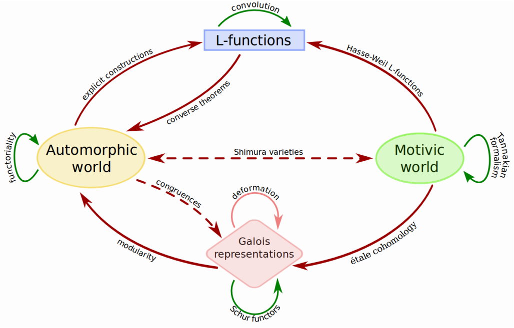
Completely decomposable modular Jacobians

Andrew V. Sutherland

Massachusetts Institute of Technology



(joint work with Jennifer Paulhus, Mount Holyoke College)

A question of Ekedahl and Serre

Definition

An abelian variety is completely decomposable if it is isogenous to a product of (not necessarily distinct) elliptic curves.

Silly question: Which abelian varieties are completely decomposable?

A question of Ekedahl and Serre

Definition

An abelian variety is completely decomposable if it is isogenous to a product of (not necessarily distinct) elliptic curves.

Silly question: Which abelian varieties are completely decomposable?
Silly answer: Products of elliptic curves.

Better question: Which Jacobians are completely decomposable?

A question of Ekedahl and Serre

Definition

An abelian variety is completely decomposable if it is isogenous to a product of (not necessarily distinct) elliptic curves.

Silly question: Which abelian varieties are completely decomposable?
Silly answer: Products of elliptic curves.

Better question: Which Jacobians are completely decomposable?

More precisely, Ekedahl and Serre asked whether there are completely decomposable Jacobians (over $\mathbb{C}$) of every genus g, and if not, for which g does this hold?

A question of Ekedahl and Serre

Definition

An abelian variety is completely decomposable if it is isogenous to a product of (not necessarily distinct) elliptic curves.

Silly question: Which abelian varieties are completely decomposable?
Silly answer: Products of elliptic curves.

Better question: Which Jacobians are completely decomposable?

More precisely, Ekedahl and Serre asked whether there are completely decomposable Jacobians (over $\mathbb{C}$) of every genus g, and if not, for which g does this hold?

This question remains open, but Ekedahl and Serre gave a list of g for which they could exhibit a completely decomposable Jacobian, most of which involved modular curves. This list has been extended by Paulhus–Rojas, Rojas–Rodriguez, and Yamauchi.

Completely decomposable modular Jacobians

Yamauchi determined (modulo corrections noted by Elkies–Howe–Ritzenthaler) the integers N for which $J_0(N)$ is completely decomposable, which examples of genus

$$0 - 11, 13, 17, 19, 21, 25, 29, 33, 37, 43, 49, 53, 55, 57, 61, 73, 97, 121, 161, 205.$$

with $N = 1, 2, 3, \ldots, 1152, 1200$ (all completely decomposable over $\mathbb{Q}$, not just $\mathbb{C}$).

The (beta version of the) LMFDB contains the isogeny decomposition of J_H for all open $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\det(H) = \widehat{\mathbb{Z}}^\times$ of level up to 70, many of which are completely decomposable. Some have genera not previously known to arise (even over $\mathbb{C}$).

Jen suggested we should look for more examples beyond level 70.

Completely decomposable modular Jacobians

Yamauchi determined (modulo corrections noted by Elkies–Howe–Ritzenthaler) the integers N for which $J_0(N)$ is completely decomposable, which examples of genus

$$0-11, 13, 17, 19, 21, 25, 29, 33, 37, 43, 49, 53, 55, 57, 61, 73, 97, 121, 161, 205.$$

with $N = 1, 2, 3, \ldots, 1152, 1200$ (all completely decomposable over $\mathbb{Q}$, not just $\mathbb{C}$).

The (beta version of the) LMFDB contains the isogeny decomposition of J_H for all open $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\det(H) = \widehat{\mathbb{Z}}^\times$ of level up to 70, many of which are completely decomposable. Some have genera not previously known to arise (even over $\mathbb{C}$).

Jen suggested we should look for more examples beyond level 70.
We did, checking all $N \leq 239$, and we found several new examples!

