A Shimura-Belyi map of degree 33, and number fields with Galois group 33T55 = $\Sigma\mathrm{L}_2(\mathbf{F}_{32})$

Noam D. Elkies

Abstract

Let K be the totally real quintic field $\mathbf{Q}(2\cos(\pi/11))$, and let A be the quaternion algebra over K ramified only at four of its five real places. Then $A^*/\{\pm 1\}$ contains the $(2,3,11)$ triangle group, which is the last example in Takeuchi's list (1977) of arithmetic triangle groups, and the only one associated to a quaternion algebra over a field of degree at least 5. We study the Shimura curve $C = \mathcal{X}_0(\mathfrak{p}_{32})$ of genus 2 associated to a congruence subgroup $\Gamma_0(\mathfrak{p}_{32})$. We find that C has the Weierstrass model

$$\begin{aligned} C : y^2 &= -28x^6 - 76x^5 - 11x^4 - 30x^3 - 91x^2 + 164x - 52 \\ &= (2x-1)(14x^5 + 45x^4 + 28x^3 + 29x^2 + 60x - 52), \end{aligned} \tag{1}$$

and determine the degree-33 Belyi function on C representing the cover $\mathcal{X}_0(\mathfrak{p}_{32}) \to \mathcal{X}(1)$ of Shimura modular curves. The preimages of $\mathbf{Q}$-rational points j on $\mathcal{X}(1)$ then yield infinitely many number fields F_j with $[F_j : \mathbf{Q}] = 33$ such that $\mathrm{Gal}(F_j/\mathbf{Q}) \cong \Sigma\mathrm{L}_2(\mathbf{F}_{32})$ with quintic resolvent K. Searching for examples with small $\Delta = \mathrm{disc}(F_j : \mathbf{Q})$ finds fields with Δ as small as $2^{78}11^{30}$ (root-discriminant 45.52), as well as the field $F_{-121} = \mathbf{Q}[x]/(x^{33} - 6x^{22} + 14x^{11} + 2)$ with smaller Galois group and $\Delta = 2^{32}11^{34}$ (root-discriminant only 23.17, now the LMFDB's second-smallest for a number field of degree 33). Along the way we find that $J(C)$ is 31-isogenous with the Jacobian of the curve

$$C' : y^2 = 8x^5 - 23x^4 + 38x^3 - 7x^2 - 16x + 8, \tag{2}$$

which has $(J_{C'}(K))_{\mathrm{tors}} \cong \mathbf{Z}/155\mathbf{Z}$, including a Galois orbit of five K-rational points on C' that comprise an exotic "Weierstrass torsion packet".

At several points in this investigation, data in the LMFDB and affiliated resources made the analysis and computations simpler or more efficient. In turn the new number fields were added to the LMFDB, which did not previously include any fields with these Galois groups.

Keywords: Shimura curve, Belyi map, Galois group, Weierstrass torsion packet

1 Introduction

Define $a = 2\cos(\pi/11) = 1.9189859\ldots$ and $K = \mathbf{Q}(a)$, so K is the totally real quintic field with LMFDB label 5.5.14641.1. The ring of integers O_K is $\mathbf{Z}[a]$. We choose a as the generator because

18 Jun 2025 21:57:49 PDT
250201-Elkies Version 2 - Submitted to LuCaNT

it is the largest root of the "`polredabs` polynomial" used by the LMFDB;[1] namely, the minimal polynomial equation satisfied by a is

$$a^5 - a^4 - 4a^3 + 3a^2 + 3a - 1 = 0. \tag{3}$$

Because K is the real subfield of the cyclotomic field $\mathbf{Q}(\boldsymbol{\mu}_{11})$, its Galois group $\mathrm{Gal}(K/\mathbf{Q})$ is $(\mathbf{Z}/11\mathbf{Z})^\times/\{\pm 1\} \cong \mathbf{Z}/5\mathbf{Z}$. We fix the generator σ of $\mathrm{Gal}(K/\mathbf{Q})$ corresponding to the generator ± 2 of $(\mathbf{Z}/11\mathbf{Z})^\times/\{\pm 1\}$; explicitly, $\sigma(a) = 2 - a^2 = -\cos(2\pi/11)$.

Let A be the quaternion algebra over K ramified only at four of the five embeddings $K \hookrightarrow \mathbf{R}$, namely the embeddings taking a to $\sigma^i(a)$ for $i = 1, 2, 3, 4$ (the other choices of a set of four embeddings are equivalent under $\mathrm{Gal}(K/\mathbf{Q})$). Because the $i = 0$ embedding is unramified, it gives an isomorphism $i : \mathsf{A} \otimes_K \mathbf{R} \xrightarrow{\sim} M_2(\mathbf{R})$. Fix a maximal order $O_\mathsf{A} \subset \mathsf{A}$, and let Γ be the subgroup of $O_\mathsf{A}^\times$ consisting of elements of norm 1. Then $i(\Gamma)$ is a discrete co-compact subgroup of $\mathrm{SL}_2(\mathbf{R})$, so $\Gamma/\{\pm 1\}$ acts on the upper half-plane $\mathcal{H}$ with quotient a compact Riemann surface. We denote this quotient surface by $\mathcal{X}(1)$. For any ideal $\mathfrak{N}$ of O_K we define a congruence subgroup $\Gamma(\mathfrak{N}) \trianglelefteq \Gamma$ by $\Gamma(\mathfrak{N}) = \{g \in \Gamma : g \equiv 1 \bmod \mathfrak{N}\}$, and thus a Shimura curve $\mathcal{X}(\mathfrak{N})$ covering $\mathcal{X}(1)$. There is an isomorphism $O_\mathsf{A}/\mathfrak{N}O_\mathsf{A} \xrightarrow{\sim} M_2(O_K/\mathfrak{N})$ of O_K-algebras, unique up to conjugation in Γ, which we use to define the usual congruence subgroups $\Gamma_0(\mathfrak{N}), \Gamma_1(\mathfrak{N})$ with $\Gamma(N) \trianglelefteq \Gamma_1(\mathfrak{N}) \trianglelefteq \Gamma_0(\mathfrak{N}) \subseteq \Gamma_0(\mathfrak{N})$, and the corresponding Shimura curves $\mathcal{X}_0(\mathfrak{N}), \mathcal{X}_1(\mathfrak{N})$ and maps $\mathcal{X}(\mathfrak{N}) \to \mathcal{X}_1(\mathfrak{N}) \to \mathcal{X}_0(\mathfrak{N}) \to \mathcal{X}(1)$.

These Shimura curves and maps for A are of particular interest to us for the following reasons. According to the list of arithmetic triangle groups in [Takeuchi 1977], $\Gamma/\{\pm 1\}$ is the $(2, 3, 11)$ triangle group in $\mathrm{Aut}(\mathcal{H})$, and is the only arithmetic triangle group coming from a quaternion algebra over a number field of degree 5 or more. Since Γ is a triangle group, its covers by $\mathcal{X}_0(\mathfrak{N}), \mathcal{X}_1(\mathfrak{N}), \mathcal{X}(\mathfrak{N})$ are Belyi maps (finite covers of $\mathbf{P}^1$ ramified above only three points). When $\mathfrak{N}$ is invariant under $\mathrm{Gal}(K/\mathbf{Q})$, the curves $\mathcal{X}_0(\mathfrak{N}), \mathcal{X}_1(\mathfrak{N}), \mathcal{X}(\mathfrak{N})$ are defined over $\mathbf{Q}$, though in general the action of $\mathrm{SL}_2(O_K/\mathfrak{N})$ on $\mathcal{X}(N)$ is defined only over some cyclotomic extension of K. Other than the case $\mathfrak{N} = O_K$ of $\mathcal{X}(1)$ itself, this first happens for $\mathfrak{N} = \mathfrak{p}_{11} := (2 + a)O_K$, which is the prime of K over the totally ramified rational prime 11, and for $\mathfrak{N} = \mathfrak{p}_{32} := 2O_K$, which is the prime of K over the inert rational prime 2. The corresponding Shimura curves $\mathcal{X}_0(\mathfrak{N})$ have genus 1 for $\mathfrak{N} = \mathfrak{p}_{11}$ and 2 for $\mathfrak{N} = \mathfrak{p}_{32}$, see for instance [Voight 2009, Table 4.5] (with $d_F = \mathrm{disc}(K/\mathbf{Q}) = 11^4 = 14641$).

