JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Sam FRENGLEY

Explicit 7-torsion in the Tate–Shafarevich groups of genus 2 Jacobians

Tome 37, nº 2 (2025), p. 727-746.

https://doi.org/10.5802/jtnb.1340

e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **37** (2025), 727–746

Explicit 7-torsion in the Tate–Shafarevich groups of genus 2 Jacobians

par Sam FRENGLEY

Résumé. Soit $C/\mathbb{Q}$ une courbe de genre 2 dont la jacobienne $J/\mathbb{Q}$ a une multiplication réelle par un ordre quadratique dans lequel 7 se décompose. Nous décrivons un algorithme qui produit une tordue galoisienne de la quartique de Klein qui paramètrise les courbes elliptiques dont la représentation galoisienne modulo 7 est isomorphe à une sous-représentation de la représentation galoisienne modulo 7 associée à $J/\mathbb{Q}$. En appliquant cet algorithme aux courbes de genre 2 de petit conducteur dans les familles de Bending et Elkies–Kumar nous donnons des exemples de courbes de genre 2 dont les groupes de Tate–Shafarevich contiennent (inconditionellement) un élément non trivial d'ordre 7 visible dans une variété abélienne de dimension 3.

Abstract. Let $C/\mathbb{Q}$ be a genus 2 curve whose Jacobian $J/\mathbb{Q}$ has real multiplication by a quadratic order in which 7 splits. We describe an algorithm which outputs twists of the Klein quartic curve which parametrise elliptic curves whose mod 7 Galois representations are isomorphic to a sub-representation of the mod 7 Galois representation attached to $J/\mathbb{Q}$. Applying this algorithm to genus 2 curves of small conductor in families of Bending and Elkies–Kumar we exhibit a number of genus 2 Jacobians whose Tate–Shafarevich groups (unconditionally) contain a non-trivial element of order 7 which is visible in an abelian three-fold.

1. Introduction

Let K be a number field and let A/K be an abelian variety. For each place v of K we denote the completion of K at v by K_v. We write $G_K = \mathrm{Gal}(\overline{K}/K)$ for the absolute Galois group of K and write $G_v = \mathrm{Gal}(\overline{K_v}/K_v)$. The Tate–Shafarevich group of A/K is the group

$$Ш(A/K) = \ker\left(H^1(G_K, A) \to \prod_v H^1(G_v, A)\right)$$

where v ranges over places of K. The non-trivial elements of the group $Ш(A/K)$ parametrise torsors for A/K which have K_v-rational points for

Manuscrit reçu le 17 mai 2024, révisé le 17 décembre 2024, accepté le 17 janvier 2025.
2020 *Mathematics Subject Classification.* 11G30, 11G10, 14H40.
Mots-clefs. Tate–Shafarevich group, Visibility, Modular curves, Galois representations.

every place v, but no K-points. In this article we prove the following theorem.

Theorem 1. *If $C/\mathbb{Q}$ is one of the genus 2 curves in Table 1.1, then the Jacobian $J = \mathrm{Jac}(C)$ of C is absolutely simple (i.e., J is not isogenous over $\overline{\mathbb{Q}}$ to a product of elliptic curves), has conductor at most $(500\,000)^2$, and the Tate–Shafarevich group $Ш(J/\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$.*

Remark 2. The genus 2 Jacobian $J/\mathbb{Q}$ of conductor 3200^2 in Table 1.1 was included in an appendix to [26] joint with Keller and Stoll where the strong Birch and Swinnerton-Dyer conjecture is also verified for J.

The group $Ш(A/K)$ is a torsion group and is conjectured to be finite. It is conjectured that for every prime number $p > 0$ and each integer $g > 0$ there exists an absolutely simple abelian variety (i.e., one which is not isogenous over $\overline{\mathbb{Q}}$ to a product) of dimension g for which $Ш(A/\mathbb{Q})[p] \neq 0$. Indeed, it is even conjectured that $Ш(A^d/\mathbb{Q})[p] \neq 0$ for a positive proportion of quadratic twists of a *fixed* abelian variety $A/\mathbb{Q}$ (see e.g., [5, Conjecture 1.1]).

In spite of this, for general values of g and p, constructing an example of an absolutely simple g-dimensional abelian variety $A/\mathbb{Q}$ with an p-torsion element contained in $Ш(A/\mathbb{Q})$ is an open problem. By allowing the dimension of A to increase with p, Shnidman and Weiss [40] construct examples of absolutely simple abelian varieties with $Ш(A/\mathbb{Q})[p] \neq 0$. Flynn and Shnidman [21] extended this result to show $Ш(A/\mathbb{Q})[p]$ can be arbitrarily large.

When A has dimension 2, Bruin, Flynn, and Testa [7, 19] found examples of absolutely simple genus 2 Jacobians with 3 and 5-torsion in their Tate–Shafarevich groups. Their approach relies on (p, p)-*descent*. That is, for several explicit examples of genus 2 curves $C/\mathbb{Q}$ they determined the ψ-Selmer groups of their Jacobians $J/\mathbb{Q}$ where ψ is a (p, p)-isogeny (i.e., a polarised isogeny with kernel isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$) for each $p = 3, 5$.

However, performing a (p, p)-descent becomes computationally costly as p increases, due to the need to perform class and unit group calculations in (a subfield of) the field $\mathbb{Q}(J[\psi])$. Our approach is to instead leverage *visibility* (see e.g., [1, 2, 10, 18]) to construct absolutely simple genus 2 Jacobians such that $Ш(J/\mathbb{Q})[7] \neq 0$.

Let K be a number field and let A/K and A'/K be abelian varieties equipped with isogenies $\psi\colon A \to B$ and $\psi'\colon A' \to B'$.

Definition 3. We say that A/K and A'/K are (ψ, ψ')-*congruent* if there exists a G_K-equivariant group isomorphism $\phi\colon A[\psi] \to A'[\psi']$. We say that ϕ is a (ψ, ψ')-*congruence*.

TABLE 1.1. Examples of genus 2 curves $C\colon y^2 = f(x)$ whose Jacobians $J/\mathbb{Q}$ have conductor $N_J < (500\,000)^2$, and such that $Ш(J/\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$ (we do not claim, nor expect, this list to be complete). The Jacobians have real multiplication by the quadratic order $\mathcal{O}_D$ of discriminant D and the subgroup of $Ш(J/\mathbb{Q})$ is made visible by a $(7, \mathfrak{p})$-congruence between $E/\mathbb{Q}$ and $J/\mathbb{Q}$ where $\mathfrak{p}$ divides 7 in $\mathcal{O}_D$. We write $N*$ for an elliptic curve of conductor N which does not appear in the LMFDB (i.e., if $N > 500\,000$). Explicit Weierstrass equations for the corresponding elliptic curves are given in [23]. The curves $C/\mathbb{Q}$ were generated from [4, Theorem 4.1] and [9, 14]. Conductors were computed using [12].

D	$f(x)$	$\sqrt{N_J}$	E
8	$-10(x^6 - 4x^5 - 3x^4 + 8x^3 + 25x^2 + 20x + 5)$	3200	3200.a1
8	$165(x^6 + 6x^5 + 27x^4 - 2x^3 + 45x^2 + 20)$	39325	39325.c1
37	$-13(27x^6 - 54x^5 - 90x^4 + 228x^3 + 15x^2 - 90x - 23)$	73008	73008.n1
8	$-51(x^6 + 6x^5 + 27x^4 - 2x^3 + 45x^2 + 20)$	93925	93925.d1
8	$285(x^6 + 6x^5 + 27x^4 - 2x^3 + 45x^2 + 20)$	117325	117325.c1
8	$-62(9x^6 - 12x^5 + 64x^4 - 56x^3 + 136x^2 - 60x + 84)$	184512	184512.bw1
8	$-46(x^6 + 6x^5 - 20x^4 + 240x^3 + 70x^2 - 84x + 12)$	203136	203136.i2
8	$-5(3x^6 + 12x^5 + 89x^4 - 56x^3 - 7x^2 - 132x + 99)$	211200	211200.c1
8	$465(9x^6 - 12x^5 + 64x^4 - 56x^3 + 136x^2 - 60x + 84)$	216225	432450.ci1
8	$-30(11x^6 - 18x^5 + 47x^4 + 6x^3 + 71x^2 + 18x + 27)$	244800	244800.dc1
8	$-13(x^6 - 2x^5 + 3x^4x^3 - 7x^2 - 2x + 1)$	256880	51376.e1
8	$-390(x^6 + 6x^5 + 27x^4 - 2x^3 + 45x^2 + 20)$	270400	270400.dc2
8	$-177(3x^6 + 12x^4 - 10x^3 - 12x + 11)$	281961	2819610*
8	$-22(x^6 - 24x^5 + 100x^4 + 102x^3 - 80x^2 - 132x - 39)$	302016	302016.p1
8	$-6(13x^6 - 116x^5 - 316x^4 + 58x^3 + 264x^2 - 116x + 13)$	313920	313920.bb1
8	$-55(13x^6 - 116x^5 - 316x^4 + 58x^3 + 264x^2 - 116x + 13)$	329725	659450*
8	$-110(x^6 - 4x^5 - 3x^4 + 8x^3 + 25x^2 + 20x + 5)$	387200	8905600*
8	$11(x^6 + 6x^5 + 11x^4 - 13x^2 + 6x - 2)$	423984	423984.by1

In this case let $\Delta = \mathrm{Graph}\,\phi \subset A \times A'$. An element of $Ш(A/K)$ is said to be *visible* in the abelian variety $Z = (A \times A')/\Delta$ if it is contained in the kernel of the induced homomorphism $H^1(G_K, A) \to H^1(G_K, Z)$.

