ELLIPTIC CURVES OVER TOTALLY REAL CUBIC FIELDS ARE MODULAR

MAARTEN DERICKX, FILIP NAJMAN, AND SAMIR SIKSEK

Abstract. We prove that all elliptic curves defined over totally real cubic fields are modular. This builds on previous work of Freitas, Le Hung and Siksek, who proved modularity of elliptic curves over real quadratic fields, as well as recent breakthroughs due to Thorne and to Kalyanswamy.

1. Introduction

Let K be a totally real number field and let E be an elliptic curve over K with conductor $\mathcal{N}$. It is conjectured that such a curve E is **modular** in the following sense: there is a level $\mathcal{N}$ Hilbert newform $\mathfrak{f}$ over K of parallel weight 2 and rational Hecke eigenvalues such that $\mathrm{L}(E, s) = \mathrm{L}(\mathfrak{f}, s)$, where the L-function on the left is the Hasse–Weil L-function of E, and the L-function on the right is the Hecke L-function of $\mathfrak{f}$. This **modularity conjecture** is the natural generalization to totally real fields of the Shimura–Taniyama conjecture for elliptic curves over the rationals. The latter is a celebrated theorem due to Wiles [24], Breuil, Conrad, Diamond and Taylor [23]. The earliest results towards the modularity conjecture for elliptic curves going beyond the rationals were due to Jarvis and Manoharmayum [13], and established modularity of semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{17})$. In the last 10 years there has been a dramatic strengthening of modularity lifting theorems due to, for example, Breuil and Diamond [5], Kisin [16], Gee [10], and Barnet-Lamb, Gee and Geraghty [2], [3].

By the aforementioned modularity lifting theorems and by now standard modularity switching arguments due to Wiles and to Manoharmayum [18], a hypothetical non-modular E/K would therefore necessarily have small mod p image for $p = 3$, 5, 7 and would give rise to a K-point on one of a number of modular curves—we make this precise later. In [8], the real quadratic points of these modular curves are shown to be either cuspidal, or to correspond to elliptic curves that have complex multiplication, or rational j-invariants, or that are $\mathbb{Q}$-curves. The authors deduce the following.

Theorem 1 (Freitas, Le Hung and Siksek)**.** *Elliptic curves over real quadratic fields are modular.*

Date: March 11, 2020.

2010 *Mathematics Subject Classification.* Primary 11F80, Secondary 11G05.

Key words and phrases. modularity, elliptic curves, totally real fields.

Derickx is supported by Simons Foundation grant 550033. Najman is supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004) and by the Croatian Science Foundation under the project no. IP-2018-01-1313.. Siksek is supported by EPSRC *LMF: L-Functions and Modular Forms* Programme Grant EP/K034383/1.

Recently these modularity lifting results have been substantially strengthened in the cases $p = 5$ and $p = 7$, respectively by Thorne [21] and Kalyanswamy [14]. This means that several difficult steps in the proof of Theorem 1 can now be eliminated. In this paper we build on these theorems of Thorne and Kalyanswamy to prove the following.

Theorem 2. *Let K be a totally real cubic number field. Let E be an elliptic curve over K. Then E is modular.*

The computations in this paper were carried out in the computer algebra system `Magma` [4]. The reader can find the `Magma` scripts for verifying these computations at:
`http://homepages.warwick.ac.uk/staff/S.Siksek/progs/cubicmodularity/`
We heartily thank the referee for many excellent suggestions that have improved the exposition of this paper.

2. Images mod 3, 5, 7 and modularity

Let $p \geq 3$ be a prime. Write $B(p)$ for a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, and $C_{\mathrm{s}}(p)$ and $C_{\mathrm{ns}}(p)$ respectively for a split and non-split Cartan subgroup. Let $C_{\mathrm{s}}^+(p)$ and $C_{\mathrm{ns}}^+(p)$ respectively be their normalizers.

The proof of Theorem 2 is based on the fact that a putative non-modular curve must have small mod p images for $p = 3$, 5 and 7 simultaneously. We now make the conditions for each prime precise.

Theorem 3. *Let K be a totally real field and E an elliptic curve over K. Suppose that $\overline{\rho}_{E,3}(G_K)$ is not conjugate to a subgroup of $B(3)$ or $C_{\mathrm{s}}^+(3)$. Then E is modular.*

Proof. By the aforementioned modularity lifting results, if $\overline{\rho}_{E,3}(G_{K(\zeta_3)})$ is absolutely irreducible, then E is modular; a proof is given in [8, Theorem 3] but the arguments are well-known.