For $\mathfrak{N} = \mathfrak{p}_{11}$ the group $\mathrm{SL}_2(O_K/\mathfrak{N})$ is $\mathrm{SL}_2(\mathbf{F}_{11})$, and the curve $\mathcal{X}(\mathfrak{p}_{11})$ with its action of $\mathrm{SL}_2(\mathbf{F}_{11})$ is the same as the classical modular curve $\mathrm{X}(11)$, because the curve $\mathcal{X}(\mathfrak{p}_{11})$ and its Shimura-Belyi map to $\mathcal{X}(1)$ have the same ramification as $\mathrm{X}(11) \to \mathrm{X}(1)$ (the elliptic point of order 11 corresponds to the classical cusp), and the monodromy generators determine the map. We choose the rational coordinate $j = j_\mathsf{A}$ on $\mathcal{X}(1)$ that takes values $1728, 0, \infty$ on the elliptic points, so that we can use the same formulas for both maps.

For $\mathfrak{N} = \mathfrak{p}_{32}$ there is no such shortcut. We compute equations for the genus-2 curve[2] $\mathcal{X}_0(\mathfrak{p}_{32})$ and the degree-33 map $\mathcal{X}_0(\mathfrak{p}_{32}) \to \mathcal{X}(1)$. The genus and degree are barely small enough that it would have

[1] The "`polredabs` polynomial" of a number field F is a canonical defining polynomial $P_1 \in \mathbf{Z}[X]$ for F, named for the GP function that computes it. It minimizes the T_2-norm $\sum_{P(z)=0} |z|^2$ over all monic $P \in \mathbf{Z}[X]$ such that $F = \mathbf{Q}[X]/(P)$, and thus tends to have reasonably small coefficients.

[2] We did not attempt to give explicit equations for the curve $\mathcal{X}_1(\mathfrak{p}_{32})$, which is already of genus 32, let alone the genus-1241 curve $\mathcal{X}(\mathfrak{p}_{32})$.

been feasible, albeit arduous, to find the curve and map using known techniques such as those of [Elkies 2006, Elkies 2013]. Fortunately the computation was considerably streamlined and simplified by the use of data already in the LMFDB and in affiliated resources (namely [CEHJMPV 2025]).

The degree-33 extension of function fields $(\mathcal{X}_0(\mathfrak{p}_{32}))(\mathbf{Q}) \to (\mathcal{X}(1)(\mathbf{Q})$ has Galois group $\Sigma\mathrm{L}_2(\mathbf{F}_{32}) = \mathrm{SL}_2(\mathbf{F}_{32}) \rtimes \mathrm{Gal}(\mathbf{F}_{32}/\mathbf{F}_2)$ acting on the 33 points of $\mathbf{P}^1(\mathbf{F}_{32})$, with quintic resolvent K. (The quintic resolvent is the subfield of the Galois closure fixed by the index-5 normal subgroup $\mathrm{SL}_2(\mathbf{F}_{32})$. Here no further cyclotomic extension is needed because $\mathbf{F}_{32}$ has characteristic 2 and K already contains $\boldsymbol{\mu}_2$.) By Hilbert irreducibility we get infinitely many distinct degree-33 extensions of $\mathbf{Q}$ by specializing to rational points of $\mathcal{X}(1)$ with the same Galois group and quintic resolvent. The group $\Sigma\mathrm{L}_2(\mathbf{F}_{32})$, in its transitive action on $\mathbf{P}^1(\mathbf{F}_{32})$, is called "33T55" in the LMFDB. The LMFDB did not include any number fields with Galois group 33T55, and apparently none was known. Now that we have the explicit map $\mathcal{X}_0(\mathfrak{p}_{32}) \to \mathcal{X}(1)$, we can generate infinitely many such fields F_j by specializing to rational $j \in \mathcal{X}(1)$. We searched for specializations with small discriminant Δ. By far the smallest Δ that we found was $2^{78}11^{30}$, for $j_{\mathsf{A}} = -121$; but this is a CM point on $\mathcal{X}(1)$ (though not on X(1)), so we expect a smaller Galois group, and indeed the `polredabs` polynomial $x^{33} - 6x^{22} + 14x^{11} + 2$ for F_{-121} shows its Galois group is solvable (it turns out to be "33T9 = $C_{33} : C_{10}$"). This field was not in the LMFDB either; it is now the number field of second-smallest discriminant among the LMFDB's degree 33 fields. The smallest discriminant we found for a 33T55 field is $2^{78}11^{30}$, for the field with $j_{\mathsf{A}} = 287496 = 66^3$ (which is a CM point on X(1) but not on $\mathcal{X}(1)$), with `polredabs` polynomial

```
      x^33 - 7*x^32 + 20*x^31 + 4*x^30 - 132*x^29 + 132*x^28 + 1056*x^27
 - 2464*x^26 - 1276*x^25 + 14608*x^24 - 17512*x^23 - 12100*x^22 + 90024*x^21
   - 102608*x^20 - 104060*x^19 + 482064*x^18 - 177386*x^17 - 703978*x^16
 + 1731268*x^15 + 196988*x^14 - 4514752*x^13 + 3205048*x^12 + 7176752*x^11
  - 9604496*x^10 - 5377240*x^9 + 16445836*x^8 + 468512*x^7 - 17393508*x^6
   + 995588*x^5 + 9545932*x^4 - 292820*x^3 - 2225432*x^2 + 102487*x + 219615 .
```

This is now the number field of sixth-smallest discriminant among the LMFDB's degree 33 fields, following the $\mathrm{SL}_2(\mathbf{F}_{32})$ field of discriminant $2^{62}157^{16}$ computed by Bosman [Bosman 2011].

The rest of this paper is organized as follows. We start (§2) by reviewing the degree-12 Belyi map $\mathrm{X}_0(11) \to X(1)$ of classical modular curves, then show that it is the same as the Shimura-Belyi map $\mathcal{X}_0(\mathfrak{p}_{11}) \to \mathcal{X}(1)$, and describe the roles of each of this curve's five $\mathbf{Q}$-rational points as points on both $\mathrm{X}_0(11)$ and $\mathcal{X}_0(\mathfrak{p}_{11})$. In the next section we close in on the degree-33 Belyi map $\mathcal{X}_0(\mathfrak{p}_{32}) \to \mathcal{X}(1)$ by combining information from the geometry of the map (§3.1) and from Hilbert modular forms for K (§3.2) to guess the model (1) for $\mathcal{X}_0(\mathfrak{p}_{32})$ (§3.3); then (§3.4) we find a degree-33 Belyi map on this curve, and prove (§3.5) that it has geometric Galois group $\mathrm{SL}_2(\mathbf{F}_{32})$ and is thus the desired Shimura-Belyi map. Along the way we find another genus-2 curve C' whose Jacobian has 155-torsion over K, generated by divisors $(Q) - (P)$ where P is a rational Weierstrass point and Q is in a $\mathrm{Gal}(K/\mathbf{Q})$ orbit of K-rational points that give an exotic "Weierstrass torsion packet" in the sense of [Poonen 2000, Poonen 2001]; we describe this situation briefly in §3.6. In the final section (§4) we describe the search for fields F_j of small discriminant and list the best examples we found (36).

