Modularity of some elliptic curves over totally real fields

Modularity of some elliptic curves over totally real fields

A dissertation presented

by

Bao Viet Le Hung

to

The Department of Mathematics

in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy
in the subject of
Mathematics

Harvard University
Cambridge, Massachusetts

March 2014

Dissertation Advisor: Professor Richard Taylor Bao Viet Le Hung

Modularity of some elliptic curves over totally real fields

Abstract

In this thesis, we investigate modularity of elliptic curves over a general totally real number field, establishing a finiteness result for the set non-modular j-invariants. By analyzing quadratic points on some modular curves, we show that all elliptic curves over certain real quadratic fields are modular.

Contents

Acknowledgements

First and foremost, I would like to thank my advisor, professor Richard Taylor, for suggesting this problem to me, for his constant guidance and encouragement, and for sharing with me his great insights on and beyond the subject of this thesis. It is impossible to overestimate his enormous impact on my mathematical life. I also want to thank Frank Calegari for suggesting the possibility of switching primes at 7, as well as pointing me to the reference [36]. I have also benefitted greatly from discussions with George Boxer, Noam Elkies, Anand Patel, Bjorn Poonen, Maarten Derickx.

I would like to thank the Harvard Mathematics Departments and my fellow graduate students. I felt very blessed to be immersed in such a wonderful intellectual environment. Among the faculty, I would like to specially thank professors Dick Gross and Mark Kisin for teaching me number theory. I especially want to thank Stergios Antonakoudis, George Boxer. Anand Deopurkar, Carl Erickson, Erick Knight, Chao Li, Anand Patel, Sam Raskin, Jack Thorne, Cheng Chiang Tsai, Jerry Wang, Matthew Woolf for countless hours of mathematical discussions that broadened my view and appreciation of diverse subjects beyond number theory. In addition, I would like to thank Oleg Ivrii, Peiyu Tsai for making the department a fun place to be. I would also like to thank the staff at the Harvard Mathematics Department, especially Susan Gilbert for always being there and sort out all administrave issues that come up.

Part of my time as a graduate student was spent at the Institute for Advanced Studies and Princeton University. It is a pleasure for me to thank various faculty, postdocs and graduate students there that made my stays enjoyable: Ana Caraiani, Tasho Kaletha, Rafael von Kanel, Arno Kret, Brandon Levine, Sophie Morel, Naser Talebizadeh Sardari, Will Savin, Peter Sarnak, Chris Skinner, Ila Varma.

Finally, I would like to thank my parents and my girlfriend Linh Pham for always being supportive. Especially I would like to thank my parents for providing a wonderful environment for me to grow up, which ultimately led me to this path in life.

1. Introduction

The classical Shimura-Taniyama conjecture [18] is the statement that every elliptic curve E over $\mathbb{Q}$ is associated to a cuspidal Hecke newform f of the group $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$. Here the meaning of "associated" is that there is an isomorphism between compatible systems of l-adic representations of $G_{\mathbb{Q}}$

$$\rho_{E,l} \simeq \rho_{f,l}$$

where the left-hand side is the representation on the l-adic Tate module of E and the right-hand side is the l-adic representation, constructed by Eichler-Shimura, attached to f, or rather the corresponding cuspidal automorphic representation π_f of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$. In the pioneering work [53], [50], Wiles and Taylor-Wiles established the conjecture for all semi-stable E, which forms the heart of Wiles'proof of Fermat's Last theorem. After many gradual improvements [17], [13], the full conjecture is finally proven in [10]. It is then natural to try to study the generalization of the conjecture to more general number fields F, that is to show that all elliptic curves over F have compatible systems of l-adic representations of G_F associated to a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$. Unfortunately, in this generality the existence of Galois representations associated to π is not known. However, when F is totally real, the required Galois representations have been constructed for some time by Carayol, Wiles, Blasius-Rogawski and Taylor [12],[52], [7] [47], [48], while when F is CM, the Galois representations have only been constructed very recently [28], [39]. In this paper, we focus our attention on the case F totally real. Previous results in this direction include [30], [29], [19], [3], establishing modularity under local restrictions on the elliptic curves or over particular fields. On the other hand, in the contemporary work [25] the authors establish modularity for elliptic curves over real

quadratic fields with full 2-torsion over the base field, as well as a finiteness statement regarding possible non-modular elliptic curves with full 2-torsion over a general totally real field. In this work, we establish the following:

Theorem 1.1. *(see Theorem 4.6) Let F be a fixed totally real number field. Then, up to isomorphism over $\overline{F}$,there are only finitely many elliptic curves E defined over a totally real extension F'/F of degree at most 2 that are not modular.*

An immediate consequence is that there are only finitely many isomorphism classes (over $\overline{\mathbb{Q}}$) of elliptic curves E over (an unspecified) real quadratic field such that E is not modular. Under some restrictions on the field, we can show that no such exceptions exists:

Theorem 1.2. *(see Theorem 5.4) If F is real quadratic such that 5 and 7 are unramified in F, then any elliptic curve E defined over F are modular.*

In fact, with the methods in this paper, it suffices to assume 5 is unramified, see Remark 5.2. In joint work with N.Freitas and S.Siksek, we show that all elliptic curves over real quadratic fields are modular [24] by slightly different computations.

The proof of the above theorems follows the framework introduced by Wiles in [53]. To prove E is modular, it suffices to show any particular $\rho_{E,l}$ is modular. Modularity is then established in three steps:

- Automorphy lifting: If $\rho_{E,l}$ is congruent mod l to an automorphic l-adic representation then $\rho_{E,l}$ is also automorphic, under suitable hypotheses.
- Establish residual automorphy ("Serre's conjecture"): $\overline{\rho}_{E,l}$ is is automorphic for some prime l, and such that the previous step applies.
- Understanding which elliptic curves can not be accessed by the previous two steps, and (ideally) establish automorphy for them by other means.

For the first step, the technology for automorphy lifting has improved greatly since [53], in our context the most important improvements are in [33]. This supplies

very strong lifting statements by combining existing statements in the literature, under usual largeness ("Taylor-Wiles") assumptions of the residual image. We note however that automorphy lifting for small residual images in the literature remain too restrictive for our needs, see Remark 5.1. In Section 2.3, we will state the statements that we need and show how to deduce them from the literature.

For the second step, we follow prime switching arguments of Wiles [53] and Manoharmayum [36]. The basis of such methods is the possibility to find lots of solvable points on modular curves, and as such is known to apply to very few modular curves. Details of the process is content of Section 3.

Having done the first two steps, we are left with understanding elliptic curves for which we fail to establish modularity. These curves are naturally interpreted as points on some special modular curve. Thus we have reduced the problem of establishing modularity of all elliptic curves to determining rational points on a handful of (complicated) modular curves. The curves that arises in this study have very high genus. This is both a blessing and a curse: On the one hand, the study of their arithmetic seems impossibly complicated, but on the other hand, their complexity will force them to have very few rational points. Indeed a study of gonality of the relevant curves in Section 4 allows us to use a theorem of Faltings to establish Theorem 1.1. Due to the dependence on Faltings' theorem, the finiteness statement in Theorem 1.1 is ineffective. Over a general totally real field, it seems hopeless at present to determine all rational points on the modular curves that we need. However, we managed to determine real quadratic points on enough of these modular curves, which in conjunction with some modularity lifting theorems with small residual image, allows us to prove Theorem 1.2. This is carried out in sections 5 and 6. The essential miracle that made the determination of quadratic points possible is that the Jacobians of the modular curves we need to study all have abelian surface factors with Mordell-Weil rank 0 over $\mathbb{Q}$, and that the quadratic points in the resulting list always correspond

to an elliptic curve where either a modularity lifting theorem applies or has CM or is a $\mathbb{Q}$-curve. We remark that there are infinitely many quadratic points of the last type. The modularity of $\mathbb{Q}$-curves follows from Serre's conjecture over $\mathbb{Q}$, which is now a Theorem of Khare-Wintenberger [31]. Conjecturally (and certainly verifiably by a finite computation for each fixed field), there are infinitely many number fields F over which the Jacobian of our modular curves still have relevant abelian surface factors with Mordell-Weil rank 0. The computational determination of their quadratic points over F then carries over for such F, at least in theory. We remark that it is practical to check when a GL_2-type abelian variety over $\mathbb{Q}$ has Mordell-Weil rank 0, by showing that the L-function does not vanish at 1, and this computation can be carried out on a computer. Given any j-invariant, one has in principle an algorithmic procedure for establishing its modularity. However, the presence of the infinite families of degree 2 points corresponding to F-curves poses a problem, since we do not know Serre's conjecture for F.

We have made extensive use of the computer algebra system Magma [9] to perform our computations.

2. Background

Throughout this section we let F be a totally real number field, and $G_F = \mathrm{Gal}(\overline{F}/F)$ the absolute Galois group of F and $\mathbb{A}_F$ the adeles ring of F. For each place v of F let F_v be the corresponding completion of v. If v is non-archimedean, let ϖ_v denote a uniformizer of F_v, $\mathcal{O}_v$ its ring of integers, κ_v its residue field and $\mathrm{N}v = |\kappa_v|$ the size of κ_v. We will fix a choice of decomposition group G_{F_v} in G_F for each finite v, and let $Frob_v$ denote a choice of *arithmetic* Frobenius in G_{F_v}. We normalize the local and global Artin maps by the requirement that arithmetic Frobenius and inverses of uniformizers match. For each prime l, fix once and for all an isomorphism of fields $\iota_l : \mathbb{C} \cong \overline{\mathbb{Q}}_l$. We denote by ϵ_p the p-adic cyclomotic character.

If K is a finite extension of $\mathbb{Q}_p$, ρ is a continuous de Rham (equivalently, potentially semi-stable) representation of G_K on a $\overline{\mathbb{Q}}_p$-vector space W, and $\tau : K \hookrightarrow \overline{\mathbb{Q}}_p$, the multi-set of τ-Hodge-Tate weight of ρ is the multi-set that contains the number i with multiplicity $\dim_{\overline{\mathbb{Q}}_p}(W \otimes_{\tau,K} \widehat{\overline{K}}(i))$. In particular, with this convention ϵ_p has τ-Hodge-Tate weight -1.

2.1. **Automorphic Galois representations.**

In this section we recall what it means for a Galois representation $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}})$ to be automorphic.

Let K_∞ be a maximal compact subgroup of $\mathrm{GL}_2(F \otimes \mathbb{R})$. Under an identification $\mathrm{GL}_2(F \otimes \mathbb{R}) \cong \mathrm{GL}_2(\mathbb{R})^{[F:\mathbb{Q}]}$, we maybe pick $K_\infty = O_2(\mathbb{R})^{[F:\mathbb{Q}]}$, a product of compact orthogonal groups. Let $\mathbb{H}$ denote the complex upper half-plane.

A cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ is an irreducible $(\mathrm{Lie}(\mathrm{GL}_2(F \otimes_{\mathbb{Q}} \mathbb{R}))_{\mathbb{C}}, K_\infty) \times \mathrm{GL}_2(\mathbb{A}_F^\infty)$-module appearing as a subquotient of the space of cuspidal automorphic forms $\mathcal{A}_0(\mathrm{GL}_2(\mathbb{A}_F))$ (see [8]). It has a central character ω_π which is a Hecke character. There is a decomposition

$$\pi \cong \otimes' \pi_v$$

into a restricted tensor product over the places of F, where the local representations π_v are irreducible $((\mathfrak{gl}_2(\mathbb{R}))_{\mathbb{C}}, \mathrm{O}_2(\mathbb{R}))$-modules if v is archimedean, and a smooth irreducible representation of $\mathrm{GL}_2(F_v)$ if v is finite.

For almost all places v, the representation π_v is *unramified*, in the sense that $\pi_v^{K_v} \neq 0$, where $K_v = \mathrm{GL}_2(\mathcal{O}_v)$. In this case, it is known that this space is 1-dimensional. The Hecke algebra $\mathcal{H}_v$ at v is the algebra $\mathcal{C}_c^\infty(K_v \setminus \mathrm{GL}_2(F_v)/K_v)$ of locally constant, K_v bi-invariant $\mathbb{C}$-valued functions, with product given by convolution (where the Haar measure is normalized so that K_v has volume 1). The Satake isomorphism (see [26]) shows that there is an isomorphism

$$\mathcal{H}_v \cong \mathbb{C}[T_v, S_v^{\pm 1}]$$

where S_v, T_v are the characteristic functions of $K_v \left(\begin{smallmatrix} \varpi_v & 0 \\ 0 & 1 \end{smallmatrix}\right) K_v$ and $K_v \left(\begin{smallmatrix} \varpi_v & 0 \\ 0 & \varpi_v \end{smallmatrix}\right) K_v$ respectively. In particular $\mathcal{H}_v$ is commutative, and hence its action on the 1-dimensional vector space $\pi_v^{K_v}$ correspond to an algebra homomorphism $\theta_v : \mathcal{H}_v \to \mathbb{C}$. It determines π_v up to isomorphism.

If π is a cuspidal automorphic representation, we say that π is *regular algebraic* if for each place $v|\infty$, the module π_v restricted to the subgroup $\mathrm{SL}_2^{\pm}(\mathbb{R})$ is a discrete series representation $\mathcal{D}_{k_v}$ described in [34] ($k_v \geq 2$), and the subgroup $\mathbb{R}_{>0} \subset Z(\mathbb{R})$ of the center acts via an algebraic character $x \to x^{w_v}$ for some integer w_v such that $k_v = w_v \bmod 2$. This is equivalent to saying that the infinitesimal character of π_v is the same as the infinitesimal character of an algebraic representation of $\mathrm{GL}_2(\mathbb{R})$. The condition that the central character ω_π is a Hecke character implies that $w_v = w$ is independent of v, because F totally real. We call the tuple $(\underline{k}, w) = ((k_v)_v, w)$ the weight of π.

A regular algebraic cuspidal automorphic representation π is related to the space of classical Hilbert modular forms (as defined in [48], say) in the following manner: There is an operator $N \in \mathrm{Lie}(\mathrm{GL}_2(F \otimes_{\mathbb{Q}} \mathbb{R}))_{\mathbb{C}}$ such that $\pi_\infty^{N=0}$ is 1-dimensional and

for each open compact subgroup $K^\infty \subset \mathrm{GL}_2(\mathbb{A}_F^\infty)$, $\pi^{N=0,K^\infty}$ is identified with a space of classical Hilbert modular form on $\mathrm{GL}_2(F)\backslash(\mathbb{C}\setminus\mathbb{R})^{[F:\mathbb{Q}]}\times \mathrm{GL}_2(\mathbb{A}_F)/K^\infty$, the latter being a finite union of quotients of $\mathbb{H}^{[F:\mathbb{Q}]}$ by congruence subgroups. This correspondence respects Hecke operators. Conversely, a cuspidal Hilbert eigenform determines a unique regular algebraic π (which is a bijection if we restrict to the set of normalized newforms).

For each v such that π_v is unramified, the local L-factor is the function in $s \in \mathbb{C}$ defined by

$$L_v(\pi, s) = (1 - \theta_v(T_v)\mathrm{N}v^{-s} + \theta_v(S_v)\mathrm{N}v^{1-2s})^{-1}$$

With a suitable definition of $L_v(\pi, s)$ for the remaining finite places (depending only on π_v), taking products over finite v we obtain

$$L(\pi, s) = \prod L_v(E, s),$$

the (a twist of the principal) L-function associated to π. It is known [1] that $L(\pi, s)$, a priori only a holomorphic function on some half-plane, admits a holomorphic continuation to all of $\mathbb{C}$, and satisfies a functional equation relating $L(\pi, s)$ and $L(\pi, 2-s)$. The following theorem is the combination of the work of many people [12],[52], [7] [47], [48]

Theorem 2.1. *Fix a prime l and an isomorphism of fields $\iota_l : \mathbb{C} \cong \overline{\mathbb{Q}}_l$. Let π is a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ which is regular algebraic of weight $(\underline{k}, w)$. Then there exists a continuous irreducible Galois representation*

$$\rho_{\pi,l} : G_F \to \mathrm{GL}_2(\overline{\mathbb{Z}}_l)$$

such that

- *$\rho_{\pi,l}$ is unramified at all places $v \not| l$ where π_v is unramified, and in which case*

$$\det(1 - \rho_{\pi,l}(Frob_v)X) = 1 - \iota_l\theta_v(T_v)X + \iota_l\theta_v(S_v)NvX^2.$$

- *For $v|l$, the representation $\rho_{\pi,l}|_{G_{F_v}}$ is potentially semi-stable with τ-Hodge-Tate weight $(k_{\iota_l^{-1}\tau} + w - 2)/2, (w - k_{\iota_l^{-1}\tau})/2$*
- *For any complex conjugation $c \in G_F$, $\det \rho_{\pi,l}(c) = -1$.*

Remark 2.1.

