliptic curve and QM abelian surface • product of non-CM elliptic curve and square of non-CM elliptic curve	$\mathbb{R} \times \mathrm{M}_2(\mathbb{R})$	$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$
• CM abelian threefold • product of CM elliptic curve and CM abelian surface • product of three CM elliptic curves	$\mathbb{C} \times \mathbb{C} \times \mathbb{C}$	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$
• product of non-CM elliptic curve and CM abelian surface • product of non-CM elliptic curve and two CM elliptic curves	$\mathbb{C} \times \mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{SU}(2)$
• product of CM elliptic curve and RM abelian surface • product of CM elliptic curve and two non-CM elliptic curves	$\mathbb{C} \times \mathbb{R} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$
• RM abelian threefold • product of non-CM elliptic curve and RM abelian surface • product of 3 non-CM elliptic curves	$\mathbb{R} \times \mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$
product of CM elliptic curve and abelian surface	$\mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{USp}(4)$
product of non-CM elliptic curve and abelian surface	$\mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{USp}(4)$
quadratic CM abelian threefold	$\mathbb{C}$	$\mathrm{U}(3)$
generic abelian threefold	$\mathbb{R}$	$\mathrm{USp}(6)$


a1 histogram of y^2 = x^7 + 3x^6 + 2x^5 + 6x^4 + 4x^3 + 12x^2 + 8x for p <= 2^10
168 data points in 13 buckets, z1 = 0.274
Moments: 1 0.180 1.787 1.517 10.487 18.166 95.714 248.342 1133.880 3645.317 15564.971



Thank you!