博士論文

論文題目　On modularity of elliptic curves over abelian totally real fields

(総実アーベル拡大体上の楕円曲線の保型性について)

氏　　名　吉川　祥

ON MODULARITY OF ELLIPTIC CURVES OVER ABELIAN TOTALLY REAL FIELDS

SHO YOSHIKAWA

ABSTRACT. In this thesis, we give two sufficient conditions on totally real fields so that every elliptic curve over the field is modular. The first condition is for a composite field of real quadratic fields, and the second one is that the base field is abelian over the rationals and unramified at 3, 5, and 7.

1. INTRODUCTION

Let E be an elliptic curve over a totally real field K. We say that E is modular if there exists a Hilbert cuspidal eigenform f over K of parallel weight 2 such that $L(E, s) = L(f, s)$. The classical Shimura-Taniyama conjecture asserts that all elliptic curves over $\mathbb{Q}$ are modular. The case for semistable elliptic curves, which was the crucial step in proving the Fermat's Last Theorem, was proved by Wiles [23] and Taylor-Wiles [20]. Later, the general case of the conjecture was completed by Breuil-Conrad-Diamond-Taylor [2].

The Shimura-Taniyama conjecture has a natural generalization to totally real fields:

Conjecture 1.1. *Let K be a totally real number field. Then, any elliptic curve over K is modular.*

A number of developments of modularity lifting theorems enable us to prove that elliptic curves with certain conditions are modular. Also, it is known that all elliptic curves over any totally real fields are potentially modular, in the sense that they become modular after a suitable totally real base change. This essentially follows from Taylor's potential automorphy argument in [19]. (The detailed proof is given in the appendix of [12], and a survey on potential modularity of elliptic curves is found in [3].) However, it has been difficult to prove the modularity of all elliptic curves over a fixed field. Recently, a breakthrough on Conjecture 1.1 was brought by Freitas-Le Hung-Siksek.

Theorem 1.2. *(*[6, Theorem 1]*) Let K be a real quadratic number field. Then, any elliptic curve over K is modular.*

Also, using the results in [21] and in Iwasawa theory for elliptic curves, Thorne recently proved the following theorem:

Theorem 1.3. *(*[22, Theorem 1]*) Let p be a prime number and K be a totally real field contained in a $\mathbb{Z}_p$-cyclotomic extension of $\mathbb{Q}$. Then, any elliptic curve over K is modular.*

The aim of this thesis is to attack Conjecture 1.1 for some abelian totally real fields. We give two results on this conjecture; the first result is concerned with some composite fields of real quadratic fields, and the second one treats abelian totally real fields unramified at 3,5, and 7.

Before stating the first result, we give the notations which we will use in the statement. For an elliptic curve X over a field F, a Galois extension K/F, and a character $s\colon \mathrm{Gal}(K/F) \to \{\pm 1\}$, we write $X^{(s)}$ for the quadratic twist of X by s. Also, we note that the modular curve $X_0(15)$ (resp. $X_0(21)$) is an elliptic curve of rank 0 with Cremona label 15A1 (resp. 21A1); for example, see [6] (Magma scripts are available at http://arxiv.org/abs/1310.7088). Let us now state our first main theorem.

Theorem 1.4. *Let $p = 5$ or 7, and X be the modular curve $X_0(3p)$. Let K be a composite field of finite number of real quadratic fields. We assume that K is unramified at every prime dividing 2, 3, or p. We furthermore assume that, for each character $s\colon \mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\}$, the group $X^{(s)}(\mathbb{Q})$ is finite. Then, any elliptic curve over K is modular.*

For example, using the database LMFDB (at http://www.lmfdb.org/), one can check that $K = \mathbb{Q}(\sqrt{5}, \sqrt{17})$ satisfies the hypotheses of Theorem 1.4. Contrary to the case of cyclic field extensions as considered in Theorem 1.3, we consider certain extensions which are far from cyclic ones.

Our second main theorem is the following.

Theorem 1.5. *Let K be a totally real number field which is abelian over $\mathbb{Q}$. Suppose that K is unramified at every prime above 3,5, and 7. Then, any elliptic curve over K is modular.*

In the rest of this introduction, let us describe the logical structure and the organization of this thesis.

