

A geometric prime switch for elliptic curves over totally real and CM fields

Discussion draft

October 7, 2026

Abstract

In recent work [35], OpenAI established the modularity of elliptic curves over imaginary quadratic fields. We show that their method also establishes modularity over totally real fields and over CM fields not containing ζ_5 .

1 Introduction

One of the great achievements of modern number theory is the proof of the Taniyama–Shimura conjecture: every elliptic curve $E/\mathbb{Q}$ is modular, that is, $L(E, s) = L(f, s)$ for a newform f of weight two and level $\Gamma_0(N)$. Equivalently, the Tate modules of E are isomorphic to the ℓ -adic representations attached to f by Eichler and Shimura [41]. The conjecture was the key to Fermat’s Last Theorem: a solution of the Fermat equation gives a semistable elliptic curve [24] which, as anticipated by Serre [39], cannot be modular by Ribet’s level-lowering theorem [36]. Wiles and Taylor–Wiles proved the conjecture for semistable curves [52, Theorem 0.4], [47], and after further work [21, 16] Breuil, Conrad, Diamond, and Taylor proved it in general [10].

Over a number field K , Langlands reciprocity [32] predicts that every elliptic curve E/K is *modular*: the compatible system $\rho_{E, \ell}$ given by $H^1(E)$ is attached to a regular algebraic automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_K)$, cuspidal unless E has complex multiplication defined over K . This formulation, and essentially all known approaches to modularity, require the construction of compatible systems of Galois representations attached to regular algebraic cuspidal automorphic representations of $\mathrm{GL}_2(\mathbb{A}_K)$. Such constructions are known when K is totally real, by work of Carayol, Wiles, Blasius–Rogawski, and Taylor [15, 51, 7, 44], and when K is CM: first over imaginary quadratic fields under a condition on the central character [27, 45, 6], and in general by Harris–Lan–Taylor–Thorne [26]. Because of this, modularity results to date are mostly confined to totally real or CM fields; a notable exception is the work of Boxer, Calegari, Gee, and Pilloni on elliptic curves over quadratic extensions of totally real fields that need not be CM [9].

The main approach to modularity follows the strategy, due to Wiles, of propagating modularity along congruences. It has two steps:

- (Modularity lifting) If ρ is an ℓ -adic representation satisfying suitable local conditions (including ℓ -adic Hodge-theoretic conditions at ℓ) and $\bar{\rho} \simeq \bar{\rho}_{\pi, \ell}$ for the Galois representation $\rho_{\pi, \ell}$ of some automorphic π , then ρ is modular. This usually requires the image of $\bar{\rho}$ to be sufficiently large.
- (Chaining) Find a chain of congruences between $\rho_{E, \ell}$ and some $\rho_{\pi, \ell'}$ with π automorphic, such that the first step applies at each link. Crucially, the prime at which the congruence holds may change along the chain.

The strategy is most developed in the totally real case. Building on Wiles’s method, work of Kisin [30], Gee [25], and Barnet-Lamb–Gee–Geraghty [4, 5] led to essentially optimal modularity lifting theorems in weight two; see [11, Théorème 3.2.2] for a convenient statement. Thus the difficulty lies in the second step: finding enough congruences to representations known to be modular. If one is willing to enlarge K , that is, to prove only *potential modularity*, this is resolved by Taylor [46]; for elliptic curves see [53, Theorem A.1], and [42, Theorem 1.1.1] for general weight-two representations. On the other hand, it seems very hard to produce enough congruences while keeping K fixed, as this is related to finding points on complicated algebraic varieties. For this reason, previous results restrict the field: to low degree, namely real quadratic [23], totally real cubic [20], quartic fields not containing $\sqrt{5}$ [8], and all but finitely many quintic fields [28]; to fields with restricted ramification at small primes [33, 54]; or to special towers, such as the cyclotomic $\mathbb{Z}_p$ -extension of $\mathbb{Q}$ [49]. These hypotheses are used to deal with exceptional collections of elliptic curves, given by points on certain modular curves, which are not known to be chainable to a modular one. Lifting theorems for small residual images [48, 29] shrink these exceptional cases, though they fall short of getting rid of them altogether.

Compared to the totally real case, the CM case is more recent and harder: automorphic forms for GL_2 over a CM field occur in the cohomology of locally symmetric spaces that are not algebraic varieties, in several degrees, and are not directly related to geometry. As a consequence, modularity lifting theorems are harder to establish. The seminal work of Calegari–Geraghty [12] generalized the Taylor–Wiles method to this setting, conditionally on conjectures on torsion in the cohomology of locally symmetric spaces. Since then many of these conjectures have been proven or bypassed [37, 1], leading to potential modularity results over CM fields [1, Theorem 1.0.1] and, more recently, to modularity lifting theorems in weight two of strength comparable to the totally real case, due to Caraiani–Newton [14, Theorem 5.2]. Combined with the residual modularity results of Allen–Khare–Thorne [2], the latter led to major progress over CM fields. For instance, Caraiani–Newton showed that all elliptic curves over an imaginary quadratic field K with $X_0(15)(K)$ finite are modular, such as $K = \mathbb{Q}(\sqrt{-d})$ with $d = 1, 2, 3, 5$ [14, Theorem 1.1], and more generally proved modularity over CM fields not containing ζ_5 under hypotheses on $\bar{\rho}_{E,3}$ or $\bar{\rho}_{E,5}$ [14, Theorem 6.1]. The main thrust behind these results is the modularity lifting step.