By [20, Proposition 6], if $\overline{\rho}_{E,3}(G_{K(\zeta_3)})$ is absolutely reducible, then it is conjugate to a subgroup of $B(3)$ or $C_{\mathrm{s}}^+(3)$. □

For $p = 5$ we use the following result due to Thorne [21].

Theorem 4 (Thorne)**.** *Let K be a totally real field and E an elliptic curve over K. Suppose 5 is not a square in K, and $\overline{\rho}_{E,5}$ is irreducible. Then E is modular.*

For $p = 7$ we use the following result of Kalyanswamy [14, Proposition 4.3 and Theorem 4.4].

Theorem 5 (Kalyanswamy)**.** *Let K be a totally real field and E an elliptic curve over K. Suppose*

- *$K \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$.*
- *$\overline{\rho}_{E,7}$ is irreducible.*
- *$\overline{\rho}_{E,7}(G_K)$ is not conjugate to a subgroup of $C_{\mathrm{ns}}^+(7)$.*

Then E is modular.

Kalyanswamy's theorem is somewhat more precise, but we shall not need its full strength. We note that $\mathbb{Q}(\zeta_7)^+$ is the only totally real cubic field for which Kalyanswamy's theorem is inapplicable. It is for this reason that we consider elliptic curves defined over that field separately in Section 4.

3. Modular Curves

We quickly sketch some background on modular curves; for fuller details the reader may want to consult [6], [8, Section 2.2.2], [19]. Let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ denote the extended upper half-plane. The modular group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ by fractional linear transformations. The quotient $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$ is a compact Riemann surface of genus 0, and hence is the analytification of a genus 0 algebraic curve defined (a priori) over $\mathbb{C}$ which is denoted by $X(1)$. The set $\mathbb{Q}\cup\{\infty\} \subset \mathbb{H}^*$ forms a single orbit under the action of $\mathrm{SL}_2(\mathbb{Z})$, and hence that orbit corresponds to a point of $X(1)$ which is called the cusp. In fact $X(1)$ has a model defined over $\mathrm{Spec}(\mathbb{Z})$ in which it is identified with $\mathbb{P}^1$, and where the cusp is simply the point at infinity.

Let p be a prime and let H be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ satisfying $\det(H) = \mathbb{F}_p^*$. Associated to H is a congruence subgroup Γ_H which is defined as the preimage of $H \cap \mathrm{SL}_2(\mathbb{F}_p)$ under the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{F}_p)$. The modular curve $X_H/\mathbb{C}$ is the proper algebraic curve whose analytification is the compact Riemann surface $\Gamma_H\backslash\mathbb{H}^*$. In fact the condition $\det(H) = \mathbb{F}_p^*$ ensures that X_H has a model over $\mathrm{Spec}(\mathbb{Z}[1/p])$. The inclusion $\Gamma_H \subset \mathrm{SL}_2(\mathbb{Z})$ induces a morphism $j : X_H \to X(1)$, which is also defined over $\mathrm{Spec}(\mathbb{Z}[1/p])$. The cusps of X_H are the preimages of $\infty \in X(1)$, and thus also the orbits of $\mathbb{Q}\cup\{\infty\}$ under the action of Γ_H.

We now come to the modular interpretation of rational points on X_H, and here it is convenient to make an additional assumption, namely $-I \in H$. Let K be a field of characteristic $\neq p$. Let E/K be an elliptic curve such that $\overline{\rho}_{E,p}(G_K)$ is conjugate to a subgroup of H. Then there is at least one non-cuspidal point $P \in X_H(K)$ such that $j(P) = j(E)$ where $j(E)$ is the j-invariant of the elliptic curve E. The converse of this statement is false in general. There is however a partial converse which is true: if $P \in X_H(K)$ is a non-cuspidal point and $j(P) \neq 0, 1728$ then there is an elliptic curve E/K such that $\overline{\rho}_{E,p}(G_K)$ is conjugate to a subgroup of H and $j(E) = j(P)$.

If we take $H = B_0(p)$, $C_{\mathrm{s}}^+(p)$, $C_{\mathrm{ns}}^+(p)$ then X_H is the modular curve usually denoted by $X_0(p)$, $X_{\mathrm{split}}(p)$ and $X_{\mathrm{nonsplit}}(p)$ respectively. For convenience, instead of using the standard notation for these modular curves, we shall mostly follow the notation of [8] and denote these modular curves by $X(\mathrm{b}p) := X_0(p)$, $X(\mathrm{s}p) := X_{\mathrm{split}}(p)$ and $X(\mathrm{ns}p) := X_{\mathrm{nonsplit}}(p)$.