2 The Shimura-Belyi map $\mathcal{X}_0(\mathfrak{p}_{11}) \to \mathcal{X}(1)$, and the Q-points on $\mathcal{X}_0(\mathfrak{p}_{11})$

We claim that as a Belyi map, the degree-12 cover $\mathcal{X}_0(\mathfrak{p}_{11}) \to \mathcal{X}(1)$ is identical with the cover $\mathrm{X}_0(11) \to \mathrm{X}(1)$ of classical modular curves. Indeed the two covers have the same geometric Galois group $\mathrm{PSL}_2(\mathbf{F}_{11})$, and the monodromy generators g_2, g_3, g_{11} of $\mathcal{X}_0(\mathfrak{p}_{11}) \to \mathcal{X}(1)$ above the elliptic points of index $2, 3, 11$ have the same cycle structures $2^6, 3^4, (1, 11)$ as those of $\mathrm{X}_0(11) \to \mathrm{X}(1)$ above the elliptic points of index $2, 3$ and the cusp respectively. These cycle structures, together with the condition $g_2 g_3 g_{11} = 1$, determine g_2, g_3, g_{11} up to conjugation in $\mathrm{PGL}_2(\mathbf{F}_{11})$; so the covers must be isomorphic as claimed.

We choose the projective coordinate j_{A} on $\mathcal{X}(1)$ that takes the same values $1728, 0, \infty$ at the elliptic points of index $2, 3, 11$ as the classical j-invariant on the elliptic points of index $2, 3$ and the cusp. We can then re-use the known equations for $\mathrm{X}_0(11)$ and the cover $\mathrm{X}_0(11) \to \mathrm{X}(1)$ in the Shimura setting. The curve has Weierstrass equation $y^2 + y = x^3 - x^2 - 10x - 20$, and

$$\begin{aligned} j &= \frac{1}{x-16}\Big(-11x^6 + 148x^5 + 643x^4 - 2704x^3 - 6780x^2 + 1781x + 3308 \\ &\qquad -(x^5 + 23x^4 - 697x^3 + 1031x^2 + 2170x + 353)y\Big). \end{aligned} \tag{4}$$

eliminating y yields a relation $j^2 + A(x)j + B(x) = 0$ where A, B are determined by

$$\begin{aligned} B(x) &= -(x^4 - 20x^3 + 62x^2 + 116x + 97)^3, \\ 1728^2 - 1728A(x) + B(x) &= -(x^6 - 30x^5 + 243x^4 - 256x^3 - 1053x^2 + 654x + 7793)^2. \end{aligned} \tag{5}$$

It is well-known that the elliptic curve $X_0(11)$ has Mordell-Weil group $\mathbf{Z}/5\mathbf{Z}$. We choose the generator $T = (16, -61)$, and list for each $n = 0, 1, 2, 3, 4$ the (x, y) coordinates of nT, and the value of j, computed from (4) or (for $n = 4$) from (5):

n	$(x(nT), y(nT))$	$j(nT) = j_{\mathsf{A}}(nT)$	$\mathrm{X}_0(11)$	$\mathcal{X}_0(11)$
0	(∞, ∞)	∞	cusp $i\infty$	$\mathrm{CM}(-(2+a)^3)$
1	$(16, -61)$	∞	cusp 0	$e_{11} = \mathrm{CM}(-(2+a))$
2	$(5, -6)$	$-121 = -11^2$	121a1, c2	$\mathrm{CM}(-(2+a)^3)$
3	$(5, 5)$	$-32768 = -2^{15}$	121b1, b2 $= \mathrm{CM}(-11)$	non − CM
4	$(16, 60)$	$-24729001 = -131^3 11$	121a2, c1	non − CM

(6)

It remains to explain the table's columns labeled $\mathrm{X}_0(11)$ and $\mathcal{X}_0(11)$. The Fricke involution w_{11} of $\mathrm{X}_0(11)$ switches the two cusps, so it must be the map $P \mapsto T - P$. In particular $3T$ is the fixed point. We recognize $j(3T) = -2^{15}$ as the j-invariant of elliptic curves such as 121b1 and 121b2 with complex multiplication (CM) by the quadratic order of discriminant -11; such an elliptic curve is 11-isogenous with its quadratic twist by $\mathbf{Q}(\sqrt{-11})$ (and indeed 121b1 and 121b2 are related by such a quadratic twist). The remaining points $2T, 4T$ yields j-invariants -11^2 and $-131^3 11$ of non-CM elliptic curves that are related by an 11-isogeny.

The Shimura curve $\mathcal{X}_0(11)$ also has an involution w, coming from the normalizer of $\Gamma_0(\mathfrak{p}_{11})$ in $\mathrm{SL}_2(\mathbf{R})$. But this involution is not the same as the Fricke involution $P \mapsto T - P$ of $\mathrm{X}_0(11)$. Instead this involution must take T to itself, because T is the simple pole of j_{A} and is thus the unique elliptic

point of $\mathcal{X}_0(11)$, related to itself by a "$\mathfrak{p}_{11}$-isogeny". Since $j_{\mathsf{A}} = \infty$ is an elliptic point of order 11, it is a CM point corresponding to the quadratic extesion $\mathbf{Q}(\boldsymbol{\mu}_{11})$ of K generated by $\sqrt{-(2+a)}$. The pole of j_{A} of multiplicity 11 at $(x, y) = (\infty, \infty)$ then gives a $\mathfrak{p}_{11}$-isogeny between $j_{\mathsf{A}} = \infty$ and $j_{\mathsf{A}}(w(\infty, \infty)) = j_{\mathsf{A}}(2T) = -121$. Thus these are also CM points on $\mathcal{X}_0(11)$, but of discriminant $-(2+a)^3$. Here it is the points $3T, 4T$ that yield non-CM points $j = -2^{15}$ and $j = -131^3 11$ related by a $\mathfrak{p}_{11}$-isogeny. We shall encounter both this isogenous pair and the CM point $j_{\mathsf{A}} = -121$ in the final section of this paper.

3 The Shimura-Belyi map $\mathcal{X}_0(\mathfrak{p}_{32}) \to \mathcal{X}(1)$

3.1 Geometry

We start by using the geometry of the Belyi map $C = \mathcal{X}_0(\mathfrak{p}_{32}) \to \mathcal{X}(1)$ and the involution w of $\mathcal{X}_0(\mathfrak{p}_{32})$ to constrain the preimages on C of the elliptic points on $\mathcal{X}(1)$. We then use the quotient map $\mathcal{X}_1(\mathfrak{p}_{32}) \to \mathcal{X}_0(\mathfrak{p}_{32}) = C$ to further constraint the arithmetic of J_C.

Since $\mathcal{X}(1)$ has genus zero, we identify a map $C \to \mathcal{X}(1)$ with a rational function on C by choosing a rational coordinate on $\mathcal{X}(1)$. We retain the coordinate of the previous section, which takes the values $1728, 0, \infty$ on the elliptic points of indices $2, 3, 11$ respectively. Again we denote the resulting function on C by j_{A}. The monodromy generators above the elliptic points are elements of order $2, 3, 11$ in $\mathrm{SL}_2(\mathbf{F}_{32})$; thus their cycle structures are respectively $(1, 2^{16}), 3^{11}, 11^3$. (Check: the Euler characteristic of C is then $33\chi(\mathbf{P}^1) - 16 - 2 \cdot 11 - 10 \cdot 3 = 66 - 16 - 22 - 30 = -2$, consistent with $g(C) = 2$.) We denote by P the unique multiplicity-1 preimage of 1728. This is the unique elliptic point on $\mathcal{X}_0(\mathfrak{p}_{32})$, and is thus fixed by the involution w of $\mathcal{X}_0(\mathfrak{p}_{32})$ coming from the normalizer of $\Gamma_0(\mathfrak{p}_{32})$ in $\mathrm{SL}_2(\mathbf{R})$. It turns out that w is the hyperelliptic involution of $\mathcal{X}_0(\mathfrak{p}_{32})$, making P a Weierstrass point. This could be checked directly by counting fixed points of w: the hyperelliptic involution fixes the six Weierstrass points, while a non-hyperelliptic involution of a genus-2 curve fixes only four points. Instead of attempting to do this calculation directly, we give an alternative argument in §3.2 using the decomposition of the relevant space of Hilbert modular forms. Alternatively, we can add the statement that w is hyperelliptic to several other guesses that we shall make on the way to computing a Belyi map, statements that we justify in §3.5 by proving that our map has the correct Galois group.