Most recently, OpenAI announced a proof that every elliptic curve over every imaginary quadratic field is modular [35, Theorem 1.1], by introducing a clever new idea for the chaining step. Unlike previous arguments, which exploit small primes such as 2, 3, 5, 7 and special moduli problems, OpenAI’s chain passes through a congruence modulo an arbitrarily large auxiliary prime p , after a large solvable base change. The use of such large primes is traditionally overlooked, since it is believed (e.g. by the Frey–Mazur conjecture, see [31]) that there are very few congruences between elliptic curves over a fixed field for large p . Since its geometric ingredients work over any number field, one expects OpenAI’s argument to extend beyond imaginary quadratic fields. This is indeed the case.

Theorem 1.1. *Assume Inputs 2.1 and 2.2 from [35]. Then every elliptic curve over every totally real number field is modular. Assume in addition Input 4.1 from [35]. Then every elliptic curve over every CM number field K with $\zeta_5 \notin K$ is modular.*

Remark 1.2. 1. The inputs are the geometric results of [35]. Input 2.1 gives the basic properties of the family of motives that carries the chain of congruences; Input 2.2 is the large monodromy of the family, which gives large residual images along the chain; and Input 4.1 concerns local properties of the family.

2. In the totally real case we use no modularity lifting theorem over CM fields.

1.1 Outline

Let E be an elliptic curve over K . Fix $n = 3p$ for a large auxiliary prime p . OpenAI constructs a family of quadratic twists B_t and cyclic degree n covers $C_n(t) \rightarrow B_t$ over an open subset $U \subset \mathbb{A}_t^1$. $C_n(t)$ comes with an action of a dihedral group defined over $F = K(\mu_n)$. The key feature of the construction is that the integral ℓ -adic cohomology $H^1(C_n(t))$ is free of rank 2 over $\mathbb{Z}_\ell[\mu_n]$ for all ℓ . In particular, it decomposes into rank-two pieces V_θ with Hodge–Tate weights 0, 1, indexed by characters θ of μ_n . One has $V_1 = H^1(B_t)$, and for η of order three, $V_\eta = H^1(A_t)$ for an elliptic curve A_t . The reduction of V_θ modulo ℓ only depends on $\theta \bmod \ell$. With ψ of order p this gives the chain of congruences (for each t)

$$V_\eta \equiv_p V_{\eta\psi} \equiv_3 V_\psi \equiv_p V_1,$$

and the idea is to propagate modularity from the left to the right. In order to do this propagation, the essential point is to keep the involved residual image large at each step so that a modularity lifting theorem applies. As p is chosen to be large, the key point is to arrange t so that $V_\psi \bmod 3$ has large image. This is achieved by the fact that the family has two opposite transvections around two points of the parameter space where the cover degenerates, and thus Hilbert irreducibility guarantees there are many such choices of t . As a byproduct, one can also guarantee that the mod 5 image of $V_\eta = H^1(A_t)$ is large, and hence that A_t is modular. Importantly, this gives the starting point for the chain.

For the case of totally real K , we first note that the V_θ in the construction are only defined over the CM field $K(\mu_{3p})$. However, twisting the cover by the reflection descends them to totally odd systems W_θ over $L = K(\zeta_{3p} + \zeta_{3p}^{-1})$ with the same congruences, and thus one can follow the above argument with the (less restrictive) modularity lifting theorems over totally real fields; thus one merely needs the existence of the chain of congruences to run the argument.

Over CM K , invoking the Caraiani–Newton modularity lifting theorem requires one to verify two additional hypotheses: that the residual representations are decomposed generic and that the motives in the chain have the same local ℓ -adic Hodge-theoretic behavior at the coefficient prime ℓ . The first is easily dealt with by applying Hilbert irreducibility to a Weil restriction, while the second is dealt with by imposing local conditions on t at the places above $3p$, using an analysis of the reduction of the family near its compact-type degeneration.

Remark 1.3. 1. The main reason for the hypothesis $\zeta_5 \notin K$ in the CM case was so that one can apply the existing modularity lifting of Caraiani–Newton at the prime 5 [14, Theorem 6.1]. An improvement to this has been obtained by AI, as released in [13]. With this improvement, OpenAI’s argument now covers all CM fields. Nevertheless, we find it instructive to treat the totally real field case on its own, as it illustrates clearly the distinctive role of the two parts of the strategy.

2. It is essential that our chain connects to an elliptic curve A_t , which is the reason to work with the prime 3 in the middle congruence of the chain. Replacing the prime 3 with a larger prime will instead connect $H^1(B_t)$ to some other motive for which one does not know how to establish modularity. On the other hand, one could contemplate using the prime 2 to establish the modularity of A_t along the lines of [2].
3. One might wonder whether it is possible to use a different prime to get the modularity of the starting motive A_t . The prime 3 does not work, since $H^1(A_t)$ turns out to always be congruent to a quadratic twist of $E \bmod 3$.

