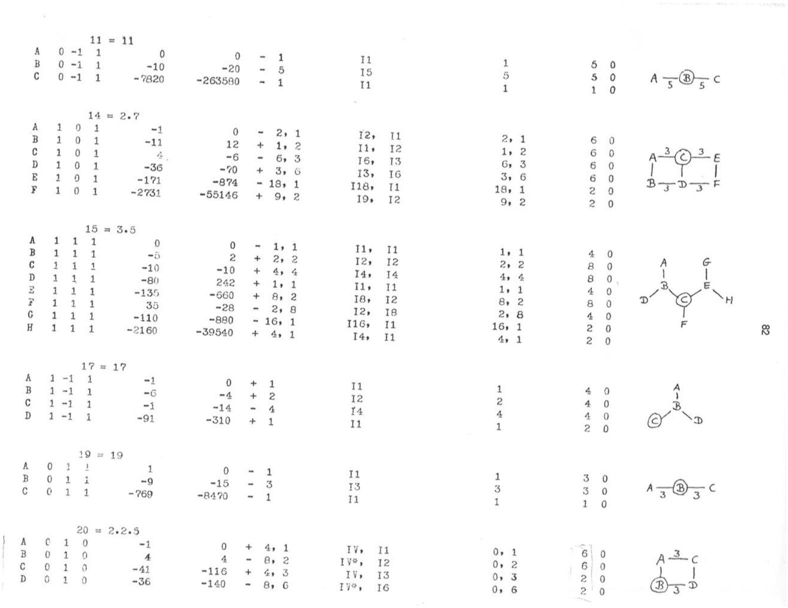
A database of genus 3 curves over $\mathbb{Q}$

Andrew V. Sutherland
MIT

May 17, 2018

Joint with Raymond van Bommel, Andrew Booker, Edgar Costa, John Cremona, Tim Dokchitser, Francesc Fité, David Harvey, Kiran Kedlaya, Davide Lombardo, Elisa Lorenzo, 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...


A
B
C
5
5
A
B
C
D
E
F
3
3
3
3
A
B
C
D
E
F
G
H
A
B
C
D
A
B
C
3
3
A
B
C
D
3
3

		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
		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									
A	C	1	0	-1	0	+	4, 1	IV, I1	0, 1	6	0
B	0	1	0	4	4	-	8, 2	IV*, I2	0, 2	6	0
C	0	1	0	-41	-116	+	4, 3	IV, I3	0, 3	2	0
D	0	1	0	-36	-140	-	8, 6	IV*, I6	0, 6	2	0

82

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

1. Prove modularity ✓
2. Enumerate rational weight 2 newforms 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 practice, if not in theory)
8. Compute endomorphism rings and Sato-Tate groups ✓ (trivial)
9. Images of Galois representations ✓ (mod-ℓ and mod-2^∞)

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

1. Prove modularity ×
2. Enumerate rational degree 2 Siegel modular forms by conductor ×
3. Construct corresponding genus 2 curves ×
4. Walk the isogeny graph $\times^*$ (some progress)
5. Compute L-functions $\checkmark^*$ (this is very feasible!)
6. Test BSD $\checkmark^*$ (this is feasible!)
7. Find integer and rational points $\checkmark^*$ (feasible in many cases)
8. Compute endomorphism rings and Sato-Tate groups ✓ (rigorous)
9. Compute images of Galois representations $\times^*$ (some progress)

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

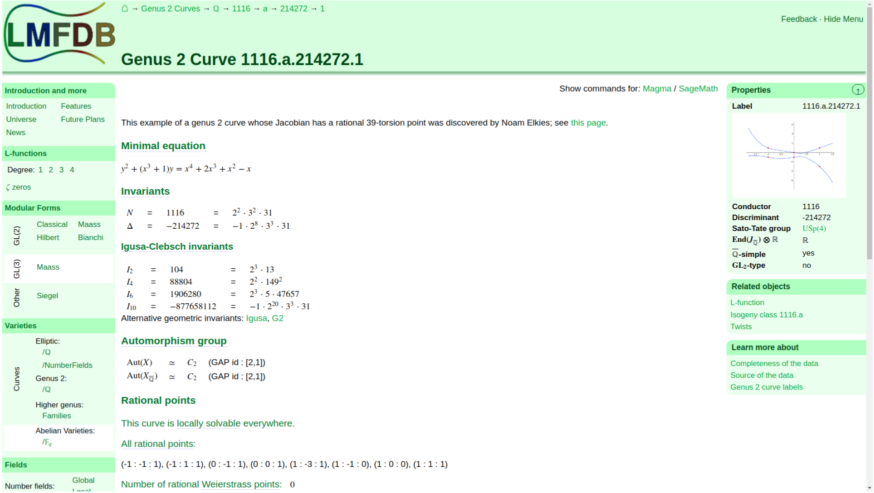
$$\Delta(X) = 2^{4g}\,\mathrm{disc}_{2g+2}(f + h^2/4) \in \mathbb{Z}$$