Visibility is useful for constructing elements of $Ш(A/K)$ since it allows us to transport information between the Mordell–Weil group of B'/K and the Tate–Shafarevich group of A/K. More precisely, if $B(K)/\psi A(K) = 0$ then, under mild hypotheses applied at the bad primes of A and A' and the primes dividing $|\Delta|$ (see [18, Theorem 2.2]), the group $\mathrm{Vis}_Z\, Ш(A/K)$

of elements of $Ш(A/K)$ that are visible in $Z = (A \times A')/\Delta$ is equal to $B'(K)/\psi' A'(K)$.

The central idea for proving Theorem 1 is to construct examples of genus 2 curves $C/\mathbb{Q}$ with the property that there exists a $(7, \psi)$-congruence between an elliptic curve $E/\mathbb{Q}$ and the Jacobian $J = \mathrm{Jac}(C)$ of C, for some isogeny $\psi \colon J \to B$. Assuming that the local conditions are satisfied, it then suffices to show that $B(\mathbb{Q})/\psi J(\mathbb{Q}) = 0$ and that $E(\mathbb{Q})/7E(\mathbb{Q}) \neq 0$ (which in practice is computationally less intensive than performing a ψ-descent on J). This approach is a mirror to that taken by Fisher [18] who used it to visualise elements of order 7 in the Tate–Shafarevich groups of elliptic curves. The main technical contribution of this article is construct examples of elliptic curves which are $(7, \psi)$-congruent to a genus 2 Jacobian.

We ensure the existence of such an isogeny ψ by choosing $J/\mathbb{Q}$ to have real multiplication (RM) by a real quadratic order $\mathcal{O}_D$ of fundamental discriminant $D > 0$. Suppose that 7 splits in $\mathcal{O}_D$ and we have an embedding $\mathcal{O}_D \subset \mathrm{End}_{\mathbb{Q}}(J)$. Writing $(7) = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_D$ by abuse of notation we write $\mathfrak{p} \colon J \to B$ for the isogeny with kernel consisting of those $P \in J(\overline{\mathbb{Q}})$ annihilated by $\mathfrak{p}$. In this case, $\ker \mathfrak{p}$ is isomorphic as a group to $(\mathbb{Z}/7\mathbb{Z})^2$ and under suitable hypotheses (see Lemma 8) comes equipped with a natural alternating bilinear pairing.

In Section 3.2 we describe an algorithm for determining (a q-adic approximation to) a pair of twists of the Klein quartic (the modular curve $X(7)$) which parametrise elliptic curves that are $(7, \mathfrak{p})$-congruent to a fixed genus 2 Jacobian $J/\mathbb{Q}$ with real multiplication by $\mathcal{O}_D$ (our algorithm is subject to the technical hypothesis that $J[\mathfrak{p}]$ is an irreducible $G_{\mathbb{Q}}$-module).

Remark 4. Since abelian surfaces $J/\mathbb{Q}$ with RM by $\mathcal{O}_D$ are modular (this follows from Serre's conjecture [27, 28]) we may associate to J a weight 2 newform with coefficients in $\mathcal{O}_D$ and level $\sqrt{N_J}$, where N_J is the conductor of J (in particular N_J is a perfect square).

We compute these twists of $X(7)$ for examples of genus 2 Jacobians of small conductor provided by the real multiplication families of Bending [3, 4] and of Elkies–Kumar [9, 14]. By searching for rational points on these twists, we find a number of putative examples of $(7, \mathfrak{p})$-congruences between an elliptic curve $E/\mathbb{Q}$ and a genus 2 Jacobian $J/\mathbb{Q}$. Adapting an approach of Fisher [18, Section 6] we prove these congruences in Proposition 22.

For an abelian variety $A/\mathbb{Q}$ we write $A^d/\mathbb{Q}$ for the quadratic twist of A by a squarefree integer $d \in \mathbb{Z}$. Note that simultaneous quadratic twists of $(7, \mathfrak{p})$-congruent pairs remain $(7, \mathfrak{p})$-congruent (cf. [22, Lemma 4.15]). To construct the examples in Theorem 1 we simply search for quadratic twists of the examples in Proposition 22 where there is a rank discrepancy between $E^d/\mathbb{Q}$ and $J^d/\mathbb{Q}$.

TABLE 1.2. Examples of genus 2 curves $C\colon y^2 = f(x)$ whose Jacobians $J/\mathbb{Q}$ have real multiplication by the quadratic order $\mathcal{O}_D$ of discriminant D and such that $Ш(J/\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$. The subgroup of $Ш(J/\mathbb{Q})$ is made visible by a $(7, \mathfrak{p})$-congruence between $E/\mathbb{Q}$ and $J/\mathbb{Q}$ where $\mathfrak{p}$ divides 7 in $\mathcal{O}_D$. We write $N*$ for an elliptic curve of conductor N which does not appear in the LMFDB (i.e., if $N > 500\,000$). Explicit Weierstrass equations for the corresponding elliptic curves are given in [23]. The curves $C/\mathbb{Q}$ were generated from [4, Theorem 4.1] and [9, 14]. Conductors were computed using [12].

D	$f(x)$	$\sqrt{N_J}$	E
8	$-10(x^6 - 4x^5 - 3x^4 + 8x^3 + 25x^2 + 20x + 5)$	3200	3200.a1
29	$-2470(8x^6-2x^5+68x^4+221x^3+122x^2+986x+1588)$	40019200	760364800*
37	$-39(x^6 - 45x^4 - 68x^3 + 504x^2 + 180x - 1193)$	73008	73008.n1
44	$-39(14x^6 - 30x^5 + 85x^4 + 700x^3 - 1325x^2 + 3000x + 18000)$	608400	608400*
57	$1479(80x^6 + 279x^4 + 186x^3 + 243x^2 + 324x + 108)$	590609070	7677917910*

In addition to Theorem 1 we prove that there exist examples of such genus 2 Jacobians with 7-torsion in their Tate–Shafarevich groups and with real multiplication by $\mathcal{O}_D$ for several fundamental discriminants $D > 0$.

Theorem 5. *For each $D = 8$, 29, 37, 44, and 57 there exists an absolutely simple genus 2 Jacobian $J/\mathbb{Q}$ with real multiplication by $\mathcal{O}_D$ such that $Ш(J/\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$. Examples are furnished by the Jacobians of the curves $C\colon y^2 = f(x)$ given in Table 1.2.*

In [26, A.3] it is observed that the Birch and Swinnerton-Dyer conjecture predicts that $Ш(J^{-11}/\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$, where $J/\mathbb{Q}$ is the Jacobian of the genus 2 curve with LMFDB label 385641.a.385641.1. Since J has RM by $\mathcal{O}_8$ it is natural to ask whether the 7-torsion in $Ш(J^{-11}/\mathbb{Q})$ is made visible by a $(7, \mathfrak{p})$-congruence with an elliptic curve. By computing the relevant twists of $X(7)$ we give evidence that this is not the case (see Section 6).

Conjecture 6. *Let $C/\mathbb{Q}$ be the genus 2 curve with LMFDB label* 385641.a.385641.1 *and let $J/\mathbb{Q}$ be its Jacobian. There exists a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$ contained in $Ш(J^{-11}/\mathbb{Q})$ that is not visible in an abelian 3-fold.*

1.1. Outline of the paper. We begin by discussing several well known facts about the modular curve $X(p)$ in Section 2.1. In Section 2.2, following [35, Section 4.4], we recall the moduli interpretation for twists of $X(p)$, which in Section 2.3 we relate to the torsion of genus 2 curves with Jacobians having real multiplication (cf. [18]). In Section 2.4 we specialise to the case when $p = 7$ and discuss the invariant theory of the Klein quartic $X(7)$ following [17].

In Section 3.2 we present our main algorithm. It takes as input a genus 2 Jacobian $J/\mathbb{Q}$ with RM by an order in which 7 splits, and outputs four twists of $X(7)$ which parametrise elliptic curves $(7, \mathfrak{p})$-congruent to $J/\mathbb{Q}$.

The outputs of the algorithm in Section 3.2 are not guaranteed to be correct, however in Section 4 we prove that the output is correct in many cases (for example for the curves in Tables 1.1 and 1.2). In particular, in Section 4 we prove that the twists we obtain are isomorphic to those which parametrise elliptic curves $(7, \mathfrak{p})$-congruent to J.

In Section 5 we prove Theorems 1 and 5 by proving that the pairs (E, J) in Tables 1.1 and 1.2 are $(7, \mathfrak{p})$-congruent, and by checking that the local hypotheses in [18, Theorem 2.2] are satisfied.

Finally in Section 6 we give explicit examples of the Klein quartic twists associated to the Jacobian of the genus 2 curve with LMFDB label `385641.a.385641.1`. By searching for rational points on these twists, we give evidence towards Conjecture 6.