Remark 1.4. The mechanism has antecedents in families of curves with real multiplication [34, 43, 19, 22], and above all in Darmon’s work on rigid local systems [17, 18]. There, hypergeometric families are related by reduction modulo primes dividing the orders of local monodromy, and modularity is propagated conditionally on a lifting conjecture [17, Conjecture 1.1].

Section 2 sets up the geometry and the congruences, Sections 3 and 4 treat the totally real and CM cases, and Section 5 contains descent and local–global compatibility.

AI disclosure. The first draft of this note, apart from the introduction, was generated by the AI system Astra. The introduction was written by the author. The whole text was proofread and edited, and its references checked, by Claude (Anthropic; model Claude Opus 5.5).

Conventions. Write $G_k = \text{Gal}(\bar{k}/k)$ and $H^1(X) = H_{\text{ét}}^1(X_{\bar{k}}, \mathbb{Q}_\ell)$, extending scalars to $\bar{\mathbb{Q}}_\ell$ when needed. The cyclotomic character ϵ_ℓ has Hodge–Tate weight -1 , so $\det H^1(E) = \epsilon_\ell^{-1}$ and $\text{HT}_\tau(H^1(E)) = \{0, 1\}$ for every τ . Bars denote semisimplified reductions. We fix embeddings of $\bar{\mathbb{Q}}$ into $\mathbb{C}$ and into every $\bar{\mathbb{Q}}_\ell$. When applying [11, 23] we dualize to the Tate-module convention.

2 The geometric construction

Let k be a number field, $E : y^2 = h(x)$ an elliptic curve over k , and $n \geq 3$ odd. Put

$$B_t : h(t)y^2 = h(x), \quad R_t = (t, 1), \quad S_t = [n]R_t,$$

and let $U \subset \mathbb{A}_k^1$ be the open set where $h(t) \neq 0$ and $O, \pm R_t, \pm S_t$ are distinct. The divisor $(S_t) - (-S_t) - n(R_t) + n(-R_t)$ is principal; let f_t be its function with $f_t(O) = 1$, so that $f_t(-Z) = f_t(Z)^{-1}$. For $m \mid n$ let $C_m(t)$ be the normalization of B_t in

$$Y^m = f_t(Z), \tag{1}$$

with rotations $u_\zeta(Z, Y) = (Z, \zeta Y)$, $\zeta \in \mu_m$, and reflection $w(Z, Y) = (-Z, Y^{-1})$, so that $wu_\zeta w = u_{\zeta^{-1}}$. The curve and w are defined over k , the rotations over $k(\mu_m)$. The map $C_n \rightarrow C_m$ is $Y \mapsto Y^{n/m}$, and $C_m(t)/\mu_m = B_t$.

Geometric input 2.1 (Cover and lattice; [35, Lemma 3.1, Propositions 3.3 and 4.2, Remark 4.3]). The curve $C_m(t)$ is smooth of genus m , and for every prime ℓ , including $\ell \mid m$,

$$H_{\text{ét}}^1(C_{m,\bar{k}}, \mathbb{Z}_\ell) \simeq \mathbb{Z}_\ell[\mu_m]^2 \tag{2}$$

as modules over the group ring of the rotation group. After pullback along $E \rightarrow \mathbb{A}^1$, $(t, s) \mapsto t$, over which $B_t \simeq E$ and R_t becomes the moving point $R = (t, s)$, the Jacobian family extends across $R = O$ with fiber E^m , whose factors the rotations permute regularly over $k(\mu_m)$.

Geometric input 2.2 (Monodromy; [35, Theorem 4.5]). After any complex embedding of k , geometric monodromy contains, in one basis of the free module (2), two opposite transvections with off-diagonal entries $\pm(2 - u - u^{-1})$, where u is $Y \mapsto e^{2\pi i/m} Y$. On the eigenspace where u acts by $\lambda \neq 1$ they are

$$T_a = \begin{pmatrix} 1 & \nu_a c_\lambda \\ 0 & 1 \end{pmatrix}, \quad T_b = \begin{pmatrix} 1 & 0 \\ \nu_b c_\lambda & 1 \end{pmatrix}, \quad c_\lambda = 2 - \lambda - \lambda^{-1}, \quad \nu_a, \nu_b \in \{\pm 1\}. \tag{3}$$

The common basis matters: triangular matrices in unrelated bases would not give irreducibility. Both inputs hold over any number field.