For our proof of Theorem 1.4 and Theorem 1.5, the following results will be a crucial step.

Theorem 1.6. *Let K be a totally real field in which 7 is unramified. If E is an elliptic curve over K with $\bar{\rho}_{E,7}\colon G_K = \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbb{F}_7)$ (absolutely) irreducible, then E is modular.*

Here, $\bar{\rho}_{E,p}$ denotes the mod p Galois representation defined by the p-torsion points of E. Note that, for $p \neq 2$, $\bar{\rho}_{E,p}$ is irreducible if and only if $\bar{\rho}_{E,p}$ is absolutely irreducible: This fact follows from the presence of the complex conjugates in G_K. So we will omit the term "absolutely" from now on. Theorem 1.6 is seen as a mod 7 variant of the following theorem due to Thorne:

Theorem 1.7. *(*[21, Theorem 7.6]*) Let K be a totally real field with $\sqrt{5} \notin K$. If E is an elliptic curve over K with $\bar{\rho}_{E,5}$ irreducible, then E is modular.*

Section 2 and Section 3 are the preparation for proving Theorem 1.6. In fact, Proposition 3.3 in Section 3 will reduce the proof of Theorem 1.6 to applying available modularity lifting theorems. In Section 2, we compute the projective images of some local Galois representations, which will be used for proving Proposition 3.3. Then, in Section 4, we prove Theorem 1.6.

With Theorem 1.6 and Theorem 1.7 in hand, we proceed to prove our main theorems; Theorem 1.4 and Theorem 1.5.

The proof of Theorem 1.4 is given in Section 5. It is motivated from the proof of [6, Lemma 1.1] and is outlined as follows: By [6, Theorem 2], an elliptic curve which is not yet proved to be modular defines a point of a certain modular curve. The modular curve we consider is actually an elliptic curve. Thus, using quadratic twists of the curve, we are able to analyze the points which take values in a composite field of some quadratic fields. As a result, we will check that the points of the modular curve are actually rational points or a real quadratic points, both of which are known to correspond to modular elliptic curves. In Section 6, we discuss how often the hypotheses of Theorem 1.4 are expected to hold.

Remark 1.8. After the author proved Theorem 1.4, Bao Le Hung pointed out that there are infinitely many composite fields K of real quadratic fields such that any elliptic curve over K is modular. This can be shown by the iterate use of Theorem A in his thesis [11]. However, such fields are not obtained in an explicit way, due to the use of the Faltings' theorem of Mordell conjecture. On the other hand, our result Theorem 1.4 gives explicit conditions on totally real fields over which any elliptic curve is modular.

Finally, Section 7 proves Theorem 1.5. We see that, for an elliptic curve E which is not yet known to be modular, a quadratic twist of E becomes semi-stable at all primes dividing 3, in which case we already know its modularity by [5].

2. Local computations

First, we fix the notation of this section:

(1) p is a prime number.
(2) F is an absolutely unramified p-adic local field.
(3) v is the normalized p-adic discrete valuation of F.
(4) $\omega_1 \colon I \to \mu_{p-1}(\bar{F}) \to \mathbb{F}_p^\times$ denotes the fundamental character of level 1, and $\omega_2, \omega_2' \colon I \to \mu_{p^2-1}(\bar{F}) \to \mathbb{F}_{p^2}^\times$ denote the fundamental characters of level 2. Here, I is the inertia subgroup of G_F.
(5) E is an elliptic curve over F having **additive reduction**.
(6) $\bar{\rho}_{E,p} \colon G_F \to \mathrm{GL}_2(\mathbb{F}_p)$ is the mod p Galois representation attached to p-torsion points of E.

The aim of this section is to capture certain cyclic groups inside the projective images of $\bar{\rho}_{E,p}|_I$. The results obtained here will be used to prove Proposition 3.3 in the next section. In this section, we only consider elliptic curves having additive reduction. More precisely, we treat the following three cases separately; additive potential multiplicative reduction, additive potential good ordinary reduction, or additive potential good supersingular reduction. In the following subsections, we treat these three cases separately, and we heavily use the results of Kraus in [10]. We remark that, although Kraus proves his results for elliptic curves over $\mathbb{Q}_p$, the proofs also work without change for those over any absolutely unramified p-adic field.

