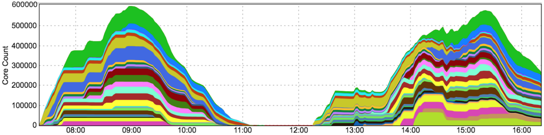
A database of nonhyperelliptic genus 3 curves over $\mathbb{Q}$

Andrew V. Sutherland[1]

Massachusetts Institute of Technology

ANTS XIII — July 18, 2018



[1] Supported by NSF grant DMS-1522526 and Simons Foundation grant 550033.

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

1. Prove modularity

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

1. Prove modularity ✓
2. Enumerate rational weight 2 newforms by conductor

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

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. Enumerate isogeny class

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. Enumerate isogeny class ✓
5. Compute L-functions

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

1. Prove modularity $\checkmark$
2. Enumerate rational weight 2 newforms by conductor $\checkmark$
3. Construct corresponding elliptic curves $\checkmark$
4. Enumerate isogeny class $\checkmark$
5. Compute L-functions $\checkmark$
6. Compute BSD invariants

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. Enumerate isogeny class ✓
5. Compute L-functions ✓
6. Compute BSD invariants ✓* (all but one of them)
7. Find integer and rational points

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. Enumerate isogeny class ✓
5. Compute L-functions ✓
6. Compute BSD invariants ✓* (all but one of them)
7. Find integer and rational points ✓* (in practice, if not in theory)
8. Compute endomorphism rings and Sato-Tate groups

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

1. Prove modularity $\checkmark$
2. Enumerate rational weight 2 newforms by conductor $\checkmark$
3. Construct corresponding elliptic curves $\checkmark$
4. Enumerate isogeny class $\checkmark$
5. Compute L-functions $\checkmark$
6. Compute BSD invariants $\checkmark^*$ (all but one of them)
7. Find integer and rational points $\checkmark^*$ (in practice, if not in theory)
8. Compute endomorphism rings and Sato-Tate groups $\checkmark$ (trivial)
9. Images of Galois representations

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

1. Prove modularity $\checkmark$
2. Enumerate rational weight 2 newforms by conductor $\checkmark$
3. Construct corresponding elliptic curves $\checkmark$
4. Enumerate isogeny class $\checkmark$
5. Compute L-functions $\checkmark$
6. Compute BSD invariants $\checkmark^*$ (all but one of them)
7. Find integer and rational points $\checkmark^*$ (in practice, if not in theory)
8. Compute endomorphism rings and Sato-Tate groups $\checkmark$ (trivial)
9. Images of Galois representations $\checkmark^*$ (mod-ℓ and mod-2^∞)

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

1. Prove modularity

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

1. Prove modularity ×

2. Enumerate rational weight 2 Siegel modular forms by conductor

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

1. Prove modularity ×
2. Enumerate rational weight 2 Siegel modular forms by conductor ×
3. Construct corresponding genus 2 curves

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

1. Prove modularity ×
2. Enumerate rational weight 2 Siegel modular forms by conductor ×
3. Construct corresponding genus 2 curves ×
4. Enumerate isogeny class

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

1. Prove modularity $\times$
2. Enumerate rational weight 2 Siegel modular forms by conductor $\times$
3. Construct corresponding genus 2 curves $\times$
4. Enumerate isogeny class $\times^*$ (some progress)
5. Compute L-functions

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

1. Prove modularity ×
2. Enumerate rational weight 2 Siegel modular forms by conductor ×
3. Construct corresponding genus 2 curves ×
4. Enumerate isogeny class $\times^*$ (some progress)
5. Compute L-functions ✓ (this is feasible!)
6. Compute BSD invariants

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

1. Prove modularity ×
2. Enumerate rational weight 2 Siegel modular forms by conductor ×
3. Construct corresponding genus 2 curves ×
4. Enumerate isogeny class $\times^*$ (some progress)
5. Compute L-functions ✓ (this is feasible!)
6. Compute BSD invariants $\checkmark^*$ (most of them)
7. Find integer and rational points

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

1. Prove modularity ×
2. Enumerate rational weight 2 Siegel modular forms by conductor ×
3. Construct corresponding genus 2 curves ×
4. Enumerate isogeny class ×* (some progress)
5. Compute L-functions ✓ (this is feasible!)
6. Compute BSD invariants ✓* (most of them)
7. Find integer and rational points ✓* (feasible in many cases)
8. Compute endomorphism rings and Sato-Tate groups

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

1. Prove modularity ×
2. Enumerate rational weight 2 Siegel modular forms by conductor ×
3. Construct corresponding genus 2 curves ×
4. Enumerate isogeny class ×* (some progress)
5. Compute L-functions ✓ (this is feasible!)
6. Compute BSD invariants ✓* (most of them)
7. Find integer and rational points ✓* (feasible in many cases)
8. Compute endomorphism rings and Sato-Tate groups ✓ (rigorous)
9. Compute images of Galois representations