2.1 Rank-two systems

Let $F \supset k(\mu_n)$. For a character θ of μ_n let $V_\theta = V_{\theta,\ell} \subset H_{\text{ét}}^1(C_{n,\overline{F}}, \overline{\mathbb{Q}}_\ell)$ be the θ -eigenspace of the rotations; it is G_F -stable, of dimension two by (2). Cup product $\langle \cdot, \cdot \rangle$ is rotation-invariant, so it pairs V_θ perfectly with $V_{\theta^{-1}} = w^*V_\theta$, and

$$[x, y]_\theta = \langle x, w^*y \rangle \quad (4)$$

is a nondegenerate G_F -equivariant pairing on V_θ with values in $\overline{\mathbb{Q}}_\ell(-1)$. It is alternating, as $\langle y, w^*x \rangle = \langle w^*y, x \rangle = -\langle x, w^*y \rangle$. Hence $\det V_\theta = \epsilon_\ell^{-1}$. Since w^* exchanges the θ - and θ^{-1} -parts of $H^{1,0}$, and complex conjugation exchanges the θ^{-1} -part of $H^{1,0}$ with the θ -part of $H^{0,1}$, each θ -part of $H^{1,0}$ is a line; so the labelled Hodge–Tate weights are $\{0, 1\}$. The V_θ are semisimple, potentially semistable, and form compatible systems (use the character projector and traces of rotations composed with Frobenius).

The trivial character gives $V_1 = H^1(B_t)$. Put

$$D_t = C_3(t)/\langle w \rangle, \quad A_t = \text{Jac}(D_t), \quad (5)$$

both defined over k . On $H^1(C_3)$, w acts by -1 on $H^1(B_t)$, since it induces inversion, and swaps the other two character spaces; so D_t has genus one. For η of order three, projecting the w -invariants to the η -space gives

$$H^1(A_t)|_{G_F} \simeq V_\eta, \quad H^1(B_t)|_{G_F} \simeq V_1. \quad (6)$$

2.2 Congruences

Let $p > 100$ be prime, $n = 3p$, let η, ψ be characters of orders $3, p$, and $\chi = \eta\psi$. For $\mathcal{O}$ the integers of a large enough finite extension of $\mathbb{Q}_\ell$, the lattice

$$T_{\theta,\ell} = H_{\text{ét}}^1(C_{n,\overline{F}}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell[\mu_n], \theta} \mathcal{O} \subset V_{\theta,\ell}$$

is G_F -stable and free of rank two by (2). Its reduction depends only on $\theta \bmod \ell$, and roots of unity of ℓ -power order reduce to 1, so

$$V_\eta \equiv_p V_\chi \equiv_3 V_\psi \equiv_p V_1, \quad (7)$$

where $\equiv_\ell$ means isomorphic semisimplified reductions modulo ℓ . No division by 3 or p occurs.

2.3 Residual irreducibility

Take $k = K$ and consider the pairs

$$(m, \ell) = (3, 5), (3, p), (p, 3), \quad (8)$$

with m the order of the character and ℓ the residual characteristic. As $\ell \nmid m$, $c_\lambda = -(\lambda - 1)^2/\lambda$ is nonzero modulo ℓ , so T_a and T_b have distinct fixed lines and geometric monodromy acts absolutely irreducibly on the reduction of each character space of order m . For $m = 3$ we have $c_\lambda = 3$, so modulo 5 these matrices generate $\text{SL}_2(\mathbb{F}_5)$.

2.4 Changing the coefficient prime

If one member of the compatible system V_θ , or W_θ of Section 3.2, is realized by an automorphic representation π , then so is every member: compare Frobenius polynomials and apply Chebotarev and Brauer–Nesbitt. This lets us change the coefficient prime along (7).

3 The totally real case

Let K be totally real.

3.1 Modularity lifting

The following is a consequence of [23, Theorem 3], [11, Théorème 3.2.2]:

Proposition 3.1. *Let L be totally real, $\ell \neq 2, 5$ a prime, and A/L an abelian variety. Let $r : G_L \rightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ be the image of an idempotent of $\mathrm{End}_L(A) \otimes \overline{\mathbb{Q}}$ on $H^1(A_{\overline{L}}, \overline{\mathbb{Q}}_\ell)$, with $\det r = \epsilon_\ell^{-1}$ and labelled weights $\{0, 1\}$. If $\bar{r}$ is modular and $\bar{r}|_{G_{L(\zeta_\ell)}}$ is absolutely irreducible, then r is modular.*

We remark that in the above Proposition, there is no need to arrange any local conditions for r to match with a modular lift.

3.2 The reflection twist

Let $M = K(\mu_{3p})$ and $L = K(\zeta_{3p} + \zeta_{3p}^{-1})$. Then L/K is abelian and totally real, and M/L is quadratic with character $\delta = (-1)^e$, $e : G_L \rightarrow \mathbb{Z}/2\mathbb{Z}$. Twisting C_m by the cocycle $g \mapsto w^{e(g)}$ (a cocycle since w is defined over K) gives a curve C_m^δ/L , whose cohomology is that of C_m with

$$\rho^\delta(g) = (w^*)^{e(g)} \rho(g). \quad (9)$$

Lemma 3.2. *The rotations and w of C_m^δ are defined over L . The θ -eigenspaces W_θ of $H^1(C_{n,\overline{L}}^\delta)$ are totally odd G_L -representations with determinant ϵ_ℓ^{-1} and labelled weights $\{0, 1\}$, and*

$$W_\eta \equiv_p W_\chi \equiv_3 W_\psi \equiv_p W_1, \quad (10)$$

$$W_\eta \simeq H^1(A_t)|_{G_L}, \quad W_1 \simeq H^1(B_t)|_{G_L} \otimes \delta. \quad (11)$$