Results

Here is an updated list of the integers g for which there exists a genus g curve $X/\mathbb{C}$ whose Jacobian is completely decomposable:

0–37, **38**, 39–55, 57–58, 61–65, 67, **68**, 69, 71–73, **75–78**, 79–82, 85, 89, 91, 93, 95, 97, 101, 103, 105–107, 109, **113**, 118, 121, 125, 129, **135**, **137**, 142, 145, 154, **157**, **159**, 161, 163, **169**, 193, 199, 205, 211, 213, 217, 244, 257, 325, **409**, 433, 649, 1297.

The 13 numbers in bold are the new values of g that we found, each of which is realized by a modular curve over $\mathbb{Q}$ whose Jacobian completely decomposes over $\mathbb{Q}$.

The smallest g for which no example is known is now 56 (it was 38).

g	LMFDB label	g	LMFDB label	g	LMFDB label	g	LMFDB label
0	1.1.0.a.1	*21*	20.360.21.a.1	45	60.640.45.a.1	85	20.1440.85.b.1
1	6.6.1.a.1	22	20.360.22.a.1	*49*	30.720.49.a.1	89	120.1152.89.?.1
2	10.30.2.a.1	23	30.360.23.a.1	50	120.640.50.?.1	*97*	60.1440.97.y.1
3	7.168.3.a.1	24	24.384.24.a.1	51	60.720.51.u.1	103	60.1440.103.a.1
4	10.90.4.a.1	*25*	24.384.25.a.1	52	60.720.52.i.1	105	60.1440.105.g.1
5	10.120.5.a.1	26	11.660.26.c.1	*53*	60.720.53.a.1	109	60.1440.109.a.1
6	10.180.6.b.1	27	20.480.27.a.1	*55*	36.864.55.a.1	**113**	120.1440.113.?.1
7	10.180.7.a.1	28	18.486.28.a.1	*57*	60.864.57.a.1	*121*	60.1728.121.a.1
8	11.220.8.a.1	*29*	20.480.29.a.1	*61*	60.864.61.c.1	129	120.1728.129.?.1
9	15.240.9.c.1	31	28.576.31.b.1	65	60.960.65.m.1	**135**	60.1920.135.a.1
10	15.180.10.a.1	32	30.540.32.a.1	**68**	60.960.68.a.1	**137**	60.1920.137.a.1
11	24.192.11.i.1	*33*	24.576.33.a.1	69	60.960.69.c.1	**157**	60.2160.157.a.1
12	11.330.12.a.1	34	30.540.34.a.1	72	60.960.72.a.1	**159**	60.2160.159.gu.1
13	10.360.13.b.1	35	60.480.35.a.1	*73*	24.1152.73.a.1	*161*	48.2304.161.cax.1
14	30.240.14.a.1	36	30.540.36.a.1	**75**	60.1080.75.gu.1	163	60.2160.163.c.1
15	20.240.15.a.1	*37*	20.720.37.i.1	**76**	60.1080.76.dc.1	**169**	120.2160.169.?.1
16	28.288.16.q.1	**38**	60.540.38.y.1	**77**	60.1080.77.ge.1	193	60.2880.193.dw.1
17	20.360.17.e.1	39	60.540.39.e.1	**78**	60.1080.78.a.1	*205*	60.2880.205.a.1
18	60.240.18.m.1	40	60.540.40.a.1	79	60.1080.79.bg.1	217	60.2880.217.c.1
19	18.324.19.c.1	41	20.720.41.i.1	81	48.1152.81.id.1	325	60.4320.325.a.1
20	20.360.20.a.1	*43*	20.720.43.a.1	82	60.1080.82.a.1	**409**	60.5760.409.c.1

Table: Minimal modular curves of level $N < 240$ with completely decomposable Jacobians.

How we searched for completely decomposable modular Jacobians

The elliptic curves that can arise as isogeny factors of a modular Jacobian of level N necessarily have conductor dividing N^2. For $N \leq 707$ these are all in the LMFDB.

How we searched for completely decomposable modular Jacobians

The elliptic curves that can arise as isogeny factors of a modular Jacobian of level N necessarily have conductor dividing N^2. For $N \leq 707$ these are all in the LMFDB.

Let $E_1, \ldots, E_n$ be isogeny class representatives of the elliptic curves of conductor dividing N^2. Let $p_1, \ldots, p_n \nmid N$ be primes for which the matrix $A = [a_{p_i}(E_j)]_{ij}$ has full rank. Compute the inverse matrix $A^{-1} \in \mathbb{Q}^{n \times n}$, which we note depends only on N.