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

1. Prove modularity ×
2. Enumerate rational weight 2 Siegel modular forms by conductor ×
3. Construct corresponding genus 2 curves ×
4. Enumerate isogeny class ×* (some progress)
5. Compute L-functions ✓ (this is feasible!)
6. Compute BSD invariants ✓* (most of them)
7. Find integer and rational points ✓* (feasible in many cases)
8. Compute endomorphism rings and Sato-Tate groups ✓ (rigorous)
9. Compute images of Galois representations ×* (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 $\deg f \le 2g+2$ and $\deg h \le g+1$. The discriminant of X is then

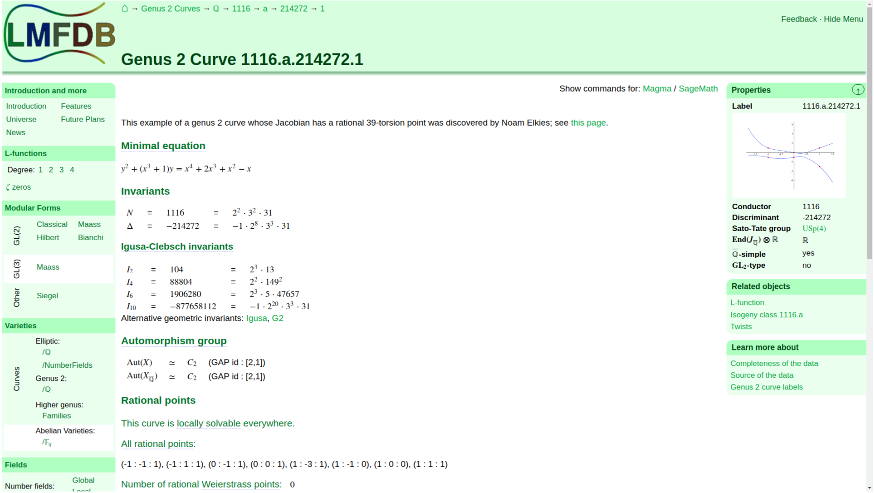
$$\Delta(X) = 2^{4g}\,\mathrm{disc}_{2g+2}(f + h^2/4) \in \mathbb{Z}$$

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

$$\begin{array}{llll} \mathrm{Aut}(X) & \simeq & C_2 & \text{(GAP id : [2,1])} \\ \mathrm{Aut}(X_{\overline{\mathbb{Q}}}) & \simeq & C_2 & \text{(GAP id : [2,1])} \end{array}$$

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

Genus 3 curves

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

1. a degree-2 cover of a smooth conic
   - (a) with a k-rational point (hyperelliptic model $y^2 + h(x)y = f(x)$),
   - (b) with no k-rational points (no hyperelliptic model over k).
2. a smooth plane quartic (the generic case).

Efficient implementations of average polynomial-time algorithm for computing $L(X,s) := \sum a_n n^{-s}$ are available in all three cases:

- rational hyperelliptic model [Harvey-S ANTS XI];
- no rational hyperelliptic model [Harvey-Massierer-S ANTS XII];
- smooth plane quartic [Harvey-S ~~ANTS XIII~~ (real soon now!)].

In all three cases we can compute a_n for $n \leq B$ in time $O(B(\log B)^3)$, and any particular Euler factor in $O(p^{1/2+o(1)})$ time.

$B = 2^{30}$ is feasible, so we can handle conductors up to 2^{50} or so.

Discriminants of smooth plane curves

Let T_d denote the set of ternary forms $f(x_0, x_1, x_2)$ of degree $d > 1$; it is a $\mathbb{C}$-vector space of dimension $n_d \coloneqq \binom{2d+2}{2}$.

The discriminant Δ_d is the unique polynomial in n_d variables corresponding to coefficients of $f \in T_d$ such that:

- $\Delta_d(f) = 0$ if and only if $f(x_0, x_1, x_2) = 0$ is a singular curve;
- Δ_d is irreducible, integral, and has content 1;
- $\Delta_d(x_0^d + x_1^d + x_2^d) < 0$.

Discriminants of smooth plane curves

Let T_d denote the set of ternary forms $f(x_0, x_1, x_2)$ of degree $d > 1$; it is a $\mathbb{C}$-vector space of dimension $n_d := \binom{2d+2}{2}$.

The discriminant Δ_d is the unique polynomial in n_d variables corresponding to coefficients of $f \in T_d$ such that:

- $\Delta_d(f) = 0$ if and only if $f(x_0, x_1, x_2) = 0$ is a singular curve;
- Δ_d is irreducible, integral, and has content 1;
- $\Delta_d(x_0^d + x_1^d + x_2^d) < 0$.