Now let K be a totally real cubic field, and for simplicity suppose $K \neq \mathbb{Q}(\zeta_7)^+$. By Theorems 3, 4 and 5, a potentially non-modular elliptic curve E defined over K would give rise to a non-cuspidal K-point P on either $X(\mathrm{b}3)$ or $X(\mathrm{s}3)$, and simultaneously a non-cuspidal K-point Q on $X(\mathrm{b}5)$, and simultaneously a non-cuspidal K-point R on either $X(\mathrm{b}7)$ or $X(\mathrm{ns}7)$. Observe that $j(P) = j(Q) = j(R) = j(E)$. Thus we obtain a K-point on one of the fibre products

$$X(\mathrm{u}3) \times_{X(1)} X(\mathrm{b}5) \times_{X(1)} X(\mathrm{v}7), \qquad \mathrm{u} \in \{\mathrm{b}, \mathrm{s}\}, \qquad \mathrm{v} \in \{\mathrm{b}, \mathrm{ns}\}. \tag{1}$$

We denote the normalization of (1) by $X(\mathrm{u}3, \mathrm{b}5, \mathrm{v}7)$. As E is hypothetically non-modular, it is non-CM, and in particular $j(E) \neq 0, 1728$. The maps $X_H \to X(1)$ are ramified only above 0, 1728 and ∞, and thus the K-point we obtain from E on (1) is a smooth point and hence gives rise to a K-point on the normalization $X(\mathrm{u}3, \mathrm{b}5, \mathrm{v}7)$. Thus to prove Theorem 2 for $K \neq \mathbb{Q}(\zeta_7)^+$ it is enough to show that K-points on the four possible curves $X(\mathrm{u}3, \mathrm{b}5, \mathrm{v}7)$ are cuspidal. In fact it is plainly enough to do this for the two curves $X(\mathrm{b}5, \mathrm{b}7)$ and $X(\mathrm{b}5, \mathrm{ns}7)$.

An overview of the proof of Theorem 2. In Section 4 we prove modularity of elliptic curves defined over $\mathbb{Q}(\zeta_7)^+$. In view of the above discussion the following two theorems immediately imply Theorem 2.

Theorem 6. *Let K be a totally real cubic field. Then $X(\mathrm{b5},\mathrm{b7})(K)$ consists only of cusps.*

Theorem 7. *Let K be a cubic field. Then $X(\mathrm{b5},\mathrm{ns7})(K)$ consists only of cusps.*

The remainder of the paper is devoted to the proof of these two theorems.

4. Modularity of Elliptic Curves over $\mathbb{Q}(\zeta_7)^+$

In this section we prove Theorem 2 for $K = \mathbb{Q}(\zeta_7)^+$.

Lemma 4.1. *Let $K = \mathbb{Q}(\zeta_7)^+$. Let E be an elliptic curve defined over K. Then E is modular.*

Proof. By Theorem 4 we may suppose that $\overline{\rho}_{E,5}$ is reducible. By Theorem 3 we may suppose that the image of $\overline{\rho}_{E,3}$ is contained in $B(3)$ or $C_{\mathrm{s}}^+(3)$. Thus E gives rise to a non-cuspidal K-point on one of the two modular curves $X(\mathrm{b3},\mathrm{b5})$, $X(\mathrm{s3},\mathrm{b5})$. It is shown in [8, Section 5.4.2] that these are in fact elliptic curves defined over $\mathbb{Q}$ with Cremona labels `15A1` and `15A3`. We computed the Mordell–Weil groups $X(K)$ for $X = X(\mathrm{b3},\mathrm{b5})$, $X(\mathrm{s3},\mathrm{b5})$ using `Magma`. In both cases we found

$$X(K) = X(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

In particular E gives rise to $\mathbb{Q}$-point on X and so is a twist of an elliptic curve defined over $\mathbb{Q}$. It is therefore modular by [23]. □

5. Proof of Theorem 6

Let $X = X(\mathrm{b5},\mathrm{b7})$ (in standard notation denoted by $X_0(35)$). It is known that X has four $\mathbb{Q}$-points and that these are cusps. Let K be a totally real cubic field. For the proof of Theorem 6 it will be sufficient to show that $X(K) = X(\mathbb{Q})$. Suppose $P \in X(K)\backslash X(\mathbb{Q})$. Let P_1, P_2, P_3 be the conjugates of P given by the three embeddings of K in $\overline{\mathbb{Q}}$, and write $D = P_1 + P_2 + P_3$. Then D is an irreducible $\mathbb{Q}$-rational divisor on X of degree 3. We shall determine all the irreducible $\mathbb{Q}$-rational divisors of degree 3 on X and show that none of them arise from totally real cubic points, giving a contradiction.