How we searched for completely decomposable modular Jacobians

The elliptic curves that can arise as isogeny factors of a modular Jacobian of level N necessarily have conductor dividing N^2. For $N \leq 707$ these are all in the LMFDB.

Let $E_1, \ldots, E_n$ be isogeny class representatives of the elliptic curves of conductor dividing N^2. Let $p_1, \ldots, p_n \nmid N$ be primes for which the matrix $A = [a_{p_i}(E_j)]_{ij}$ has full rank. Compute the inverse matrix $A^{-1} \in \mathbb{Q}^{n \times n}$, which we note depends only on N.

For each X_H of level N we use the point-counting algorithm of [RSZB22] to compute

$$v(H) := \left(a_{p_1}(J_H), \ldots, a_{p_n}(J_H)\right)$$

If $J_H \sim \prod E_i^{e_i}$ is completely decomposable, then $(e_1, \ldots, e_n) \cdot A = v(H)$, and $v(H)A^{-1}$ must have nonnegative integer entries that sum to $g(X_H)$.

How we searched for completely decomposable modular Jacobians

The elliptic curves that can arise as isogeny factors of a modular Jacobian of level N necessarily have conductor dividing N^2. For $N \leq 707$ these are all in the LMFDB.

Let $E_1, \ldots, E_n$ be isogeny class representatives of the elliptic curves of conductor dividing N^2. Let $p_1, \ldots, p_n \nmid N$ be primes for which the matrix $A = [a_{p_i}(E_j)]_{ij}$ has full rank. Compute the inverse matrix $A^{-1} \in \mathbb{Q}^{n \times n}$, which we note depends only on N.

For each X_H of level N we use the point-counting algorithm of [RSZB22] to compute

$$v(H) := \left(a_{p_1}(J_H), \ldots, a_{p_n}(J_H)\right)$$

If $J_H \sim \prod E_i^{e_i}$ is completely decomposable, then $(e_1, \ldots, e_n) \cdot A = v(H)$, and $v(H)A^{-1}$ must have nonnegative integer entries that sum to $g(X_H)$.

The converse is not necessarily true, so proving that J_H is completely decomposable requires an additional step, but we are happy to skip this step while we search.

How we searched for completely decomposable modular Jacobians

For any open $K \leq H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, if J_H is not completely decomposable, neither is J_K.

This allows us to search for completely decomposable modular Jacobians of level N by enumerating the subgroup lattice of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ from the top down by computing maximal subgroups (restricting to H with $\det(H) = \widehat{\mathbb{Z}}^\times$) and not pursuing any branch for which J_H is not completely decomposable (which we test by computing $v(H)A^{-1}$).

How we searched for completely decomposable modular Jacobians

For any open $K \leq H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, if J_H is not completely decomposable, neither is J_K.

This allows us to search for completely decomposable modular Jacobians of level N by enumerating the subgroup lattice of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ from the top down by computing maximal subgroups (restricting to H with $\det(H) = \widehat{\mathbb{Z}}^\times$) and not pursuing any branch for which J_H is not completely decomposable (which we test by computing $v(H)A^{-1}$).

We performed this search for all $N < 240$ over a weekend (using 256 cores), and found 561,077 distinct examples, including examples in 13 new genera which we verified using a larger A with rows for *every* modular form in $S_2(\Gamma_0(N^2) \cap \Gamma_1(N))$.

How we searched for completely decomposable modular Jacobians

For any open $K \leq H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, if J_H is not completely decomposable, neither is J_K.

This allows us to search for completely decomposable modular Jacobians of level N by enumerating the subgroup lattice of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ from the top down by computing maximal subgroups (restricting to H with $\det(H) = \widehat{\mathbb{Z}}^\times$) and not pursuing any branch for which J_H is not completely decomposable (which we test by computing $v(H)A^{-1}$).

We performed this search for all $N < 240$ over a weekend (using 256 cores), and found 561,077 distinct examples, including examples in 13 new genera which we verified using a larger A with rows for *every* modular form in $S_2(\Gamma_0(N^2) \cap \Gamma_1(N))$.

Every quotient of a completely decomposable Jacobian is completely decomposable, so you might be able to obtain new genera as quotients of one of the completely decomposable X_H that we found. You can download all 561,077 H from

https://github.com/AndrewVSutherland/CompletelyDecomposableModularJacobians