Δ_d is homogeneous of degree $3(d-1)^2$. For $d > 2$ it can be computed via

$$\Delta_d(f) = -d^{-d^2+3d-3}\mathrm{Res}_{d-1}(\partial_0 f, \partial_1 f, \partial_2 f) = \pm d^{-d^2+3d-3} \det \Phi_f,$$

where Φ_f is a $(2d^2 - 5d + 3) \times (2d^2 - 5d + 3)$ matrix with polynomial entries that can be computed using Sylvester's resultant formula.

The discriminant polynomial Δ_4

The size of Δ_d grows rapidly with d:

- $\Delta_2 = a_{200}a_{011}^2 + a_{101}^2 a_{020} + a_{110}^2 a_{002} - a_{110}a_{101}a_{011} - 4a_{200}a_{020}a_{002}$.
- Δ_3 is a degree 12 polynomial in 10 variables with 2940 terms and largest coefficient 26 244.
- Δ_4 is a degree 27 polynomial in 15 variables with 50 767 957 terms and largest coefficient 9 393 093 476 352.

$\Delta_4 = I_{27}$ is the largest of the Dixmier-Ohno invariants

$$I_3,\ I_6,\ I_9,\ I_{12},\ I_{15},\ I_{18}, I_{27},\ J_9,\ J_{12},\ J_{15},\ J_{18},\ I_{21}, J_{21},$$

which generate the full ring of invariants of ternary quartic forms.

Efficient algorithms to compute invariants of a given $f \in T_4$ are known [Gerard-Kohel ANTS VII], [Elsenhans 15], [Lercier-Ritzenthaler-Sijsling 16], but do not provide a feasible method to compute the polynomial Δ_4.

We used partial evaluation of Sylvester's formula and interpolation.

Evaluating multivariate polynomials with monomial trees

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 of $P(x_1, \ldots, x_n)$.
- nodes at level $n-1$: monomials of $P(x_1, \ldots, x_{n-1}, a_n)$.
- ...
- nodes at level 1: monomials of $P(x_1, a_2, \ldots, a_n) = P_1(x_1)$.

Nodes at level $m+1$ are connected to those at level m via an edge corresponding to the substitution $x_{m+1} = a_{m+1}$. We store a coefficient value at each node that is updated whenever we make a substitution.

Evaluating multivariate polynomials with monomial trees

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 of $P(x_1, \ldots, x_n)$.
- nodes at level $n-1$: monomials of $P(x_1, \ldots, x_{n-1}, a_n)$.
- ...
- nodes at level 1: monomials of $P(x_1, a_2, \ldots, a_n) = P_1(x_1)$.

Nodes at level $m+1$ are connected to those at level m via an edge corresponding to the substitution $x_{m+1} = a_{m+1}$. We store a coefficient value at each node that is updated whenever we make a substitution.

At level 1 we evaluate a univariate polynomial $P'(x_1)$ of degree $\deg_{x_1}(P)$.

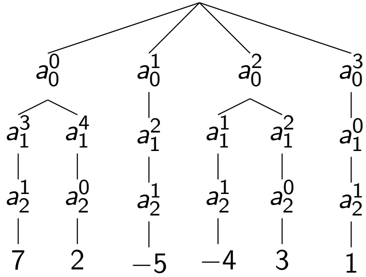
We can efficiently enumerate values of $P_1(x_1)$ using finite differences (as in [Kedlaya-S ANTS VIII]), or using a hard-wired straight-line program.

Monomial tree example

Consider the polynomial

$$g(a_0, a_1, a_2) \coloneqq a_0^3 a_2 + 3a_0^2 a_1^2 - 4a_0^2 a_1 a_2 - 5a_0 a_1^2 a_2 + 2a_1^4 + 7a_1^3 a_2.$$

A monomial tree for $g(a_0, a_1, a_2)$.

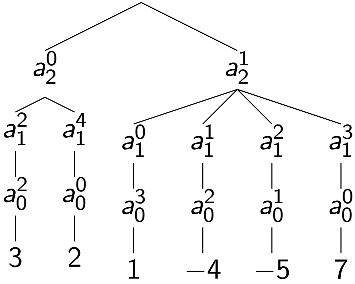


Monomial tree example

Consider the polynomial

$$g(a_0, a_1, a_2) \coloneqq a_0^3 a_2 + 3a_0^2 a_1^2 - 4a_0^2 a_1 a_2 - 5a_0 a_1^2 a_2 + 2a_1^4 + 7a_1^3 a_2.$$

A better monomial tree for $g(a_0, a_1, a_2)$.