The arithmetic of X and its Jacobian are studied in [8, Section 5.1]. The curve X is hyperelliptic of genus 3. A model for X, derived by Galbraith [9, Section 4.4], is given by

$$X \ : \ y^2 = (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1). \tag{2}$$

Write $\infty_\pm$ for the two points at infinity. Write J for $J_0(35)$—the Jacobian of X. Then

$$J(\mathbb{Q}) = \frac{\mathbb{Z}}{24\mathbb{Z}} \cdot [\infty_- - \infty_+] + \frac{\mathbb{Z}}{2\mathbb{Z}} \cdot [3(0,-1) - 3\infty_+].$$

Let $D_1, \ldots, D_{48}$ be rational divisors of degree 0 on X representing the 48 classes in $J(\mathbb{Q})$, and let $D_i' = D_i + 3\infty_+$. Recall that D is an irreducible $\mathbb{Q}$-rational divisor of degree 3. Then $D \sim D_i'$ for some i. We shall write $\mathcal{L}(D_i')$ for the Riemann–Roch space corresponding to D_i' and $|D_i'|$ for the corresponding complete linear system. By Riemann–Roch and Clifford's inequality, $\dim \mathcal{L}(D_i') = 1$ or 2. Moreover, if

$\dim \mathcal{L}(D_i') = 2$, then $|D_i'|$ contains a base point (c.f. [1, Chapter I, Exercise D.9]), and therefore cannot contain an irreducible divisor. To sum up, $D \sim D_i'$ for some $1 \leq i \leq 48$ such that $\dim \mathcal{L}(D_i') = 1$. We computed these spaces using `Magma`; for this `Magma` uses an algorithm of Hess [11]. We found that $\dim \mathcal{L}(D_i') = 1$ for precisely 44 of the 48 divisors D_i'. For these, letting f_i be a $\mathbb{Q}$-basis for $\mathcal{L}(D_i')$, gives $D = D_i' + \operatorname{div}(f_i)$ for some i. We found that precisely 28 of the effective degree 3 divisors $D_i' + \operatorname{div}(f_i)$ are irreducible. However, all of these split over a cubic field with a complex embedding giving the required contradiction.

6. The modular curve $X(\mathrm{b5}, \mathrm{ns7})$

We shall henceforth restrict our attention to $X(\mathrm{b5}, \mathrm{ns7})$. To simplify the notation we write $X = X(\mathrm{b5}, \mathrm{ns7})$. We denote the Jacobian of X by $J = J(\mathrm{b5}, \mathrm{ns7})$. The curve X and its Jacobian J are studied in Le Hung's thesis [12, Section 6.4] and we make extensive use of his results. In particular, this curve is non-hyperelliptic and has genus 6.

The Jacobian $J = J(\mathrm{b5}, \mathrm{ns7})$. Le Hung shows that

$$J \sim A_1 \times A_2 \times A_3$$

where $\sim$ here denotes isogeny over $\mathbb{Q}$, and A_1, A_2, A_3 are modular abelian surfaces defined over $\mathbb{Q}$. Morever the A_i are absolutely simple. The involution w_5 on J is compatible with the isogeny and acts by multiplication by 1, -1, -1 respectively on A_1, A_2, A_3. The analytic ranks of A_1, A_2, A_3 are respectively 2, 0, 0. In particular, by the work of Kolyvagin and Logachëv [17], the Mordell–Weil groups $A_2(\mathbb{Q})$ and $A_3(\mathbb{Q})$ are torsion. We immediately deduce the following.