The ramification behavior of our map means that the polar divisor of our rational function $j_{\mathsf{A}} \in \mathbf{Q}(C)$, and the zero divisors of j_{A} and $j_{\mathsf{A}} - 1728$, are given by

$$(j_{\mathsf{A}})_\infty = 11D_3, \quad (j_{\mathsf{A}})_0 = 3D_{11}, \quad (j_{\mathsf{A}})_{1728} = 2D_{16} + (P) \tag{7}$$

for some divisors D_3, D_{11}, D_{16} of degrees $3, 11, 16$ on C. Because the map is ramified only above $\{1728, 0, \infty\}$, the differential $\mathrm{d}j_{\mathsf{A}}$ has divisor

$$(\mathrm{d}j_{\mathsf{A}}) = (\mathrm{d}j_{\mathsf{A}})_0 - (\mathrm{d}j_{\mathsf{A}})_\infty = 2D_{11} + D_{16} - 12D_3. \tag{8}$$

Now the three divisors in (7) are linearly equivalent to each other, and the divisor of a differential of a nonconstant function is linearly equivalent to the canonical divisor K on C. This gives relations

among $D_3, D_{11}, D_{16}, (P), K$ in $\mathrm{Pic}(C)$:

$$11D_3 \sim 3D_{11} \sim 2D_{16} + (P), \quad 2D_{11} + D_{16} - 12D_3 \sim K \tag{9}$$

The first equation gives

$$D_3 \sim 3D_1, \quad D_{11} \sim 11D_1 \tag{10}$$

where D_1 is the degree-1 divisor $4D_3 - D_{11}$. Then

$$D_{16} \sim K - 2D_{11} + 12D_3 \sim K - 22D_1 + 36D_1 = K + 14D_1, \tag{11}$$

whereupon the remaining condition $3D_{11} \sim 2D_{16} + (P)$ of (9) gives $33D_1 \sim 2K + 28D_1 + (P)$ and finally

$$5D_1 \sim 2K + (P). \tag{12}$$

Since P is a Weierstrass point, $K \sim 2(P)$, so (12) gives $5D_1 \sim 4(P) + (P) = 5(P)$, whence $5(D_1 - (P)) \sim 0$. (The factor of 5 can be identified with the numerator of the factor

$$\frac{5}{66} = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{11} \tag{13}$$

in the formula for the hyperbolic area of $\mathcal{X}(1)$.) It remains to show that the class $[D_1 - (P)] \in \mathrm{Pic}^0(C) = J_C$ is actually 5-torsion, not zero. Suppose it were zero; that is, suppose $D_1 \sim (P)$. Then $D_3 \sim 3D_1 \sim 3(P)$ would imply that P is one of the points in D_3: by Riemann-Roch $h^0(3P) = 2 = h^0(K) = h^0(2P)$. But the divisors $(j_{\mathsf{A}})_\infty = 11D_3$ and $(j_{\mathsf{A}})_{1728} = 2D_{16} + (P)$ are disjoint, so D_3 cannot contain P. □

The curve $C = \mathcal{X}_0(\mathfrak{p}_{32})$ also admits a cyclic cover $\mathcal{X}_1(\mathfrak{p}_{32}) \to \mathcal{X}_1(\mathfrak{p}_{32})/\mathbf{F}_{32}^* \cong \mathcal{X}_0(\mathfrak{p}_{32})$ over K. The map is unramified because it is cyclic of degree 31, and the only elliptic point of $\mathcal{X}_0(\mathfrak{p}_{32})$ has index 2 which is coprime with 31. By Kummer theory this unramified cyclic cover gives a subgroup of J_C that isomorphic over K with $\boldsymbol{\mu}_{31}$. We shall use this to choose C from a pair of candidate curves whose Jacobians are related by a 31-isogeny.

3.2 Modular forms

We next use modular forms to surmise that J_C is in the isogeny class of the simple factor of the Jacobian of $\mathrm{X}_0(242)$ corresponding to the modular form 242.2.a.f.

The LMFDB does not at present include Shimura modular forms (other than those associated to congruence subgroups of $\mathrm{SL}_2(\mathbf{Z})$), but we can get at J_C indirectly via Hilbert cusp forms of parallel weight 2 with base field K. We find that at level $\mathfrak{p}_{32}$ there is a unique Hecke orbit of such forms, namely the orbit labeled 5.5.14641.1-32.1-a, with dimension 2 (as expected because C has genus 2) and eigenvalue field $\mathbf{Q}(\sqrt{5})$. This also gives us a proof that the involution w of $\mathcal{X}_0(\mathfrak{p}_{32})$ must be hyperelliptic: otherwise this space of cusp form would split into $+1$ and -1 subspaces.

Since the level is invariant under $\mathrm{Gal}(K/\mathbf{Q})$, so are the Hecke eigenvalues, and in particular the Hecke eigenvalue at a prime $\mathfrak{p}$ depends only on its norm $\mathbf{N}\mathfrak{p}$. Consulting the LMFDB's "home page"

for 5.5.14641.1-32.1-a, we tabulate Hecke eigenvalues for $\mathbf{N}\mathfrak{p} \le 131$, and also for $\mathfrak{p} = 3O_K$, which has norm $3^5 = 243$ and is the first $\mathfrak{p}$ above a prime inert in K that does not divide the level:

$\mathbf{N}\mathfrak{p}$	11	23	32	43	67	89	109	131	$\cdots$	243	$\cdots$
$a_{\mathfrak{p}}$	e	$2e$	1	$-9e-3$	$5e+8$	$-5e-5$	$8e+14$	$11e$	$\cdots$	$20e+4$	$\cdots$

(14)

Here e is a solution of $e^2 + e - 1 = 0$. In particular the coefficient field is $\mathbf{Q}(e) = \mathbf{Q}(\sqrt{5})$, and J_C has K-endomorphisms by $\mathbf{Z}[e]$. But C is defined over $\mathbf{Q}$, and $\mathrm{Gal}(K/\mathbf{Q})$ has no nontrivial action on $\mathbf{Z}[e]$, so the endomorphisms of $\mathbf{Z}[e]$ on J_C must be defined over $\mathbf{Q}$.

Since J_C is a RM surface over $\mathbf{Q}$, it is a simple factor up to isogeny of some modular Jacobian $J_0(N) = J_{\mathrm{X}_0(N)}$, and thus corresponds to a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-orbit of modular eigenforms ϕ of weight 2 for $\Gamma_0(N)$. Since C has good reduction away from $\{2, 11\}$, the level N must be of the form $2^{e_2}11^{e_{11}}$ for some integers e_2, e_{11}. We search the LMFDB and find that the first spaces of such forms with coefficients in $\mathbf{Q}(\sqrt{5})$ occur for $N = 242$ (with $(e_2, e_{11}) = (1, 2)$), namely 242.2.a.d and 242.2.a.f, which are related by quadratic twist by $\mathbf{Q}(\sqrt{-11})$. For a rational prime $p \equiv \pm 1 \bmod 11$, the q^p coefficient of ϕ should equal the $T_{\mathfrak{p}}$ eigenvalue of 5.5.14641.1-32.1-a where $\mathfrak{p}$ is any of the primes of K with $\mathbf{N}\mathfrak{p} = (p)$. We find that this condition is already satisfied by 242.2.a.f, at least for the primes $p \le 131$ tabulated in (14). (Note that the LMFDB page for 242.2.a.f gives the eigenvales in terms of $\beta = -e$. For classical modular forms the LMFDB gives only 100 coefficients, but this is enough information to extend the q-expansion further in Magma.) Moreover, the q^3 coefficient a_3 of 242.2.a.f is $-e+1$, and we calculate that the T_{3O_K} eigenvalue $20e+4$ of 5.5.14641.1-32.1-a equals $\lambda^5 + \overline{\lambda}^5$ where $\lambda, \overline{\lambda}$ are the roots of the characteristic equation $F^2 - a_3F + 3$.