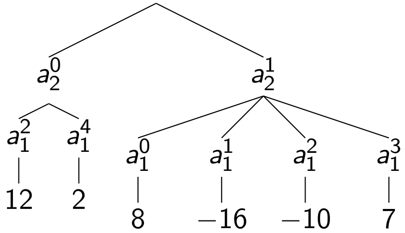


Monomial tree example

Consider the polynomial

$$g(a_0, a_1, a_2) := a_0^3 a_2 + 3a_0^2 a_1^2 - 4a_0^2 a_1 a_2 - 5a_0 a_1^2 a_2 + 2a_1^4 + 7a_1^3 a_2.$$

Monomial tree for $g(2, a_1, a_2)$.

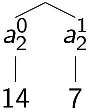


Monomial tree example

Consider the polynomial

$$g(a_0, a_1, a_2) := a_0^3 a_2 + 3a_0^2 a_1^2 - 4a_0^2 a_1 a_2 - 5a_0 a_1^2 a_2 + 2a_1^4 + 7a_1^3 a_2.$$

Monomial tree for $g(2, -1, a_2)$.



Monomial trees in practice

Discriminant monomial trees for hyperelliptic curves $y^2 + h(x)y = f(x)$ with $h(x)$ fixed (we can assume coefficients of h are 0 or 1).

- For $g = 2$, we get 246 terms and 703 nodes in our monomial tree.
- For $g = 3$, we get 5247 terms and 19916 nodes in our monomial tree.

For nonhyperelliptic curves of genus 3 the monomial tree for Δ_4 has 50 767 957 terms and 246 798 254 nodes (for suitably ordered variables).

Monomial trees in practice

Discriminant monomial trees for hyperelliptic curves $y^2 + h(x)y = f(x)$ with $h(x)$ fixed (we can assume coefficients of h are 0 or 1).

- For $g = 2$, we get 246 terms and 703 nodes in our monomial tree.
- For $g = 3$, we get 5247 terms and 19916 nodes in our monomial tree.

For nonhyperelliptic curves of genus 3 the monomial tree for Δ_4 has 50 767 957 terms and 246 798 254 nodes (for suitably ordered variables).

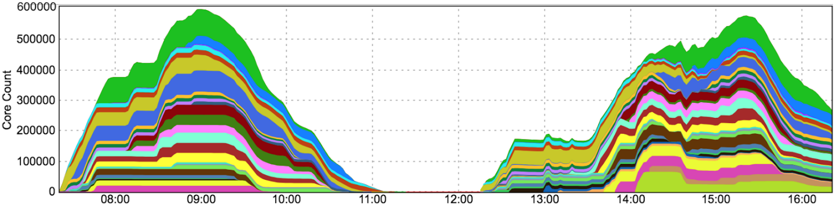
Enumerating ternary quartics of bounded naïve height with their discriminants using this monomial tree is not only feasible, but dramatically faster than computing discriminants individually.

In our computations with a height bound of $B_c := 9$ the inner loop reduces to four 64-bit multiplications and six 64-bit additions, and uses 22 Haswell clock cycles (under 10ns); about $2/3$ total time is spent in the inner loop.

Parallel computation

The computation was parallelized by dividing boxes into sub-boxes then run on Google's Cloud Platform. We spread the load across 24 data centers in nine geographic zones.

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



This 300 vCPU-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 $|f_i| \leq 31$, yielding approximately 3×10^{17} equations.

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 nonhyperelliptic curve equations with discriminants below this bound.

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

Among the nonhyperelliptic curves we found 82,241 non-isomorphic curves in (at least) 82,201 isogeny classes of Jacobians.

Isomorphism testing

Among the ten million nonhyperelliptic curve equations there are many isomorphisms (average isomorphism class size ≈ 100, several over 1000).

Pairwise isomorphism testing is slow (and unreliable!).

Instead, we use efficiently computable geometric and isogeny invariants to partition curve equations into equivalence classes that we know must be unions of isomorphism classes. We obtain 82,240 equivalence classes.

Isomorphism testing

Among the ten million nonhyperelliptic curve equations there are many isomorphisms (average isomorphism class size ≈ 100, several over 1000).

Pairwise isomorphism testing is slow (and unreliable!).

Instead, we use efficiently computable geometric and isogeny invariants to partition curve equations into equivalence classes that we know must be unions of isomorphism classes. We obtain 82,240 equivalence classes.

We then try to prove each equivalence class actually is an isomorphism class by exploring the $\mathrm{GL}_3(Z)$-orbit of a chosen representative using a pruned Cayley-search (a breadth-first search using a fixed set of generators that is restricted to forms of small height). This succeeds for all but one equivalence class, containing the non-isomorphic curves:

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

A few highlights

- Smallest hyperelliptic conductor found is 3993 for 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 $X_0(33)$.

- Smallest nonhyperelliptic conductor is 2940, for the curve

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

- Smallest nonhyperelliptic prime conductor 8233 arises for the curve

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

  This is also the smallest hyperelliptic prime conductor for the 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.