(1) By the Chebotarev density theorem, knowing the equality above for a density one set of places v determines $\rho_{\pi,l}$ up to semi-simplification, and hence $\rho_{\pi,l}$.

(2) $\det \rho_{\pi,l}$ correspond via class field theory to the l-adic character associated to the algebraic Hecke character $\omega_\pi||^{-1}$.

(3) It is known that for π regular algebraic, the collection $\theta_v(T_v), \theta_v(S_v)$ generates a number field, and hence the $\rho_{\pi,l}$ form a weakly compatible system in the sense of [49]. They in fact form a strongly compatible system.

(4) (Local-global compatibility) The (Frobenius-semisimplification of the) Weil-Deligne representation associated to $\rho_{\pi,l}|_{G_{F_v}}$ and π_v determine each other via the Local Langlands Correspondence.

2.2. **Modular elliptic curves.** Let E be an elliptic curve defined over F. The l-adic Tate module T_lE is defined as

$$T_lE = \varprojlim E[l^n](\overline{F})$$

where the transition maps are multiplication by l. It is a free $\mathbb{Z}_l$-module of rank 2 with a continuous action of G_F, hence a 2-dimensional l-adic representation $\rho_{E,l}$ of G_F. It is known that

- For all places $v \not| l$ such that E has good reduction, $\rho_{E,l}$ is unramified at v, and

$$\det(1 - \rho_{E,l}(Frob_v)X) = 1 - a_v(E)X + \mathrm{N}vX^2,$$

  where $a_v(E) = 1 + \mathrm{N}v - |\overline{E}_v(k_v)|$ and $\overline{E}_v$ is the reduction of E mod v.
- For all places $v|l$, the representation $\rho_{E,l}|_{G_{F_v}}$ is potentially semi-stable with τ-Hodge-Tate weight 0, -1 for any $\tau : F_v \hookrightarrow \overline{\mathbb{Q}}_l$. It is (potentially) reducible if and only if E has multiplicative or potentially good ordinary reduction at v.
- $\det \rho_{E,l} = \epsilon_l$ is the l-adic cyclotomic character.
- $\rho_{E,l}$ is irreducible.

For $v \not| l$ a place of good reduction, the local L-factor at v is the function in $s \in \mathbb{C}$

$$L_v(E,s) = (\det(1 - \rho_{E,l}(Frob_v)\mathrm{N}v^{-s}))^{-1} = (1 - a_v(E)\mathrm{N}v^{-s} + \mathrm{N}v^{1-2s})^{-1}$$

With a suitable definition of $L_v(E,s)$ for the remaining finite places (depending only on the local behavior of E at v), taking products over all finite v we obtain

$$L(E,s) = \prod L_v(E,s),$$

the L-function of E. The product converges on $\Re s > 3/2$ to a holomorphic function. It is a central problem is to establish holomorphic (or at least meromorphic) continuation of $L(E,s)$ to the whole complex plane, e.g. to formulate the Birch-Swinnerton-Dyer conjecture for E. We come to the following central definition

Definition 2.2. *An elliptic curve E defined over F is called modular if for one (equivalently, any) prime l, there is a regular algebraic cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ such that there is an isomorphism of Galois representations*

$$\rho_{E,l} \cong \rho_{\pi,l}.$$

Remark 2.2.

(1) Since $\rho_{\pi,l}$ determines π, there is at most one π satisfying the above. Such a π must have Hecke eigenvalues in $\mathbb{Z}$, have trivial central character and weight $((2,2,..,2),0)$ (i.e. correspond to a Hilbert eigenform of parallel weight 2).

(2) By a theorem of Faltings, $\rho_{E,l}$ determines E up to F-isogeny. Thus if every elliptic curve over F is modular then we have an injection from the set F-isogeny classes of elliptic curves over F to the set of normalized Hilbert newforms with rational Hecke eigenvalues. It is expected to be a bijection, as discussed in the remark below.

(3) If E is modular, $L(E,s) = L(\pi,s)$, and thus the L-function of E has holomorphic continuation and expected functional equation. The only known method to establish these analytic properties for $L(E,s)$ is via modularity of E.

(4) Over $\mathbb{Q}$, the above is one possible formulation of modularity of E [18]. An equivalent formulation for modularity of an elliptic curve E defined over $\mathbb{Q}$ is that there is a non-constant morphism of algebraic curves (either over $\mathbb{C}$ or $\mathbb{Q}$) $X_0(N) \to E$, where $X_0(N)$ is the standard modular curve of level $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$, i.e. E is dominated by a modular curve. Furthermore, given a weight 2 modular form on $\Gamma_0(N)$, there is a construction of an elliptic curve E_f with the same l-adic representation as $\rho_{f,l}$, and modularity of E is equivalent to E being isogenous to one such E_f.

Over a general totally real field, one does not know how to construct an elliptic curve from a parallel weight 2 Hilbert eigenform (or the corresponding automorphic representation π). One difficulty is that one does not expect to find E in the Albanese variety of any Shimura variety (and in fact, it seems that the motive of some E does not show up in any Shimura variety at all. We learnt this from [6]). However, when $[F:\mathbb{Q}]$ is odd, or π_v is essentially square-integrable at some finite v, one can construct an elliptic curve E_π in

the Jacobian of a suitable Shimura curve, exactly as in the situation over $\mathbb{Q}$. Consequently, if either $[F : \mathbb{Q}]$ is odd or E has multiplicative reduction at some finite place, then modularity of E is equivalent to E being dominated by a Shimura curve over F. In general, Blasius [6] has shown that E exists conditional on Deligne's conjecture that all Hodge cycles are absolutely Hodge.

Definition 2.3. *An elliptic curve E defined over $\overline{\mathbb{Q}}$ is called a $\mathbb{Q}$-curve if $E^\sigma = E \otimes_{\overline{\mathbb{Q}},\sigma} \overline{\mathbb{Q}}$ is isogenous to E for all $\sigma \in G_{\mathbb{Q}}$.*

In particular, an elliptic curve over $\mathbb{Q}$ is a $\mathbb{Q}$-curve, but the converse is false. The following proposition collects some general facts that will be used later:

Proposition 2.4. *Let E be an elliptic curve defined over a totally real field F.*

(1) If E has CM, then E is modular.

(2) If E is a $\mathbb{Q}$-curve then E is modular.

(3) If E is modular and E' is another curve such that $j(E') = j(E)$ then E' is modular.

Proof.

(1) If E has CM by an order in an imaginary quadratic field K, then $\rho_{E,l}|_{G_{FK}}$ has abelian image, hence $\rho_{E,l}$ is isomorphic to the induction of a character of G_K, which corresponds to an algebraic Hecke character by class field theory. The automorphic induction of this Hecke character gives the required automorphic representation π.

(2) It is shown in [38] that Serre's modularity conjecture over $\mathbb{Q}$ (proven in [31], [32]) implies that any $\mathbb{Q}$-curve is an isogeny factor of the Jacobian of a modular curve $X_0(N)$ over $\overline{\mathbb{Q}}$. In [23], it is shown how to extend the Galois representation $\rho_{E,l} : G_F \to \mathrm{GL}_2(\mathbb{Q}_l)$ to an l-adic representation $\rho_l : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_l)$, and that the modularity of E (in the sense of [38]) is equivalent to ρ_l being automorphic. Thus there is a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$

such that $\rho_{\pi,l} \cong \rho_l$. By [**?**], there exists a cuspidal automorphic representation $BC(\pi)$ of $\mathrm{GL}_2(\mathbb{A}_F)$ such that $\rho_{BC(\pi),l} \cong \rho_{\pi,l}|_{G_F}$, and hence E is modular.

(3) If $j(E) = 0$ or 1728 then E is CM and thus is modular. Otherwise, E' must be a quadratic twist of E, so $\rho_{E,l} \cong \rho_{E',l} \otimes \chi$ for a quadratic character χ, because the automorphism group of E is $\{\pm 1\}$. χ corresponds to a Hecke character which we abusively also call χ. If $\rho_{E,l} \cong \rho_{\pi,l}$ then $\rho_{E',l} \cong \rho_{\pi\otimes\chi,l}$.

□

2.3. **Modularity lifting theorems.** If $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Z}}_p)$ is a continuous representation and $\rho_v = \rho|_{G_{F_v}}$ is the local representation at a place $v|p$, recall that ρ_v is ordinary if

$$\rho_v \cong \begin{pmatrix} \psi_1^{(v)} & * \\ 0 & \psi_2^{(v)} \end{pmatrix},$$

where $\psi_1^{(v)}$, $\psi_2^{(v)}$ are Hodge-Tate characters of G_{F_v} with τ-Hodge-Tate weights $k_{\tau,1} < k_{\tau,2}$, for each $\tau : F_v \hookrightarrow \overline{\mathbb{Q}}_p$. In this case, we say that ρ_v is distinguished if the reduction of the characters $\overline{\psi}_1^{(v)} \neq \overline{\psi}_2^{(v)}$. If $\rho' : G_F \to \mathrm{GL}_2(\overline{\mathbb{Z}}_p)$ is another representation lifting $\overline{\rho}$, we say that ρ' is a $\overline{\psi}_2$-good lift of $\overline{\rho}$ if $\rho'_v \cong \left(\begin{smallmatrix} \phi_1 & * \\ 0 & \phi_2 \end{smallmatrix}\right)$ and ϕ_2 is lifts $\overline{\psi}_2$.

We record the following modularity lifting statement which is optimized for our purposes:

Theorem 2.5. *Let $p > 2$ be prime, F a totally real field, $\rho : G_F \to GL_2(\mathbb{Z}_p)$ a continuous representation. Assume*

- *ρ is unramified for almost all places v of F.*
- *For each place $v|p$, $\rho_v = \rho|_{G_{F_v}}$ is potentially semi-stable of with τ-Hodge-Tate weight 0, -1 for each embedding $\tau : F_v \hookrightarrow \overline{\mathbb{Q}}_p$.*
- $\det \rho \cong \epsilon$ *is the (p-adic) cyclotomic character.*
- $\overline{\rho}|_{G_{F(\zeta_p)}}$ *is absolutely irreducible.*

- *$\overline{\rho}$ is modular of weight 2, that is there exists a regular algebraic cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight $((2,2,\cdots 2),0)$ with associated Galois representation $\rho_{\pi,p}$ such that $\overline{\rho}_{\pi,p} \cong \overline{\rho}$.*

Then ρ is modular

Proof. This is the combination of various theorems in the literature. When $p \neq 5$, this follows from Theorem 3.2.3 of [11] (when ρ_v is potentially crystalline for all $v|p$ and $\overline{\rho}$ admits an ordinary lift then it follows from the main result of [33]). For the convenience of the reader, we now give a summary of the argument in [11].

The essential point is to find (after a totally real solvable base change) an automorphic representation π_0 with the property that for all $v|p$, the local representations $\rho_{\pi_1,p}|_{G_{F_v}}$ and $\rho|_{G_{F_v}}$ lie in the same irreducible component inside the semi-stable (framed) deformation space with τ-Hodge-Tate weights 0, -1 of the trivial mod p G_{F_v}-representation. This deformation space has exactly three irreducible component when F_v is large enough (which we can assume after a solvable base change), corresponding to ordinary crystalline lifts, non-ordinary crystalline lifts and lifts that are extensions of the trivial character by ϵ. Call S_{ord}, S_{nord} and S_{st} the set of places $v|p$ where ρ is ordinary crystalline, non-ordinary crystalline and semi-stable non-crystalline, respectively. From our hypothesis, [5] shows that we can find an automorphic representation π_1 such that $\rho_{\pi_1,p}$ lifts $\overline{\rho}$ and is ordinary crystalline at all $v|p$. After a further solvable base change one can construct an automorphic representation π_2 for $D^{\times}_{\mathbb{A}}$, with D the quaternion algebra ramified at ∞ and at $v \in S_{st}$, such that $(\pi_2)_v$ is trivial at $v \in S_{st}$ and is ordinary at all other $v|p$. Exactly the same argument as in Corollary (3.1.6) [33] for the space of automorphic forms on D then produces the desired π_0. The theorem now follows from an $R^{red} = T$ theorem similar to the one in [33], with the difference that at places $v \in S_{st}$ we use the non-crystalline component of the local deformation space.

We now show what needs to be done when $p = 5$. In [11], the authors assumed that the projective image of $\overline{\rho}|_{G_{F(\zeta_5)}}$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_5)$ is not isomorphic to $\mathrm{PSL}_2(\mathbb{F}_5)$. This is only used to assure the existence of Taylor-Wiles systems as in [33] 3.2.3. We now show that we can still choose Taylor-Wiles systems without this hypothesis, but with the assumption that $\overline{\rho}$ has cyclotomic determinant. With the notation in [33] 3.2.3 and following the proof of Theorem 2.49 in [15], what we need to show is that we can find for each n and a non-trivial cocycle $\psi \in H^1(G_{F,S}, \mathrm{ad}^0\overline{\rho}(1))$, we can find a place $v \notin S$ of F such that

- $|k(v)| = 1 \bmod p^n$ and $\overline{\rho}(Frob_v)$ has distinct eigenvalues.
- The image of ψ under the restriction map

$$H^1(G_F, \mathrm{ad}^0\overline{\rho}(1)) \to H^1(G_{F_v}, \mathrm{ad}^0\overline{\rho}(1))$$

  is non-trivial.

Let F_m be the extension of $F(\zeta_{p^m})$ cut out by $\mathrm{ad}^0\overline{\rho}$, then the argument in [15] works once we can show that the restriction of ψ to $H^1(G_{F_0}, \mathrm{ad}^0\overline{\rho}(1))$ is non-trivial. To do this we want to show that $H^1(\mathrm{Gal}(F_0/F), \mathrm{ad}^0\overline{\rho}(1)^{G_{F_0}}) = 0$. Because G_{F_0} acts trivially on $\mathrm{ad}^0\overline{\rho}$, the coefficient module vanishes unless $\zeta_p \in F_0$. We now assume that $\zeta_p \in F_0$. Let $\chi : \mathrm{PGL}_2(\mathbb{F}_p) \to \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ be the character induced by the determinant. Because $H^1(\mathrm{PSL}_2(\mathbb{F}_5), \mathrm{Sym}^2\mathbb{F}_5^2) = H^1(\mathrm{PGL}_2(\mathbb{F}_5), \mathrm{Sym}^2\mathbb{F}_5^2(\chi)) = \mathbb{F}_5$ does not vanish, the extra hypothesis when $p = 5$ was needed to exclude the possibility that $\mathrm{Gal}(F_0/F) = \mathrm{PSL}_2(\mathbb{F}_5)$ or $\mathrm{PGL}_2(\mathbb{F}_5)$ and $\zeta_5 \in F_0$. However, under our cyclotomic determinant assumption, these cases can not occur: If $\mathrm{Gal}(F_0/F) = \mathrm{PSL}_2(\mathbb{F}_5)$, the determinant of $\overline{\rho}$ must take value in $(\mathbb{F}_5^\times)^2$, and thus $\sqrt{5} \in F$. But $\zeta_5 \in F_0 \setminus F$ implies $\mathrm{Gal}(F_0/F) = \mathrm{PSL}_2(\mathbb{F}_5) = A_5$ has a quotient of order 2, a contradiction. If $\mathrm{Gal}(F_0/F) = \mathrm{PGL}_2(\mathbb{F}_5)$, the determinant of $\overline{\rho}$ takes non-square values, and hence $\sqrt{5} \notin F$. It follows that $\mathrm{Gal}(F_0/F) = \mathrm{PGL}_2(\mathbb{F}_5)$ admits a surjection onto $\mathbb{F}_5^\times$, which is impossible. $\square$

Remark 2.3. The lifting theorem in [33] requires one to have a modular lift which lies in the same connected component ("ordinary" or "non-ordinary") as ρ at all places above v. guarantees such a lift once we have an ordinary automorphic lift of $\overline{\rho}$. In general, one can appeal to [4], for the existence of ordinary lifts, however in situations when we apply Theorem 2.5, we could always guarantee an ordinary automorphic lift (either by Hida theory or by choosing our auxilliary elliptic curves in the argument below judiciously).