Proof. An element $g \in G_L$ acts on μ_m by $\zeta \mapsto \zeta^{\pm 1}$ according to $e(g)$, and $w^{e(g)} u_{g(\zeta)} w^{e(g)} = u_\zeta$, so the twisted descent datum fixes each u_ζ and w . The integral lattice is unchanged and commutes with Galois, which gives (10) as in Section 2.2. Since w and cup product are defined over L , (4) gives the determinant, which is -1 on complex conjugations. The quotient C_3^δ/w is D_t , giving the first endpoint; w acts by -1 on $H^1(B_t)$, so (9) gives the second. $\square$

3.3 The parameter

Let E/K be non-CM. By Serre's open image theorem [38, §4.2, Théorème 2], choose $p > 100$ with $\bar{\rho}_{E,p}(G_K) \supset \mathrm{SL}_2(\mathbb{F}_p)$. As $\mathrm{SL}_2(\mathbb{F}_p)$ is perfect and $D = K(\mu_{15p})$ is abelian over K , $\bar{\rho}_{E,p}(G_D) = \mathrm{SL}_2(\mathbb{F}_p)$.

The local systems $H^1(C_m, \mathbb{F}_\ell)$ over U_D , for the pairs (8), cut out a finite quotient Q of $\pi_1(U_K)$ mapping onto $\mathrm{Gal}(D/K)$ (take the normal core of their common kernel). By Hilbert irreducibility [40, Proposition 3.3.1 and Theorem 3.4.1] there is $t \in U(K)$ with $G_K \rightarrow Q$ surjective; then G_D maps onto $\ker(Q \rightarrow \mathrm{Gal}(D/K))$, which contains geometric monodromy. By Section 2.3, the reductions of V_η modulo 5 and p and of V_ψ modulo 3 are absolutely irreducible on $G_D \subset G_{L(\zeta_\ell)}$, and so are those of the W_θ , since $\delta|_{G_D} = 1$. The mod-5 image of A_t contains two noncommuting elements of order 5, so A_t is non-CM.

3.4 Proof for totally real fields

By [23, Theorem 3], A_t/L is modular, hence so is W_η . Apply Proposition 3.1 as follows, changing the coefficient prime after each row (Section 2.4):

Modular	Prime	Target	Residual irreducibility from
W_η	p	W_χ	order-three piece modulo p
W_χ	3	W_ψ	order- p piece modulo 3
W_ψ	p	W_1	E modulo p

By (11), B_t/L is modular. Descending along L/K (Lemma 5.1) and twisting back to E proves the theorem for totally real K .

4 The CM case

Let K be CM with $\zeta_5 \notin K$, E/K non-CM, and $F = K(\mu_{3p})$.

4.1 The lifting theorem

The seed is [14, Theorem 6.1]: an elliptic curve A/K is modular if $\bar{\rho}_{A,5}$ is decomposed generic and absolutely irreducible on $G_{K(\zeta_5)}$. For the chain we use [14, Theorem 5.2] at $\ell = 3, p$. Besides the determinant and weight conditions of Section 2, it requires $\bar{\rho}$ to be decomposed generic and irreducible on $G_{F(\zeta_\ell)}$, and the following match at each $v \mid \ell$ with the automorphic source π : either ρ is potentially crystalline, $r_\ell(\pi)$ is potentially ordinary exactly when ρ is, and $\text{rec}(\pi_v)$ has zero monodromy; or ρ and $r_\ell(\pi)$ are not potentially crystalline and π is ι -ordinary at v . Here $\bar{\rho}$ is *decomposed generic* if some prime $q \neq \ell$ splits completely in F and, at each $v \mid q$, $\bar{\rho}$ is unramified with no ratio of Frobenius eigenvalues equal to q .

4.2 Local reduction

Geometric input 4.1 (Local reduction; [35, Propositions 7.3 and 7.5, Corollary 7.6]). For each $v_0 \mid 3p$ of K there is a nonempty open subset of $U(K_{v_0})$ such that, for t in it, the Jacobian of $C_n(t)$ has at every $v \mid v_0$ of F the same potential reduction type as E^n : good ordinary, good with all slopes $1/2$, or semistable of toric rank n .

In [35] this is stated over imaginary quadratic fields, but the argument is general. On each character space the three types give, respectively, potentially crystalline and ordinary, potentially crystalline and non-ordinary, and monodromy of rank one, for every coefficient prime [35, Corollary 7.6].

4.3 Local matching

Let π realize the source of a row of (7), and let $v \mid \ell$. The source and the target are summands of the same Jacobian, so by Input 4.1 they are both potentially crystalline or neither, with the same potential ordinarity. It remains to check π_v , using semisimplified local–global compatibility [50, Theorem 1] at another prime. In the potentially good case the two Frobenius eigenvalues have equal absolute value, so $\text{rec}(\pi_v)$ has zero monodromy. In the toric case they differ by the norm; as π_v is generic, it is a twist of Steinberg, by a quadratic character since the central character is trivial. Then π is ι -ordinary at v by the argument of [14, Lemma 6.1.3(4)].