Potential multiplicative reduction case.

Proposition 2.1. *Let $p \geq 3$ be a prime number, F an unramified extension of $\mathbb{Q}_p$, and E an elliptic curve over F with additive potential multiplicative reduction. Then, the restriction of $\bar{\rho}_{E,p}$ to the inertia subgroup I is of the form*

$$\bar{\rho}_{E,p}|_I \simeq \begin{pmatrix} \omega_1^{\frac{p+1}{2}} & * \\ 0 & \omega_1^{\frac{p-1}{2}} \end{pmatrix}. \tag{1}$$

Proof. See [10, PROPOSITION 10]. □

Since the projective image of (1) is of the form $\begin{pmatrix} \omega_1 & * \\ 0 & 1 \end{pmatrix}$, we obtain the following corollary:

Corollary 2.2. *In the setting of Proposition 2.1, the projective image $\mathbb{P}\bar{\rho}_{E,p}(G_F)$ contains a cyclic subgroup of order $p-1$.*

Potential ordinary reduction case.

Proposition 2.3. *Let $p \geq 5$ be a prime number, F an unramified extension of $\mathbb{Q}_p$, and E an elliptic curve over F with additive potential ordinary reduction. Denote Δ for a minimal discriminant of E and v for the normalized discrete valuation of F. Set $\alpha = (p-1)v(\Delta)/12$, which is an integer as noted just before 2.3.2 in* [10]. *Then, the restriction of $\bar{\rho}_{E,p}$ to the inertia subgroup I is of the form*

$$\bar{\rho}_{E,p}|_I \simeq \begin{pmatrix} \omega_1^{1-\alpha} & * \\ 0 & \omega_1^{\alpha} \end{pmatrix}. \tag{2}$$

Proof. See [10, PROPOSITION 1]. □

The projective image of (2) is of the form $\begin{pmatrix} \omega_1^{1-2\alpha} & * \\ 0 & 1 \end{pmatrix}$, and $\omega_1^{1-2\alpha}$ is a character of order $m := \frac{p-1}{(p-1,1-2\alpha)}$. Thus, the projective image $\mathbb{P}\bar{\rho}_{E,p}(G_F)$ contains a cyclic subgroup of order m. In the following, we compute the order m for certain p, which we will take as 5 or 7 in Section 3

Suppose first that p is a prime number of the form $p = 2^a + 1$ for an integer $a \geq 2$. Since $1 - 2\alpha$ is an odd integer, $1 - 2\alpha$ is prime to $p - 1 = 2^a$ so that we have $m = p - 1$. Thus, we have the following corollary.

Corollary 2.4. *Let p be a prime number of the form $p = 2^a + 1$ with $a \geq 2$ an integer, $F/\mathbb{Q}_p$ an unramified extension, and E an elliptic curve over F with additive potential good ordinary reduction. Then, the projective image $\mathbb{P}\bar{\rho}_{E,p}(G_F)$ contains a cyclic group of order $p-1$.*

Suppose next that p is a prime number of the form $p = 3 \cdot 2^a + 1$ with $a \geq 1$ an integer. Since $\alpha = (p-1)v(\Delta)/12$ is an integer, $1 - 2\alpha = 1 - 2^{a-1}v(\Delta)$ is odd. Thus, we have

$$m = \begin{cases} \frac{p-1}{3} & (v(\Delta) \equiv (-1)^{a-1} \bmod 3) \\ p-1 & (\text{otherwise}). \end{cases}$$

Therefore, we obtain the following corollary:

Corollary 2.5. *Let p be a prime number of the form $p = 3 \cdot 2^a + 1$ for an integer $a \geq 1$, $F/\mathbb{Q}_p$ an unramified extension, and E be an elliptic curve over F with additive potential good ordinary reduction. Let also Δ be a minimal discriminant of E. Then, $\mathbb{P}\bar{\rho}_{E,p}(G_F)$ contains a cyclic group of order $(p-1)/3$ or $p-1$, depending on whether $v(\Delta) \equiv (-1)^{a-1}$ mod 3 or not, respectively.*

Potential supersingular reduction case. As in the previous subsections, we begin with Kraus' result.