The following is an immediate corollary of Theorem 2.5, the above remark and the fact that the representation $\rho_{E,p}$ coming from an elliptic curve E is potentially semi-stable at all $v|p$ with Hodge-Tate weights 0, -1:

Corollary 2.6. *Let E be an elliptic curve defined over a totally real field F and $p > 2$ is a prime such that $\overline{\rho}_{E,p}|_{G_{F(\zeta_p)}}$ is absolutely irreducible, and $\overline{\rho}_{E,p}$ is modular. Then E is modular.*

We now recall the following theorem of Skinner-Wiles [44], as corrected in Theorem 1, [42].

Theorem 2.7. *Let $p > 2$ $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Z}}_p)$ be a continuous representation such that*

- *ρ is unramified for almost all places v of F.*
- *For each place $v|p$, ρ_v is ordinary and distinguished.*
- *$\det \rho = \psi \epsilon^{w-1}$ for some $w \in \mathbb{Z}$ and ψ a finite order character, and $\det \rho(c) = -1$ for all complex conjugation $c \in G_F$.*
- *$\overline{\rho}$ is absolutely irreducible.*
- *There is a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ such that ρ_π is a $\overline{\psi}_2^{(v)}$-good lift of $\overline{\rho}$ for all $v|p$.*
- *If $\overline{\rho}|_{G_{F(\zeta_p)}}$ is reducible and the quadratic subfield F^* of $F(\zeta_p)/F$ is a CM extension, then not every place $v|p$ of F splits in F^*.*

Then ρ is modular.

Compared to Theorem 2.5, the most important difference is that we require a weaker hypothesis on $\overline{\rho}$, at the expense of more restrictive condition on the local representations at $v|p$.

Corollary 2.8. *Let $p > 2$ be a prime, and F a totally real number field such that p is unramified in F. Let E be an elliptic curve defined over F such that E has multiplicative or potentially good ordinary reduction at all places $v|p$, and that the representation $\overline{\rho}_{E,p}$ is irreducible. If $\overline{\rho}_{E,p}|_{G_{F(\zeta_p)}}$ is absolutely irreducible, assume furthermore that $\overline{\rho}_{E,p}$ is modular. Then E is modular.*

Proof. Put $\rho = \rho_{E,p}$. In view of Corollary 2.6, we only need to consider the case $\overline{\rho}$ is irreducible, but absolutely reducible when restricted to $G_{F(\zeta_p)}$. Since the latter is a normal subgroup of G_F, this can only happen if $\overline{\rho}$ is the induction of a character of G_{F^*}, where F^* is the quadratic subextension of $F(\zeta_p)/F$. Since p is unramified in F, the extension F^*/F is totally ramified at all places $v|p$, so the last condition in theorem 2.8 holds. The assumption on the local behavior of E at $v|p$ implies (in fact, is equivalent to) that ρ is ordinary at all $v|p$. Furthermore, we know that for some finite Galois extension F'_v/F_v, there is a line $L \subset V_pE$ in the rational Tate module of E which is $G_{F'_v}$-stable on which $I_{F'_v}$ acts via the cyclotomic character, and $I_{F'_v}$ acts trivially on V_pE/L. As $G_{F'_v}$ is a normal subgroup of G_{F_v}, this implies that L is in fact stable under G_{F_v}.

We claim that ρ_v is distinguished. Since ρ_v preserves the flag $L \subset V_pE$ and $\det \rho = \epsilon$, we see that

$$\begin{pmatrix} \epsilon\psi^{-1} & * \\ 0 & \psi \end{pmatrix}$$

where ψ is a $\mathbb{Z}_p^\times$-valued character. If ρ_v were not distinguished, that means $\epsilon = \psi^2$ mod p, contradicting the fact that $\overline{\epsilon}(G_{F_v}) = \mathbb{F}_p^\times$, since F_v and $\mathbb{Q}_p(\zeta_p)$ are linearly

disjoint. Finally, it remains to find a $\overline{\psi}$-good automorphic lift of $\overline{\rho}$. This is possible by the following lemma (see Lemma 5.1.2 of [3])

Lemma 2.9. *If $\overline{\rho}$ has dihedral image, then $\overline{\rho}$ admits a ($\overline{\psi}$-)good p-ordinary regular algebraic cuspidal lift.*

Thus all conditions of Theorem 2.8 are satisfied and E is modular. □

3. Residual modularity and prime switching

If $\rho_{E,p}$ is a Galois representation coming from the Tate module of an elliptic curve over E, then the first three items of 2.5 are satisfied, and it remains to consider the last two items. In particular, we need to have access to enough mod p modular Galois representations (of weight 2). The basic starting point is

Theorem 3.1. *(Langlands-Tunnell* [35], [51]*) If F is a totally real field and $\rho : G_F \to \mathrm{GL}_2(\mathbb{C})$ is an odd Artin representation with solvable projective image then ρ is modular.*

Using this, the argument at the beginning of [53], Chapter 5 shows that if E is an elliptic curve F then $\overline{\rho}_{E,3}$ is congruent to the Galois representation ρ_π associated to a Hilbert modular form of weight 1. Such a representation is ordinary at all places $v|3$, and hence [52], Theorem 1.4.1 shows that ρ_π is obtained by the specialization of a Hida family to parallel weight 1. Specializing the family at parallel weight 2 then shows that $\overline{\rho}_{E,3}$ is in fact modular of weight 2. Thus $\overline{\rho}_{E,3}$ is always modular of weight 2. Starting from this, we can propagate residual modularity:

Proposition 3.2. *Let E be an elliptic curve over a totally real field F. Then*

(1) There exists an elliptic curve E' over F such that

- $\overline{\rho}_{E,5} \cong \overline{\rho}_{E',5}$
- $\mathrm{Im}\, \overline{\rho}_{E',3} \supset \mathrm{SL}_2(\mathbb{F}_3)$

In particular, $\overline{\rho}_{E,5} \cong \overline{\rho}_{E',5}$ is modular of weight 2.

(2) There exists an elliptic curve E' over a solvable extension F' of F such that

- $\overline{\rho}_{E,7}|_{G_{F'}} \cong \overline{\rho}_{E',7}$
- $\operatorname{Im} \overline{\rho}_{E',7} = \operatorname{Im} \overline{\rho}_{E,7}$
- $\operatorname{Im} \overline{\rho}_{E',3} \supset \mathrm{SL}_2(\mathbb{F}_3)$

Before giving the proof, we first collect various facts that we will use.

Given an elliptic curve E over F, we have a finite (étale) group scheme $E[p]$ over F, and thus we have a twisted modular curve $X_E(p)$ defined over F which classifies isomorphism classes of (generalized) elliptic curves E' together with a symplectic isomorphism of group schemes

$$E[p] \cong E'[p]$$

Indeed one has such a twisted modular curve over F for any Galois representation $\overline{\rho} : G_F \to \mathrm{GL}_2(\mathbb{F}_p)$ with cyclotomic determinant, by replacing $E[p]$ with the group scheme $\mathcal{G}$ with descent data given by ρ. Then:

- $X_E(5)$ has genus 0 and has a rational point (corresponding to E), hence is isomorphic to $\mathbb{P}^1$ over F. The variety parameterizing bases (P, Q) of the 3-torsion subscheme of the universal elliptic curve over $X_E(5)$ is defined over F and has two geometric connected components, which are covers of $X_E(5)$ of degree $|\mathrm{SL}_2(\mathbb{F}_3)|$ (each component is isomorphic to $X(15)$ over $\mathbb{C}$).
- The modular curve $X_{\overline{\rho}}$ for the mod 7 Galois representation $\overline{\epsilon}_7 \oplus 1$ is isomorphic (over F) to the Klein quartic

$$X^3Y + Y^3Z + Z^3X = 0$$

in $\mathbb{P}^2$. The twisted modular curve $X_E(7)$ is thus a form of the Klein quartic over F, and hence is a smooth non-hyperelliptic curve of genus 3. The canonical embedding realizes $C = X_E(7)$ as a plane quartic $C \hookrightarrow \mathbb{P}^2$ over F.

Lemma 3.3. *Let C be the Klein quartic over $\mathbb{C}$. Let $L = \mathbb{P}H^0(C, \Omega^1) \hookrightarrow \mathrm{Sym}^4 C$ and $Z = L \times_{\mathrm{Sym}^4 C} C^4$ be the space of ordered quadruple of collinear points on C. Then Z irreducible and $Z \to L$ is generically Galois with Galois group S_4.*

Proof. Let $\Sigma \subset C \times L$ be the incidence correspondence of pairs (P, l) where P is a point on C and l is a line passing through P. The projection $\Sigma \to C$ realizes Σ as a $\mathbb{P}^1$-bundle over C, hence is irreducible. We claim that the monodromy group of the degree 4 covering $\Sigma \to L$ is S_4. The plane quartic C has only finitely many bitangents and finitely many flexes (over $\mathbb{C}$) [22], hence for a general point in the plane, the projection from the point gives a ramified covering $C \to \mathbb{P}^1$ which is simply ramified, that is each fiber has at most one ramification point, and if there is one it has ramification index 2. The monodromy group of this cover must be S_4, as it is a subgroup of S_4 which is transitive and is generated by transposition (see the lemma below). The above covering can be realized as the the pullback of the covering $\Sigma \to L$ over the $\mathbb{P}^1$ of lines passing through the chosen general point, and thus the monodromy group of this cover must be all of S_4, and its Galois closure must be birational to Z and Z must be irreducible. □

We thank Omar Antolin Camarena for showing us the following lemma and its proof:

Lemma 3.4. *If G is a subgroup of the symmetric group S_d which is transitive and is generatd by transpositions, then $G = S_d$.*

Proof. Draw a graph on $\{1, ...d\}$, where there is an edge between i and j if there is a transposition (ij) in the generating set of G. Because G is transitive, the graph is connected. Given any vertices i, j there is thus a path $i_0 = i, i_1, \cdots, i_n = j$ joning them. Then $(i_n i_{n-1}) \cdots (i_2 i_1)(i_0 i_1)(i_2 i_1) \cdots (i_n i_{n-1}) = (ij)$ is in G, hence Gcontains all transpositions. □

Lemma 3.5. *Let $C = X(7)$ be the modular curve with full level 7 structure over $\mathbb{C}$. Fix a non-trivial $\zeta \in \mu_3(\mathbb{C})$, and let T_ζ denote the space parameterizing bases (P, Q) of the 3-torsion subgroup of the universal elliptic curve over C, such that the Weil pairing $e_3(P, Q) = \zeta$. Let $Z \hookrightarrow C^4$ denote space of ordered quadruples which are collinear (under the canonical embedding of C). Put $Y = Z \times_{C^4} T_\zeta^4$. Then each irreducible component of Y has degree $\geq 24^4/3$ over Z.*

Proof. Put $G = \mathrm{SL}_2(\mathbb{F}_3)$. $\widetilde{G} = G^4 \rtimes S_4$, where S_4 acts by permuting the coordinates on G^4. Let $L = \mathbb{P}H^0(C, \Omega^1) \hookrightarrow \mathrm{Sym}^4 C$ as in the previous lemma. The cover $Y \to L$ is generically étale with Galois group $\widetilde{G}$. Let Y_0 be an irreducible component of Y, then $Y_0 \to L$ is generically étale with Galois group a subgroup $\widetilde{H} \subseteq \widetilde{G}$, which surjects onto S_4. Let $H = \widetilde{H} \cap G^4$.Now for each pair (i, j) with $1 \leq i, j \leq 4$ we have a comutative diagram

$$\begin{array}{ccccc} Y_0 & \longrightarrow & T_\zeta^4 & \xrightarrow{pr_{ij}} & T_\zeta^2 \\ \downarrow & & \downarrow & & \downarrow \\ Z & \longrightarrow & C^4 & \xrightarrow{pr_{ij}} & C^2 \end{array}$$

The composition map $Z \to C^2$ is generically a 2 to 1 cover. Because $G/[G, G] \cong \mathbb{Z}/3\mathbb{Z}$, $G \times G$ has no non-trivial homomorphism to $\mathbb{Z}/2\mathbb{Z}$, hence the function fields $\mathbb{C}(Z)$ and $\mathbb{C}(T_\zeta^2)$ are linearly disjoint over $\mathbb{C}(C^2)$. It follows that via the projection to the (i, j) factors, there is a surjection $H \twoheadrightarrow G^2$. Let us now consider the image $\overline{H}$ of H under the projection to any 3 coordinates G^3. Then for each $a, b \in G$, there is some $(a, 1, \phi_1(a)) \in \overline{H}$ and $(b, \phi_2(b), 1) \in \overline{H}$. Thus the commutator $(aba^{-1}b^{-1}, 1, 1) \in \overline{H}$. It follows that $\overline{H} \supseteq [G, G]^3$. Now for any $a \in [G, G]$, $b \in G$ we have some $(a, 1, 1, \psi_1(a)) \in H$ by what we just proved, and some $(b, \psi_2(b), \psi_3(b), 1) \in G$. Taking commutators and noting that $[G, [G, G]] = [G, G]$ we see that $H \supset [G, G]^4$ strictly. The image of H in $(G/[G, G])^4$ is an $\mathbb{F}_3$-vector space, whose projection to any two coordinates are surjective. Because the composition factor of the natural representation

of S_4 on $\mathbb{F}_3^4$ consists of the trivial representation and a three-dimensional representation, the image of H must be either an irreducible three-dimensional subrepresenation or all of $\mathbb{F}_3^4$. In particular, the index of H in G^4 is at most 3. $\square$

Lemma 3.6. *(see* [37]*) Let C be a smooth plane quartic defined over $\mathbb{F}_q$. If $q > 300$, then there exists a line l that intersects C at 4 distinct rational points.*

Finally, we record a variant of Ekedahl's effective version of Hilbert's irreducibility theorem:

Lemma 3.7. *Let X be a geometrically irreducible variety over a number field K. Assume X satisfies weak approximation. Let G be a finite group and $Y \to X$ a G-torsor defined over K. Let H be the stablilizer of an irreducible component of $Y \otimes_K \mathbb{C}$. Then the set of rational points $x \in X(K)$ such that each point in the fiber Y_x has degree $\geq |G|/|H|$ satisfies weak approximation.*

Proof. The cover $Y \to X$ is Galois of degree $|G|$ and the number of geometrically irreducible component of Y is $|G|/|H|$. Let us pick a large number field K' such that $Y \otimes K'$ is isomorphic to a disjoint union $Y = \coprod Y_0$, and the map $Y \to L$ factorizes as $\coprod Y_0 \to \coprod L \to L$ over F'. Now the (proof of) the main result of [20] shows that the fiber of a point u $L(F')$ in $Y_0(F')$ (for the covering $Y_0 \to L$ coming from the first term in the above disjoint union) is connected as long as u is chosen to lie in a finite list of suitable (v-adic) open subsets of $L(F'_v)$ for a finite list of finite places v with large norm. We can then in particular assume in addition that the v we choose above are lying over primes in F that are completely split in F'. This allows us to identify $U_v \subset L(F_v)$. Now if we pick a rational point $l \in L(F)$ such that $l \in U_v \subset L(F_v)$ for the above chosen U_v, it follows that the fiber over l must contain a point of degree $\geq g/h \geq 24^5/3$ over F. But as the Galois group of the cover act transitively on this fiber, the same must hold for all other points in the fiber. Since L satisfy weak

approximation, we could furthermore require l to land in small neighborhood at any given finite list of places. $\square$

Proof. (1) (see [53]) The variety parameterizing bases (P, Q) of the 3-torsion subscheme of the universal elliptic curve over $X_E(5)$ has 2 geometric connected components, which are covers of $X_E(5)$ of degree $|\mathrm{SL}_2(\mathbb{F}_3)|$ (they are geometrically isomorphic to $X(15)$). Hence Hilbert's irreducibility theorem shows that one can find an F-rational point on $X_E(5)$, corresponding to an elliptic curve E' such that the field cut out by $E'[3]$ has degree ≥ 24 over F, giving the desired curve because $\mathrm{SL}_2(\mathbb{F}_3)$ is the unique proper subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ of size ≥ 24. Theorem 2.5 then shows that E' is modular, hence the last assertion.