At this point we are almost certain that 242.2.a.f is our desired modular form ϕ. We cannot claim to have proven this, because for all we know ϕ might have level $N = 2^{e_2}11^{e_{11}}$ beyond the LMFDB's range. If we knew in advance that $N = 242$ then we would already have a proof.[3] Once we surmise an explicit Weierstrass model for the curve, and find a degree-33 Belyi map on that curve, we shall be able to identify that map with the Shimura-Belyi map $\mathcal{X}_0(\mathfrak{p}_{32}) \to \mathcal{X}(1)$ by proving that it has the correct Galois group.

3.3 The curves C' and C

We next combine the information from §§3.1,3.2 to surmise an equation for $\mathcal{X}_0(\mathfrak{p}_{32})$.

Here we were not able to simply look up the curve in the LMFDB. The LMFDB's 66158 genus-2 curves over $\mathbf{Q}$ include 99 whose Jacobians' $\mathbf{Q}$-endomorphism algebra are orders in real quadratic fields, in 92 isogeny classes, each linked to a classical modular eigenform ψ of weight 2 with coefficients in the same quadratic field. But this is a small fraction of the LMFDB's 80387 weight-2 eigenforms with quadratic coefficients. Moreover, even when ψ does link to an isogeny class of curves, the LMFDB might not contain every curve in the class. This already happens for the first

[3] We did guess that $N = 242$ by analogy with the known case of $\mathcal{X}_0(\mathfrak{p}_{27})$ for the $(2, 3, 7)$ triangle group. This triangle group is $\Gamma(1)$ for the quaternion algebra over $\mathbf{Q}(2\cos(\pi/7))$ ramified only at two of this field's three real embeddings, and we found in [Elkies 2006] that the Shimura curve $\mathcal{X}_0(\mathfrak{p}_{27})$, with $\mathfrak{p}_{27} = 3\mathbf{Z}[2\cos(\pi/7)]$, is an elliptic curve of conductor $147 = 3^1 7^2$, suggesting $N = 2^1 11^2$ for the presesnt curve $\mathcal{X}_0(\mathfrak{p}_{32})$.

two such ψ, of levels $N = 23$ and $N = 29$, where the LMFDB contains a genus-2 curve of discriminant N^2 whose Jacobian also has discriminant N^2, but does not contain the modular curve $X_0(N)$ because its discriminant (23^6 or 29^5) falls outside the LMFDB's range $|\Delta| \le 10^6$. The homepage of our form 242.2.a.f does not link to any genus-2 curves.

Given an eigenform ψ for $\Gamma_0(N)$ whose coefficients generate a quadratic field, and which thus corresponds to an isogeny class of abelian surfaces, one can try to find a genus-2 Jacobian in the isogeny class by numerically integrating ψ over cycles of $\mathrm{X}_0(N)$ to compute a period lattice to enough precision that its Igusa invariants can be recognized as rational numbers. In [CEHJMPV 2025] we report on a computation that tried this for each of the 16929 such ψ with $N \le 10^4$. We succeeded for most of them, including all cases where ψ has coefficients in a field of narrow class number 1 such as $\mathbf{Q}(\sqrt{5})$ and $\mathbf{Q}(\sqrt{2})$ and the $\overline{\mathbf{Q}}$-endomorphism algebra is contained in the coefficient field, in which case the isogeny class always contains a surface with a principal polarization defined over $\mathbf{Q}$. In particular we have already found a curve C' whose Jacobian is in the isogeny class corresponding to 242.2.a.f. In the github repository (see the end of the bibliographic entry for [CEHJMPV 2025]) this curve is reported as [[35,79,77,43,14,2],[0,-1,-1]], which is to say

$$y^2 - (x^2 + x)y = 2x^5 + 14x^4 + 43x^3 + 77x^2 + 79x + 35; \tag{15}$$

completing the square and substituting $x - 2$ for x gives a reduced model in narrow Weierstrass form,

$$C' : y^2 = 8x^5 - 23x^4 + 38x^3 - 7x^2 - 16x + 8. \tag{16}$$

This looks promising, because C' has a Weierstrass point (at infinity), and $J_{C'}$ has a 5-torsion point over $\mathbf{Q}$, represented by the divisor $x^2 - x - 1 = 0$, $y = 4x + 1$ with Weil function

$$4x^5 - x^4 + 14x^3 + 17x^2 - 2x - 4 - (3x^2 + 5x + 2)y. \tag{17}$$

Moreover, $\mathcal{X}_0(\mathfrak{p}_{32})$ must have good reduction outside $\{2, 11\}$, and C' satisfies this condition. (This does not follow automatically from the good reduction of $J_{C'}$ outside $\{2, 11\}$; see 20.) Over K, the curve C' also has good reduction at $\mathfrak{p}_{11}$: the right-hand side factors as $8(x + 3)^5 \bmod 11$, and translating x to $x - 3$ yields

$$y^2 = 8x^5 - 13 \cdot 11x^4 + 94 \cdot 11x^3 - 31 \cdot 11^2x^2 + 56 \cdot 11^2x + 40 \cdot 11^2; \tag{18}$$

so we can choose a local uniformizer π at $\mathfrak{p}_{11}$, scale (x, y) to (π^2x, π^5y), and divide through by π^{10} to get a model that remains smooth mod $\mathfrak{p}_{11}$. But we saw that the Jacobian of $\mathcal{X}_0(\mathfrak{p}_{32})$ must contain a subgroup $\boldsymbol{\mu}_{31}$ over K; it turns out that $J_{C'}$ instead contains a subgroup $\mathbf{Z}/31\mathbf{Z}$, which makes C' a curve of independent interest (see §3.6 below), but means C' cannot be our desired curve $\mathcal{X}_0(\mathfrak{p}_{32})$.

This suggests that $\mathcal{X}_0(\mathfrak{p}_{32})$ might be a curve whose Jacobian is the quotient of $J_{C'}$ by its 31-torsion group. We use period matrices to compute a putative equation for such a curve:

$$\begin{aligned} y^2 &= -28x^6 - 76x^5 - 11x^4 - 30x^3 - 91x^2 + 164x - 52 \\ &= (2x - 1)(14x^5 + 45x^4 + 28x^3 + 29x^2 + 60x - 52). \end{aligned} \tag{19}$$

This curve, too, has a rational Weierstrass point, good reduction outside $\{2, 11\}$, good reduction at $\mathfrak{p}_{11}$ over K, and a Jacobian with a $\mathbf{Q}$-rational 5-torsion point. Our isogeny class contains the Jacobians of at least two further curves, related by 5-isogenies with those we already found, namely

$$y^2 = -7(256x^6 - 16x^5 + 40x^4 - 1249x^3 + 56x^2 - 784x),$$

$$y^2 \;=\; 8x^5 - 1199x^4 - 7546x^3 + 10769x^2 + 67760x - 100672. \tag{20}$$

But neither of them can be $\mathcal{X}_0(\mathfrak{p}_{32})$. Indeed each curve in (20) fails two criteria: neither curve's Jacobian has a rational 5-torsion point, and each curve has bad reduction also at 7 (though their Jacobians still have good reduction outside $\{2, 11\}$).

We found no further Jacobians in this isogeny class. We thus proceed on the assumption that $\mathcal{X}_0(\mathfrak{p}_{32}) = C$.