2. The modular curve $X(p)$ and its twists $X_M^{\pm}(p)$

We recall a number of standard facts about the modular curve $X(p)$ and its twists $X_M^{\pm}(p)$ following e.g., [17] and [35]. In the case when $p = 7$ the curve $X(7)$ is the Klein quartic [29] (see [13] for a detailed discussion).

Let K be a field of characteristic zero. A symplectic abelian group over K is a pair (M, e_M) where M is a G_K-module equipped with a (G_K-equivariant) alternating, bilinear pairing $e_M \colon M \times M \to \overline{K}^{\times}$. We equip $\mu_p \times \mathbb{Z}/p\mathbb{Z}$ with the natural alternating pairing $\langle (\zeta, n), (\xi, m) \rangle = \zeta^m \xi^{-n}$.

2.1. The modular curve $X(p)$. Let E/K be an elliptic curve defined over a field K of characteristic zero. If p is a prime number, we equip $E[p]$ with the structure of a symplectic abelian group via the p-Weil pairing $e_{E,p} \colon E[p] \times E[p] \to \mu_p$.

Let $Y(p)/\mathbb{Q}$ denote the geometrically irreducible (non-compact) modular curve parametrising elliptic curves with full (symplectic) level p structure. Explicitly, for each field $K/\mathbb{Q}$ the K-points on $Y(p)$ parametrise (isomorphism classes of) pairs (E, ι) where E/K is an elliptic curve and $\iota \colon \mu_p \times \mathbb{Z}/p\mathbb{Z} \cong E[p]$ is a G_K-equivariant isomorphism of symplectic abelian groups. Let $X(p)$ denote the smooth compactification of $Y(p)$.

The group Γ_p of symplectic automorphisms of $\mu_p \times \mathbb{Z}/p\mathbb{Z}$ acts naturally on $Y(p)$ on the right via $(E, \iota) \mapsto (E, \gamma\iota)$. As an abstract group Γ_p is isomorphic to $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, but it comes equipped with a non-trivial action of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. The matrix $\pm I$ acts trivially on $Y(p)$ and therefore the action of Γ_p factors through $\Gamma_p/\{\pm I\}$. This action extends to an action on $X(p)$, and the quotient realises the forgetful morphism $X(p) \to X(1)$ given by taking j-invariants.

2.2. The twist $X_M^{\pm}(p)$. Let (M, e_M) be a symplectic abelian group over K. Let r be an integer coprime to p and suppose that there exists a $\overline{K}$-isomorphism $\phi\colon M \cong \mu_p \times \mathbb{Z}/p\mathbb{Z}$ such that $\langle \phi(P), \phi(Q) \rangle = e_M(P,Q)^r$ for each $P, Q \in \mu_p \times \mathbb{Z}/p\mathbb{Z}$.

By the twisting principle we may attach to ϕ a cohomology class $\xi \in H^1(G_K, \Gamma_p)$. We have an inclusion $\Gamma_p/\{\pm I\} \hookrightarrow \mathrm{Aut}(X(p))$ and therefore an induced map on cohomology $H^1(G_K, \Gamma_p) \to H^1(G_K, \mathrm{Aut}(X(p)))$. The image of ξ corresponds (again by the twisting principle) to a twist $X_M^r(p)$ of $X(p)$.

The following lemma is well known and follows by construction (cf. [35, Section 4.4]).

Lemma 7. *For each field L/K the L-rational points on $X_M^r(p)$ correspond to pairs (E, ϕ) where E/L is an elliptic curve and $\phi\colon M \cong E[p]$ is an isomorphism of G_L-modules for which $e_{E,p}(\phi(P), \phi(Q)) = e_M(P,Q)^r$ for each $P, Q \in M$.*

If a is an integer coprime to p, pre-composing an isomorphism $\phi\colon M \cong E[p]$ with the multiplication-by-a-map on M yields an isomorphism ϕ' for which $e_{E,p}(\phi'(P), \phi'(Q)) = e_M(P,Q)^{a^2 r}$. It therefore suffices to consider the class of r in $(\mathbb{Z}/p\mathbb{Z})^\times$ modulo squares. We write $X_M(p) = X_M^+(p)$ when r is a square in $(\mathbb{Z}/p\mathbb{Z})^\times$ and $X_M^-(p)$ when r is not a square in $(\mathbb{Z}/p\mathbb{Z})^\times$.

2.3. The twist $X_{J[\mathfrak{p}]}^r(p)$. Let C/K be a genus 2 curve and let $J = \mathrm{Jac}(C)$ be the Jacobian of C. Let $\widehat{J}$ denote the dual of J and equip J with the canonical principal polarisation $\lambda\colon J \to \widehat{J}$ arising from the theta divisor. The principal polarisation λ induces an involution on the endomorphism ring of J known as the *Rosati involution.* Precisely, if $\psi \in \mathrm{End}(J)$ then the Rosati involution is given by $\psi \mapsto \psi^\dagger = \lambda^{-1}\widehat{\psi}\lambda$. Here $\widehat{\psi}\colon \widehat{J} \to \widehat{J}$ denotes the dual isogeny.

Let $D \equiv 0, 1 \pmod 4$ be a positive non-square integer and let $\mathcal{O}_D$ be the quadratic ring of discriminant D. We say that J has *real multiplication (RM) by $\mathcal{O}_D$* if there exists an inclusion $\mathcal{O}_D \hookrightarrow \mathrm{End}_K^\dagger(J)$ where $\mathrm{End}_K^\dagger(J) \subset \mathrm{End}_K(J)$ is the subring of endomorphisms fixed by the Rosati involution.

The choice of principal polarisation λ induces the alternating, bilinear p-Weil pairing $e_{J,p}\colon J[p] \times J[p] \to \mu_p$.

Lemma 8. *Let J/K be a genus 2 Jacobian with RM by $\mathcal{O}_D$. Suppose that p is a prime number such that p splits as a product $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in $\mathcal{O}_D$. Then there exists an isomorphism of G_K-modules $J[p] \cong J[\mathfrak{p}] \oplus J[\overline{\mathfrak{p}}]$. Moreover,* *the p-Weil pairing $e_{J,p}$ restricts to an alternating pairing $J[\mathfrak{p}] \times J[\mathfrak{p}] \to \mu_p$, and likewise for $J[\bar{\mathfrak{p}}]$.*

Proof. This is [9, Lemma 3.4], cf. the proof of [18, Proposition 6.1] when $\mathcal{O}_D = \mathbb{Z}[\sqrt{2}]$. □

Note that by Lemma 8 we may define the twists $X^{\pm}_{J[\mathfrak{p}]}(p)$ and $X^{\pm}_{J[\bar{\mathfrak{p}}]}(p)$ which (by Lemma 7) parametrise elliptic curves which are $(p, \mathfrak{p})$-congruent (respectively $(p, \bar{\mathfrak{p}})$-congruent) to the genus 2 Jacobian J/K.

2.4. Explicit twisting for $X(7)$. Following [17] we give an explicit description for the twists $X^{\pm}_M(7)$ as plane quartic curves. Recall that we write Γ_7 for the automorphism group (scheme) of the symplectic abelian group $\mu_7 \times \mathbb{Z}/7\mathbb{Z}$. Following Klein [13, 17, 29] consider the representation $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) \to \mathrm{GL}_3(\overline{K})$ which maps the generators $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ to

$$\frac{1}{\sqrt{-7}}\begin{pmatrix} \zeta_7 - \zeta_7^6 & \zeta_7^2 - \zeta_7^5 & \zeta_7^4 - \zeta_7^3 \\ \zeta_7^2 - \zeta_7^5 & \zeta_7^4 - \zeta_7^3 & \zeta_7 - \zeta_7^6 \\ \zeta_7^4 - \zeta_7^3 & \zeta_7 - \zeta_7^6 & \zeta_7^2 - \zeta_7^5 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \zeta_7 & 0 & 0 \\ 0 & \zeta_7^4 & 0 \\ 0 & 0 & \zeta_7^2 \end{pmatrix}.$$

Composing with the natural $\overline{K}$-isomorphism $\Gamma_7 \cong \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ gives a G_K-equivariant homomorphism $\rho\colon \Gamma_7 \to \mathrm{GL}_3(\overline{K})$. When Γ_7 acts on $\mathbb{P}^2$ via ρ the Klein quartic curve $X(7) \subset \mathbb{P}^2$ given by

$$X(7) : x_0^3 x_1 + x_1^3 x_2 + x_0 x_2^3 = 0$$

is fixed.

Let $\phi\colon M \cong \mu_7 \times \mathbb{Z}/7\mathbb{Z}$ be a symplectic $\overline{K}$-isomorphism. Let $\xi\colon G_K \to \mathrm{GL}_3(\overline{K})$ denote the cocycle obtained from ϕ by the twisting principle. Explicitly, ξ may be taken to be the cocycle $\sigma \mapsto \rho(\sigma(\phi)\phi^{-1})$ where $\sigma(\phi)\colon M \cong \mu_7 \times \mathbb{Z}/7\mathbb{Z}$ is the $\overline{K}$-isomorphism given by $P \mapsto \sigma(\phi(\sigma^{-1}P))$. By Hilbert's Theorem 90 the cocycle ξ is a coboundary, that is, there exists a matrix $A \in \mathrm{GL}_3(\overline{K})$ such that $\sigma(A^{-1})A = \xi(\sigma)$ for every $\sigma \in G_K$.