(2) This is a more elaborate version of the above argument. We will follow the general approach in [36], giving some further details. Let L denote the space of lines inside this $\mathbb{P}^2$, then L is the dual projective space and is isomorphic to $\mathbb{P}^2$. Let $Z \hookrightarrow C^4$ be the subvariety consisting of ordered quadruple of points on C that are collinear. Note that $Z = L \times_{\mathrm{Sym}^4 C} C^4$, where $\mathrm{Sym}^4 C = C^4/S_4$ is the fourth symmetric power of C. By lemma 3.3 Z is geometrically irreducible and the cover $Z \to L$ is generically Galois with Galois group S_4.

Let T denote the variety parameterizing bases (P, Q) for the 3-torsion subscheme of the universal elliptic curve over C, it is a $\mathrm{GL}_2(\mathbb{F}_3)$-torsor over the complement of the cusps on C. Define $Y = Z \times_{C^4} T^4$. By lemma 3.5, each geometric irreducible component of Y has degree $\geq 24^5/3$ over L. We claim that the subset of F-rational lines l such that the fibers in Y over l each have degree $\geq 24^5/3$ and the fiber in Z over l is connected also satisfies weak approximation. Indeed, the cover $Y \to L$ is Galois of degree g, and suppose h is the number of geometrically irreducible component of Y. Let us pick a large number field F' such that $Y \otimes F'$ is isomorphic to a disjoint union $Y = \coprod Y_0$,

and the map $Y \to L$ factorizes as $\coprod Y_0 \to \coprod L \to L$ over F'. Now the (proof of) the main result of [20] shows that the fiber of a point u $L(F')$ in $Y_0(F')$ (for the covering $Y_0 \to L$ coming from the first term in the above disjoint union) is connected as long as u is chosen to lie in a finite list of suitable (v-adic) open subsets of $L(F'_v)$ for a finite list of finite places v with large norm. We can then in particular assume in addition that the v we choose above are lying over primes in F that are completely split in F'. This allows us to identify $U_v \subset L(F_v)$. Now if we pick a rational point $l \in L(F)$ such that $l \in U_v \subset L(F_v)$ for the above chosen U_v, it follows that the fiber over l must contain a point of degree $\geq g/h \geq 24^5/3$ over F. But as the Galois group of the cover act transitively on this fiber, the same must hold for all other points in the fiber. Since L satisfy weak approximation, we could furthermore require l to land in small neighborhood at any given finite list of places.

If a line l has the above properties, l intersects C at four points whose residue field is an S_4 Galois extension of F' of F. The 4 intersection points give rise to 4 elliptic curves E_i over F', which are conjugates of each other, hence the degree d of the extension $F'(E_i[3])$ obtained by adjoining the 3-torsion points of E_i is independent of i. On the other hand, the extension over F' generated by adjoining all the 3-torsion points of all the E_i has degree $\geq 24^4/3$ over F', thus we have $d^4 \geq 24^4/3$. But any subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ of such size d must contain $\mathrm{SL}_2(\mathbb{F}_3)$. Thus to finish the proof, we only need to arrange that the intersection points are defined over a totally real extension of F, and that the mod 7 Galois representation of the elliptic curves corresponding to the intersection points have as large image as $\mathrm{Im}\,\overline{\rho}_{E,7}$. This will be done by using the weak approximation property to find a line l as above which lies in open subsets U_v for v running over a finite set of places of F chosen as follows:

- For each $v|\infty$, because $\overline{\rho}_{E,7}$ has cyclotomic determinant, $X_E(7) \times_F F_v$ is actually isomorphic to the Klein quartic, and thus we find an explicit line l_v which intersects C at 4 non-cuspidal real points, for example the line $3X + Y = 0$. Every line in a small open neighborhood (for the strong topology) of l_v will then have the same property. Shrinking U_v, we can assume it contains no line passing through a cusp.
- By the Chebotarev density theorem, for each element $g \in \operatorname{Im} \overline{\rho}_{E,7}$, there are infinitely many places v such that $\overline{\rho}|_{G_{F_v}}$ is unramified and the image of $Frob_v$ is conjugate to g. Pick such a v for each g, such that C has good reduction and reduces to a smooth plane quartic $\overline{C}$. If a Galois extension F' of F is such that all places v in this list splits completely, then F' is linearly disjoint from $F^{\ker\overline{\rho}}$. By lemma 3.6, if we pick v with $\mathrm{N}v > 300$, the reduction $\overline{C}$ will contain four collinear rational points. By Hensel's lemma, any line that reduces to the line going through these four points will intersect $C \times_F F_v$ at four F_v- rational points. This gives an open subset U_v of $L(F_v)$ all whose members have intersect C at F_v-rational points and does not contain a line passing through a cusp.

It is now clear that if an F-rational line l is in U_v for the above choice, the 4 intersection points of l with C will have coordinates in a totally real extension F' of F, and the image of the mod 7 representation corresponding to each intersection point is the same as that of E.

□

4. Gonality of modular curves

Fix a totally real field F. In view of Theorem 2.5 and section 3, an elliptic curve E over F is modular, unless $\overline{\rho}_{E,p}|_{G_{F(\zeta_p)}}$ is not absolutely irreducible for each $p = 3, 5, 7$.

Lemma 4.1. *If G is a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ which is not absolutely irreducible then G is a subgroup of a Borel subgroup or a non-split torus.*

Proof. Let V be the underlying $\mathbb{F}_p$-vector space. We know G preserves a line L in $V \otimes \overline{\mathbb{F}}_p$. If L is rational then G acts reducibly on V and G is a subgroup of a Borel subgroup. If L is not rational, it has a Galois conjugate distinct from it, which is also preserved by G. Thus G is a subgroup of a torus. □

Thus the elliptic curves that we don't yet know to be modular gives rise to non-cuspidal $F(\zeta_{105})$-points on the modular curves $X(3*, 5*, 7*)$, where $* \in \{b, ns\}$, indicating a Borel level structure and non-split Cartan level structure respectively. To analyze rational points on those curves, it is useful to understand how their Jacobians decompose into isogeny factors. We now explain how this can be done in general.

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of square-free level N such that the image of Γ mod p is either the Borel, the normalizer of the split or non-split Cartan subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ for each prime $p|N$. The modular curve $X(\Gamma) = \mathbb{H}^*/\Gamma$ has a canonical model defined over $\mathbb{Q}$, because for each prime p dividing the level, the corresponding subgroup in $\mathrm{SL}_2(\mathbb{F}_p)$ admits an extension to a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ with determinant surjecting onto $\mathbb{F}_p^\times$, and the corresponding (open) modular curve is identified with the Shimura variety $\mathrm{Sh}_K = \mathrm{GL}_2(\mathbb{Q}) \setminus \mathrm{GL}_2(\mathbb{A})/\mathbb{R}^\times \mathrm{O}(\mathbb{R})K$, where K is the unique open compact subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ lifting each subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ as above. Note because $\det(K)$ is surjective, the Shimura variety is geometrically irreducible, and its $\mathbb{C}$-points are naturally given by $\mathbb{H}/\Gamma$. We will use both notations when talking about modular curves.

Given a list of distinct primes p_i and label $* \in \{b, s^+, ns^+\}$, we write $X(p_i*)$ to denote the modular curve of the above kind such that mod p_i the congruence subgroup is Borel, normalizer of split or non-split Cartan respectively.

For a prime p, denoting the Borel, normalizer of split/non-split Cartan subgroups of $G = \mathrm{GL}_2(\mathbb{F}_p)$ by B, S and N, we have a relation (see [16])

$$\pi_N + \pi_B = v\pi_S v^{-1} + \pi_G$$

inside the group algebra $\mathbb{Q}[G]$, where π_H denotes the projector onto the H-invariant part, and v is an invertible element in $\mathbb{Q}[G]$. Applying this relation onto $\mathrm{End}(\mathrm{Sh}_{K(N)})\otimes \mathbb{Q}$, we can thus express (up to isogeny) the Jacobian of each modular curve of the kind we are considering in terms of Jacobian the modular curves of the same kind, but where only Borel or normalizer of split Cartan level structures appear. Let $K(ps)$ and $K(p^+)$ be the open compact subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}}_p)$ coming from the split Cartan and normalizer of split Cartan subgroup in $\mathrm{GL}_2(\mathbb{F}_p)$. Let $K_0(p^r)$ be the subgroup of matrices that are upper triangular mod p^r. Then we have

$$K(ps) = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) K_0(p^2) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$$
$$K(ps^+) = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \langle K_0(p^2), \left(\begin{smallmatrix} 0 & \frac{-1}{p} \\ p & 0 \end{smallmatrix}\right)\rangle \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1},$$

Thus the modular curves with normalizer split Cartan level at p are isomorphic to one with level $K_0(p^2)^+$ (that is, the level generated by $K_0(p^2)$ and $\left(\begin{smallmatrix} 0 & \frac{-1}{p} \\ p & 0 \end{smallmatrix}\right)$).

The modular curve $\mathrm{Sh}_{K_0(p^m)K^p}$ has a moduli interpretation in terms of elliptic curves with a cyclic subgroup C_{p^m} of order p^m and level structure K^p away from p, and the Atkin-Lehner involution w_{p^m} given by

$$(E, C_{p^m}, K^p) \to (E/C_p, E[p^m]/C_{p^m}, K^p),$$

which corresponds to right multiplication by $\left(\begin{smallmatrix} 0 & -1 \\ p^m & 0 \end{smallmatrix}\right)$ at the level of the double coset description. Thus we have

Lemma 4.2. *If p is any prime and K^p is a level structure away from p, up to isogeny over $\mathbb{Q}$*

$$\mathrm{Jac}(\mathrm{Sh}_{K(pns^+)K^p}) \times \mathrm{Jac}(\mathrm{Sh}_{K_0(p)K^p}) \sim \mathrm{Jac}(\mathrm{Sh}_{K(ps^+)K^p}) \times \mathrm{Jac}(\mathrm{Sh}_{\mathrm{GL}_2(\mathbb{Z}_p)K^p})$$

$$\mathrm{Jac}(\mathrm{Sh}_{K(ps^+)K^p}) \sim \mathrm{Jac}(\mathrm{Sh}_{K_0(p^2)K^p})^{w_{p^2}}$$

Recall that a curve is hyperelliptic (resp. bielliptic) over a field k if it is a double cover of $\mathbb{P}^1$ (resp. an elliptic curve) over k.

Lemma 4.3. *None of the modular curves $X(3*, 5*, 7*)$ above are hyperelliptic or bielliptic over $\mathbb{C}$.*

Proof. We will make use of the following two facts

Proposition 4.4. *(Castelnuovo-Severi inequality) Let F, F_1, F_2 be function fields of curves over a field k, of genera g, g_1, g_2, respectively. Suppose that $F_i \subseteq F$ and $F = F_1F_2$. Let $d_i = [F : F_i]$. Then*

$$g \leq g_1d_1 + g_2d_2 + (d_1 - 1)(d_2 - 1)$$

Proof. See [46], III.10.3. □

Theorem 4.5. *(Abramovich [2]) Let $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$ be a congruence subgroup of index d. Then the $\mathbb{C}$-gonality of the modular curve associated to Γ is at least $\frac{7}{800}d$.*

Recall that the gonality of a curve defined over a field k is the smallest d such that there exists a map from the curve to $\mathbb{P}^1$ defined over k of degree d. Hyperelliptic and bielliptic curves have gonality ≤ 4. A non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ has index $p(p-1)$ and a Borel subgroup has index $p+1$. Both groups contain the center and have surjects onto $\mathbb{F}_p^\times$. Consider the following cases:

- $X(3*, 5*, 7*)$ where either $5* = 5ns$ or $7* = 7ns$: The index of the corresponding subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ is at least 640 or 1008 respectively, and hence

Abramovich's bound gives a $\mathbb{C}$-gonality ≥ 5. Thus the lemma holds in this case.

- $X(3b, 5b, 7b)$:

  The space of cusp forms for $\Gamma_0(105)$ has dimension 13. The subspace fixed by the Atkin-Lehner operator w_{35} has dimension 3, with the q-expansion of a basis (computed by Magma) given by

$$\begin{aligned}
f_1 &= q - q^2 - q^3 - q^4 + q^5 + q^6 - 7q^7 + 3q^8 + q^9 - q^{10} - \\
&\quad - 4q^{11} + q^{12} - 2q^{13} + 7q^{14} - q^{15} - q^{16} + 2q^{17} - q^{18} + 4q^{19} + O(q^{20}), \\
f_2 &= q - q^2 + q^3 - q^4 + 3q^5 - q^6 - q^7 + 3q^8 + q^9 - 3q^{10} \\
&\quad + 4q^{11} - q^{12} - 2q^{13} + q^{14} + 3q^{15} - q^{16} - 6q^{17} - q^{18} + 4q^{19} + O(q^{20}), \\
f_3 &= q + q^2 + q^3 - q^4 + q^5 + q^6 + q^7 - 3q^8 + q^9 + q^{10} \\
&\quad - q^{12} - 6q^{13} + q^{14} + q^{15} - q^{16} + 2q^{17} + q^{18} - 8q^{19} + O(q^{20})
\end{aligned}$$

  These cusp forms form a basis for $H^0(X_0(105)/w_{35}, \Omega^1)$, and the q-expansion is the expansion in the formal neighborhood of the image of the cusp ∞. If the forms f_i satisfy a homogenous quadratic relation, then so will their power series expansion. A linear algebra check by Magma shows that there is no such relation between the q-series. Thus the canonical map of $X_0(105)/w_{35}$ does not factor through a conic, hence it must be a quartic plane curve, and not hyperelliptic. Now suppose there exists a map $\pi : X_0(105) \to \mathbb{P}^1$ of degree $d \leq 4$. Of π does not factor through the quotient map, the Castelnuovo-Severi inequality for π and the quotient map to $X_0(105)/w_{35}$ would imply

$$13 = g(X_0(105)) \leq 0 + 2 \times 3 + (d - 1)$$

which is a contradiction. Thus π factor through the quotient map, and in particular $d = 2$ or 4. But that would imply $X_0(105)/w_{35}$ is either rational or hyperelliptic, a contradiction.

- $X(3ns, 5b, 7b)$:

  If $X(3ns, 5b, 7b)$ were hyperelliptic or bielliptic, so is any curve dominated by it, by Proposition 1 of [27].

  Thus it suffices to show the curve $X(3ns^+, 5b, 7b)$ is not hyperelliptic or bielliptic. Using lemma 4.2, we have up to isogeny

$$\begin{aligned} &\mathrm{Jac}(X(3ns^+, 5b, 7b)) \times \mathrm{Jac}(X(3b, 5b, 7b)) \\ \sim\ &\mathrm{Jac}(X(3s^+, 5b, 7b)) \times \mathrm{Jac}(X(5b, 7b)) \\ \sim\ &\mathrm{Jac}(X(9b, 5b, 7b)/w_9) \times \mathrm{Jac}(X(5b, 7b)) \end{aligned}$$

  and

$$\begin{aligned} &\mathrm{Jac}(X(3ns^+, 5b)) \times \mathrm{Jac}(X(3b, 5b)) \\ \sim\ &\mathrm{Jac}(X(9b, 5b)/w_9) \end{aligned}$$

  The space of cusp forms for $\Gamma_0(315)$ has dimension 41, and the subspace fixed by w_9 has dimension 21. The space of cusp forms for $\Gamma_0(35)$ had dimension 3, thus $X(3ns^+, 5b, 7b)$ has genus 11. The w_9-fixed subspace of cusp forms for $\Gamma_0(45)$ has dimension 1, and the space of cusp forms of $\Gamma_0(15)$ has dimension 1, thus $X(3ns^+, 5b)$ has genus 0. Suppose there is a map $\pi : X(3ns^+, 5b, 7b) \to C$ of degree 2, where C has genus $g \leq 1$. If the forgetting level structure at 7 map $X(3ns^+, 5b, 7b) \to X(3ns^+, 5b)$ (which has degree 8) does not factor through

π, the Castelnuovo-Severi inequality would imply

$$11 \leq 2g + 0 + 7$$

which is a contradiction. Thus the forgetting level structure at 7 map factors through π. But such a factorization would correspond to a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing the congruence subgroup corresponding to $X(3ns^+, 5b, 7b)$ with index 2. However, the table in [14] shows no such groups exists.