Lemma 6.1. *Let $A/\mathbb{Q}$ be the abelian subvariety of J that is the image of $w_5 - 1$. Then $A \sim A_2 \times A_3$ has dimension 4. Moreover, the Mordell–Weil group $A(\mathbb{Q})$ is torsion.*

Le Hung's model for $X = X(\mathrm{b5}, \mathrm{ns7})$. We need a good model for $X(\mathrm{b5}, \mathrm{ns7})$. Le Hung [12, p. 47] gives a model which will be a good starting point for us. We briefly sketch Le Hung's derivation of his model, but work with projective rather than affine coordinates. Later we explain how to derive a better model. The curves $X(\mathrm{b5})$ and $X(\mathrm{ns7})$ are both isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$. Let

$$F_1(x_1, x_2) = (x_1^2 + 10x_1x_2 + 5x_2^2)^3, \qquad F_2 := x_1x_2^5,$$

$$G_1(y_1, y_2) = 64 \cdot \left(y_1 \cdot (y_1^2 + 7y_2^2) \cdot (y_1^2 - 7y_1y_2 + 14y_2^2) \cdot (5y_1^2 - 14y_1y_2 - 7y_2^2)\right)^3,$$

and

$$G_2(y_1, y_2) = (y_1^3 - 7y_1^2y_2 + 7y_1y_2^2 + 7y_2^3)^7.$$

For appropriate choices of projective coordinates $(x_1 : x_2)$ for $X(\mathrm{b5})$ and $(y_1 : y_2)$ on $X(\mathrm{ns7})$, the j-maps are given by

$$j : X(\mathrm{b5}) \to X(1), \qquad (x_1 : x_2) \mapsto (F_1(x_1, x_2) : F_2(x_1, x_2)),$$

and

$$j : X(\mathrm{ns7}) \to X(1), \qquad (y_1, y_2) \mapsto (G_1(y_1, y_2) : G_2(y_1, y_2)).$$

As X is the normalization of $X(\mathrm{b5}) \times_{X(1)} X(\mathrm{ns7})$ we immediately deduce the following model for X in $\mathbb{P}^1 \times \mathbb{P}^1$:

$$C \ : \qquad F_1(x_1, x_2)G_2(y_1, y_2) = F_2(x_1, x_2)G_1(y_1, y_2).$$

The curve X is the normalization of this model. The parameterization $(x_1 : x_2)$ on $X(\mathrm{b5})$ is chosen so that the 0 and ∞ cusps are $(x_1 : x_2) = (0 : 1)$ and $(x_1 : x_2) = (1 : 0)$ respectively. We shall denote these by a_0, a_∞. Let ζ_7 be a primitive 7-th root of unity. Let $\eta = 2(\zeta_7 + \zeta_7) + 3 \in \mathbb{Q}(\zeta_7)^+$. Then $G_2(\eta : 1) = 0$. The three cusps of $X(\mathrm{ns7})$ are $(\eta : 1)$ and its Galois conjugates. It follows that the cusps of X are the points belonging to the normalization of C lying above the points $(x_1 : x_2, y_1 : y_2) = (0 : 1, \eta : 1)$, $(1 : 0, \eta : 1)$ and their Galois conjugates. Although these points on C are singular, it is easy to check (c.f. [8, Section 5.5.1]) that there is only one point on the normalization above each, and to deduce:

- X has two Galois orbits of cusps, both of degree 3 and defined over $\mathbb{Q}(\zeta_7)^+$, which we denote by c_0, c_∞;
- The three cusps in c_0 map to a_0, and the three cusps in c_∞ map to a_∞ on $X(\mathrm{b5})$.
- The divisor of x_1/x_2 interpreted as a function on X is $7 \cdot (c_0 - c_\infty)$. In particular, the class $[c_0 - c_\infty]$ is an element of order 1 or 7. There are several ways to show that the divisor $c_0 - c_\infty$ is not principal, and so its class has order 7. One way is by direct computation using `Magma`, working with the model D introduced below. Here is another way: we shall show below that X has gonality 4. As c_0, c_∞ have degree 3 they cannot be linearly equivalent.

A plane degree 6 model for $X = X(\mathrm{b5}, \mathrm{ns7})$. We used `Magma` to compute, starting with the model C, the canonical map and its image. The latter is indeed a smooth genus 6 curve cut out in $\mathbb{P}^5$ by six homogeneous degree 2 polynomials. By the Enriques–Babbage Theorem [1, p. 124], we know that X is neither trigonal, nor isomorphic to a plane quintic. Moreover, as the factors A_i of the Jacobian are 2-dimensional and absolutely simple, we see that the curve is not bi-elliptic. It follows (c.f. [1, 209–210]) that X has gonality 4 and a degree 6 planar model, with four ordinary double points as singularities. We used the inbuilt `Magma` implementation for writing down this model, and found that two of the four double points are defined over $\mathbb{Q}(i)$ and the other two over $\mathbb{Q}(\sqrt{5})$. After applying a $\mathbb{Q}$-rational automorphism of $\mathbb{P}^2$ to slightly simplify this degree 6 model, it is given by the following equation:

$$D \ : \ 5u^6 - 50u^5v + 206u^4v^2 - 408u^3v^3 + 321u^2v^4 + 10uv^5 - 100v^6 + 9u^4w^2 - 60u^3vw^2 + 80u^2v^2w^2 + 48uv^3w^2 + 15v^4w^2 + 3u^2w^4 - 10uvw^4 + 6v^2w^4 - w^6 = 0.$$