3.4 The Shimura-Belyi map

We now compute the Shimura-Belyi map using the known technique of mod-p search followed by p-adic lift. We choose $p = 5$, the smallest prime at which the elliptic points $j = 0, 1728$ are distinct. If we had not surmised C in advance, we would have to try all pairs (C, D) of a genus-2 curve C mod 5 with a 5-torsion class $D \in J_C$, which would be more complicated to implement and would take about 5^3 times longer to run. Starting from C the search took little more than an hour on two processors, each trying a different choice of D (since there are two choices up to the hyperelliptic involution).

It is convenient to put the Weierstrass point P at infinity, even though this makes the coefficients of C larger. We thus work with the model

$$y^2 = 64x^5 - 1095x^4 - 1248x^3 - 1224x^2 - 640x - 112. \tag{21}$$

The divisors that differ from K by 5-torsion are

$$D : 8x^2 + 3x + 2 = 0,\ y = (77x - 66)/8; \qquad D' : x^2 + x + 2 = 0,\ y = 37x - 2; \tag{22}$$

and their images under the hyperelliptic involution $\iota : (x, y) \mapsto (x, -y)$. (Here and later we do not reduce mod 5 because we shall soon need the same formulas over the 5-adic numbers.) We find the functions

$$f_1 = 32x^3 + 29x^2 + 24x - (y + 4), \quad f_2 = 16x^3 + 21x^2 + y + 12 \tag{23}$$

with divisors $(f_1) = 2D + \iota^* D' - 6P$, $(f_2) = D + 2D' - 6P$.

We search for sections s_3, s_{11} of $5P - D$ and $13P - D'$, which we normalize by setting the "leading coefficient" (coefficient of xy and $x^5 y$ respectively) equal 1. Thus

$$s_3 = y - \frac{77x - 66}{8} + c_0(8x^2 + 3x + 2) \tag{24}$$

for some $c_0 \in \mathbf{F}_5$, and

$$s_{11} = A(x)(y - (37x - 2)) + B(x)(x^2 + x + 2) \tag{25}$$

for some monic polynomial A of degree 4 and some polynomial B of degree at most 4. Thus we have 5^{10} candidates, which is just under 10^7. For each s_3 and s_{11} we compute the sections

$$\frac{s_3^{11} \iota^*(f_1^4 f_2^2)}{(8x^2 + 3x + 2)^{10}(x^2 + x + 2)^4},\ \frac{s_{11}^3 f_1 \iota^* f_2}{(8x^2 + 3x + 2)(x^2 + x + 2)^3} \tag{26}$$

of $35P-D$, find the linear combination that cancels the leading $x^{15}y$ coefficient and is thus a section of $34P - D$, and test whether its norm from C to $\mathbf{P}^1$ (which is a degree-32 polynomial in x) is a square. This finds two solutions mod 5, one of which is spurious (the linear combination is actually a section of $32P - D$); the other search, with D, D' replaced by $D', \iota^* D$, finds only a spurious solution.

We now take the vector of coefficients of our s_3 and s_{11}, lift it to $\mathbf{Z}_5$, and regard it as an approximation to the actual 5-adic solution. Four iterations of Newton's algorithm improve the error from $O(5)$ to $O(5^{16})$, which is enough to recognize c_0 as $-17/8$ and the quartics $A(t)$ and $B(t)$ as

$$\begin{aligned} A(x) &= x^4 + \frac{115x^3 + 10x^2 + 356x - 248}{3}, \\ B(x) &= \frac{545x^4 + 2991x^3 + 3298x^2 - 12620x - 1464}{3}. \end{aligned} \tag{27}$$

We finally obtain our Shimura-Belyi function as the ratio of the sections (26) of $35P-D$,'composed with the fractional linear transformation of $\mathbf{P}^1$ that puts the ramified points at $1728, 0, \infty$.

3.5 Conclusion of the proof

At this point we have found a Belyi map whose monodromy generators $g_2, g_3, g_{11} \in S_{33}$ have the same cycle structures as those of the Shimura-Belyi map $\mathcal{X}_0(\mathfrak{p}_{32}) \to \mathcal{X}(1)$. For the degree-12 map $\mathcal{X}_0(\mathfrak{p}_{11}) \to \mathcal{X}(1)$ the cycle structures suffice to determine the map, because the cycle structures $(2^6), (3^4), (1, 11)$ together with the condition $g_2 g_3 g_{11} = 1$ determine g_2, g_3, g_{11} uniquely up to conjugation in S_{12}. This is no longer true for the cycle structures $(1, 2^{16}), (3^{11}), (11^3)$ in S_{33}.[4] We next show that the Belyi map constructed in §3.4 has geometric Galois group $\mathrm{SL}_2(\mathbf{F}_{32})$. This will suffice, because in $\mathrm{SL}_2(\mathbf{F}_{32})$ the equation $g_2 g_3 g_{11} = 1$ does have a solution in elements of order $2, 3, 11$ that is unique up to conjugation in $\Sigma\mathrm{L}_2(\mathbf{F}_{32}) \subset S_{33}$.

Denote the geometric Galois group by G_0, and the Galois group over $\mathbf{Q}$ by G. We soon guess that G_0 and G must be $\mathrm{SL}_2(\mathbf{F}_{32})$ and $\Sigma\mathrm{L}_2(\mathbf{F}_{32})$ respectively by specializing j_{A} to "random" rational numbers and computing the Galois group of the resulting degree-33 extension of $\mathbf{Q}$, or by factoring specializations modulo many primes. But such calculations cannot prove that G_0 and G are the expected groups. We do, however, learn that G_0 and G must contain $\mathrm{SL}_2(\mathbf{F}_{32})$ and $\Sigma\mathrm{L}_2(\mathbf{F}_{32})$ respectively. Indeed it is already enough to take $j_{\mathsf{A}} = -2$ and factor the resulting polynomial mod 23: there are two linear factors and an irreducible factor of degree 31, so G and G_0 must contain elements of order 31, and the only transitive subgroups of S_{33} with such elements are $\mathrm{SL}_2(\mathbf{F}_{32}), \Sigma\mathrm{L}_2(\mathbf{F}_{32}), A_{33}, S_{33}$. Moreover G_0 cannot be $\Sigma\mathrm{L}_2(\mathbf{F}_{32})$ or S_{33}, because it is generated by even permutatios of orders $2, 3, 11$.

[4] We construct a counterexample as follows. Let $\alpha = \bar{a}+1 \in \mathbf{F}_{32}$, and let $g_2, g_3 \in S_{33}$ be the permutations $z \mapsto z + \alpha$ and $z \mapsto (z+1)/z$ of $\mathbf{P}^1(\mathbf{F}_{32})$, correspondinging to the matrices $\left[\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbf{F}_{32})$. Then $g_2 g_3(z) = (\bar{a}z + 1)/z$ corresponds to the matrix $\left[\begin{smallmatrix} \bar{a} & 1 \\ 1 & 0 \end{smallmatrix}\right]$ of trace $\bar{a}$, so $g_2 g_3$ has order 11. Now let $g_2' = \tau g_2 \tau$ where τ is the simple transposition (0 1), and let $g_{11}' = (g_2' g_3)^{-1}$. Then g_2', g_3, g_{11}' have the same cycle structures as g_2, g_3, g_{11} and satisfy the same equation $g_2' g_3 g_{11}' = 1$. But $g_2' g_{11}'^3$ has order 70, so the subgroup generated by g_2', g_3, g_{11}' cannot be isomorphic with $\mathrm{SL}_2(\mathbf{F}_{32})$. Indeed that subgroup is the full alternating group A_{33}, because $g_2' g_{11}'^2$ has order 31 and A_{33} has no proper transitive subgroup whose order is a multiple of $31 \cdot 70$.