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).

The L-functions and modular forms database (LMFDB)



Genus 2 Curve 1116.a.214272.1

This example of a genus 2 curve whose Jacobian has a rational 39-torsion point was discovered by Noam Elkies; see this page.

Minimal equation

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

Invariants

$$\begin{array}{lllll} N & = & 1116 & = & 2^2 \cdot 3^2 \cdot 31 \\ \Delta & = & -214272 & = & -1 \cdot 2^8 \cdot 3^3 \cdot 31 \end{array}$$

Igusa-Clebsch invariants

$$\begin{array}{lllll} I_2 & = & 104 & = & 2^3 \cdot 13 \\ I_4 & = & 88804 & = & 2^2 \cdot 149^2 \\ I_6 & = & 1906280 & = & 2^3 \cdot 5 \cdot 47657 \\ I_{10} & = & -877658112 & = & -1 \cdot 2^{20} \cdot 3^3 \cdot 31 \end{array}$$

Alternative geometric invariants: Igusa, G2

Automorphism group

$$\begin{array}{lll} \mathrm{Aut}(X) & \simeq & C_2 \\ \mathrm{Aut}(X_{\overline{\mathbb{Q}}}) & \simeq & C_2 \end{array}$$

(GAP id : [2,1])
(GAP id : [2,1])

Rational points

This curve is locally solvable everywhere.

All rational points:

(-1 : -1 : 1), (-1 : 1 : 1), (0 : -1 : 1), (0 : 0 : 1), (1 : -3 : 1), (1 : -1 : 0), (1 : 0 : 0), (1 : 1 : 1)

Number of rational Weierstrass points: 0

Properties

Label	1116.a.214272.1
Conductor	1116
Discriminant	-214272
Sato-Tate group	$\mathrm{USp}(4)$
$\mathrm{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$	$\mathbb{R}$
$\overline{\mathbb{Q}}$**-simple**	yes
GL_2**-type**	no

Related objects

L-function
Isogeny class 1116.a
Twists

Learn more about

Completeness of the data
Source of the data
Genus 2 curve labels

www.lmfdb.org

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.

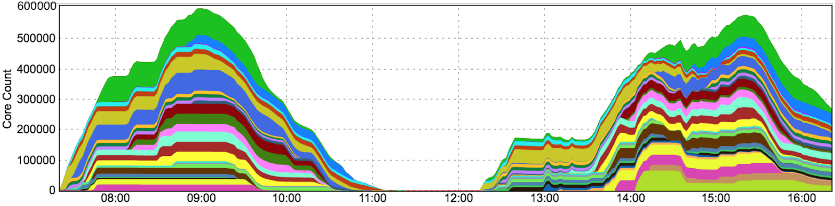
Remarkably, using a monomial tree is not only feasible, but dramatically faster than computing discriminants individually (for a big enough box).

The inner loop boils down to ten 64-bit word operations (22 clock cycles).

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 found 82,240 non-isomorphic curves in (at least) 82,011 isogeny classes of Jacobians.

Isomorphism testing

From a practical perspective, isomorphism testing of curves over number fields is an unsolved problem (even for smooth plane quartics over $\mathbb{Q}$).

Some open problems in this area:

- Practical isomorphism testing with *certifiable* results.
  (This is non-trivial even over finite fields).
- Exhibit non-isomorphic genus g curves X_1, X_2 over $\mathbb{Q}$ with isomorphic reductions at all good primes. For which g is this possible?
- Let $S(g, K)$ be the set of genus g curves over a number field K.
  Give an effectively computable map $\varphi\colon S \to \{0,1\}^*$ such that:
  1. $\varphi(X_1) = \varphi(X_2)$ if and only if $X_1 \simeq X_2$ (over K);
  2. $|\varphi(X)| = \widetilde{O}(|X|)$.