Proposition 2.6. *Let $p \geq 5$ be a prime number, F an unramified extension of $\mathbb{Q}_p$, and E an elliptic curve over F with additive potential supersingular reduction. We choose a minimal model*

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

of E. Also, let Δ denote a minimal discriminant of E.

(a) *If $(v(\Delta), v(A), v(B))$ is one of the triples $(2,1,1), (3,1,2), (4,2,2)$, $(8,3,4)$, $(9,3,5)$, or $(10,4,5)$, then $\bar{\rho}_{E,p}$ is wildly ramified.*

(b) *If $(v(\Delta), v(A), v(B))$ is not any of the above triples, then the restriction of $\bar{\rho}_{E,p}$ to the inertia subgroup I is given by*

$$\bar{\rho}_{E,p}|_I \otimes \mathbb{F}_{p^2} \simeq \begin{pmatrix} \omega_2^{\alpha}{\omega'_2}^{p-\alpha} & 0 \\ 0 & {\omega'_2}^{\alpha}{\omega_2}^{p-\alpha} \end{pmatrix}. \tag{3}$$

Here, $\alpha = (p+1)v(\Delta)/12$ is an integer as noted in [10, PROPOSITION 2].

Proof. The part (a) is a consequence of LEMME 2 and PROPOSITION 4 in [10]. The part (b) follows directly from PROPOSITION 2 and LEMME 2 in [10]. □

From the case (a) in the above proposition, we immediately obtain the following corollary:

Corollary 2.7. *Let the notation be as in Proposition 2.6. If the condition of (a) holds, then the projective image $\mathbb{P}\bar{\rho}_{E,p}(G_F)$ contains a p-group.*

Next, we consider the case (b) in the Proposition 2.6. The image of (3) in $\mathrm{PGL}_2(\mathbb{F}_{p^2})$ is of the form $\begin{pmatrix} \omega_2^{-(p-1)(2\alpha+1)} & 0 \\ 0 & 1 \end{pmatrix}$. Since the character $\omega_2^{-(p-1)(2\alpha+1)}$ is of order $n := \frac{p+1}{(p+1,2\alpha+1)}$, the projective image $\mathbb{P}(\bar{\rho}_{E,p} \otimes \mathbb{F}_{p^2})(G_F)$ (and hence $\mathbb{P}(\bar{\rho}_{E,p})(G_F)$) contains a cyclic subgroup of order n. In the rest of this subsection, we make computations of the number n for certain p. We will apply them to the case $p = 5$ or 7 in Section 3.

Suppose first that p is a prime number of the form $p = 2^a - 1$ with $a \geq 3$ an integer. Since α is an integer, $2\alpha + 1$ is prime to $p + 1 = 2^a$ so that $n = p + 1$. Thus, we have proved the following corollary:

Corollary 2.8. *Let p be a prime number of the form $p = 2^a - 1$ with $a \geq 3$ an integer, $F/\mathbb{Q}_p$ an unramified extension, and E an elliptic curve over F with additive potential good supersingular reduction. Assume the condition of (b) in Proposition 2.6 holds. Then, the projective image $\mathbb{P}\bar{\rho}_{E,p}(G_F)$ contains a cyclic group of order $p + 1$.*

Suppose next that p is a prime number of the form $p = 3 \cdot 2^a - 1$ with $a \geq 1$ an integer. Since $\alpha = (p + 1)v(\Delta)/12$ is an integer, $2\alpha + 1 = 2^{a-1}v(\Delta) + 1$ is odd. Thus, we have

$$n = \begin{cases} \frac{p+1}{3} & (v(\Delta) \equiv (-1)^a \bmod 3) \\ p+1 & (\text{otherwise}). \end{cases}$$

Therefore, we obtain the following corollary:

Corollary 2.9. *Let p be a prime number of the form $p = 3 \cdot 2^a - 1$ with $a \geq 1$ an integer, $F/\mathbb{Q}_p$ an unramified extension, and E an elliptic curve over F with additive potential good supersingular reduction. Let also Δ be a minimal discriminant of E. Assume the condition of (b) in Proposition 2.6 holds. Then, $\mathbb{P}\bar{\rho}_{E,p}(G_F)$ contains a cyclic group of order $(p + 1)/3$ or $p + 1$, depending on whether $v(\Delta) \equiv (-1)^a$ mod 3 or not, respectively.*

3. Irreducibility of mod 5 or 7 representations

As we will see in the next section (Theorem 4.1), for an elliptic curve E over a totally real field K, it is an important condition that $\bar{\rho}_{E,p}|_{G_{K(\zeta_p)}}$ is absolutely irreducible. So, it is natural to ask when such irreducibility holds. The following result will be useful for deducing absolute irreducibility of $\bar{\rho}_{E,p}|_{G_{K(\zeta_p)}}$ from irreducibility of $\bar{\rho}_{E,p}$.