On this model D the double points are

$$p_1 = (i : 0 : 1), \quad p_2 = (-i : 0 : 1), \quad p_3 = (0 : \frac{1}{\sqrt{5}} : 1), \quad p_4 = (0 : -\frac{1}{\sqrt{5}} : 1).$$

It is clear that D has an automorphism $(u : v : w) \mapsto (-u : -v : w)$. The curve X has an obvious modular involution which is w_5. The following lemma proves that w_5 coincides with the automorphism $(u : v : w) \mapsto (-u : -v : w)$.

Lemma 6.2. *The $\mathbb{Q}$-rational automorphism group of $X(b5, ns7)$ is generated by w_5, i.e. $\mathrm{Aut}_{\mathbb{Q}}(X) = \langle w_5 \rangle \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. As described in [1, p 210–211.] a degree 6 planar curve with four ordinary double points such as D has exactly five different g^1_4. Namely, one given by the pencil of quadrics going through all four points, and the other four coming from the pencil of lines through each of the p_i. Since none of the p_i are $\mathbb{Q}$-rational, only

the first g^1_4 is defined over $\mathbb{Q}$. Now every g^2_6 on such a curve is residual to a g^1_4. This means that there is only one $\mathbb{Q}$-rational g^2_6, namely the one corresponding to the degree 6 model given by u, w, v above. In particular every $\mathbb{Q}$-rational automorphism has to come from an automorphism $h : \mathbb{P}^2_{\mathbb{Q}} \to \mathbb{P}^2_{\mathbb{Q}}$ in the degree 6 model. Such an automorphism h has to preserve the singular locus $\{p_1, p_2, p_3, p_4\}$ and is in fact uniquely determined by what it does on this singular locus. Of the 24 automorphisms of $\mathbb{P}^2_{\mathbb{Q}}$ preserving $\{p_1, p_2, p_3, p_4\}$, only the ones of the form $(u : v : w) \mapsto (\pm u : \pm v : w)$ are $\mathbb{Q}$-rational. One easily sees that of these four only the identity and $(u : v : w) \mapsto (-u : -v : w)$ are actually automorphisms of the curve. □

Transferring c_0 and c_∞ to our new model D, we find that they respectively are the Galois orbits of the following two points defined over $\mathbb{Q}(\eta) = \mathbb{Q}(\zeta_7)^+$ by

$$(-4\eta^2 + 21\eta + 7 : -\eta^2 + 7\eta : 14), \qquad (4\eta^2 - 21\eta - 7 : \eta^2 - 7\eta : 14).$$

We note that these are interchanged by $w_5 : (u : v : w) \mapsto (-u : -v : w)$ as expected.

The Mordell–Weil group $A(\mathbb{Q})$. In Lemma 6.1 we defined the abelian subvariety A of J as the image of $w_5 - 1$ and observed that $A(\mathbb{Q})$ is torsion. We can now pin down $A(\mathbb{Q})$ precisely. In particular, applying the function field class group algorithm of Hess [11] (implemented in `Magma`) to our model D, we obtain

$$J(\mathbb{F}_3) \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/(7 \cdot 23)\mathbb{Z},$$

and

$$J(\mathbb{F}_{17}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2^2 \cdot 7^3 \cdot 31 \cdot 271)\mathbb{Z}.$$

Hence $J(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/7\mathbb{Z}$. Recall that the class $[c_0 - c_\infty]$ has order 7. Thus $[c_0 - c_\infty]$ generates $J(\mathbb{Q})_{\mathrm{tors}}$. Now since w_5 interchanges c_0 and c_∞,

$$(w_5 - 1)([3c_0 - 3c_\infty]) = 6[c_\infty - c_0] = [c_0 - c_\infty].$$

Therefore $[c_0 - c_\infty] \in A(\mathbb{Q})$. As $A(\mathbb{Q}) = A(\mathbb{Q})_{\mathrm{tors}} \subseteq J(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/7\mathbb{Z}$ we have now proved the following.