4.4 Decomposed genericity

Regular semisimple elements. For a pair in (8), $\text{tr}(T_a T_b^j) = 2 + \nu_a \nu_b j c_\lambda^2$, and an element of SL_2 is regular semisimple if and only if its trace is not ± 2 . For $m = 3$ take $j = 2$: the traces 20 and -16 differ from ± 2 by 18, 22, or 14, so they are not ± 2 modulo 5 or p . For $(m, \ell) = (p, 3)$ take $j = 1$: a bad trace forces $(\lambda - 1)^4 = \pm 4\lambda^2$, so $\lambda \in \mathbb{F}_{3^a}$ with $a \leq 4$, impossible since λ has order $p > 80 \geq 3^a - 1$.

All conjugates. Let $d = [K : \mathbb{Q}]$, K^{nor} the Galois closure of K , D a finite Galois extension of $\mathbb{Q}$ containing $K^{\text{nor}}(\mu_{15p})$, and $X = \text{Res}_{K/\mathbb{Q}} U \subset \mathbb{A}_{\mathbb{Q}}^d$, so that $X_D \simeq \prod_{\sigma: K \hookrightarrow D} U_D^\sigma$. The local systems $H^1(C_m^\sigma, \mathbb{F}_\ell)$ on the factors, for the pairs (8), cut out a finite quotient Q of $\pi_1(X)$ mapping onto $\text{Gal}(D/\mathbb{Q})$. By Hilbert irreducibility with weak approximation [35, Lemma 8.3] (see also [40, Proposition 3.3.1, Theorems 3.4.1 and 3.5.3]) there is $t \in X(\mathbb{Q}) = U(K)$, in any prescribed nonempty open subsets of finitely many $U(K_{v_0})$, with $G_{\mathbb{Q}} \rightarrow Q$ surjective. Then G_D maps onto $\ker(Q \rightarrow \text{Gal}(D/\mathbb{Q}))$, which contains geometric monodromy, a product over the factors. So for each pair some $g \in G_D$ acts regularly semisimply on every nontrivial character space in every factor. By Chebotarev, infinitely many primes q have Frobenius conjugate to g . They split in D , so $q \equiv 1 \pmod{\ell}$, and every Frobenius above q is regular semisimple on every character space, since conjugation permutes factors and characters. This is decomposed genericity: over K for $A_t[5]$, and over F for the pairs $(3, p)$ and $(p, 3)$. As in Section 3.3, $A_t[5]$ is absolutely irreducible on $G_{K(\zeta_5)}$, A_t is non-CM, and the residual representations are absolutely irreducible on $G_D \subset G_{F(\zeta_\ell)}$. This replaces the two conjugates of [35, Proposition 8.4]; no Galois assumption on K is needed.

The final switch. Choose p so that $\bar{\rho}_{E^\sigma, p}(G_{K^{\text{nor}}}) \supset \text{SL}_2(\mathbb{F}_p)$ for every $\sigma : K \hookrightarrow K^{\text{nor}}$ [38, §4.2, Théorème 2], and

$$p > \max\{100, 2d + 1\}. \quad (12)$$

Then G_{D_0} , for $D_0 = K^{\text{nor}}(\mu_{15p})$, has image $\text{SL}_2(\mathbb{F}_p)$ on each $E^\sigma[p]$. Exactly $2p^2$ elements of $\text{SL}_2(\mathbb{F}_p)$ have trace ± 2 , so the proportion of the joint image that is not regular semisimple in some factor is at most

$$d \frac{2p^2}{p(p^2 - 1)} = \frac{2dp}{p^2 - 1} < 1, \quad (13)$$

as $p(p - 2d) > 1$; for $d = 2$ this is [35, Lemma 8.2]. Chebotarev for a good element, avoiding the primes of bad reduction of B_t once t is fixed, gives decomposed genericity of $\bar{\rho}_{E, p}$, hence of the reductions of V_ψ and V_1 , over F .

4.5 The parameter

Choose p as in (12), and by the specialization above a single $t \in U(K)$ in the open sets of Input 4.1 for all $v_0 \mid 3p$. Then:

1. $\bar{\rho}_{A_t, 5}$ is decomposed generic over K and absolutely irreducible on $G_{K(\zeta_5)}$, and A_t is non-CM;
2. each residual representation in (7) is decomposed generic over F and absolutely irreducible on $G_{F(\zeta_\ell)}$;
3. above $3p$, all pieces have the reduction type of Input 4.1, so Section 4.3 applies.

4.6 Proof for CM fields

By [14, Theorem 6.1], A_t is modular over K , hence over F by solvable base change, cuspidally since A_t is non-CM; so V_η is automorphic. Apply [14, Theorem 5.2] as follows, changing the coefficient prime after each row:

Automorphic	Prime	Target	Residual input
V_η	p	V_χ	$(m, \ell) = (3, p)$
V_χ	3	V_ψ	$(m, \ell) = (p, 3)$
V_ψ	p	V_1	(13)

Thus $V_1 = H^1(B_t)|_{G_F}$ is automorphic. Descending along F/K (Lemma 5.1) and twisting back gives modularity of E/K .