Theorem 3.1. *([6, Proposition 9.1]) Let $p = 5$ or 7, and K be a totally real field satisfying $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$. For an elliptic curve E over K such that $\bar{\rho}_{E,p}$ is irreducible but $\bar{\rho}_{E,p}|_{G_{K(\zeta_p)}}$ is absolutely reducible, we have the following:*

1. *If $p = 5$, then $\bar{\rho}_{E,5}(G_K)$ is a group of order 16, and its projective image $\mathbb{P}\bar{\rho}_{E,5}(G_K)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.*
2. *If $p = 7$, then $\mathbb{P}\bar{\rho}_{E,7}(G_K)$ is isomorphic to S_3 or D_4.*

Using this theorem, Freitas-Le Hung-Siksek obtain the following result.

Proposition 3.2. [6, Theorem 7] *Let $p = 5$ or 7. Let K be a totally real field having some unramified prime $\mathfrak{p}$ above p. Let E be an elliptic curve semistable at $\mathfrak{p}$ and suppose that $\bar{\rho}_{E,p}$ is irreducible. Then, $\bar{\rho}_{E,p}|_{G(K(\zeta_p))}$ is absolutely irreducible.*

In this section, we give a result complement to Proposition 3.2; that is, we prove a similar proposition for elliptic curves with additive reduction at a prime dividing $p = 5$ or 7, instead of semi-stable reduction. More precisely, we have the following Proposition.

Proposition 3.3. *Let $p = 5$ or 7. Let K be a totally real field, $\mathfrak{p}$ a prime of K dividing p, and $v_{\mathfrak{p}}$ the normalized discrete valuation of K at $\mathfrak{p}$. Also, let E be an elliptic curve over K. Assume that K is unramified at $\mathfrak{p}$, that the j-invariant j_E of E is nonzero, and that E has additive reduction at $\mathfrak{p}$ with $\bar{\rho}_{E,p}$ irreducible. Then, $\bar{\rho}_{E,p}|_{G(K(\zeta_p))}$ is absolutely irreducible, unless either of the following exceptional cases holds:*

1. *$p = 5$, $v_{\mathfrak{p}}(j_E) \equiv 1 \bmod 3$, and E has additive potential good (supersingular) reduction at $\mathfrak{p}$, or*
2. *$p = 7$, $v_{\mathfrak{p}}(j_E) \equiv 2 \bmod 3$, and E has additive potential good (ordinary) reduction at $\mathfrak{p}$.*

The basic strategy for the proof of Proposition 3.3 is the same as Proposition 3.2, but because we treat the cases of additive reduction, we need to look at local mod p Galois representations more carefully. Since all the local computations we need has been carried out in the previous section, it is now easy to deduce Proposition 3.3.

Proof. Denote by Δ a minimal discriminant of $E_{\mathfrak{p}} := E \otimes_K K_{\mathfrak{p}}$. We split the proof into three cases according to reduction of E:

(i) If E has additive potential multiplicative reduction at $\mathfrak{p}$, then Corollary 2.2 for $E_{\mathfrak{p}}$ implies that $\mathbb{P}\bar{\rho}_{E,p}(G_K)$ has a cyclic subgroup of order $p-1$. Thus, Theorem 3.1 implies that $\bar{\rho}_{E,p}|_{G_{K(\zeta_p)}}$ cannot be absolutely reducible.

(ii) Suppose next that E has additive potential good ordinary reduction at $\mathfrak{p}$.

If $p = 5$, then Corollary 2.4 for $E_{\mathfrak{p}}$ shows that $\mathbb{P}\bar{\rho}_{E,5}(G_K)$ contains a cyclic subgroup of order 4. Thus, by Theorem 3.1 (1), $\bar{\rho}_{E,5}|_{G_{K(\zeta_5)}}$ is absolutely irreducible.