  Such a φ would have many other applications.

A few 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
$$\Lambda(s) = \varepsilon \overline{\Lambda(1 - \overline{s})},$$
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 $L_{\mathrm{an}}(s, X) := L(X, s + \frac{1}{2})$ 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). This theorem can be made completely effective with $p = O(N^{1/2+\varepsilon})$.

Algorithms to compute zeta functions

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

	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 $p^2 \leq B$, and a_{p^3} for $p^3 \leq B$.
For $1 < r \leq g$ we can compute all a_{p^r} with $p^r \leq B$ 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 $L_p(T)$ mod 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 $\mathrm{End}(\mathrm{Jac}(X))$:

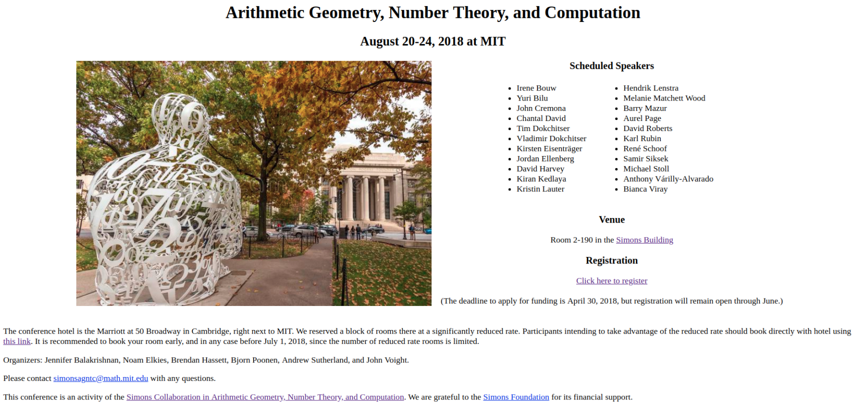
- Choose a symplectic basis $\gamma_1, \ldots, \gamma_{2g}$ of $H_1(X, \mathbb{Z})$ and a basis $\omega_1, \ldots, \omega_g$ of $H^0(X, \omega_X)$ over $\mathbb{Q}$;
- Realize $\mathrm{Jac}(X)(\mathbb{C})$ as a complex torus $\mathbb{C}^g/\Lambda$ by computing the period matrix $\Pi = (\int_{\gamma_j} \omega_i)_{i,j}$;
- 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	$\mathbf{End}(A_K)_{\mathbb{R}}$	$\mathbf{ST}(A)^0$
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	$\mathbb{R}$	$\mathrm{USp}(6)$

An invitation



Arithmetic Geometry, Number Theory, and Computation

August 20-24, 2018 at MIT

Scheduled Speakers

- Irene Bouw
- Yuri Bilu
- John Cremona
- Chantal David
- Tim Dokchitser
- Vladimir Dokchitser
- Kirsten Eisenträger
- Jordan Ellenberg
- David Harvey
- Kiran Kedlaya
- Kristin Lauter
- Hendrik Lenstra
- Melanie Matchett Wood
- Barry Mazur
- Aurel Page
- David Roberts
- Karl Rubin
- René Schoof
- Samir Siksek
- Michael Stoll
- Anthony Várilly-Alvarado
- Bianca Viray

Venue

Room 2-190 in the Simons Building

Registration

Click here to register

(The deadline to apply for funding is April 30, 2018, but registration will remain open through June.)

The conference hotel is the Marriott at 50 Broadway in Cambridge, right next to MIT. We reserved a block of rooms there at a significantly reduced rate. Participants intending to take advantage of the reduced rate should book directly with hotel using this link. It is recommended to book your room early, and in any case before July 1, 2018, since the number of reduced rate rooms is limited.

Organizers: Jennifer Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Andrew Sutherland, and John Voight.

Please contact simonsagntc@math.mit.edu with any questions.

This conference is an activity of the Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation. We are grateful to the Simons Foundation for its financial support.

`http://math.mit.edu/~drew/2018Conference.html`