Lemma 9. *The curves $X_M(7)$ and $X^-_M(7)$ are isomorphic to the images of the morphisms $X(7) \to \mathbb{P}^2$ given by*

$$\mathbf{x} \mapsto A\mathbf{x} \quad \textit{and} \quad \mathbf{x} \mapsto A^{-T}\mathbf{x}$$

respectively. Here $\mathbf{x}$ is a point in $\mathbb{P}^2$ written as a column vector and A^{-T} denotes the inverse transpose of A.

Proof. The proof is identical to [17, Lemma 3.2]. □

Finally, we note that it is simple to recover the moduli interpretation for a given twist of $X(7)$ following [17, Section 4.1] (cf. [35, Section 7.1]).

Lemma 10. *Let $\mathcal{X}/K$ be a twist of the Klein quartic given by the vanishing of a homogeneous quartic polynomial $\mathcal{F}(x_0, x_1, x_2)$ in $\mathbb{P}^2$. The j-invariant map $\mathcal{X} \to X(1)$ is defined over K and is given by $1728\frac{c_4^3}{c_4^3 - c_6^2}$ where c_4 and c_6 are defined by*

$$D = \frac{-1}{54} \times \begin{vmatrix} \frac{\partial^2 \mathcal{F}}{\partial x_0^2} & \frac{\partial^2 \mathcal{F}}{\partial x_0 \partial x_1} & \frac{\partial^2 \mathcal{F}}{\partial x_0 \partial x_2} \\ \frac{\partial^2 \mathcal{F}}{\partial x_0 x_1} & \frac{\partial^2 \mathcal{F}}{\partial x_1^2} & \frac{\partial^2 \mathcal{F}}{\partial x_1 \partial x_2} \\ \frac{\partial^2 \mathcal{F}}{\partial x_0 x_2} & \frac{\partial^2 \mathcal{F}}{\partial x_1 \partial x_2} & \frac{\partial^2 \mathcal{F}}{\partial x_2^2} \end{vmatrix},$$

$$c_4 = \frac{1}{9} \times \begin{vmatrix} \frac{\partial^2 \mathcal{F}}{\partial x_0^2} & \frac{\partial^2 \mathcal{F}}{\partial x_0 \partial x_1} & \frac{\partial^2 \mathcal{F}}{\partial x_0 \partial x_2} & \frac{\partial D}{\partial x_0} \\ \frac{\partial^2 \mathcal{F}}{\partial x_0 \partial x_1} & \frac{\partial^2 \mathcal{F}}{\partial x_1^2} & \frac{\partial^2 \mathcal{F}}{\partial x_1 \partial x_2} & \frac{\partial D}{\partial x_1} \\ \frac{\partial^2 \mathcal{F}}{\partial a \partial x_2} & \frac{\partial^2 \mathcal{F}}{\partial x_1 \partial x_2} & \frac{\partial^2 \mathcal{F}}{\partial x_2^2} & \frac{\partial D}{\partial x_2} \\ \frac{\partial D}{\partial x_0} & \frac{\partial D}{\partial x_1} & \frac{\partial D}{\partial x_2} & 0 \end{vmatrix}, \quad c_6 = \frac{1}{14} \times \begin{vmatrix} \frac{\partial \mathcal{F}}{\partial x_0} & \frac{\partial \mathcal{F}}{\partial x_1} & \frac{\partial \mathcal{F}}{\partial x_2} \\ \frac{\partial D}{\partial x_0} & \frac{\partial D}{\partial x_1} & \frac{\partial D}{\partial x_2} \\ \frac{\partial c_4}{\partial x_0} & \frac{\partial c_4}{\partial x_1} & \frac{\partial c_4}{\partial x_2} \end{vmatrix}.$$

3. Computing approximations to twists of $X(7)$

Fix a primitive 7^{th} root of unity ζ_7, and let $J/\mathbb{Q}$ be the Jacobian of a genus 2 curve $C/\mathbb{Q}$. Suppose that J has RM by the quadratic order $\mathcal{O}_D$ of fundamental discriminant $D > 0$. Suppose that 7 splits in $\mathcal{O}_D$ and that we have a factorisation $(7) = \mathfrak{p}\bar{\mathfrak{p}}$ (where $\bar{\mathfrak{p}}$ denotes the conjugate of $\mathfrak{p}$). We assume throughout this section that $J[\mathfrak{p}]$ is an irreducible $G_{\mathbb{Q}}$-module.

Let $\mathcal{K} = J/\{\pm 1\}$ denote the Kummer surface of J. We identify $\mathcal{K}$ with a singular quartic surface in $\mathbb{P}^3$ by the embedding in [8, (3.1.8)]. Let x_J denote the quotient morphism $J \to \mathcal{K}$. If $\psi \colon J \to J'$ is an isogeny we write $\mathcal{K}[\psi] = x_J(J[\psi])$.

3.1. Hilbert's Theorem 90 is effective. To compute twists of $X(7)$ using Lemma 9 we will need to compute matrices which realise a given cocycle as a coboundary. Towards this, note that the standard proof of Hilbert's Theorem 90 is "nearly" effective. Indeed following [38, Proposition X.3] let L/K be a finite extension of infinite fields, let $\xi \in H^1(\mathrm{Gal}(L/K), \mathrm{GL}_n(L))$ be a 1-cocycle, and choose an element $c \in \mathrm{GL}_n(L)$. Define a matrix $b \in \mathrm{M}_n(L)$ by the Poincaré series

$$b = \sum_{\sigma \in \mathrm{Gal}(L/K)} \xi(\sigma)\sigma(c).$$

If c is chosen so that b is invertible, then $\xi(\sigma) = \sigma(b)^{-1} b$ and it is immediate that ξ is a coboundary. If L is infinite the linear independence of field embeddings guarantees the existence of c. Indeed, for a fixed cocycle ξ, the failure of b to be invertible is a Zariski closed condition on the matrix c. In particular, for a generic choice of c, the matrix b will be invertible. The proof therefore suggests an algorithm.

Algorithm 11 Generating matrices which realise Hilbert's Theorem 90.

Input: A cocycle $\xi \in H^1(\mathrm{Gal}(L/K), \mathrm{GL}_n(L))$.
Output: A matrix $b \in \mathrm{GL}_n(L)$ such that $\xi(\sigma) = \sigma(b)^{-1}b$ for each $\sigma \in \mathrm{Gal}(L/K)$.

```
1: Choose "randomly" a matrix c ∈ GL_n(L).
2: Compute the matrix b = ∑_σ ξ(σ)σ(c).
3: if det(b) ≠ 0 then
4:     return b
5: else
6:     Return to Step 1.
7: end if
```

Remark 12. In Step 1 of Algorithm 11 the user must choose a matrix $c \in \mathrm{GL}_n(L)$. In our application the extension $L/\mathbb{Q}$ will be a finite extension and we will have access to a LLL-reduced $\mathbb{Z}$-basis $\{a_1, \ldots, a_m\}$ for the ring of integers $\mathcal{O}_L \subset L$. We choose "small" elements of L by generating a tuple $x_1, \ldots, x_m \in \{0, \pm 1\}$ and considering the element $\sum_{i=1}^m x_i a_i \in \mathcal{O}_L$. This approach extends to choosing a matrix $c \in \mathrm{GL}_n(L)$ by choosing the n^2 entries as described (in practice, we also choose almost all x_i to be equal to zero).

Remark 13. In principle the iteration in Step 6 in Algorithm 11 may be called many times. In practice, however, we have found very few instances when Algorithm 11 fails to terminate in one iteration.

3.2. The main algorithm. We write $L = \mathbb{Q}(\mathcal{K}[\mathfrak{p}])$. Note that for generic $J/\mathbb{Q}$, we have an isomorphism of abstract groups

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})/\{\pm 1\}.$$

Suppose that we have degree 24 polynomials $g_1(t)$, $g_2(t)$, $g_3(t) \in \mathbb{Q}[t]$ such that

$$\mathcal{K}[\mathfrak{p}] \subset \{(1 : \alpha_1 : \alpha_2 : \alpha_3) \in \mathcal{K} : g_1(\alpha_1) = g_2(\alpha_2) = g_3(\alpha_3) = 0\} \cup \{(0 : 0 : 0 : 1)\}. \tag{3.1}$$

In Section 3.3 we discuss how the polynomials $g_i(t)$ may be computed.

We fix an auxiliary prime $q \neq 7$ not dividing the discriminant of $g_1(t)$ and at which J has good reduction. Further suppose that the minimal polynomial of ζ_7 is irreducible over $\mathbb{F}_q$ and that L is equal to the splitting field of $g_1(t)$. Let $\mathfrak{q}$ be a prime of L dividing q and denote by $L_\mathfrak{q}$ and $l_\mathfrak{q}$ the completion and residue field of L at $\mathfrak{q}$ respectively.