□

Theorem 4.6. *There is a finite list of pairs (j, F') where F'/F is a totally real quadratic extension and $j \in F'$, such that an elliptic curve E over any totally real quadratic extension of F is modular unless $j(E)$ is in the list.*

Proof. From what we have said, an elliptic curve E over F' will be modular unless it gives rise to a $F'(\zeta_{105})$-rational point on one of the modular curves $X = X(3*, 5*, 7*)$ above. Such a point is the same as a $F(\zeta_{105})$-rational effective degree 2 divisor, that is a $F(\zeta_{105})$-rational point of $\mathrm{Sym}^2 X$. By the above lemma, none of them are bielliptic or hyperelliptic, hence Collorary 3 of [27] applies and gives the desired finiteness.

□

Remark 4.1. The finiteness result in [27] hinges on Faltings' theorem on subvarieties of abelian varieties, and thus the above theorem is ineffective for a general totally real field F. However in good cases (e.g. $F = \mathbb{Q}$), one can make the list computable, and we will attempt to do this with some other simplifying assumptions in the next section.

5. Modularity over real quadratic fields

By the previous section, we see that there are only finitely many pairs (j, F) where F is a real quadratic field and $j \in F$ is the j-invariant of an elliptic curve over F

that is not modular, namely the ones whose mod p Galois representation have small image for all p =3, 5, 7. However this finiteness statement is ineffective due to the use of Falting's theorem. The goal of this section is to make the exceptional pairs explicit and proving modularity of the corresponding curves, under the simplifying assumption that F is a totally real quadratic field unramified above 5 and 7.

Let E be an elliptic curve over a totally real field F such that $\sqrt{5} \notin F$. If E were to be not modular, by theorem 2.5 and section 3, $\overline{\rho}_{E,p}|_{F(\zeta_p)}$ must be not absolutely irreducible for all $p \in \{3, 5, 7\}$, equivalently, the mod p Galois representation becomes absolutely reducible over the quadratic subextension of $F(\zeta_p)/F$. This means that either $\overline{\rho}_p$ is absolutely reducible (hence reducible since it is odd), or absolutely irreducible but becomes absolutely reducible over $F(\sqrt{(-1)^{(p-1)/2}p})$ (because this is the unique quadaratic subextension of $F(\zeta_p)$ under our assumptions). In the latter case, $\overline{\rho}_p$ is the induction of a character from the Galois group of $F(\sqrt{(-1)^{(p-1)/2}p})$, and this character is valued either in $\mathbb{F}_p^\times$ or valued in $\mathbb{F}_{p^2}^\times$ but not in $\mathbb{F}_p^\times$. The above possibilities are reflected in terms the image of $\overline{\rho}$ as being conjugate to a subgroup of the Borel subgroup (reducible case), the normalizer of a split torus (irreducible but becomes reducible over $\mathbb{F}_p^\times$), or the normalizer of a non-split torus (irreducible, becomes irreducible but absolutely reducible over $\mathbb{F}_p^\times$) of $\mathrm{GL}_2(\mathbb{F}_p)$. Note that in the case $p = 5$, the restriction of $\overline{\rho}_5$ to $F(\sqrt{5})$ is still odd, and hence this restriction will be absolutely irreducible if it is irreducible. We say that the elliptic curve E has small image at p for each p=3, 5, 7 if $\rho_{E,p}$ has one of the above form. Oberserve that the normalizer of a split torus in $\mathrm{GL}_2(\mathbb{F}_3)$ is a subgroup of index 2 in the normalizer of a non-split torus in $\mathrm{GL}_2(\mathbb{F}_3)$, as the latter are the 2-Sylow subgroups. Thus we only need to consider the Borel and normalizer of non-split Cartan level structures at 3, and Borel and normalizer of split Cartan level structure at 5.

We have the following observation over general totally real fields:

Proposition 5.1. *Let F is any totally real field where 5, 7 are unramified, and E is an elliptic curve defined over F with small image at 3, 5, 7. Then E is (nearly) ordinary at all places $v|5$ or is (nearly) ordinary at all places $v|7$.*

Proof. We first recall some facts about the type of a p-adic Galois representation. E gives rise to a strictly compatible system of Galois representation $\rho_{E,l}$ defined over $\mathbb{Q}$, which in particular means that for each finite place v of F, there exists a 2-dimensional Weil-Deligne representation WD_v of W_{F_v} with rational traces such that WD_{F_v} is the Weil-Deligne representation associated to the Galois representations $\rho_l|_{G_{F_v}}$ via Grothendieck's l-adic monodromy theorem if $v \not| l$ or via a recipe of Fontaine if $v|l$. In the case $v \not| l$, if the monodromy operator $N = 0$, then the Weil-Deligne and the Galois representation agree on the inertia subgroup I_{F_v}, and in particular is a representation defined over $\mathbb{Q}_l$. Note that as the compatible system has cyclotomic determinant, $WD_v|_{I_{F_v}}$ has trivial determinant.

Lemma 5.2. *If v is a place of F above a prime $p > 3$ then the inertial type $WD_v|_{I_{F_v}} \cong \phi \oplus \phi^{-1}$ where ϕ is a character of I_{F_v} which has order dividing 4 or 6.*

Proof. We know that the inertia type is a finite image representation with trivial determinant. Because it also has a model over $\mathbb{Z}_2$, the size of the image can not be divisible by p, hence the representation factors through the tame quotient of I_{F_v}, which is pro-cyclic, with a topological generator u. The eigenvalues of u must be ζ, ζ^{-1} for some root of unity ζ, and since the trace of u is rational, this forces ζ to have order dividing 4 or 6.

Alternatively, one could work with (reduced) minimal Weiestrass equations to show that any elliptic curve over F_v acquires semi-stable reduction over an extension with ramification index dividing 4 or 6, see [41] □

Observe that the lemma shows that the image of the inertia in WD_v must be a subgroup of $\mathrm{Im}\overline{\rho}_l \cap \mathrm{SL}_2(\mathbb{F}_l)$ if $l > 3$ and $v \not| l$, since the kernel of the reduction map

$\mathrm{GL}_2(\mathbb{Z}_l) \to \mathrm{GL}_2(\mathbb{F}_l)$ is a pro-l group. When $l = 3$ and the inertial type has order divisible by 3, the same statement still holds, because if $g \in GL_2(\mathbb{Z}_3)$ with $g^3 = 1$ then g must reduce to a non-trivial unipotent element in $GL_2(\mathbb{F}_3)$ (because such g gives an isomorphism of $\mathbb{Z}_3^2 \cong \mathbb{Z}_3[\zeta_3]$ identifying g with ζ_3, and the mod 3 reduction of multiplication by ζ_3 is a non-trivial unipotent element).

We now prove the proposition. We split into the following cases:

- E admits a Borel level structure at 3 and either a Borel or normalizer of split Cartan level structure at 7.

  For any place $v|7$ of F, the image of $WD_v|_{I_{F_v}}$ has order dividing 6. If E has potential multiplicative reduction at v then E is potentially ordinary, hence is nearly ordinary at v. So we assume now that E has potential good reduction at v. Suppose E has minimal Weierstrass equation

  $$y^2 = x^3 + Ax + B$$

  over $\mathcal{O}_{F_v}$. Let $v(\Delta) = v(4A^3 + 27B^2) < 12$ be the valuation of the minimal discriminant. The order of the image of $WD_v|_{I_{F_v}}$ is the degree of the smallest extension of F_v^{nr} such that E acquires good reduction [40]. It is also the minimal e such that $12|v(\Delta)e$. Since E has potential good reduction, $v(A^3) \geq v(\Delta)$. Replacing E with a quadratic twist, it suffices to consider the cases $e = 3$ or $e = 1$.

  If $e = 3$, $v(\Delta)$ is 4 or 8, and hence $v(A^3) \neq v(B^2)$, since otherwise $v(A^3) \geq v(\Delta) \geq v(A^3) = \min\{v(A^3), v(B^2)\}$ which forces $v(A^3) = v(\Delta) = v(B^2)$, a contradiction. Thus $v(\Delta) = \min\{v(A^3), v(B^2)\}$ is not divisible by 3, so $v(A^3) > v(B^2)$, and thus $j(E) = 0 \bmod v$. But this means E has potential good ordinary reduction, hence E is nearly ordinary at v.

  If $e = 1$, E has good reduction. Because F_v is unramified over $\mathbb{Q}_7$ and $\rho_{E,7}|_{G_{F_v}}$ is crystalline with Hodge-Tate weight 0, -1, $(\overline{\rho}_{E,7}|_{I_{F_v}})^{ss} \cong \omega_2 \oplus \omega_2^7$ or

$\cong \omega_1 \oplus 1$, where ω_n is the tame character of niveau n of $\mathrm{Gal}(\overline{\mathbb{Q}}_7/\mathbb{Q}_7^{ur})$. If first case occur, the image of $\overline{\rho}_{E,7}$ contains an element which has non-zero trace and irreducible characteristic polynomial, hence can not be a subgroup of the Borel or normalizer of split Cartan subgroup. Hence the second case occur, which means that E has good ordinary reduction, and hence is ordinary.

- Either E admits a normalizer of non-split Cartan level structure at 3, or a normalizer of non-split Cartan level structure at 7.

  For any place $v|5$ of F, the image of $WD_v|_{I_{F_v}}$ must be a 2-group, and hence has order dividing 4. Let e denote its order, as above. As above, we work with the minimal Weierstrass equation of E and we can assume E has potential good reduction. Replacing E with a quadratic twist, we can assume $e = 4$ or $e = 1$.

  If $e = 4$, $v(\Delta)$ is 3 or 9, and hence $v(A^3) \neq v(B^2)$, since otherwise $v(A^3) \geq v(\Delta) \geq v(A^3) = \min\{v(A^3), v(B^2)\}$ which forces $v(A^3) = v(\Delta) = v(B^2)$, a contradiction. Thus $v(\Delta) = \min\{v(A^3), v(B^2)\}$ is not divisible by 2, so $v(A^3) < v(B^2)$, and thus $j(E) = 1728 \bmod v$. But this means E has potential good ordinary reduction, hence E is nearly ordinary at v.

  If $e = 1$, E has good reduction at v. By exactly the same argument as in the previous case, the fact that E admits either a Borel or normalizer of split Cartan level structure at 5 forces E to have good ordinary reduction, hence E is nearly ordinary at v.

□

Remark 5.1. Being nearly ordinary at all places v above a prime is the crucial local condition to apply the modularity lifting theorems with small residual images of Skinner-Wiles [43], [44]. Under our assumptions, their modularity lifting theorems for irreducible residual representations apply. Unfortunately the very restrictive conditions required in the residually reducible case (namely, that the splitting field of

the ratio of the characters occurring in the residual representation is required to be abelian over $\mathbb{Q}$. This is only an issue for $p > 3$) prevents us from fully exploiting the above proposition.

Proposition 5.3. *Let F be a totally real quadratic field where 5 and 7 are unramified, and E is an elliptic curve over F. Then E is modular unless $j(E)$ is the j-invariant of a degree at most 2 point on one of the following curves*

- $X(3b, 5s^+)$
- $X(3ns^+, 7s^+)$
- $X(5b, 7b)$
- $X(5b, 7ns^+)$

Proof. We already know that E is modular unless it has small image at all primes p=3, 5, 7. There are 12 possible combination of level structures at 3, 5, 7, and hence E is modular unless it has the same j-invariant as an elliptic curve that comes from an F-point of $X(3*, 5*, 7*)$ where the choice of the level structure $* \in \{b, ns^+\}$ at 3;$* \in \{b, s^+\}$ at 5, and $* \in \{b, s^+, ns^+\}$ at 7. The 12 curves are listed in Table 1 below, and the rightmost column gives a curve in $\{X(3b, 5s^+), X(3ns^+, 7s^+), X(5b, 7b), X(5b, 7ns^+)\}$ that it covers. if there is one. We see that either E gives rise to a quadratic point on one of the four curve listed, or on one of the curves $X(3b, 5b, 7s^+)$, $X(3ns^+, 5s^+, 7b)$, $X(3ns^+, 5s^+, 7ns^+)$

By Proposition 5.1 (or rather, its proof), we can apply Theorem 2.7 for the prime 5 for the last two curves, and for the prime 7 for the first curve. □

Theorem 5.4. *Suppose F is a totally quadratic field such that 5 and 7 are unramified in F. Then every elliptic curve over F is modular.*

Proof. This follows from Proposition 5.3 and the study of quadratic points on some modular curves in section 6 below. □

p	3	5	7	
	b	b	b	$X(5b, 7b)$
	b	b	s^+	
	b	b	ns^+	$X(5b, 7ns^+)$
	b	s^+	b	$X(3b, 5s^+)$
	b	s^+	s^+	$X(3b, 5s^+)$
	b	s^+	ns^+	$X(3b, 5s^+)$
	ns^+	b	b	$X(5b, 7b)$
	ns^+	b	s^+	$X(3ns^+, 7s^+)$
	ns^+	b	ns^+	$X(5b, 7ns^+)$
	ns^+	s^+	b	
	ns^+	s^+	s^+	$X(3ns^+, 7s^+)$
	ns^+	s^+	ns^+	

TABLE 1.

Remark 5.2. As the proof of proposition 5.3 shows, to get modularity for a real quadratic field different from $\mathbb{Q}(\sqrt{5})$, we only need to study quadratic points on the four curves listed there and $X(3b, 5b, 7s^+)$, $X(3ns^+, 5s^+, 7b)$, $X(3ns^+, 5s^+, 7ns^+)$. We can further reduce to understanding quadratic points on the curves $X(3b, 7s^+)$, $X(3ns^+, 7b)$ and $X(5s^+, 7ns^+)$.

- The curve $X(3b, 7s^+)$ has genus 6, its Jacobian decomposes up to isogeny as

$$\mathrm{Jac}(X(3b, 7s^+)) \sim E_1 \times A_1 \times A_2 \times E_2$$

  where the first three factors have conductor 147 while the last one has conductor 21, the factors E_i are elliptic curves while the factors A_i are abelian surfaces. All factors except for A_1 has rank 0 over $\mathbb{Q}$. An approach similar to the one used to handle the curve $X(3ns^+, 7s^+)$ below allows one to explicitly write down maps from $X(3b, 7s^+)$ to the elliptic curves E_1, E_2, and hence find its quadratic points by the same method.
- The curve $X(3ns^+, 7b)$ has genus 2, and its Jacobian has rank 0 and the hyperelliptic involution given by the Atkin-Lehner involution w_7. Using the same method for the curve $X(5b, 7b)$ below, we can determine all the quadratic

points on it that does not come from the hyperelliptic class, while the points coming from the hyperelliptic class only gives rise j-invariants of $\mathbb{Q}$-curves, and hence the corresponding elliptic curves are modular by lemma 6.1.

- The curve $X(5s^+, 7ns^+)$ has genus 19, and its Jacobian admits two abelian surface factors that has rank 0 over $\mathbb{Q}$. Thus it is in theory possible to determine all quadratic points on it. However due to practical (computational) complications in executing this, we have not done it here.

In particular, using the methods in this paper, for modularity of elliptic curves over all real quadratic fields different from $\mathbb{Q}(\sqrt{5})$, the only curve we can not directly handle is the genus 19 curve $X(5s^+, 7ns^+)$. However, proposition 5.1 shows that an elliptic curve corresponding to a quadratic point defined over a field unramified at 5 on this curve is ordinary at all places above 5, and Theorem 2.7 shows such curves a modular. The methods of this paper can be adapted to show that all elliptic curves over a real quadratic field unramified at 5 are modular (that is, we do not need the field to be unramified at 7).