Also, if $p = 7$ and $v(\Delta) \equiv 0, 2 \bmod 3$, then Corollary 2.5 shows that $\mathbb{P}\bar{\rho}_{E,7}(G_K)$ has a cyclic subgroup of order 6. Hence, Theorem 3.1 (2) implies that $\bar{\rho}_{E,7}|_{G_{K(\zeta_7)}}$ is absolutely irreducible.

We consider the remaining case; that is, $p = 7$ and $v_{\mathfrak{p}}(\Delta) \equiv 1$. These cases are equivalent to the case $v_{\mathfrak{p}}(j_E) \equiv 2$ modulo 3; in fact, this follows by taking a minimal model $y^2 = x^3 + Ax + B$ of $E_{\mathfrak{p}}$ and noting that $j_E = 1728A^3/\Delta$.

(iii) Finally, suppose that E has additive potential good supersingular reduction at $\mathfrak{p}$.

If the condition (a) in Proposition 2.6 holds, then Corollary 2.7 and Theorem 3.1 show that $\bar{\rho}_{E,p}|_{G_{K(\zeta_p)}}$ is absolutely irreducible.

Assume the condition (b) in Proposition 2.6 holds. Then we have the following two cases:

- If $p = 5$ and $v(\Delta) \equiv 0, 1 \bmod 3$, then $\mathbb{P}\bar{\rho}_{E,5}(G_K)$ contains a cyclic subgroup of order 6 by Corollary 2.9. Hence, Theorem 3.1 (1) shows that $\bar{\rho}_{E,5}|_{G_{K(\zeta_5)}}$ is absolutely irreducible. The remaining case when $p = 5$ and $v_{\mathfrak{p}}(\Delta) \equiv 2$ mod 3 can be rephrased as $v_{\mathfrak{p}}(j_E) \equiv 1$ modulo 3.

- If $p = 7$, then $\bar{\rho}_{E,7}|_{G_{K(\zeta_7)}}$ is absolutely irreducible by Corollary 2.8 with Theorem 3.1 (2).

In summary, combining (i), (ii), and (iii), we have seen that $\bar{\rho}_{E,p}|_{G_{K(\zeta_p)}}$ is absolutely irreducible unless the following conditions hold:

(1) $p = 5$, $v_{\mathfrak{p}}(j_E) \equiv 1 \bmod 3$, and E has additive potential good (supersingular) reduction at $\mathfrak{p}$, or

(2) $p = 7$, $v_{\mathfrak{p}}(j_E) \equiv 2 \bmod 3$, and E has additive potential good (ordinary) reduction at $\mathfrak{p}$.

This shows Proposition 3.3. □

4. Proof of Theorem 1.6

To prove Theorem 1.6, we first need the following modularity theorem for elliptic curves, which is deduced from deep modularity lifting theorems due to many people. Note that we do not have to care about residual modularity, thanks to the theorem of Langlands-Tunnell and the modularity switching arguments.

Theorem 4.1. *(*[6, Theorem 2]*) Let E be an elliptic curve over a totally real field K. If $p = 3, 5,$ or 7, and if $\bar{\rho}_{E,p}|_{G_{K(\zeta_p)}}$ is absolutely irreducible, then E is modular.*

We also employ another modularity lifting theorem for residually dihedral representations due to Skinner-Wiles. Since there is a mistake in the original paper [18], we will state the modified version as corrected in [16, Theorem 1].

As [16] has not been published, we begin with introducing some notation and terminology from *loc.cit.*