Our algorithm proceeds as follows:

1: We compute the Galois group of $g_1(t)$ using `GaloisGroup` in `Magma`. This gives a group $G \subset S_{24}$ and a G-set $\{r_1, \dots, r_{24}\}$ of ($\mathfrak{q}$-adic approximations to) the roots of $g_1(t)$ in $L_\mathfrak{q}$ such that G gives the action of $\mathrm{Gal}(L/\mathbb{Q})$ on the roots of $g_1(t)$ in L.

2: We compute (a $\mathfrak{q}$-adic approximation to) an embedding $\mathbb{Q}_q(\zeta_7) \hookrightarrow L_\mathfrak{q}$ by computing a $\mathfrak{q}$-adic approximation to ζ_7.

3: We compute a $\mathbb{Z}/7\mathbb{Z}$-basis $\{\overline{P}, \overline{Q}\}$ for $J(l_\mathfrak{q})[\mathfrak{p}]$ such that $e_{J,7}(\overline{P}, \overline{Q}) = \zeta_7$ (via the `Magma` intrinsic `WeilPairing`). This uniquely determines a pair $x_J(P), x_J(Q) \in \mathcal{K}(L_\mathfrak{q})$ which reduce modulo $\mathfrak{q}$ to $x_J(\overline{P})$ and $x_J(\overline{Q})$ respectively.

4: Let $\phi\colon J[\mathfrak{p}] \cong \mu_7 \times \mathbb{Z}/7\mathbb{Z}$ be the isomorphism given by $P \mapsto (\zeta_7, 0)$ and $Q \mapsto (1, 1)$. We explicitly determine the 1-cocycle

$$\xi\colon \mathrm{Gal}(L/\mathbb{Q}) \cong G \to \mathrm{GL}_3(\mathbb{Q}(\zeta_7))$$

given by $\sigma \mapsto \rho(\sigma(\phi)\phi^{-1})$ where ρ is the representation given in Section 2.4.

5: We compute (a $\mathfrak{q}$-adic approximation to) a matrix $A \in \mathrm{GL}_3(L) \subset \mathrm{GL}_3(L_\mathfrak{q})$ which realises ξ as a coboundary, using Algorithm 11.

6: We twist $X(7)$ by A and A^{-T} to obtain curves $\mathcal{X}^\pm \subset \mathbb{P}^2_{L_\mathfrak{q}}$. By Lemma 9 these twists are $\mathfrak{q}$-adic approximations to the Klein quartic twists $X^\pm_{J[\mathfrak{p}]}(7) \subset \mathbb{P}^2_\mathbb{Q}$. After normalising each equation so that the first non-zero coefficient is equal to 1, the curves obtained therefore have coefficients in $\mathbb{Q}$ (up to a numerical error).

7: We recognise the coefficients of the twists $\mathcal{X}^\pm$ as rational numbers using the LLL algorithm.

8: We minimise and reduce the models for $\mathcal{X}^\pm$ using the algorithm of Elsenhans–Stoll [16], which is implemented in `Magma` as the function `MinRedTernaryForm`.

Remark 14. Computing the matrix $A \in \mathrm{GL}_3(L_\mathfrak{q})$ must be done with some care in order to control coefficient explosion (and to minimise the $\mathfrak{q}$-adic precision we must carry throughout the calculation). In our implementation we assume that $J[\mathfrak{p}]$ is an irreducible $G_\mathbb{Q}$-module and (heavily) rely on the following observation:

Let α be a root of $g_1(t)$ (so that L is the splitting field of $\mathbb{Q}(\alpha)$). Since the Galois module $J[\mathfrak{p}]$ is irreducible, there exists a subfield $\mathbb{Q} \subset K \subset \mathbb{Q}(\alpha)$ (which is unique up to conjugacy) such that $\mathcal{K}[\mathfrak{p}]$ contains a $\mathrm{Gal}(L/K)$-stable "cyclic subgroup" (or more precisely, the image of a cyclic subgroup of $J[\mathfrak{p}]$). From the properties of the Weil pairing we have $L = \widetilde{K}(\zeta_7)$, where $\widetilde{K}$ is the Galois closure of K in L. We first compute an LLL-reduced basis $\{1, k_1, \dots, k_7\}$ for $K/\mathbb{Q}$. The elements $k\zeta_7^i$ span $L/\mathbb{Q}$ where $0 \le i \le 6$ and

k ranges over the $\mathrm{Gal}(L/\mathbb{Q})$-conjugates of k_j for each $1 \le j \le 7$. We then apply Algorithm 11 noting Remark 12.

3.3. Computing the polynomials $g_i(t)$. It remains to describe how the polynomials $g_1(t)$, $g_2(t)$, and $g_3(t)$ which cut out $\mathcal{K}[\mathfrak{p}]$ may be computed. Let $C/\mathbb{Q}$ be a genus 2 curve given by a Weierstrass equation $C : y^2 = f(x)$ whose Jacobian $J/\mathbb{Q}$ has RM by $\mathcal{O}_D$, and such that 7 splits in $\mathcal{O}_D$.

Our approach follows that of Fisher [18, Theorem 6.3]. Using the analytic Jacobian machinery in `Magma` (in particular the functions `AnalyticJacobian` and `EndomorphismRing`) we compute complex approximations to a $\mathfrak{p}$-torsion divisor $\mathfrak{D} = (x_1, y_1) + (x_2, y_2) - (\infty^+ + \infty^-) \in J(\overline{\mathbb{Q}})$.

The model for the Kummer surface $\mathcal{K}$ of J given in [8, Chapter 3] and maps $\mathfrak{D}$ to the point $(1 : x_1+x_2 : x_1x_2 : \beta_0) \in \mathcal{K}$ where $\beta_0 \in \mathbb{Q}(x_1, x_2, y_1, y_2)$ is the rational function in [8, (3.1.4)]. Using the LLL algorithm we compute polynomials $h_1(t)$, $h_2(t)$, and $h_3(t) \in \mathbb{Q}(t)$ which approximate the minimal polynomials of $x_1 + x_2$, x_1x_2, and β_0 (in particular we utilise the `Magma` function `MinimalPolynomial`). Using the description of the multiplication-by-n-map on $\mathcal{K}$ given in [8, Chapter 3] it is simple to verify (unconditionally) that the polynomials $h_i(t)$ cut out a 7-torsion point in $\mathcal{K}(\overline{\mathbb{Q}})$. Polynomials $g_i(t)$ which satisfy (3.1) are then the product over the distinct polynomials $h_i(t)$ occurring for such divisors $\mathfrak{D}$.

When $D = 8$ we also have the following approach which avoids the numerical instability issues which can occur when using `AnalyticJacobian`.

3.3.1. *A numerically stable approach when $D = 8$.* Fix an isomorphism $\mathcal{O}_8 \cong \mathbb{Z}[\sqrt{2}]$. The prime number 7 is a norm from $\mathbb{Z}[\sqrt{2}]$ and we may write $(7) = (3 + \sqrt{2})(3 - \sqrt{2})$. Let $[\sqrt{2}]\colon J \to J$ denote the multiplication-by-$\sqrt{2}$-map on J. The morphism $[\sqrt{2}]$ is a Richelot isogeny and using the approach in [33, Section 5.7] (which is implemented in [32]) we determine explicit polynomials giving the morphism $[\sqrt{2}]\colon \mathcal{K} \to \mathcal{K}$ induced by the action of $\sqrt{2}$ on J.

Remark 15. By interpolation it is not difficult to give an explicit morphism $\mathcal{K} \to \mathcal{K}$ realising the $\sqrt{2}$-action on the Jacobian of the generic member of the generic family of genus 2 curves $\mathcal{C}/\mathbb{Q}(A, P, Q)$ provided by Bending [3, 4]. We record explicit equations for this (generic) morphism in [23].

Formulae for the multiplication-by-3-map $[3]\colon \mathcal{K} \to \mathcal{K}$ are given in [8, Section 3.5]. Note that $\mathcal{K}[3+\sqrt{2}] \cup \mathcal{K}[3-\sqrt{2}]$ is exactly the set $\{P \in \mathcal{K} : 3P = \sqrt{2}P\}$. By taking successive resultants (and fixing a choice of sign so that $\mathfrak{p} = (3 \pm \sqrt{2}))$ it is simple to compute polynomials $g_1(t), g_2(t), g_3(t) \in \mathbb{Q}[t]$ satisfying (3.1).

3.4. Outputs of the main algorithm. We provide a `Magma` implementation of the algorithm described in Section 3.2. The main non-trivial input in the algorithm is a genus 2 curve $C/\mathbb{Q}$ with RM by an order $\mathcal{O}_D$ in which 7 splits. The fundamental discriminants $D < 100$ for which this occurs are $D = 8$, 29, 37, 44, 53, 57, 60, 65, 85, 88, 92, and 93.

A generic family of genus 2 curves $C/\mathbb{Q}$ whose Jacobians have RM by $\mathcal{O}_8$ are given by Bending [3, 4], who also records many examples of small conductor in [3, Appendix A]. Bending's family is given by a triple of parameters $A, P, Q \in \mathbb{Q}$. It is simple to search for further examples of small conductor (noting from [3, Section 6.3] that it is often useful to specialise at $P \in \{\pm 1, \pm 1/2, \pm 1/3, \pm 1/5\}$). Combining these with the examples found in the LMFDB [30] we obtain a small (non-exhaustive) database of curves with RM by $\mathbb{Z}[\sqrt{2}]$ and whose Jacobians have conductor $\sqrt{N_J} \leq 500\,000$ (these may be found in [23]).