6. Quadratic points on modular curves

The goal of this section is to show that any elliptic curve that gives rise to a real quadratic point on one of the modular curves in Proposition 5.3 are modular. For each such modular curve X, at each prime p such that X has a Borel level structure at p, there is an Atkin-Lehner involution w_p which is an involution of X over $\mathbb{Q}$, which in the moduli interpretation of X correspond to

$$(E, \phi) \mapsto (E/C_p, \phi')$$

where C_p is the line that defines the Borel subgroup in the level structure at p. The Atkin-Lehner involutions generate an elementary abelian $2-$subgroup of

$\mathrm{Aut}(X/\mathbb{Q})$. We call any non-trivial element of this subgroup an Atkin-Lehner involution. We have the following useful fact

Lemma 6.1. *Let E is an elliptic curve over a quadratic field F that gives rise to a point $P \in X(F)$. Assume that there is an Atkin-Lehner involution w such that P maps to a rational point in X/w. Then E is modular*

Proof. We only need to consider the case that E has no CM.

Let $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ denote the non-trivial element. Then E^σ gives rise to the point $P^\sigma \in X(F)$, and $P^\sigma = w(P)$ or $P^\sigma = P$. In either case, a quadratic twist of E^σ must be F-isogenous to E. Thus for any $\tau \in G_{\mathbb{Q}}$, E^τ is isogenous to E over $\overline{Q}$, that is E is a $\mathbb{Q}$-curve defined over F. By Proposition 2.4 , E is modular.

□

In the following sections, the assertions regarding Mordell-Weil ranks of modular abelian varieties are obtained by the procedure mentioned in the introduction, and the results can be found in William Stein's database [45].

6.1. **The curve $X(5b, 7b)$.** The curve $X = X(5b, 7b)$ has Jacobian $\mathrm{Jac}(X) \sim E \times A$ where E is an elliptic curve and A is an abelian surface of conductor 35. Both E and A has rank 0 over $\mathbb{Q}$. A corresponds to a pair of conjugate newforms with coefficient field $\mathbb{Q}[x]/(x^2+x-4)$. The pair of Atkin Lehner involutions (w_3, w_5) has sign $(1, -1)$ and $(-1, 1)$ on E and A respectively. It follows that $w_{35} = w_5 w_7$ is the hyperelliptic involution on X, as the quotient X/w_{35} has genus 0. The q-expansion of a basis for $H^0(X, \Omega^1)$ is given by

$$f_1 = q + q^3 - 2q^4 - q^5 + q^7 - 2q^9 - 3q^{11} + O(q^{12})$$

$$f_2 = 2q - q^2 - q^3 + 5q^4 + 2q^5 - 8q^6 - 2q^7 - 9q^8 + 3q^9 - q^{10} + q^{11} + O(q^{12})$$

$$f_3 = q^2 - q^3 - q^4 + q^8 + q^9 + q^{10} + q^{11} + O(q^{12})$$

where the f_1 corresponds to E and f_2, f_3 corresponds to A. The canonical map is given by $X \to X/w_{35} \hookrightarrow \mathbb{P}^2$ as a double cover of the conic

$$-4X^2 + Y^2 + 2YZ + 17Z^2$$

The quotient X/w_7 is a genus 2 curve with Jacobian isogenous to A. Putting $x = f_3/f_2$, $y = 4dx/(f_2 dq/q)$, an equation for this curve is given by

$$y^2 = -7599x^6 - 3682x^5 - 1217x^4 - 284x^3 - 17x^2 - 2x + 1$$

The group of rational points of $\mathrm{Jac}(X/w_7)$ has order 16, and the rational degree 2 divisors that are not the hyperelliptic class is given by in Mumford's notation (divisors of degree 2 on a hyprelliptic curve are represented by $(p(x), q(x))$ where p, q are polynomials of degree 2 and 1. It desribes the effecive divisor such that $p(x) = 0$ and $y = q(x)$ on the hyperelliptic curve):

$(x^2 + 7/50x + 3/50, 701/2500x - 121/2500)$, $(x^2, -x + 1)$,

$(x^2 + 5/58x + 3/58, -3345/3364x - 905/3364)$, $(x^2 + 4/19x + 1/19, -776/361x + 72/361)$

$(x^2 + 1/8x + 1/8, -55/64x + 145/64)$, $(x^2 + 2/15x + 1/15, 2/75x - 14/75)$

$(x^2 + 1/3x, -3x - 1)$, $(x^2 + 2/17x + 1/17, 0)$.

or their images under the hyperelliptic involution.

Thus if $P \in X(F)$ is a quadratic point, then $P + P^\sigma$ must become one of the above 15 divisors, or becomes the hyperelliptic class in X/w_7. But in the latter case, because the hyperelliptic involution on X/w_7 is induced by w_5, this means that there is an Atkin-Lehner involution on X such that $wP = P^\sigma$, hence all such points must come from a modular elliptic curve by lemma 6.1. Since we are only interested in quadratic points defined over totally real fields, we only need to consider the cases where the image of $P + P^\sigma$ is $2(0,1)$, $2(0,-1)$, $(0,-1/3) + (-1/3,0)$ or $(0,1/3) + (-1/3,0)$.

However since $X \to X/w_7$ is a double cover, the second case can not happen since the fiber of a rational point on X/w_7 is stable under the Galois action, hence if P occurs in a fiber then P^σ occurs in the same fiber. Thus the only case left is when P, P^σ are in the fiber of $(0,1)$ or $(0,-1)$, but in that case $P = w_7 P^\sigma$ and hence the corresponding elliptic curve is modular, again by lemma 6.1.

6.2. **The curve $X(3b, 5s^+)$.** We have $X = X(3b, 5s^+) \cong X_0(75)/w_{5^2}$, hence $\mathrm{Jac}(X(3b, 5s^+)) \sim E_1 \times E_2 \times E_3$ in the isogeny category. Here E_1 is isogenous to $X_0(15)$ while E_2 and E_3 are elliptic curves of conductor 75, and each of them have rank 0 over $\mathbb{Q}$.

The q-expansion of the three newforms corresponding to E_i are

$$f_1 = q - q^2 - q^3 - q^4 + q^5 + q^6 + 3q^8 + q^9 - q^{10} - 4q^{11} + O(q^{12})$$
$$f_2 = q + q^2 + q^3 - q^4 + q^6 - 3q^8 + q^9 - 4q^{11} + O(q^{12})$$
$$f_3 = q - 2q^2 + q^3 + 2q^4 - 2q^6 + 3q^7 + q^9 + 2q^{11} + O(q^{12})$$

Those can be thought of as the formal expansion around the cusp ∞ of the curve $X_0(75)$. Using that $X = X_0(75)/w_{25}$ and the description of w_{25} in terms of double cosets, we find that a basis or $H^0(X, \Omega^1)$ is given by $(-5f_1(z) + f_1(z/5))dz$, $f_2(z/5)dz$ and $f_3(z/5)dz$. Using their q-expansion, we see there are no degree 2 relations between them and there is a degree 4 relation, hence the canonical map realizes X as the quartic

$$9X^4 + 30X^2Y^2 + 108X^2YZ - 48X^2Z^2 + 25Y^4 - 60Y^3Z - 80Y^2Z^2 + 16Z^4$$

and thus X is not hyperelliptic. Over $\mathbb{Q}$, the automorphism group of X has an element order 2, generated by the Atkin-Lehner involution w_3, which in the above model correspond to $[X : Y : Z] \mapsto [-X : Y : Z]$. Using Magma we find that the

quotient curve is the elliptic curve E_1 with equation

$$y^2 + xy + y = x^3 + x^2 - 5x + 2$$

and the quotient map $\phi_1 : X \to E_1$ is given in terms of homogenous coordinates by

$$\begin{aligned}
&[-9/4X^2Y^2 - 15/2Y^4 + 9/20X^2YZ - 51/2Y^3Z + 9/50X^2Z^2 + 18Y^2Z^2 - 6/25YZ^3 \\
&- 24/25Z^4 : 45/16X^2Y^2 + 135/16Y^4 + 9/10X^2YZ + 39Y^3Z - 81/100X^2Z^2 - 39/10Y^2Z^2 \\
&- 363/25YZ^3 + 93/25Z^4 : -9/4X^2Y^2 - 15/2Y^4 + 9/5X^2YZ - 21Y^3Z - 9/25X^2Z^2 \\
&+ 162/5Y^2Z^2 - 348/25YZ^3 + 48/25Z^4]
\end{aligned}$$

We have $E_1(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Over $\mathbb{Q}(\sqrt{5})$, the automorphism group of X contains an S_3, andan automorphism of order 3 given by

$$[X : Y : Z] \mapsto [-1/2X + \sqrt{5}/2Y : -3\sqrt{5}/10X - 1/2Y : Z]$$

the quotient curve is the elliptic curve E_2 with equation

$$y^2 + y = x^3 + x^2 + 2x + 4$$

and the quotient map $\phi_2 : X \to E_2$ is given by

$$
\begin{aligned}
[&- 12/5X^3Y^4 - 36/5XY^6 - 357/250X^3Y^3Z - 1719/50XY^5Z + 27/25X^3Y^2Z^2 \\
&- 687/125XY^4Z^2 + 402/625X^3YZ^3 + 2268/125XY^3Z^3 + 12/125X^3Z^4 + 864/625XY^2Z^4 \\
&- 984/625XYZ^5 - 144/625XZ^6 : -3/4X^3Y^4 + 81/100X^2Y^5 - 9/4XY^6 + 63/20Y^7 \\
&- 12/25X^3Y^3Z - 81/50X^2Y^4Z - 54/5XY^5Z + 117/50Y^6Z - 81/25X^2Y^3Z^2 - 84/25XY^4Z^2 \\
&- 891/25Y^5Z^2 + 48/625X^3YZ^3 - 162/125X^2Y^2Z^3 + 144/125XY^3Z^3 - 702/25Y^4Z^3 \\
&+ 12/625X^3Z^4 + 396/625XY^2Z^4 + 1188/125Y^3Z^4 + 48/625XYZ^5 + 216/25Y^2Z^5 \\
&- 144/125YZ^6 - 288/625Z^7 : 3/2X^3Y^4 + 9/2XY^6 + 24/25X^3Y^3Z + 108/5XY^5Z \\
&+ 168/25XY^4Z^2 - 96/625X^3YZ^3 - 288/125XY^3Z^3 - 24/625X^3Z^4 - 792/625XY^2Z^4 \\
&- 96/625XYZ^5]
\end{aligned}
$$

We have $E_2(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$ is cyclic of order 5, generated by the point $[-1 : 1 : 1]$. If P, P^σ is a pair of conjugate quadratic points, then $\phi_i(P) + \phi_i(P^\sigma)$ is a rational torsion point on E_i, thus we have $\phi_2(P) - a[-1 : 1 : 1] = -(\phi_2(P^\sigma) + a[-1 : 1 : 1])$ for some integer a mod 5, while $2\phi_1(P) - b[0 : 1 : 1] = -(2\phi_1(P^\sigma) - b[0 : 1 : 1])$ for $b = 0$ or 1. The two equality implies $\phi_i(P)$, $\phi_i(P^\sigma)$ have the same image under a suitable two-to-one map $E_i \to \mathbb{P}^1$, thus P, P^σ have the same image under a map $C \to \mathbb{P}^1 \times \mathbb{P}^1$, where the two coordinate map have degree 6 and 16. Depending on the value of a, b, this maps X birationally onto its image or maps X/w_3 birationally onto its image. Thus, either P and P^σ map to the same point in X/w_3, or they map to the same singular point (which is necessarily defined over $\mathbb{Q}$) in the image of the map. Using Magma, under a birational isomorphism $\mathbb{P}^1 \times \mathbb{P}^1 \simeq \mathbb{P}^2$, we find the plane curve which is the image of X, and find its singular points over $\mathbb{Q}$. The resulting quadratic points that we get either satisfies $w_3P = P^\sigma$ (hence correspond to $\mathbb{Q}$-curves), are CM or is defined over a real quadratic field with 5 ramified, except for two conjugate

pair of points defined over $\mathbb{Q}(\sqrt{41})$. For the last two conjugate pair of points, we check directly that the j-invariant is not in the image of a $\mathbb{Q}(\sqrt{41})$-point of $X(7b)$, $X(7s^+)$ or $X(7ns^+)$ (using the equations in [22]), so that the image of the mod 7 representation is large and hence the points are modular by Corollary 2.6. Thus all points defined over quadratic fields where 5 is unramified gives rise to modular elliptic curves.

Remark 6.1. The interested reader can see the table in [24] for the full list of quadratic points on X.

6.3. **The curve** $X(3ns^+, 7s^+)$**.** We compute an equation for $X = X(3ns^+, 7s^+)$ by a method due to Noam Elkies (private communication), which is reproduced below. The modular curve $X_0(49)$ is isomorphic to the elliptic curve

$$y^2 + xy = x^3 - x^2 - 2x - 1$$

The only rational points on $X_0(49)$ are the origin O and the 2-torsion poin $T = [2 : -1 : 1]$. Under a suitable identification, O and T are the two cusps and the Atkin-Lehner involution w_{49} must be $P \mapsto T - P$, since it acts as -1 on the space of holomorphic differentials and swaps the cusps. The quotient of $X_0(49)$ by w_7 is the genus 0 curve with coordinate $h = (1 + y)/(2 - x)$. The q-expansion of h can be computed from the modular parametrization of $X_0(49)$, and gives

$$h = q^{-1} + 2q + q^2 + 2q^3 + 3q^4 + 4q^5 + 5q^6 + 7q^7 + 8q^8 + \cdots$$

Writing $j(q^7)$ as a rational function of degree 28 of h by solving a linear system of equations in the coefficients we have

$$j(q^7) = \frac{(h+2)((h+3)(h^2-h-5)(h^2-h+2)(h^4+3h^3+2h^2-3h+1))^3}{(h^3+2h^2-h-1)^7}$$

One the other hand the curve $X(3ns^+)$ is the cyclic triple cover of the j-line obtained by adjoining $j^{1/3}$. Hence the curve X is a cyclic triple cover of the h-line, obtained by adjoining a cube root of $(h^3+2h^2-h-1)/(h+2)$. This gives the following quartic model for X

$$(h+2)g^3 = (h^3+2h^2-h-1).$$

Using lemma 4.2, we compute up to isogeny over $\mathbb{Q}$

$$\mathrm{Jac}(X) \sim E \times A$$

where E is an elliptic curve of conductor 441 (and has rank 1) while A is an abelian surface of rank 0 and conductor 63. To determine the quadratic points on X, we wish to compute a model for A and a map $X \to A$. The abelian surface A is (isogenous to) the Weil restriction of a $\mathbb{Q}$-curve E defined over $K = \mathbb{Q}(\zeta_3)$. There is a map $X_0(441) \to X$ via the identification $X_0(441) = X(3s, 7s)$ and the map is obtained by containment of the corresponding congruence subgroups. Thus it suffices to write down a parametrization of E by $X_0(441)$ which factors through X. Below we describe a procedure to get such a parametrization.