Lemma 6.3. *$A(\mathbb{Q}) = (\mathbb{Z}/7\mathbb{Z}) \cdot [c_0 - c_\infty]$.*

7. Proof of Theorem 7

In this section we prove Theorem 7 thereby completing the proof of Theorem 2. Recall $X = X(\mathrm{b5}, \mathrm{ns7})$. Write $X^{(3)}$ for the third symmetric power of X. We shall prove the following result which immediately implies Theorem 7.

Proposition 7.1. *$X^{(3)}(\mathbb{Q}) = \{c_0, c_\infty\}$.*

Proof. Let $x \in X^{(3)}(\mathbb{Q})$. By Lemma 6.3 we have $(1 - w_5)[x - c_\infty] = \ell \cdot [c_0 - c_\infty]$ for some $\ell \in \mathbb{Z}/7\mathbb{Z}$. As $w_5(c_\infty) = c_0$ we may rewrite this as

$$(x - w_5(x)) \sim k \cdot (c_0 - c_\infty)$$

for some $k \in \{-3, \ldots, 3\}$. We write $x_{\mathbb{F}_3}$, $c_{0,\mathbb{F}_3}$, $c_{\infty,\mathbb{F}_3} \in X^{(3)}(\mathbb{F}_3)$ for the reductions of x, c_0, c_∞ modulo 3 respectively. It follows that

$$(y - w_5(y)) \sim k \cdot (c_{0,\mathbb{F}_3} - c_{\infty,\mathbb{F}_3}) \tag{3}$$

where $y = x_{\mathbb{F}_3}$. Using our model D we enumerated $X^{(3)}(\mathbb{F}_3)$; this has precisely 40 elements. For each $y \in X^{(3)}(\mathbb{F}_3)$ and for each $k = -3, \ldots, 3$ we tested the relation (3) and found that it holds only for $y = c_{0,\mathbb{F}_3}$ and $k = 1$ and for $y = c_{\infty,\mathbb{F}_3}$ and $k = -1$. We therefore deduce that $x_{\mathbb{F}_3} = c_{0,\mathbb{F}_3}$ or $c_{\infty,\mathbb{F}_3}$. We would like to conclude that $x = c_0$ or c_∞. As w_5 swaps c_0 and c_∞ and also their mod 3 reductions, we may suppose that $x_{\mathbb{F}_3} = c_\infty$. Let $\mu : X^{(3)} \to J$ be given by $z \mapsto [z - c_\infty]$ and $t : J \to A$ be simply $t = w_5 - 1$. Since $x_{\mathbb{F}_3} = c_{\infty,\mathbb{F}_3}$, the point $(t \circ \mu)(x) \in A(\mathbb{Q})$ belongs to the kernel of reduction $A(\mathbb{Q}) \to A(\mathbb{F}_3)$. However as $A(\mathbb{Q})$ is torsion, this kernel of reduction is trivial [15, Appendix]. Thus $(t \circ \mu)(x) = 0$. To conclude that $x = c_\infty$ it is now enough to check that $t \circ \mu$ is a formal immersion at $c_{\infty,\mathbb{F}_3}$, and for this we shall use the formal immersion criterion due to Derickx, Kamienny, Stein and Stoll [7, Proposition 3.7].

Write $\Omega_X \cong \Omega_J$ for the 6-dimensional space of 1-forms on $X/\mathbb{F}_3$. We would like to write down the 4-dimensional subspace $t^*(\Omega_A)$. We easily do this since it is precisely that -1-eigenspace of w_5^* acting on Ω_X, and we know the action of w_5 on our model D from which can write down the corresponding action on the 1-forms. Let $\omega_1, \ldots, \omega_4$ be an $\mathbb{F}_3$-basis for $t^*(\Omega_A)$. To check the formal immersion criterion of Derickx et al. at $c_{\infty,\mathbb{F}_3}$ we need to check that a certain 4×3 matrix defined in [7, Proposition 3.7], which we denote by M, has rank 3. As 3 is inert in $\mathbb{Q}(\zeta_7)^+$, we have $c_{\infty,\mathbb{F}_3} = P_1 + P_2 + P_3$, where $P_i \in X(\mathbb{F}_{27})$ are distinct. This slightly simplifies the description of the matrix M. Let $u_j \in \mathbb{F}_{27}(X)$ be a uniformizing element for P_j. Then ω_i/du_j is a regular function at P_j and we may evaluate $(\omega_i/du_j)(P_j) \in \mathbb{F}_{27}$. That matrix is simply

$$M = \left((\omega_i/du_j)(P_j)\right)_{i=1,2,3,4;\, j=1,2,3}.$$

We computed M and checked that it has rank 3 as required. This completes the proof. □