Remark 4.2. We do not claim $\zeta_5 \notin F$. For example, $K = \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}, i)$ is CM and does not contain ζ_5 , but $K(\zeta_3) = \mathbb{Q}(\zeta_{60})$ does. This is why A_t is made modular over K before base change, and why the ramification argument of [35, (5.2)] is not used. The later lifts are at 3 and p , so the exceptional case at 5 does not arise. For CM fields containing ζ_5 we have no seed.

5 Descent and local–global compatibility

Lemma 5.1. *Let F/K be an abelian extension of totally real fields or of CM fields, and r a rank-two representation of G_K with $r|_{G_F}$ absolutely irreducible and automorphic. Then r is automorphic.*

This is standard: descend one cyclic step at a time by solvable base change [3, Chapter 3, Theorems 4.2(d) and 5.1], and adjust by a character using Schur’s lemma.

For non-CM E , the resulting π_E realizes $H^1(E)$ at every coefficient prime, with the expected local parameters at finite places by local–global compatibility (over CM fields, [14, Lemma 6.1.3]); in particular $L(E/K, s) = L(\pi_E, s - 1/2)$.

If E has CM by an imaginary quadratic field T , then $H^1(E)|_{G_{KT}}$ is a sum of two Hecke-character systems; use automorphic induction if $T \not\subset K$ (always the case for totally real K), and the isobaric sum if $T \subset K$.

5.1 Source and status

We use [35] at commit `adc7f12`. The new arguments here are the reflection twist, the d -conjugate specialization with (13), the order of seed modularity and base change in the CM case, and the two applications of existing lifting theorems. The geometric inputs are taken from [35], and Theorem 1.1 is stated conditionally on them. The construction uses special features of elliptic curves: the group law gives the two-branch-point cover, every character space has rank two, the order-three quotient is an elliptic curve, and one integral lattice gives congruences at several primes.

References

- [1] P. B. Allen, F. Calegari, A. Caraiani, T. Gee, D. Helm, B. V. Le Hung, J. Newton, P. Scholze, R. Taylor, and J. A. Thorne, *Potential automorphy over CM fields*, Ann. of Math. (2) **197** (2023), 897–1113.

- [2] P. B. Allen, C. Khare, and J. A. Thorne, *Modularity of $\mathrm{GL}_2(\mathbb{F}_p)$ -representations over CM fields*, Camb. J. Math. **11** (2023), 1–158.
- [3] J. Arthur and L. Clozel, *Simple algebras, base change, and the advanced theory of the trace formula*, Annals of Mathematics Studies **120**, Princeton University Press, 1989.
- [4] T. Barnet-Lamb, T. Gee, and D. Geraghty, *Congruences between Hilbert modular forms: constructing ordinary lifts*, Duke Math. J. **161** (2012), 1521–1580.
- [5] T. Barnet-Lamb, T. Gee, and D. Geraghty, *Congruences between Hilbert modular forms: constructing ordinary lifts, II*, Math. Res. Lett. **20** (2013), 67–72.
- [6] T. Berger and G. Harcos, *ℓ -adic representations associated to modular forms over imaginary quadratic fields*, Int. Math. Res. Not. IMRN (2007), no. 23, Art. ID rnm113.
- [7] D. Blasius and J. D. Rogawski, *Motives for Hilbert modular forms*, Invent. Math. **114** (1993), 55–87.
- [8] J. Box, *Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular*, Trans. Amer. Math. Soc. **375** (2022), 3129–3172.
- [9] G. Boxer, F. Calegari, T. Gee, and V. Pilloni, *Abelian surfaces over totally real fields are potentially modular*, Publ. Math. Inst. Hautes Études Sci. **134** (2021), 153–501.
- [10] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.
- [11] C. Breuil and F. Diamond, *Formes modulaires de Hilbert modulo p et valeurs d’extensions entre caractères galoisiens*, Ann. Sci. Éc. Norm. Supér. (4) **47** (2014), 905–974.
- [12] F. Calegari and D. Geraghty, *Modularity lifting beyond the Taylor–Wiles method*, Invent. Math. **211** (2018), 297–433; Correction, Invent. Math. **227** (2022), 855–856.
- [13] CaptainSude, *Every elliptic curve over a CM number field is modular*, manuscript, v1.0.0, October 7, 2026, github.com/CaptainSude.
- [14] A. Caraiani and J. Newton, *On the modularity of elliptic curves over imaginary quadratic fields*, [arXiv:2301.10509v3](https://arxiv.org/abs/2301.10509v3) (2025).
- [15] H. Carayol, *Sur les représentations ℓ -adiques associées aux formes modulaires de Hilbert*, Ann. Sci. Éc. Norm. Supér. (4) **19** (1986), 409–468.
- [16] B. Conrad, F. Diamond, and R. Taylor, *Modularity of certain potentially Barsotti–Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), 521–567.
- [17] H. Darmon, *Modularity of fibres in rigid local systems*, Ann. of Math. (2) **149** (1999), 1079–1086.
- [18] H. Darmon, *Rigid local systems, Hilbert modular forms, and Fermat’s last theorem*, Duke Math. J. **102** (2000), 413–449.
- [19] H. Darmon and J.-F. Mestre, *Courbes hyperelliptiques à multiplications réelles et une construction de Shih*, Canad. Math. Bull. **43** (2000), 304–311.
- [20] M. Derickx, F. Najman, and S. Siksek, *Elliptic curves over totally real cubic fields are modular*, Algebra Number Theory **14** (2020), 1791–1800.