Similar generic families are provided for each $D = 8$, 29, 37, 44, and 53 in [9] building on work of Elkies–Kumar [14], who compute the moduli of such curves for all fundamental discriminants $D < 100$. Some examples of curves with RM by $\mathcal{O}_D$ and with small conductor are recorded in [14]. We record a (non-exhaustive) list of such curves with $\sqrt{N_J} \leq 500\,000$ in [23]. Note that when $D > 17$ the moduli space of curves with RM by $\mathcal{O}_D$ is not rational, so examples are sparser than when $D = 8$.

We run the algorithm in Section 3.2 for each curve recorded in [23].

Remark 16. It would be interesting to compute the twists $X^{\pm}_{\mathcal{J}[\mathfrak{p}]}(7)$ for the Jacobian $\mathcal{J}$ of the generic curves $\mathcal{C}/\mathbb{Q}(a, b, c)$ with RM by $\mathcal{O}_D$ given in [3, 4] and [9] for each $D = 8$, 29, 37, 44, and 53 (i.e., those D where 7 splits in $\mathcal{O}_D$ and for which [9] gives a generic model for a curve by $\mathcal{O}_D$). Unfortunately the algorithm we describe is ill suited to this task. One might hope to interpolate over twists computed for a large number of specialisations. However these twists are only defined up to the action of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{P}^2) \cong \mathrm{PGL}_3(\mathbb{Q})$ and our algorithm for generating matrices which satisfy Hilbert's Theorem 90 does not do so in a compatible way (it requires a choice of $\mathfrak{p}|7$, a choice of basis for $J[\mathfrak{p}]$, and a "randomly" generated matrix).

4. Proving twists of $X(7)$ are isomorphic to $X^{\pm}_M(7)$

Let $M/\mathbb{Q}$ be an irreducible $G_{\mathbb{Q}}$-module and let $\mathcal{X}/\mathbb{Q}$ be a plane quartic curve (in our case we will take $M = J[\mathfrak{p}]$ and $\mathcal{X}$ to be an output of the algorithm in Section 3.2). We now outline an approach for proving that $\mathcal{X}$ is isomorphic to a twist $X^{\pm}_M(7)$ of the Klein quartic (for some choice of sign). We assume that $\mathcal{X}$ is a twist of $X(7)$ (note that this is simple to check by computing Dixmier–Ohno invariants [11, 15, 34] in `Magma`).

For the purpose of proving Theorem 1 it suffices to consider only the case when $\mathcal{X}$ has a rational point (i.e., it suffices to recall [18, Lemma 6.2], see Lemma 18 below). In Section 4.2 we note how one may prove that a twist is isomorphic to $X^{\pm}_M(7)$ more generally.

4.1. When $\mathcal{X}$ has a rational point. Let K be a field of characteristic zero. Suppose that $\mathcal{X}$ has a K-rational point which corresponds (through the moduli interpretation in Lemma 10) to an elliptic curve E/K (defined up to quadratic twist) with j-invariant $j(E) \neq 0, 1728, \infty$. In this case, the following lemma reduces the problem of showing that $\mathcal{X}$ is isomorphic to $X_M^{\pm}(7)$ to the problem of showing that $X_E(7)$ is isomorphic to $X_M^{\pm}(7)$.

Lemma 17. *Let $\mathcal{X}/K$ be a twist of $X(7)$ and suppose that there exists a point $P \in \mathcal{X}(K)$ with $j(P) \neq 0, 1728, \infty$. If E/K is an elliptic curve with $j(E) = j(P)$ then $\mathcal{X}$ is isomorphic to $X_E(7)$ over K.*

Proof. Let $\varphi\colon \mathcal{X} \cong X_E(7)$ be a $\overline{K}$-isomorphism. By composing with a $\overline{K}$-automorphism of $X_E(7)$ we may assume that $\varphi(P)$ is equal to the tautological point $Q = (E, \mathrm{id}) \in X_E(7)(K)$. Since P and Q are K-rational, for each $\sigma \in G_K$ we have $\sigma\varphi\sigma^{-1}(P) = Q$, so that $\varphi^{-1}\sigma\varphi\sigma^{-1}(P) = P$ for each $\sigma \in G_K$. Since $j(P) \neq 0, 1728, \infty$ the only $\overline{K}$-automorphism of $\mathcal{X}$ which fixes P is the identity. In particular, $\varphi = \sigma\varphi\sigma^{-1}$ for all $\sigma \in G_K$ and therefore φ is defined over K. □

To show that $X_E(7)$ is isomorphic to $X_M^{\pm}(7)$ for some choice of sign, it suffices to show that $E[7]$ is isomorphic to M as a $G_{\mathbb{Q}}$-module, up to quadratic twist. We recall the following lemma of Fisher (based on an argument of Serre using Goursat's lemma [37, Lemme 8]) which allows us to prove such congruences, up to quadratic twists.

Lemma 18. *Let K be a number field and let M be a G_K-module which is isomorphic as an abstract group to $(\mathbb{Z}/p\mathbb{Z})^2$ for some $p \geq 5$. Suppose that M comes equipped with a (G_K-equivariant) alternating pairing $M \times M \to \mu_p$. Let E/K be an elliptic curve with surjective mod p Galois representation, let $x_M\colon M \to M/\{\pm 1\}$, and let $x_E\colon E \to \mathbb{P}^1$ be the quotient by $\{\pm 1\}$. If there exist non-identity elements $P \in M$ and $Q \in E[p]$ such that $K(x_M(P)) = K(x_E(Q))$ then there exists a quadratic twist E^d of E such that $M \cong E^d[p]$.*

Proof. This follows immediately from [18, Lemma 6.2] (cf. [18, Proposition 6.1]). Note that the hypothesis that $K = \mathbb{Q}$ in [18, Lemma 6.2] is not used. □

4.2. When $\mathcal{X}$ has no rational points. We rely on the approach in Section 4.1 together with the following criterion. In practice when X and Y are twists of $X(7)$ defined over $\mathbb{Q}$ it is simple to find number fields for which the statement holds. In this case there exist infinitely many points on X and Y defined over quartic fields. One expects that if X and Y are isomorphic (and have no non-trivial automorphisms defined over $\mathbb{Q}$), then for a generic such field the conditions of the lemma hold.

Lemma 19. *Let X/K and Y/K be (geometrically integral) curves defined over a number field K. Suppose that there exist extensions $L_1, L_2/K$ for which $L_1 \cap L_2 = K$ and such that we have isomorphisms $\varphi_i \colon X_{L_i} \cong Y_{L_i}$ for each $i = 1, 2$. If X (or Y) does not admit a non-trivial automorphism over the compositum $L_1 L_2$, then X and Y are isomorphic over K.*

Proof. The assumption on the automorphism group of X over $L_1 L_2$ implies that the composition $\varphi_1^{-1}\varphi_2$ is the identity, and therefore over $L_1 L_2$ we have an equality $\varphi_1 = \varphi_2$. But then φ_1 is defined over $L_1 \cap L_2 = K$ and the claim follows. □

Proposition 20. *Consider any of the data in* [23, `data/twists.m`] *which consists of*

(i) *a genus 2 curve $C/\mathbb{Q}$,*
(ii) *a fundamental discriminant $D > 0$ such that the Jacobian of C has RM by $\mathcal{O}_D$, and*
(iii) *a twist $\mathcal{X}/\mathbb{Q}$ of the Klein quartic.*

Then $\mathcal{X}$ is isomorphic over $\mathbb{Q}$ to $X^{\pm}_{J[\mathfrak{p}]}(7)$ for some choice of sign and choice of prime $\mathfrak{p} \subset \mathcal{O}_D$ above 7.

Proof. If $\mathcal{X}$ has a $\mathbb{Q}$-rational point of small height corresponding to an elliptic curve $E/\mathbb{Q}$, we apply Lemma 18. In each case, applying [37, Proposition 19] at several good primes (or using Zywina's algorithm [42]) suffices to show that the mod 7 Galois representation attached to $E/\mathbb{Q}$ is surjective. In the electronic data we exhibit an explicit isomorphism between the fields $x_J(P)$ and $x_E(Q)$ for some $P \in J[\mathfrak{p}]$ and $Q \in E[7]$ (note that a minimal polynomial for the extension $\mathbb{Q}(x_J(P))/\mathbb{Q}$ was computed in the course of the algorithm in Section 3.3).