References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths, J. Harris, *Geometry of Algebraic Curves, Vol. I*, Springer Verlag, 1985. 5, 6, 6

[2] T. Barnet-Lamb, T. Gee and D. Geraghty, *Congruences between Hilbert modular forms: constructing ordinary lifts*, Duke Math. Journal **161** (2012), 1521–1580. 1

[3] T. Barnet-Lamb, T. Gee and D. Geraghty, *Congruences between Hilbert modular forms: constructing ordinary lifts II*, Mathematical Research Letters **20** (2013), 81–86. 1

[4] W. Bosma, J. Cannon and C. Playoust: *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`) 1

[5] C. Breuil and F. Diamond, *Formes modulaires de Hilbert modulo p et valeurs d'extensions galoisiennes*, Annales Scientifiques de l'École Normale Supérieure **47** (2014), no. 5, 905–974. 1

[6] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1973, pp. 143–316. Lecture Notes in Math., Vol. 349. 3

[7] M. Derickx, S. Kamienny, W. Stein and M. Stoll, *Torsion points on elliptic curves over number fields of small degree*, preprint, `https://arxiv.org/abs/1707.00364` 7

[8] N. Freitas, B. V. Le Hung and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), no. 1, 159–206. 1, 2, 3, 4, 5, 6

[9] S. D. Galbraith, *Equations for Modular Curves*, DPhil thesis, University of Oxford, 1996. 5

[10] T. Gee, *Automorphic lifts of prescribed types*, Mathematische Annalen **350** (2011), 107–144. 1

[11] F. Hess, *Computing Riemann–Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445. 5, 6

[12] B. V. Le Hung, *Modularity of some elliptic curves over totally real fields*, Doctoral dissertation, Harvard University, 2014. 6, 6
[13] F. Jarvis and J. Manoharmayum, *On the modularity of supersingular elliptic curves over certain totally real number fields*, Journal of Number Theory **128** (2008), no. 3, 589–618. 1
[14] S. Kalyanswamy, *Remarks on Automorphy of Residually Dihedral Representations*, Mathematical Research Letters **25** (2018), 1285–1304. 1, 2
[15] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. 7
[16] M. Kisin, *Moduli of finite flat group schemes, and modularity*, Annals of Mathematics. Second Series **170** (2009), no. 3, 1085–1180. 1
[17] V. A. Kolyvagin and D. Yu. Logachëv, *Finiteness of the Shafarevich–Tate group and the group of rational points for some modular abelian varieties* (Russian), Algebra i Analiz **1** (1989), no. 5, 171–196; translation in Leningrad Math. J. **1** (1990), no. 5, 1229–1253. 6
[18] J. Manoharmayum, *On the modularity of certain* $\mathrm{GL}_2(\mathbb{F}_7)$ *Galois representations*, Math. Res. Lett. **8** (2001), no. 5-6, 703–712. 1
[19] D. E. Rohrlich, *Modular curves, Hecke correspondences, and* L*-functions*, pages 41–100 of G. Cornell, J. H. Silverman, and G. Stevens (eds.) *Modular Forms and Fermat's Last Theorem*, Springer, Berlin, 1997. 3
[20] K. Rubin, *Modularity of mod 5 representations*, pp. 463–474 of G. Cornell, J. H. Silverman, and G. Stevens (eds.) *Modular Forms and Fermat's Last Theorem*, Springer, Berlin, 1997. 2
[21] J. Thorne, *Automorphy of some residually dihedral Galois representations*, Mathematische Annalen **364** (2016), no. 1–2, 589–648 1, 2
[22] J. Thorne, *Elliptic curves over* $\mathbb{Q}_\infty$ *are modular*, to appear in Journal of the European Mathematical Society.
[23] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild* 3*-adic exercises*, Journal of the American Mathematical Society **14** (2001), 843–939. 1, 4
[24] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics **141** (1995), no. 3, 443–551.

1

Department of Mathematics, MIT 2-252B, 77 Massachusetts Ave, Cambridge, MA 02139
Email address: drx@mit.edu

Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address: fnajman@math.hr

Mathematics Institute, University of Warwick, CV4 7AL, United Kingdom
Email address: s.siksek@warwick.ac.uk