- [21] F. Diamond, *On deformation rings and Hecke rings*, Ann. of Math. (2) **144** (1996), 137–166.
- [22] J. S. Ellenberg, *Endomorphism algebras of Jacobians*, Adv. Math. **162** (2001), 243–271.
- [23] N. Freitas, B. V. Le Hung, and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), 159–206.
- [24] G. Frey, *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Sarav. Ser. Math. **1** (1986), no. 1, iv+40 pp.
- [25] T. Gee, *Automorphic lifts of prescribed types*, Math. Ann. **350** (2011), 107–144.
- [26] M. Harris, K.-W. Lan, R. Taylor, and J. Thorne, *On the rigid cohomology of certain Shimura varieties*, Res. Math. Sci. **3** (2016), Paper No. 37.
- [27] M. Harris, D. Soudry, and R. Taylor, *ℓ -adic representations associated to modular forms over imaginary quadratic fields. I. Lifting to $\mathrm{GSp}_4(\mathbb{Q})$* , Invent. Math. **112** (1993), 377–411.
- [28] Y. Ishitsuka, T. Ito, and S. Yoshikawa, *The modularity of elliptic curves over all but finitely many totally real fields of degree 5*, Res. Number Theory **8** (2022), Paper No. 82.
- [29] S. Kalyanswamy, *Remarks on automorphy of residually dihedral representations*, Math. Res. Lett. **25** (2018), 1285–1304.
- [30] M. Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), 1085–1180.
- [31] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.
- [32] R. P. Langlands, *Problems in the theory of automorphic forms*, in: Lectures in Modern Analysis and Applications III, C. T. Taam (ed.), Lecture Notes in Math. **170**, Springer, 1970, 18–61.
- [33] B. V. Le Hung, *Modularity of some elliptic curves over totally real fields*, preprint, 2013, [arXiv:1309.4134](https://arxiv.org/abs/1309.4134).
- [34] J.-F. Mestre, *Familles de courbes hyperelliptiques à multiplications réelles*, in: Arithmetic Algebraic Geometry (Texel, 1989), G. van der Geer, F. Oort, and J. Steenbrink (eds.), Progr. Math. **89**, Birkhäuser, Boston, 1991, 193–208.
- [35] OpenAI, *Modularity of elliptic curves over imaginary quadratic fields*, manuscript, October 4, 2026, github.com/openai/math.
- [36] K. A. Ribet, *On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*, Invent. Math. **100** (1990), 431–476.
- [37] P. Scholze, *On torsion in the cohomology of locally symmetric varieties*, Ann. of Math. (2) **182** (2015), 945–1066.
- [38] J.-P. Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
- [39] J.-P. Serre, *Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. **54** (1987), 179–230.

- [40] J.-P. Serre, *Topics in Galois theory*, Research Notes in Mathematics **1**, 2nd ed., A K Peters, 2008.
- [41] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan **11**, Iwanami Shoten and Princeton University Press, 1971.
- [42] A. Snowden, *On two dimensional weight two odd representations of totally real fields*, preprint, 2009, [arXiv:0905.4266](https://arxiv.org/abs/0905.4266).
- [43] W. Tautz, J. Top, and A. Verberkmoes, *Explicit hyperelliptic curves with real multiplication and permutation polynomials*, Canad. J. Math. **43** (1991), 1055–1064.
- [44] R. Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), 265–280.
- [45] R. Taylor, *ℓ -adic representations associated to modular forms over imaginary quadratic fields. II*, Invent. Math. **116** (1994), 619–643.
- [46] R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu **1** (2002), 125–143.
- [47] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), 553–572.
- [48] J. A. Thorne, *Automorphy of some residually dihedral Galois representations*, Math. Ann. **364** (2016), 589–648.
- [49] J. A. Thorne, *Elliptic curves over $\mathbb{Q}_\infty$ are modular*, J. Eur. Math. Soc. (JEMS) **21** (2019), 1943–1948.
- [50] I. Varma, *Local-global compatibility for regular algebraic cuspidal automorphic representations when $\ell \neq p$* , Forum Math. Sigma **12** (2024), Paper No. e21.
- [51] A. Wiles, *On ordinary λ -adic representations associated to modular forms*, Invent. Math. **94** (1988), 529–573.
- [52] A. Wiles, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) **141** (1995), 443–551.
- [53] J.-P. Wintenberger, Appendix to: J. Nekovář, *On the parity of ranks of Selmer groups. IV*, Compos. Math. **145** (2009), 1351–1359.
- [54] S. Yoshikawa, *Modularity of elliptic curves over abelian totally real fields unramified at 3, 5, and 7*, J. Théor. Nombres Bordeaux **30** (2018), 729–741.