The general case proceeds similarly. Taking hyperplane sections of $\mathcal{X}$ we construct non-isomorphic quartic fields $L_1, L_2/\mathbb{Q}$ over which $\mathcal{X}$ obtains a point and such that L_i contains no non-trivial subfield for each $i = 1, 2$ (in particular $L_1 \cap L_2 = \mathbb{Q}$ and $L_1 \cap \mathbb{Q}(\zeta_7) = L_2 \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$). These points correspond to elliptic curves E_1/L_1 and E_2/L_2 whose mod 7 Galois representations may be seen to be surjective by applying [37, Proposition 19] at several places of good reduction. Applying Lemma 18 as above shows that E_1 and E_2 are $(7, \mathfrak{p})$-congruent to J, up to a quadratic twist. Since the mod 7 Galois representations of E_1/L_1 and E_2/L_2 are surjective we have $\mathbb{Q}(\mathcal{K}[\mathfrak{p}]) \cap L_1 L_2 = \mathbb{Q}$, where $\mathcal{K} = J/\{\pm 1\}$ is the Kummer surface of J.

It follows from the construction that $\mathrm{Aut}(X^{r}_{J[\mathfrak{p}]}(7))$ is isomorphic (as a $G_{\mathbb{Q}}$-module) to the group $\mathrm{Aut}_r(J[\mathfrak{p}])/\{\pm 1\}$ consisting of automorphisms of $J[\mathfrak{p}]$ which are symplectic with respect to $(e_{J,7})^r$. Therefore, the field of definition of the automorphisms of $X^{\pm}_{J[\mathfrak{p}]}(7)$ is equal to $\mathbb{Q}(\mathcal{K}[\mathfrak{p}])$ and $X^{\pm}_{J[\mathfrak{p}]}(7)$ admits no non-trivial automorphisms over $L_1 L_2$ that are not defined over $\mathbb{Q}$. Suppose there is such an automorphism τ defined over $\mathbb{Q}$. Since the mod 7

Galois representation attached to $J[\mathfrak{p}]$ is surjective ($J[\mathfrak{p}]$ is isomorphic over L_i to a quadratic twist of $E_i[7]$ for each $i = 1, 2$) the element τ is contained in the centre of $\mathrm{Aut}_r(J[\mathfrak{p}])/\{\pm 1\}$ which is isomorphic to $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$ as an abstract group. Therefore τ is the identity and the claim follows from Lemma 19. □

5. Proving $(7, \mathfrak{p})$-congruences and Theorem 1

We now prove Theorem 1. In order to apply visibility we must first show that the pairs (C, E) in Table 1.1 are in fact $(7, \mathfrak{p})$-congruent (not simply up to quadratic twist, as we proved in Section 4).

Lemma 21. *Let $E/\mathbb{Q}$ be an elliptic curve and let $J/\mathbb{Q}$ be a genus 2 Jacobian with RM by $\mathcal{O}_D$. Suppose that $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_D$ and that there exists a squarefree integer $d \in \mathbb{Z}$ such that E^d and J are $(p, \mathfrak{p})$-congruent. Then d is supported on the set of primes consisting of p, the bad primes of E, and the bad primes of J.*

Proof. This is similar to [22, Proposition 4.18] and [25, Lemma 3.6] (see also [37, Lemme 8]). Let $\ell \neq p$ be a prime at which J has good reduction and at which E has potentially good reduction. Let $\mathbb{Q}_\ell^{\mathrm{ur}}$ be the maximal unramified extension of $\mathbb{Q}_\ell$ and let $K = \mathbb{Q}_\ell^{\mathrm{ur}}(J[p])$. By [39, Section 2, Corollary 3] if $A/\mathbb{Q}_\ell$ is an abelian variety with potential good reduction at ℓ, then for each $p \neq \ell$ the field $\mathbb{Q}_\ell^{\mathrm{ur}}(A[p])$ is the smallest extension of $\mathbb{Q}_\ell^{\mathrm{ur}}$ over which A attains good reduction. But then we have $\mathbb{Q}_\ell^{\mathrm{ur}}(E[p]) = \mathbb{Q}_\ell^{\mathrm{ur}}(J[\mathfrak{p}]) \subset K = \mathbb{Q}_\ell^{\mathrm{ur}}$, as required. □

Proposition 22. *For each pair (E, C) of elliptic curve $E/\mathbb{Q}$ and genus 2 curve $C/\mathbb{Q}$ in Table 1.1 we have a $(7, \mathfrak{p})$-congruence between E and $J = \mathrm{Jac}(C)$ for some choice of $\mathfrak{p}|7$ in $\mathcal{O}_D$.*

Proof. Let $\ell \neq 7$ be a good prime for C and E. By [18, (5.2)] (which follows from [20, Section 2.1] or [31, Lemma 3]) a $(7, \mathfrak{p})$-congruence between $E^d/\mathbb{Q}$ and $J/\mathbb{Q}$ gives a congruence modulo 7

$$a_\ell(E^d)^2 - t_\ell a_\ell(E^d) + n_\ell \equiv 0 \pmod 7 \tag{5.1}$$

where $t_\ell = \ell + 1 - N_1$ and $n_\ell = (N_1^2 + N_2)/2 - (\ell + 1)N_1 - \ell$ where $N_1 = \#C(\mathbb{F}_\ell)$ and $N_2 = \#C(\mathbb{F}_{\ell^2})$.

Testing (5.1) on the divisors d of the product of 7 and the bad primes of E and C shows that E^d and J are not $(7, \mathfrak{p})$-congruent for any $d \neq 1$ (by Lemma 21). By Proposition 20 E and J are $(7, \mathfrak{p})$-congruent up to quadratic twist since E corresponds to a point on one of the twists $X^{\pm}_{J[\mathfrak{p}]}(7)$. It therefore follows that E and J are $(7, \mathfrak{p})$-congruent for some choice of $\mathfrak{p}$ dividing 7. □

Using the congruences supplied by Proposition 22 we now prove Theorems 1 and 5 by applying [18, Theorem 2.2].

Proof of Theorems 1 and 5. This follows from [18, Theorem 2.2], as we detail below.

Let $E/\mathbb{Q}$ and $J/\mathbb{Q}$ be one of the pairs of elliptic curve and genus 2 Jacobian from Theorem 1 or 5. We check that in each case J is geometrically simple by applying the condition in [8, Section 14.4] and [41]. The 7-torsion subgroups of $E(\mathbb{Q})$ and $J(\mathbb{Q})$ are trivial. The rank of $E/\mathbb{Q}$ is 2 and the rank of $J/\mathbb{Q}$ is 0 (the rank of $J/\mathbb{Q}$ is bounded using 2-descent, which is implemented as `RankBounds` in `Magma`). For each discriminant D appearing in Theorems 1 and 5 the prime 7 not only splits in $\mathcal{O}_D$, but $7 = \mathrm{Nm}\,\eta$ for some $\eta \in \mathcal{O}_D$. In particular the isogeny $\mathfrak{p}$ is equal to the multiplication-by-η-map on J, and $J(\mathbb{Q})/\mathfrak{p}J(\mathbb{Q}) = 0$.

By Proposition 22 the elliptic curve E is $(7, \mathfrak{p})$-congruent to J. The abelian varieties E and J have good reduction at 7, so by [18, Theorem 2.2] it suffices to show that the Tamagawa numbers of $E/\mathbb{Q}$ and $J/\mathbb{Q}$ are coprime to 7.

We compute the Tamagawa numbers of $E/\mathbb{Q}$ using `Magma`. Except for the Jacobian of conductor 3200^2 in Table 1.1, for each bad prime p of J one may check that the order of the geometric component group of J at p is coprime to 7 using Liu's `genus2reduction` in `SageMath` and Donnelly's `Magma` functions `RegularModel` and `ComponentGroup`.

For the Jacobian of conductor 3200^2 in Table 1.1 the computation of the Tamagawa number of $J/\mathbb{Q}$ at 2 was carried out in the appendix to [26] (where it is shown that the Tamagawa number is 1). □

6. Evidence towards Conjecture 6

Consider the genus 2 curve $C/\mathbb{Q}$ with LMFDB label `385641.a.385641.1` and Weierstrass equation

$$C : y^2 + (x^3 + 1)y = -6x^4 + 6x^3 + 27x^2 - 30x - 22.$$

The Jacobian $J/\mathbb{Q}$ of C has RM by $\mathbb{Z}[\sqrt{2}]$. In [26, A.3] it is noted that the Birch and Swinnerton-Dyer conjecture predicts $|\text{Ш}(J^{-11}/\mathbb{Q})| = 7^2$. By Proposition 20, for some choice of factorisation $(7) = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathbb{Z}[\sqrt{2}]$ we have models

$$\begin{aligned} X^{\pm}_{J[\mathfrak{p}]}(7) : &- 2x_0^4 + 39x_0^3x_1 + 11x_0^3x_2 - 42x_0^2x_1^2 - 18x_0^2x_1x_2 \\ &+ 20x_0x_1^3 - 6x_0x_1^2x_2 + 12x_0x_1x_2^2 - 7x_0x_2^3 - 24x_1^4 + 13x_1^3x_2 \\ &+ 15x_1^2x_2^2 + 9x_1x_2^3 + x_2^4 = 0, \end{aligned}$$

$$\begin{aligned}X^{\mp}_{J[\mathfrak{p}]}(7) :\ & 2x_0^4 + 5x_0^3x_1 + 9x_0^3x_2 + 6x_0^2x_2^2 - x_0x_1^3 - 6x_0x_1^2x_2 + 12x_0x_1x_2^2 \\ & + 2x_0x_2^3 - x_1^4 - 3x_1^3x_2 + 3x_1^2x_2^2 + 17x_1x_2^3 + 12x_2^4 = 0, \\ X^{\pm}_{J[\bar{\mathfrak{p}}]}(7) :\ & x_0^4 - 3x_0^3x_1 - 28x_0^3x_2 - 15x_0^2x_1^2 - 3x_0^2x_1x_2 + 39x_0^2x_2^2 - 6x_0x_1^3 \\ & - 12x_0x_1^2x_2 - 6x_0x_1x_2^2 - 29x_0x_2^3 + 3x_1^4 + 9x_1^3x_2 + 30x_1^2x_2^2 \\ & - 3x_1x_2^3 - 10x_2^4 = 0, \\ X^{\mp}_{J[\bar{\mathfrak{p}}]}(7) :\ & -4x_0^4 + 6x_0^3x_1 + 7x_0^3x_2 + 3x_0^2x_1^2 + 12x_0x_1^3 + 6x_0x_1^2x_2 \\ & - 9x_0x_1x_2^2 - x_0x_2^3 - 6x_1^4 - 3x_1^3x_2 + 3x_1^2x_2^2 + 6x_1x_2^3 + x_2^4 = 0.\end{aligned}$$