Let $f_1 dz$, $f_2 dz$ be an integral basis of a Hecke-stable two dimensional subspace of $H^0(X_0(63), \Omega^1)$ on which the Hecke operators act through the system of Hecke eigenvalues correspond to A. We normalize this choice by requiring the q-expansion $f_1 = q + \cdots$ and $f_2 = q^2 + \cdots$. Let π_1, π_2 denote the two degeneracy maps $X_0(441) \to X_0(63)$ (where π_1 is the quotient map from the inclusion of congruence subgroups). Putting

$$\Omega = (\pi_1^* - \pi_2^*)(f_1 + (2 - \zeta_3^{-1})f_2)$$

we compute the integration map $\int_{i\infty} \Omega : X_0(441) \to \mathbb{C}$. Up to high precision, the image of the homology of $X_0(441)$ is a lattice Λ with

$$g_2(\Lambda) = \frac{7\sqrt{-3} - 41}{6144}$$
$$g_3(\Lambda) = \frac{42\sqrt{-3} - 43}{884736}$$

Suppose that $D \int_{i\infty} \Omega : X_0(441) \to \mathbb{C}/\Lambda = \{y^2 = 4x^3 - g_2 x - g_3\}$ factors through $X_0(441) \to X$, for some integer D. This is equivalent to a map $X \to \{y^2 = 4x^3 - g_2 D^4 x - g_3 D^6\}$ such that the pullback of dz is Ω. The coordinates x, y of such a map must satisfy the differential system

$$y^2 = 4x^3 - g_2 D^4 x - g_3 D^6$$

$$dx/y = \Omega$$

This system has a unique solution with $x = q^{-2} + \cdots$ in the ring of Laurent series $K((q))$, but only for suitable choice of D will the formal solution lie in the function field of X. Note that there is an automorphism of X of order 3, defined over K given by $g \to \zeta_3 g$. This automorphism fixes the cusps ∞, hence is continuous for the q-adic topology on the formal neighborhood at ∞. From the q-expansion, we see that the automorphism must be $q \to \zeta_3 q$, because this is q-adically continuous and sends $(g, h) \mapsto (\zeta_3 g, h)$. Hence given a formal solution (x, y) to the above differential system, we can recognize whether (x, y) lives in the function field of X by separating the q-expansion into 3 pieces according to the exponent of q mod 3, and testing whether each piece is a rational function of h times g^i.

Using this procedure, we found that for $D = 12$, the formal solution is actually in the function field of X, and subsequent direct algebraic manipulation verifies that we indeed have a map of curves $\phi : X \to E$ defined over K given by those functions. The group $E(K)$ is trivial, hence for any pair of conjugate quadratic points P, P^τ

satisfies $\phi(P) = -\phi(P^\sigma)$, in particular they map to the same point after composing ϕ with the x-coordinate map $E \to \mathbb{P}^1$. Our computation shows that this composition map is of the form

$$P_0(h)^2 + P_1(h)g + P_2(h)g^2$$

where $P_i(h)$ are rational functions in h of degree 13, 29, 29. Note that the same argument applies to the maps $\phi \circ c$ and $\phi \circ c^2$, where c is the automorphism $(g, h) \mapsto (\zeta_3 g, h)$, and also when we replace ϕ with the map ϕ^σ, where σ is the non-trivial automorphism of K. But this implies that the all three functions $P_0(h)^2$, $P_1(h)g$, $P_2(h)g^2$ and their σ-conjugates take the same values at P and P^σ, because the system of linear equations

$$\begin{aligned}
&(P_0(h)^2 - P_0(h^\tau)^2) + (P_1(h)g - P_1(h^\tau)g^\tau) + (P_2(h)g^2 - P_2(h^\tau)(g^\tau)^2) = 0\\
&(P_0(h)^2 - P_0(h^\tau)^2) + (P_1(h)g - P_1(h^\tau)g^\tau)\zeta_3 + (P_2(h)g^2 - P_2(h^\tau)(g^\tau)^2)\zeta_3^2 = 0\\
&(P_0(h)^2 - P_0(h^\tau)^2) + (P_1(h)g - P_1(h^\tau)g^\tau)\zeta_3^2 + (P_2(h)g^2 - P_2(h^\tau)(g^\tau)^2)\zeta_3 = 0
\end{aligned}$$

only has trivial solution. This forces the h-coordinate of P to be a zero of a suitable resultant, from which we easily get the list of possible h-coordinates of a P. We end up with the following list of quadratic points $[1 : h : g]$

$$\begin{aligned}
&[0:1:0], [0:0:1], [1:-1:1], [1:\frac{-1+\sqrt{5}}{2}:\frac{1-\sqrt{5}}{2}], [1:\frac{-3-\sqrt{5}}{2}:\frac{1-\sqrt{5}}{2}],\\
&[1:\frac{-1+\sqrt{13}}{2}:1], [1:\sqrt{5}:\frac{1+\sqrt{5}}{2}], [1:\frac{3+\sqrt{17}}{2}:\frac{5+\sqrt{17}}{4}].
\end{aligned}$$

From the formula for j in terms of h, we check that all the above points gives rise to cusps or CM j-invariants, hence the corresponding elliptic curves are modular.

6.4. **The curve $X(5b, 7ns^+)$.** Throughout this section we use the abbreviation $X = X(5b, 7ns^+)$, $\alpha = \frac{-1+\sqrt{-7}}{2}$, $K = \mathbb{Q}(\sqrt{-7})$ and σ the non-trivial automorphism of

$K/\mathbb{Q}$. First we recall that the modular curve $X(5b) = X_0(5)$ is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$, and an explicit rational coordinate x such that

$$j = \frac{(x^2 + 10x + 5)^3}{x},$$

see [21]. The Atkin-Lehner involution on $X_0(5) = X(5b)$ in terms of this coordinate is given by $x \mapsto 125/x$. The modular curve $X(7ns^+)$ parameterizing normalizer of non-split Cartan level structure at 7 is also isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$, with a rational coordinate ϕ such that

$$j = 64\frac{(\phi(\phi^2 + 7)(\phi^2 - 7\phi + 14)(5\phi^2 - 14\phi - 7))^3}{(\phi^3 - 7\phi^2 + 7\phi + 7)^7}.$$

The normalizer of non-split Cartain subgroup of $\mathrm{PSL}_2(\mathbb{F}_7)$ is not maximal, but is contained in a subgroup of order 24 isomorphic to S_4. All such subgroups are conjugate under $\mathrm{PGL}_2(\mathbb{F}_7)$, but breaks up into two conjugacy class in $\mathrm{PSL}_2(\mathbb{F}_7)$. A choice of this conjugacy class gives a modular curve that parameterizes an "S_4" level structure at 7 is defined over $\mathbb{Q}(\sqrt{-7})$, and has coordinate ψ such that

$$\psi = \frac{(2 + 3\alpha)\phi^3 - (18 + 15\alpha)\phi^2 + (42 + 21\alpha)\phi + (14 + 7\alpha)}{\phi^3 - 7\phi^2 + 7\phi + 7}$$

$$j = (\psi - 3(1 + \alpha))(\psi - (2 + \alpha))^3(\psi + 3 + 2\alpha)^3$$

(We refer the reader to [22] for these facts). Thus X has is birational to the plane curve given by

$$\frac{(x^2 + 10x + 5)^3}{x} = 64\frac{(\phi(\phi^2 + 7)(\phi^2 - 7\phi + 14)(5\phi^2 - 14\phi - 7))^3}{(\phi^3 - 7\phi^2 + 7\phi + 7)^7}$$

and if we let Y denote the modular curve with Borel level structure at 5 and "S_4" level structure at 7, Y has birational model

$$\frac{(x^2 + 10x + 5)^3}{x} = (\psi - 3(1 + \alpha))(\psi - (2 + \alpha))^3(\psi + 3 + 2\alpha)^3$$

We have a map $\pi : X \to Y$ given by

$$(x, \phi) \mapsto (x, \frac{(2+3\alpha)\phi^3 - (18+15\alpha)\phi^2 + (42+21\alpha)\phi + (14+7\alpha)}{\phi^3 - 7\phi^2 + 7\phi + 7})$$

and its conjugate $\pi^\sigma : X \to Y^\sigma$.

Using lemma 4.2, we have up to isogeny over $\mathbb{Q}$

$$Jac(X) \simeq A_1 \times A_2 \times A_3$$

where A_i are the abelian surface factors of $J_0(245)^{new}$ on which w_7 acts trivially, and the action of w_5 is 1,-1,-1 respectively. Checking for inner twists of the newforms contributing to X, we see that theA_i are absolutely simple, are non-isogenous over $\mathbb{Q}$, but A_1 is isogenous to A_2 over K. A_3 is not isogenous to A_1 even over $\mathbb{C}$. The factors A_2, A_3 have rank 0 over $\mathbb{Q}$, and the order of the group $A_2(\mathbb{Q})$ divides 7. The Hecke field of A_1, A_2 are $\mathbb{Q}(\sqrt{2})$ (These facts can be extracted from the tables in [45], the assertion about the rank follows from numerically computing the value at $s = 1$ of the L-function)

Let us now consider the three open compact subgroups G_1, G_2, H of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ given by the following local conditions

- The component at $p \not| 35$ is $GL_2(\mathbb{Z}_p)$
- The component at 5 is the inverse image of the upper triangular matrices under the reduction map $\mathrm{GL}_2(\mathbb{Z}_5) \to \mathrm{GL}_2(\mathbb{F}_5)$
- The component at 7 of G_1 is the subgroup of $\mathrm{GL}_2(\mathbb{Z}_7)$ that reduces to the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$
- The component at 7 of G_2 is the subgroup of $\mathrm{GL}_2(\mathbb{Z}_7)$ that reduces to the normalizer of the subgroup of the non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ whose determinant is a square in $\mathbb{F}_7$.
- The component at 7 of H is the subgroup of $\mathrm{GL}_2(\mathbb{Z}_7)$ that reduces to the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ which under the projection map to $\mathrm{PGL}_2(\mathbb{F}_7)$ is the

subgroup of order 24 of $\mathrm{PSL}_2(\mathbb{F}_7)$ containing the normalizer of non-split Cartan subgroup defining G_2.

We have the containments $G_2 \subset G_1$, $G_2 \subset H$, and $\det G_1 = \widehat{\mathbb{Z}}^\times$ while $\det G_2 = \det H$ is the subgroup of index 2 of $\widehat{\mathbb{Z}}^\times$ consisting of elements whose component at 7 reduces to a square. Thus the Shimura variety $\mathrm{Sh}_{G_1} = X$ is geometrically connected while Sh_{G_2}, Sh_H have 2 connected component over $\mathbb{Q}(\sqrt{-7})$. Since the element $\left(\begin{smallmatrix} 0 & -1 \\ 5 & 0 \end{smallmatrix}\right)_5$ normalizes all three open compact subgroup and has determinant $5 \notin (\mathbb{F}_7^\times)^2$, it induces an involution w over $\mathbb{Q}$ on all three Shimura varieties, and permutes the geometric connected components transitively. Putting $\Gamma_G = G_1 \cap \mathrm{SL}_2(\mathbb{Q}) = G_2 \cap \mathrm{SL}_2(\mathbb{Q})$ and $\Gamma_H = H \cap \mathrm{SL}_2(\mathbb{Q})$, we have a commuting diagram of complex curves with involution w:

$$\begin{array}{ccc} \mathrm{Sh}_{G_2} = \Gamma_G \setminus \mathbb{H} \amalg \Gamma_G \setminus \mathbb{H} & \longrightarrow & \mathrm{Sh}_{G_1} = \Gamma_G \setminus \mathbb{H} \\ \downarrow & & \downarrow \\ \mathrm{Sh}_H = \Gamma_H \setminus \mathbb{H} \amalg \Gamma_H \setminus \mathbb{H} & \longrightarrow & X(5b) \end{array} \tag{6.1}$$

where the vertical map is given by the quotient map on each component, while the horizontal map is the identity on the first component and w on the second component. The above diagram descends to K. The $\mathbb{Q}$-structure on $\mathrm{Sh}_{G_1} = X$ is determined by the subfield $\mathbb{Q}(x, \phi)$ inside its function field over $\mathbb{C}$. Since all arrows respect the $\mathbb{Q}$-structures, we see that there is an isomorphism of curves over K

$$d : Y \cong Y^\sigma = Y \times_{K,\sigma} K$$

and a commutative diagram of curves over K

$$\begin{array}{ccc} X & \xrightarrow{\pi} & Y \\ \downarrow{\scriptstyle w} & & \downarrow{\scriptstyle d} \\ X & \xrightarrow{\pi^\sigma} & Y^\sigma \end{array} \tag{6.2}$$

such that $d(x) = 125/x$. Note that there is at most one d with such property, and using Magma we compute that

$$d(-\psi) = \frac{P(x,\psi)}{(x^2+4x-1)(x^2+10x+5)^2}$$

with

$P(x,\psi) = 4x\psi^6 + (-9x^2 - 48x + 25)\psi^5 + (1/2(3\sqrt{-7}+3)x^3 + (22\sqrt{-7}+22)x^2 + 1/2(177\sqrt{-7}+33)x)\psi^4 + (-x^4 - 24x^3 + 1/2(135\sqrt{-7}-453)x^2 + (336\sqrt{-7}-536)x + 1/2(-375\sqrt{-7}+375))\psi^3 + ((-3\sqrt{-7}-3)x^4 + 1/2(-97\sqrt{-7}+47)x^3 + (-252\sqrt{-7}+894)x^2 + 1/2(-459\sqrt{-7}+6621)x + (125\sqrt{-7}-125))\psi^2 + ((-\sqrt{-7}-1)x^5 + (-21\sqrt{-7}-30)x^4 + (-99\sqrt{-7}-363)x^3 + 1/2(727\sqrt{-7}-1923)x^2 + (1512\sqrt{-7}+2208)x + 1/2(-1125\sqrt{-7}-5625))\psi + ((-3\sqrt{-7}-69)x^4 + (-180\sqrt{-7}-1092)x^3 + (-2331\sqrt{-7}-4761)x^2 + (-6228\sqrt{-7}-3444)x + (750\sqrt{-7}+750))$.

Lemma 6.2. *Inside* $H^0(X_K,\Omega^1) = H^0(X,\Omega^1)\otimes_{\mathbb{Q}} K$ *we have*

$$\pi^* H^0(Y,\Omega^1) \cap w^*\pi^* H^0(Y,\Omega^1) = 0$$

Proof. By looking at the pullbacks of differentials in the diagram (6.1), we see that $V \cap w^*V$ is stable under the anemic Hecke algebra $\mathbb{T}$ (the algebra generated by Hecke operators at good primes), we see that $V \cap w^*V$ is $\mathbb{T}$-stable. Because the Hecke fields of A_i are totally real quadratic fields, the $H^0(A_i,\Omega^1)\otimes K$ are exactly the irreducible $\mathbb{T}\otimes K$ submodules of $H^0(X_K,\Omega^1)$. Hence if $V \cap w^*V \neq 0$, it must be 2-dimensional and hence $V = w^*V = V^\sigma$ must be $H^0(A_i,\Omega^1)\otimes K$ for some i. But a non-zero element of this intersection gives rise to a vector $v \in \pi_i$ which is unramified away from 5 and 7, fixed under the Iwahori open compact at 5, the normalizer of the non-split Cartan open compact at 7 n and also under an S_4 subgroup of $\mathrm{PSL}_2(\mathbb{F}_7)$. The last two condition however forces v be invariant under $\mathrm{GL}_2(\mathbb{Z}_7)$, contradicting the fact that $\pi_{i,7}$ has conductor 7^2 (since it appears in the new part of $X_0(245)$). □

The lemma implies

$$\pi^* H^0(Y, \Omega^1) \oplus w^* \pi^* H^0(Y, \Omega^1) = (H^0(A_1, \Omega^1) \oplus H^0(A_2, \Omega^1)) \otimes K$$

Lemma 6.3. *Let D be a degree 1 divisor on X. Then the map $\Pi_D : X \to J(Y)$ given by*

$$P \mapsto \pi^\sigma(P) - \pi^\sigma(wP) - (\pi^\sigma(D) - \pi^\sigma(wD))$$

factorizes through the composition of $AJ_D : X \to J(X)$ and a $\mathbb{Q}$-quotient of $J(X)$ isogenous to A_2, and in particular through a quotient that has $\mathbb{Q}$-rank 0.