But it takes more work to exclude the possibility that $G_0 = A_{33}$. We use the method that we introduced in [Elkies 2013, §3] (and was later used also in [Barth–Wenz 2019]). Here we show that G_0 does not act transitively on the $\binom{33}{4}$ 4-element subsets of the 33 roots. If it did, then we would have a degree $\binom{33}{4}$ cover C_4 of $\mathbf{P}^1$ by a connected curve of genus at most

$$1 + \frac{1}{2}\Big(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{11}\Big)\binom{33}{4} = 1551, \tag{28}$$

so over a q-element field $\mathbf{F}_q$ the curve C_4 would have at most $q + 1 + 2 \cdot 1551\sqrt{q}$ points by the Weil bound. Since we expect that in fact $G_0 = \mathrm{SL}_2(\mathbf{F}_{32})$, the action should have 5 orbits, and so C_4 will be a union of 5 curves and should have about $5q$ points if $\mathbf{F}_q$ contains a quotient field of O_K. So the assumption $G_0 = A_{33}$ will yield a contradiction if q is large enough, and we expect to succeed if q is comfortably larger than $(2 \cdot 1551/(5-1))^2$. We chose $q = 10^6 + 33$, the smallest prime above 10^6 that splits in K. Using the Lemma in [Elkies 2013, §3] we counted most of the points of $\mathbf{F}_q(C_4)$ by factoring q polynomials over $\mathbf{F}_q$ and discarding the handful that had repeated factors. This took under 10 minutes on a single processor. We found that $|C_4(\mathbf{F}_q)| \geq 4779840$, while the Weil bound for a curve of genus at most 1551 is $|C_4(\mathbf{F}_q)| \leq 4102085$. This contradiction shows that $G_0 \neq A_{33}$ and completes the proof.

3.6 Scenic detour: 155-torsion in $J_{C'}(K)$ and an exotic Weierstrass torsion packet on C'

Using the table (14) of Hecke eigenvalues or otherwise, we soon see that $\#J_C(K)_{\mathrm{tors}} \mid 155$; for example, $\#J_C(O_K/\mathfrak{p}_{11}) = 155$, and there can be no 11-torsion because $\#J_C(O_K/\mathfrak{p}) = 4 \cdot 155$ for $\mathbf{N}\mathfrak{p} = 23$. The same bound thus holds for any other abelian surface K-isogenous with J_C. Computing $\#J_C(O_K/\mathfrak{p})$ for further primes $\mathfrak{p}$ suggests that $J_C(O_K/\mathfrak{p})$ has 155-torsion for every prime $\mathfrak{p}$ of O_K other than $\mathfrak{p}_{32}$, and thus that the isogeny class may contain a surface with 155-torsion over K.

We find that in fact $J_{C'}(K) \cong \mathbf{Z}/155\mathbf{Z}$. We already know a 5-torsion point of $J_{C'}(\mathbf{Q})$, so we need only find 31-torsion. A search for points of low height on $C'(K)$ other than the Weierstrass point soon finds the $\mathrm{Gal}(K/\mathbf{Q})$ orbit of

$$Q : (x, y) = (a^4 - 2a^3 + a, 11(13a^4 - 35a^3 + 7a^2 + 28a - 8)) \tag{29}$$

We find that the function

$$f = y + (a^3 - a^2 - a)(4x^2 - 20x + 14) + (7x^2 - 13x + 8) \tag{30}$$

on C' has divisor $2Q + \iota(\sigma Q) + D - 5(P)$, where ι is the hyperellitic involution, P is the Weierstrass point at infinity, σ is our generator of $\mathrm{Gal}(K/\mathbf{Q})$ taking a to $2 - a^2$, and D is the divisor $2x^2 - 10x + 7 = 0$, $y = -22x + 33/2$ such that $5D \sim 5K$. Since $\iota(\sigma Q) + \sigma Q \sim K \sim 2(P)$, we deduce

$$(\sigma Q) - (P) \sim 2((Q) - (P)) + D - K. \tag{31}$$

Applying σ, and noting that P, D, K are σ-invariant, gives

$$(\sigma^2 Q) - (P) \sim 2((\sigma Q) - (P)) + D - K \sim 4((Q) - (P)) + 3(D - K), \tag{32}$$

and then

$$(\sigma^3 Q) - (P)\ 8((Q) - (P)) + 7(D - K), \tag{33}$$

$$(\sigma^4 Q) - (P)\ 16((Q) - (P)) + 15(D - K), \tag{34}$$

and finally

$$(Q) - (P) = (\sigma^5 Q) - (P) \sim 32((Q) - (P)) + 31(D - K). \tag{35}$$

Hence $31((Q) - (P))$ is equivalent to the 5-torsion divisor $31(D - K)$, whence $(Q) - (P)$ is a 155-torsion divisor.

Thus $C'(\bar{\mathbf{Q}})$ contains at least 10 non-Weierstrass points P' such that $(P') - (P)$ is torsion, namely the $\mathrm{Gal}(K/\mathbf{Q})$ orbits of Q and ιQ. This is an "unlikely intersection" for a curve of genus 2 with no automorphisms other than ι and the identity: such curves vary over a 3-dimensional moduli space, so we might expect at most three pairs of non-Weierstrass points in the "Weierstrass torsion packet". I thank Bjorn Poonen for using his `gp` program to check that there are no further such P' on our curve. Poonen notes that already in [Leprévost 1995, p.293] there is an example of a curve C_{27} with six pairs, all in $C_{27}(\mathbf{Q})$ and differing by 27-torsion divisors; but our C' seems to have the largest torsion order among the known examples of such unlikely intersections of a genus-2 curve C with $J_C(\bar{\mathbf{Q}})_{\mathrm{tors}}$.

4 Specializations to $\Sigma\mathrm{L}(\mathbf{F}_{32})$ extensions of Q with low discriminant

We now have a family of degree-33 fields F_j with generic Galois group $\Sigma\mathrm{L}(\mathbf{F}_{32})$. For any rational $j = j_{\mathsf{A}} \neq 0, 1728$, we can compute the discriminant Δ of F_j; this does not require factoring a large polynomial discriminant because we know that all prime factors of Δ other than 2 and 11 appear in the denominator of j or the numerator of j or $j - 1728$. We first tried all $j \in \mathbf{Z}$ with $|j| \leq 10 \cdot 1728$, and also all $j = 1728m/n$ for small m, n. This revealed the outlier F_{-121} with $\Delta = 2^{32}11^{34}$; this is the only example we found for which $\mathrm{Gal}(F_j/\mathbf{Q})$ is smaller than $\Sigma\mathrm{L}(\mathbf{F}_{32})$.

Listing j's in order of increasing Δ, we recognized several of the best j values as j-invariants of elliptic curves with small and smooth conductor. We thus asked the LMFDB for the list of all elliptic curves in the database whose conductors are $\{2, 3, 5, 7, 11\}$-smooth, and tried all of their j-invariants. There were 137612 curves, with 6086 distinct j-invariants other than $0, 1728$. This found several new small values of Δ, corresponding to j-values outside the range of our first search.

In (36) we list the 17 values of j_{A} that yield the fields F_j of smallest Δ that we found. In each case we list also: the LMFDB labels of the elliptic curves $E_{\min}$ of minimal conductor that have j-invariant j_{A}; the factorization of Δ: and the root-discriminant $\Delta^{1/33}$ rounded to the nearest .01 (which is the LMFDB's convention), as a measure of the size of Δ.