We were unable to find rational points on any of these curves, except on $X^{\mp}_{J[\mathfrak{p}]}(7)$ where we find exactly one point which corresponds to the elliptic curve $E/\mathbb{Q}$ with LMFDB label `1242.m1` and Weierstrass equation

$$y^2 + xy + y = x^3 - x^2 - 1666739x - 2448131309.$$

Using the argument in Proposition 22 it can be shown that E and J are $(7, \mathfrak{p})$-congruent. However, the quadratic twist of E by -11 has trivial Mordell–Weil group, so cannot be used to visualise the (conjectural) non-trivial elements of $Ш(J^{-11}/\mathbb{Q})[7]$.

Acknowledgements

This article formed part of my PhD thesis [24, Chapter 6]. I would like to thank my PhD supervisor Tom Fisher for many discussions and for extensive comments on previous versions of this article. I am grateful to Timo Keller for helpful correspondences and to Maria Corte-Real Santos and Ross Paterson for useful comments and discussions.

This work was supported by the Woolf Fisher and Cambridge Trusts, and by the Royal Society through Céline Maistret's Dorothy Hodgkin Fellowship. The code associated to this article is written in `Magma` [6] and `SageMath` [36] and is publicly available in the GitHub repository [23].

References

[1] A. Agashe & W. Stein, "Visibility of Shafarevich–Tate groups of abelian varieties", *J. Number Theory* **97** (2002), no. 1, p. 171-185.

[2] ———, "Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero", *Math. Comput.* **74** (2005), no. 249, p. 455-484, with an appendix by J. Cremona and B. Mazur.

[3] P. R. Bending, "Curves of genus 2 with $\sqrt{2}$-multiplication", PhD Thesis, University of Oxford, 1998.

[4] ———, "Curves of genus 2 with sqrt2 multiplication", 1999, `https://arxiv.org/abs/math/9911273`.

[5] M. Bhargava, Z. Klagsbrun, R. J. Lemke Oliver & A. Shnidman, "Elements of given order in Tate–Shafarevich groups of abelian varieties in quadratic twist families", *Algebra Number Theory* **15** (2021), no. 3, p. 627-655.

[6] W. Bosma, J. Cannon & C. Playoust, "Magma algebra system. I. The user language", *J. Symb. Comput.* **24** (1997), no. 3-4, p. 235-265.

[7] N. Bruin, E. V. Flynn & D. Testa, "Descent via $(3,3)$-isogeny on Jacobians of genus 2 curves", *Acta Arith.* **165** (2014), no. 3, p. 201-223.

[8] J. W. S. Cassels & E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, 1996, xiv+219 pages.

[9] A. Cowan, S. Frengley & K. Martin, "Generic models for genus 2 curves with real multiplication", 2024, https://arxiv.org/abs/2403.03191.

[10] J. E. Cremona & B. Mazur, "Visualizing elements in the Shafarevich–Tate group", *Exp. Math.* **9** (2000), no. 1, p. 13-28.

[11] J. Dixmier, "On the projective invariants of quartic plane curves", *Adv. Math.* **64** (1987), no. 3, p. 279-304.

[12] T. Dokchitser & C. Doris, "3-torsion and conductor of genus 2 curves", *Math. Comput.* **88** (2019), no. 318, p. 1913-1927.

[13] N. D. Elkies, "The Klein quartic in number theory", in *The eightfold way*, Mathematical Sciences Research Institute Publications, vol. 35, Cambridge University Press, 1999, p. 51-101.

[14] N. D. Elkies & A. Kumar, "K3 surfaces and equations for Hilbert modular surfaces", *Algebra Number Theory* **8** (2014), no. 10, p. 2297-2411.

[15] A.-S. Elsenhans, "Explicit computations of invariants of plane quartic curves", *J. Symb. Comput.* **68** (2015), p. 109-115.

[16] A.-S. Elsenhans & M. Stoll, "Minimization of hypersurfaces", *Math. Comput.* **93** (2024), no. 349, p. 2513-2555.

[17] T. A. Fisher, "On families of 7- and 11-congruent elliptic curves", *LMS J. Comput. Math.* **17** (2014), no. 1, p. 536-564.

[18] ———, "Visualizing elements of order 7 in the Tate–Shafarevich group of an elliptic curve", *LMS J. Comput. Math.* **19** (2016), no. suppl. A, p. 100-114.

[19] E. V. Flynn, "Descent via $(5,5)$-isogeny on Jacobians of genus 2 curves", *J. Number Theory* **153** (2015), p. 270-282.

[20] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. Stein & M. Stoll, "Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves", *Math. Comput.* **70** (2001), no. 236, p. 1675-1697.

[21] E. V. Flynn & A. Shnidman, "Arbitrarily large p-torsion in Tate–Shafarevich groups", *J. Inst. Math. Jussieu* **24** (2025), no. 2, p. 481-502.

[22] N. Freitas & A. Kraus, *On the symplectic type of isomorphisms of the p-torsion of elliptic curves*, Memoirs of the American Mathematical Society, vol. 1361, AMS, 2022, v+105 pages.

[23] S. Frengley, "GitHub repository", https://github.com/SamFrengley/sha-7-examples.git.

[24] ———, "Explicit moduli spaces for curves of genus 1 and 2", PhD Thesis, University of Cambridge, 2023.

[25] ———, "On 12-congruences of elliptic curves", *Int. J. Number Theory* **20** (2024), no. 2, p. 565-601.

[26] T. Keller & M. Stoll, "Complete verification of strong BSD for many modular abelian surfaces over $\mathbf{Q}$", *Forum Math. Sigma* **13** (2025), article no. e20 (82 pages).

[27] C. Khare & J.-P. Wintenberger, "Serre's modularity conjecture. I", *Invent. Math.* **178** (2009), no. 3, p. 485-504.

[28] ———, "Serre's modularity conjecture. II", *Invent. Math.* **178** (2009), no. 3, p. 505-586.

[29] F. Klein, "Ueber die Transformation siebenter Ordnung der elliptischen Functionen", *Math. Ann.* **14** (1878), no. 3, p. 428-471.

[30] The LMFDB Collaboration, "The L-functions and Modular Forms Database", 2025, http://www.lmfdb.org [accessed 20 January 2025].

[31] J. R. Merriman & N. P. Smart, "Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point", *Math. Proc. Camb. Philos. Soc.* **114** (1993), no. 2, p. 203-214.

[32] C. Nicholls, "GitHub repository", https://github.com/cgnicholls/phd-code.git [accessed November 2023].

[33] ———, "Descent methods and torsion on Jacobians of higher genus curves", PhD Thesis, University of Oxford, 2018.

[34] T. Ohno, "The graded ring of invariants of ternary quartics I", preprint, https://aeb.win.tue.nl/math/ohno-preprint.2007.05.15.pdf.

[35] B. Poonen, E. F. Schaefer & M. Stoll, "Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$", *Duke Math. J.* **137** (2007), no. 1, p. 103-158.

[36] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2022, https://www.sagemath.org.

[37] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), no. 4, p. 259-331.

[38] ———, *Local fields*, Springer, 1979, translated from the French by Marvin Jay Greenberg., viii+241 pages.

[39] J.-P. Serre & J. Tate, "Good reduction of abelian varieties", *Ann. Math. (2)* **88** (1968), p. 492-517.

[40] A. Shnidman & A. Weiss, "Elements of prime order in Tate–Shafarevich groups of abelian varieties over $\mathbb{Q}$", *Forum Math. Sigma* **10** (2022), article no. e98 (10 pages).

[41] M. Stoll, "Two simple 2-dimensional abelian varieties defined over $\mathbb{Q}$ with Mordell–Weil group of rank at least 19", *C. R. Math.* **321** (1995), no. 10, p. 1341-1345.

[42] D. Zywina, "Explicit open images for elliptic curves over $\mathbb{Q}$", 2022, https://arxiv.org/abs/2206.14959.

Sam Frengley
School of Mathematics, University of Bristol
Bristol, BS8 1UG, United Kingdom
E-mail: sam.frengley@gmail.com
URL: https://samfrengley.github.io/