Proof. Since D maps to 0 in $J(Y^\sigma)$, there is a factorization through the Abel-Jacobi map associated to D. Let I be the ideal of $\mathbb{T}$ which cuts out the Hecke field of A_3. The observation after the previous lemma shows that $IJ(X)$ gets killed in $J(Y^\sigma)$. On the other hand, the image of $(w+1)(P-D) = (wP-D)+(P-D)-(wD-D)$ in $J(Y^\sigma)$ is

$$\pi^\sigma(wP) - \pi^\sigma(w^2P) + \pi^\sigma(P) - \pi^\sigma(wP)$$
$$- (\pi^\sigma(wD) - \pi^\sigma(w^2P)) - (\pi^\sigma(D) - \pi^\sigma(wD)) = 0$$

hence the map in consideration factors through $J(X)/((w+1)J(X) + IJ(X))$. This factor is defined over $\mathbb{Q}$ and is $\mathbb{Q}$-isogenous to A_2. □

A convenient choice for the base divisor D is given below

Proposition 6.4. *Let*

$$X^3 - 7X^2 + 7X + 7 = (X - \phi_1)(X - \phi_2)(X - \phi_3)$$

$$X^2 + 22X + 125 = (X - x_1)(X - x_2)$$

- *In terms of the coordinate (x, ϕ), the 6 cusps of X are given by $(0, \phi_i)$ and (∞, ϕ_i)*

- *In terms of the coordinate* (x, ψ)*, the* 2 *cusps of* Y *are given by* $(0, \infty)$ *and* (∞, ∞)
- *Put* $D = (0, \phi_1) + (0, \phi_2) + (0, \phi_3) - (x_1, 3) - (x_2, 3)$ *is a rational divisor of degree* 1 *on* X*, and*

$$\pi^\sigma(D) - \pi^\sigma(wD) = 3((0, \infty) - (\infty, \infty))$$

is a torsion point of exact order 7 *in* $J(Y^\sigma)$*.*

Proof. The first two statements are clear: Note that in terms of the singular plane model with coordinates (x, ϕ), the points (∞, ϕ_i) are singular points which are of the type $x^5 = y^7$, and the singularity is resolved after 3 blowups, and at each step there is a unique point in the pre-image of the singularity. Hence each (x, ϕ_i) actually gives exactly 1 point in the smooth curve X (alternatively, one could check that X has exactly 6 cusps, and we have written down at least 6 of them). A similar analysis gives the statement for Y and Y^σ. Because the involution w on X descends to the Atkin-Lehner involution on $X(5b)$, we see that w switches the fibers of $X \to X(5b)$ above $x = 0$ and $x = \infty$. On the other hand, one checks that $(x_i, 3)$ are the only $\mathbb{Q}(\sqrt{-1})$-rational points with $x = x_i$, and hence w must switch them. From this the equality in the last item follows. Finally, we have $7((0, \infty) - (\infty, \infty)) = \mathrm{div}(x)$ is principal, and $(0, \infty) - (\infty, \infty)$ is not principal since Y^σ has genus 2. □

Let us now take D as in the proposition and consider the map $\Pi = \Pi_D$ defined above. If P, $Q = P^\tau$ are a conjugate pair of quadratic points on X, $AJ_D(P + Q)$ is a rational point on $J(X)$ and hence must map to a 7-torsion point in $J(Y^\sigma)$ under Π, since it factors through a quotient isogenous to A_2. On the other hand wD is also rational and maps to $6((0, \infty) - (\infty, \infty))$, which has exact order 7 in $J(Y^\sigma)$, thus we have

$$\pi^\sigma(P) + \pi^\sigma(Q) - \pi^\sigma(wP) - \pi^\sigma(wQ) \sim a((0, \infty) - (\infty, \infty))$$

for some $a \in \mathbb{Z}$. Thus P and Q maps to the same point in the Kummer surface $K(Y^\sigma) = J(Y^\sigma)/\pm$ under the map Π_b

$$P \mapsto \pi^\sigma(P) - \pi^\sigma(wP) - b((0,\infty) - (\infty,\infty))$$

for some suitable integer b.

By finding an explicit basis Ω_1, Ω_2 for the space of homolorphic differentials on Y^σ using Magma, we compute in terms of x, ψ a double cover map

$$u : Y^\sigma \to \mathbb{P}^1$$

and a rational function v realizing Y^σ as a hyperelliptic curve of genus 2 of the form

$$v^2 = \text{sextic in } u$$

Lemma 6.5. *The map $\Pi_b : X \to J(Y^\sigma)$ is birational onto its image.*

Proof. Suppose the contrary, so we have infinitely many pairs (P_i, Q_i) of distinct points which have the same image via Π_b. We have

$$\pi^\sigma(P_i) + \pi^\sigma(wQ_i) \sim \pi^\sigma(wP_i) + \pi^\sigma(Q_i)$$

Suppose first that for infinitely many i, this effective degree 2 divisor is not the hyper elliptic class in Y^σ. This forces the above linear equivalence to be an equality of divisors. Note that π^σ has degree 3, so $\pi^\sigma \circ w \neq \pi^\sigma$. Hence for infinitely many i we must have $\pi^\sigma(P_i) = \pi^\sigma(Q_i)$, $\pi^\sigma(wP_i) = \pi^\sigma(wQ_i)$.

If the above case does not happen, $\pi^\sigma(P_i) + \pi^\sigma(wQ_i)$ and $\pi^\sigma(wP_i) + \pi^\sigma(Q_i)$ must be the hyperelliptic class for infinitely many i, as the hyperelliptic class is the unique g^1_2 on a genus 2 curve. This forces $P_i \neq wQ_i =: Q_i'$ for all but finitely many i, and we

have

$$u(\pi^\sigma(P_i)) = u(\pi^\sigma(Q_i'))$$

$$u(\pi^\sigma(wP_i)) = u(\pi^\sigma(wQ_i'))$$

Thus in either case we see that the map

$$(u \circ \pi^\sigma, u \circ \pi^\sigma \circ w) : X \to \mathbb{P}^1 \times \mathbb{P}^1$$

is not generically injective. However a Magma computation shows that the pair $(u \circ \pi^\sigma, u \circ \pi^\sigma \circ w)$ generates the function field of X, a contradiction. □

Consequently, composing the above map with the quotient map to the Kummer surface, we get a map $X \to \mathcal{K}(Y^\sigma)$ which is either birational onto its image or factors through X/w, which then is birational onto its image (since $X \to X/w$ is the only degree 2 map from X to any curve). The second case happens if and only if pairs of the form (P, wP) have the same image, and this happens if and only if $b = 0$.

We are therefore reduced to finding conjugate pairs of quadratic points $(P, Q = P^\tau)$ on X which maps to the same point in the Kummer surface via one of the above maps (note that we only need to consider $b \in \{0, 1, 2, 3\}$, by replacing P, Q with wP, wQ if needed).

Let us first study the case $b = 0$. The same argument in the proof of lemma 6.5 implies that either P,P^τ or P, wP^τ have the same image under the map

$$(u \circ \pi^\sigma, u \circ \pi^\sigma \circ w) : X \to \mathbb{P}^2$$

which is birational onto its image. One checks that $u \circ \pi^\sigma$ realizes $K(X)$ as a degree 6 extension of $K(u \circ \pi^\sigma \circ w)$ and vice versa, and hence the image of X is an irreducible plane curve of degree 12. Using Magma, we computed this plane curve explicitly and determined all its singular points defined over a quadartic extension of K. Hence

either $P \neq P^\tau$ and $P \neq wP^\tau$, their common image must be one of the above singular points of the image of X in $\mathbb{P}^2$; or $P = P^\tau$ or $P = wP^\tau$. One checks that the elliptic curves corresponding to such P must be either a $\mathbb{Q}$-curve or have CM.

Finally, we now turn to the case $b \neq 0$. We are looking for pairs (P, Q) such that

$$\pi^\sigma(P) + \pi^\sigma(Q) - \pi^\sigma(wP) - \pi^\sigma(wQ) \sim 2b((0,\infty) - (\infty,\infty))$$

and we know a priori that there are only finitely many such pairs $(P, Q = P^\tau)$ (note that this was not true when $b = 0$). By enumerating such pairs (P, Q) over some primes p split in K where the whole situation has good reduction, we found for some primes p there were no pairs $(P, Q) \in X(\mathbb{F}_p)^2$ or conjugate pairs $(P, P^\tau) \in X(\mathbb{F}_{p^2})$ satisfying the above equation, and hence there are no conjugate pairs of quadratic points on X of this type. For $b = 2$, a similar enumeration for the prime $p = 71$ shows that the pairs (P, Q) mod p satisfying the linear equivalence relation for $b = 2$ are either the cusps or the mod p reduction of the pair of conjugate points corresponding to the CM point $P = (125\sqrt{5} + 250, -\frac{1}{2}(\sqrt{5} - 1))$ in the coordinates (x, ϕ). Furthermore, one checks that these are only possible pairs in $\mathbb{Q}_{71^2}$ lifting the pairs mod 71. This shows that in this case all pairs of conjugate quadratic points we look for gives rise to CM elliptic curves.

Putting everything together, we found that all quadratic points on X gives rise to modular j-invariants.

References

[1] *Automorphic forms on GL(2)*. Lecture Notes in Mathematics, Vol. 114. Berlin.

[2] D. Abramovich. A linear lower bound on the gonality of modular curves. *International Mathematics Research Notices*, (20):1005–1011, 1996.

[3] P. B. Allen. Modularity of nearly ordinary 2-adic residually dihedral Galois representations. arXiv e-print 1301.1113, Jan. 2013.

[4] T. Barnet-Lamb, T. Gee, and D. Geraghty. Congruences between Hilbert modular forms: constructing ordinary lifts. arXiv e-print 1006.0466, June 2010.

[5] T. Barnet-Lamb, T. Gee, and D. Geraghty. Congruences betwen Hilbert modular forms: constructing ordinary lifts II. arXiv e-print 1205.4491, May 2012.

[6] D. Blasius. Elliptic curves, Hilbert modular forms, and the Hodge conjecture. In *Contributions to automorphic forms, geometry, and number theory*, pages 83–103. Johns Hopkins Univ. Press, Baltimore, MD, 2004.

[7] D. Blasius and J. D. Rogawski. Motives for Hilbert modular forms. *Inventiones Mathematicae*, 114(1):55–87, 1993.

[8] A. Borel and H. Jacquet. Automorphic forms and automorphic representations. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*, Proc. Sympos. Pure Math., XXXIII, page 189–207. Amer. Math. Soc., Providence, R.I., 1979. With a supplement "On the notion of an automorphic representation" by R. P. Langlands.

[9] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. the user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[10] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939 (electronic), 2001.

[11] C. Breuil and F. Diamond. Formes modulaires de Hilbert modulo p et valeurs d'extensions Galoisiennes. arXiv e-print 1208.5367, Aug. 2012.

[12] H. Carayol. Sur les représentations l-adiques attachées aux formes modulaires de Hilbert. *Comptes Rendus des Séances de l'Académie des Sciences. Série I. Mathématique*, 296(15):629–632, 1983.

[13] B. Conrad, F. Diamond, and R. Taylor. Modularity of certain potentially barsotti-tate Galois representations. *Journal of the American Mathematical Society*, 12(2):521–567, 1999.

[14] C. J. Cummins and S. Pauli. Congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. In *Symmetry in physics*, volume 34 of *CRM Proc. Lecture Notes*, pages 23–29. Amer. Math. Soc., Providence, RI, 2004.

[15] H. Darmon, F. Diamond, and R. Taylor. Fermat's last theorem. In *Current developments in mathematics, 1995 (Cambridge, MA)*, page 1–154. Int. Press, Cambridge, MA, 1994.

[16] B. de Smit and B. Edixhoven. Sur un résultat d'Imin chen. *Mathematical Research Letters*, 7(2-3):147–153, 2000.

[17] F. Diamond. The Taylor-Wiles construction and multiplicity one. *Inventiones Mathematicae*, 128(2):379–391, 1997.

[18] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[19] L. Dieulefait and N. Freitas. Fermat-type equations of signature $(13, 13, p)$ via Hilbert cusp-forms. arXiv e-print 1112.4521, Dec. 2011.

[20] T. Ekedahl. An effective version of Hilbert's irreducibility theorem. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, page 241–249. Birkhäuser Boston, Boston, MA, 1990.

[21] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, page 21–76. Amer. Math. Soc., Providence, RI, 1998.

[22] N. D. Elkies. The Klein quartic in number theory. In *The eightfold way*, volume 35 of *Math. Sci. Res. Inst. Publ.*, page 51–101. Cambridge Univ. Press, Cambridge, 1999.

[23] J. S. Ellenberg. $\mathbb{Q}$-curves and Galois representations. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 93–103. Birkhäuser, Basel, 2004.

[24] N. Freitas, B. V. Le Hung, and S. Siksek. Elliptic curves over real quadratic fields are modular. arXiv e-print 1310.7088, Oct. 2013.

[25] N. Freitas and S. Siksek. Modularity and the Fermat equation over totally real fields. arXiv e-print 1307.3162, July 2013.

[26] B. H. Gross. On the satake isomorphism. In *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, volume 254 of *London Math. Soc. Lecture Note Ser.*, page 223–237. Cambridge Univ. Press, Cambridge, 1998.

[27] J. Harris and J. Silverman. Bielliptic curves and symmetric products. *Proceedings of the American Mathematical Society*, 112(2):347–356, 1991.

[28] M. Harris, K.-W. Lan, R. Taylor, and J. Thorne. On the rigid cohomology of certain Shimura varieties, preprint. 2013.
`http://www.math.ias.edu/~rtaylor/`.

[29] F. Jarvis and J. Manoharmayum. On the modularity of supersingular elliptic curves over certain totally real number fields. *Journal of Number Theory*, 128(3):589–618, 2008.

[30] F. Jarvis and P. Meekin. The Fermat equation over $\mathbb{Q}(\sqrt{2})$. *Journal of Number Theory*, 109(1):182–196, 2004.

[31] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. i. *Inventiones Mathematicae*, 178(3):485–504, 2009.

[32] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. II. *Inventiones Mathematicae*, 178(3):505–586, 2009.

[33] M. Kisin. Moduli of finite flat group schemes, and modularity. *Annals of Mathematics. Second Series*, 170(3):1085–1180, 2009.

[34] A. W. Knapp. Representations of $\rm GL_2(\bf r)$ and $\rm GL_2(\bf c)$. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*, Proc. Sympos. Pure Math., XXXIII, page 87–91. Amer. Math. Soc., Providence, R.I., 1979.

[35] R. P. Langlands. *Base change for GL*(2), volume 96 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, N.J., 1980.

[36] J. Manoharmayum. On the modularity of certain $\mathrm{GL}_2(\mathbb{F}_7)$ Galois representations. *Mathematical Research Letters*, 8(5-6):703–712, 2001.

[37] R. Oyono and C. Ritzenthaler. On rationality of the intersection points of a line with a plane quartic. In *Arithmetic of finite fields*, volume 6087 of *Lecture Notes in Comput. Sci.*, page 224–237. Springer, Berlin, 2010.

[38] K. A. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, page 241–261. Birkhäuser, Basel, 2004.

[39] P. Scholze. On torsion in the cohomology of locally symmetric varieties. arXiv e-print 1306.2070, June 2013.

[40] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Annals of Mathematics. Second Series*, 88:492–517, 1968.

[41] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, Nov. 1994.

[42] C. Skinner. Nearly ordinary deformations of residually dihedral representations, preprint. 2009.

[43] C. M. Skinner and A. J. Wiles. Residually reducible representations and modular forms. *Institut des Hautes Études Scientifiques. Publications Mathématiques*, (89):5–126 (2000), 1999.

[44] C. M. Skinner and A. J. Wiles. Nearly ordinary deformations of irreducible residual representations. *Annales de la Faculté des Sciences de Toulouse. Mathématiques. Série 6*, 10(1):185–215, 2001.

[45] W. Stein. The Modular Forms Database. 2012.
`http://wstein.org/Tables`.

[46] H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.

[47] R. Taylor. On Galois representations associated to Hilbert modular forms. *Inventiones Mathematicae*, 98(2):265–280, 1989.

[48] R. Taylor. On Galois representations associated to Hilbert modular forms. II. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, page 185–191. Int. Press, Cambridge, MA, 1995.

[49] R. Taylor. Galois representations. In *Proceedings of the International Congress of Mathematicians, Vol. I (Beijing, 2002)*, page 449–474. Higher Ed. Press, Beijing, 2002.

[50] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Annals of Mathematics. Second Series*, 141(3):553–572, 1995.

[51] J. Tunnell. Artin's conjecture for representations of octahedral type. *American Mathematical Society. Bulletin. New Series*, 5(2):173–175, 1981.

[52] A. Wiles. On ordinary λ-adic representations associated to modular forms. *Inventiones Mathematicae*, 94(3):529–573, 1988.

[53] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Annals of Mathematics. Second Series*, 141(3):443–551, 1995.