Two of those fields arise more than once. The triple coincidence includes $j_{\mathsf{A}} = -2^{15}$ and $j_{\mathsf{A}} = -131^3 11$, which we already know are related by a $\mathfrak{p}_{11}$-isogeny and thus give rise to isomorphic Galois representations mod $\mathfrak{p}_{32}$, but we have no explanation for the third value of j_{A} that yields the same field. Nor can we explain the double appearance of the field of discriminant $2^{36}5^{30}11^{24}$. Curiously $j_{\mathsf{A}} = -15^3$ and $j_{\mathsf{A}} = 255^3$ yield different fields of the same discriminant $2^{32}7^{16}11^{34}$; they

are j-invariants of 2-isogenous elliptic curves with complex multiplication in discriminant -7 and -28, but again we have no explanation (except that we might expect the occasional collision of Δ's when both fields are ramified above the same primes), and it might be a mere curiosity.

j_{A}	$E_{\min}$	Δ	$rd = \Delta^{1/33}$
$-121 = -11^2$	121a1, 121c2	$2^{32}11^{34}$	23.17
$287496 = 66^3$	32a1, 32a2	$2^{78}11^{30}$	45.52
$10976 = 2^5 7^3$	128a1, b1, c1, d1	$2^{88}11^{28}$	48.57
$\begin{cases} -14641/80 = -11^4/2^4 5; \\ -616295051/64000 = -(23\cdot 37/40)^3 \end{cases}$	$\begin{cases} 1210\text{c}1,\ 1210\text{j}1; \\ 1210\text{d}1, 1210\text{i}1 \end{cases}$	$2^{36}5^{30}11^{24}$	52.63
$-937024/9 = -2^6 11^4/3^2$	11616f1, g1, v1, w1	$2^{62}3^{30}11^{24}$	57.11
$2048 = 2^{11}$	200b2, 200d2	$2^{38}5^{16}11^{34}$	57.34
$-3375 = -15^3$	49a2, 49a4	$2^{32}7^{16}11^{34}$	59.51
$16581375 = (3\cdot 5\cdot 17)^3$	49a1, 49a3	$2^{32}7^{16}11^{34}$	59.51
$54000 = 2^4 3^3 5^3$	36a1, 36a2	$2^{52}3^{16}11^{34}$	60.07
$8000 = 20^3$	256a1, a2, d1, d2	$2^{78}11^{34}$	60.88
$-121945/32 = -29^3 5/2^5$	50a2, 50b3	$2^{48}5^{22}11^{28}$	61.30
$-3072 = -2^{12}3$	216a1, 216d1	$2^{40}3^{38}11^{28}$	62.79
$43307231/82944 = 11^2 71^3/(2^{10}3^4)$	726a1, 726f1	$2^{32}3^{30}11^{34}$	62.89
$\begin{cases} -32768 = -2^{15}; \\ -24729001 = -131^3 11; \\ -128667913/4096 = -227^3 11/2^{12} \end{cases}$	$\begin{cases} 121\text{b}1,\ 121\text{b}2; \\ 121\text{a}2,\ 121\text{c}1; \\ 242\text{a}1,\ 242\text{b}1 \end{cases}$	$2^{32}11^{48}$	64.07

(36)

Six of the seventeen j_{A} values are among the thirteen rational j-invariants of CM curves, for discriminants $-7, -8, -11, -12, -16, -28$. Of the remaining seven such discriminants, -3 and -4 correspond to ramified points $j_{\mathsf{A}} = 0, 1728$ of the cover, and the discriminant -27 value $-160^3 3$ (curves 27a1, 27a2) was already on our list of candidates; we added the remaining four (discriminants $-19, -43, -67, -163$), but found no further small Δ. Three of the j_{A} values are j-invariants of non-CM elliptic curves involved in sporadic isogenies, of degrees 11 and 15 (conductors 121 and 50); we tried the remaining ones (from the 17-isogenous curves of conductor 14450 — the 37-isogenous pair in conductor 1225 was already in our list), but again the resulting number fields had considerably larger discriminants than those in (36).

Acknowledgements: This work was supported in part by the Simons Foundation[5]. The calculations were done with Maxima, (Pari-)GP, and Magma. I also thank Bjorn Poonen for information about Weierstrass torsion packets, Drew Sutherland for observing that the model of C' in [CEHJMPV 2025] is not quite reduced, and John Jones for quickly adding the new fields F_j to the LMFDB. Finally I am grateful to the referees for their careful reading of the initial manuscript and for their detailed corrections and suggestions.

[5] Grant #550031 under the Collaboration on Arithmetic Geometry, Number Theory, and Computation.

References

[Barth–Wenz 2019] Dominik Barth and Andreas Wenz: On Elkies' method for bounding the transitivity degree of Galois groups, *J. Symbolic Computation* **108** (Jan.-Feb. 2022), 17-22. arXiv:1905.05624

[Bosman 2011] Johan Bosman: Modular forms applied to the computational inverse Galois problem. preprint, 2011 (arXiv.org:1109.6879v1).

[CEHJMPV 2025] Edgar Costa, Noam D. Elkies, Sachi Hashimoto, Aashraya Jha, Kimball Martin, Bjorn Poonen, and John Voight: A database of curves with modular Jacobians (2025), in preparation; data at https://github.com/edgarcosta/ModularAbelianSurfaces/blob/master/olddata/label_to_curve_QQ.txt

[Elkies 2006] Noam D. Elkies: Shimura Curves for Level-3 Subgroups of the $(2, 3, 7)$ Triangle Group, and Some Other Examples. In: *ANTS-VII: Proceedings of the Seventh Algorithmic Number Theory Symposium, Berlin, Germany, July 2006* (ed. Florian Hess, Sebastian Pauli, and Michael Pohst), Berlin: Springer (*Lect. Notes. in Computer Sci.* **4076**, pages 302–316 (doi: 10.1007/11792086_22; arXiv: 0409020).

[Elkies 2013] Noam D. Elkies: The complex polynomials $P(x)$ with $\mathrm{Gal}(P(x) - t) \cong M_{23}$. In: *ANTS X. Proceedings of the Tenth Algorithmic Number Theory Symposium, San Diego, CA, USA, July 9–13, 2012*. Berkeley, CA: Mathematical Sciences Publishers (MSP), 2013, pages 359–367

[Fu–Stoll 2019] Hang Fu and Michael Stoll: Elliptic curves with common torsion x-coordinates and hyperelliptic torsion packets. Preprint, 2019–2022 (arXiv:1912.09766)

[Leprévost 1995] Franck Leprévost: Jacobiennes de certaines courbes de genre 2 : torsion et simplicité, *J. Th. Nombers de Bordeaux* **7** #1 (1995), 283–306, https://jtnb.centre-mersenne.org/article/JTNB_1995__7_1_283_0.pdf .

[LMFDB] The LMFDB Collaboration: The L-functions and modular forms database, http://www.lmfdb.org and http://beta.lmfdb.org, 2024 [Online; accessed December 2024 and January 2025].

[Poonen 2000] Bjorn Poonen: Genus-two curves with 22 torsion points, *C. R. Acad. Sci. Paris Sér. I Math.* **330** (2000) #7, 573–576 (English, with English and French summaries). doi:10.1016/S0764-4442(00)00222-6; MR1760441

[Poonen 2001] Bjorn Poonen: Computing torsion points on curves, *Experimental Math.* **10** (2001) #3, 449–465. MR1917430

[Takeuchi 1977] K[isao] Takeuchi: Commensurability classes of arithmetic triangle groups, *J. Fac. Sci. Univ. Tokyo* **24** (1977), 201–212.

[Voight 2009] John Voight: Shimura curves of genus at most two, *Math. of Comp.* **78** (#266), April 2009, 115–127 S0025-5718(08)02163-7 (electronically published August 14, 2008); arXiv:0802.0911.

[Voight 2021] John Voight: *Quaternion algebras.* Cham, Switzerland: Springer 2021 (GTM **288**); open access: `https://www.springer.com/us/book/9783030566920`; Version 1.0.6u (May 5, 2024) at `https://math.dartmouth.edu/~jvoight/quat-book.pdf`

Noam D. Elkies
Mathematics Department
Harvard University
1 Oxford Street
Cambridge, MA 02138 USA
elkies@math.harvard.edu