First, let p be a prime number, K a totally real field, and $\bar{\rho}\colon G_K \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ a 2-dimensional mod p Galois representation such that

$$\bar{\rho}|_{D_{\mathfrak{p}}} \simeq \begin{pmatrix} \bar{\chi}_1^{(\mathfrak{p})} & * \\ 0 & \bar{\chi}_2^{(\mathfrak{p})} \end{pmatrix}$$

for each $\mathfrak{p}|p$. We say that $\bar{\rho}$ is $D_{\mathfrak{p}}$-distinguished if $\bar{\chi}_1^{(\mathfrak{p})} \neq \bar{\chi}_2^{(\mathfrak{p})}$, in which case we fix the ordering of $\bar{\chi}_1^{(\mathfrak{p})}$ and $\bar{\chi}_2^{(\mathfrak{p})}$. Write $\bar{\chi}_2 = (\bar{\chi}_2^{(\mathfrak{p})})_{\mathfrak{p}|p}$. We say that a lift $\rho'\colon G_K \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$ of $\bar{\rho}$ is a $\bar{\chi}_2$-good lift of $\bar{\rho}$, if for each $\mathfrak{p}|p$,

$$\rho'|_{D_{\mathfrak{p}}} \simeq \begin{pmatrix} \chi_1^{(\mathfrak{p})} & * \\ 0 & \chi_2^{(\mathfrak{p})} \end{pmatrix}$$

and the reduction of $\chi_2^{(\mathfrak{p})}$ is $\bar{\chi}_2^{(\mathfrak{p})}$.

Next, let $\rho\colon G_K \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$ be a 2-dimensional p-adic Galois representation. Fix an isomorphism $\mathbb{C} \simeq \bar{\mathbb{Q}}_p$ and consider the following properties of ρ:

(i) ρ is continuous and irreducible,

(ii) ρ is unramified at all finite places outside of some finite set Σ,

(iii) $\det \rho(\tau) = -1$ for all complex conjugations τ,

(iv) $\det \rho = \psi \chi_p^{w-1}$ for some integer $w \geq 2$ and $\psi_2^{(\mathfrak{p})}|_{I_{\mathfrak{p}}}$ has finite order, where χ_p is the p-adic cyclotomic character, and

(v) for each prime $\mathfrak{p}|p$ of K

$$\rho|_{D_{\mathfrak{p}}} \simeq \begin{pmatrix} \psi_1^{(\mathfrak{p})} & * \\ 0 & \psi_2^{(\mathfrak{p})} \end{pmatrix}.$$

Here, the condition (iv) can be generalized to treat the case of non-parallel weights, but for our purpose it suffices to consider (iv) in the above form; indeed, when ρ arises from an elliptic curve, ψ is trivial and $w = 2$.

Now we state the Skinner-Wiles' modularity lifting theorem:

Theorem 4.2. *([16, Theorem 1]) Suppose that $\rho\colon G_K \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$ satisfies (i)-(v) above. Suppose also that*

(a) *$\bar{\rho}^{ss}$ is irreducible and $D_{\mathfrak{p}}$-distinguished for all $\mathfrak{p}|p$; .*
(b) *there exists a cuspidal representation π_0 of $\mathrm{GL}_2(\mathbb{A}_K)$ such that the p-adic Galois representation ρ_{π_0} associated to π_0 is a $\bar{\chi}_2$-good lift of $\bar{\rho}^{ss}$, where$\bar{\chi}_2^{(\mathfrak{p})}$ is the reduction of $\psi_2^{\mathfrak{p}}$ for $\mathfrak{p}|p$;*
(c) *if $\bar{\rho}^{ss}|_{G_{K(\zeta_p)}}$ is reducible and the quadratic subfield K^* of $K(\zeta_p)/K$ is a CM extension, then not every prime $\mathfrak{p}|p$ of K splits in K^*.*

Then ρ is modular.

To ensure the conditions (a) and (b) in our situation, we use the following lemma.

Lemma 4.3. *Let $p > 2$ be a prime number and $\bar{\rho}\colon G_K \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ a mod p Galois representation such that*

$$\bar{\rho}|_{D_{\mathfrak{p}}} \simeq \begin{pmatrix} \bar{\chi}_1^{(\mathfrak{p})} & * \\ 0 & \bar{\chi}_2^{(\mathfrak{p})} \end{pmatrix}$$

for each $\mathfrak{p}|p$. Assume that $\bar{\rho}$ is irreducible and $\bar{\rho}|_{G(K(\zeta_p))}$ is reducible.

(1) *If K is unramified at p, then $\bar{\rho}$ is $D_{\mathfrak{p}}$-distinguished for every $\mathfrak{p}|p$.*
(2) *([1, Lemma 5.1.2]) There exists a regular cuspidal automorphic representation π_0 which gives a $\bar{\chi}_2$-good lift of $\bar{\rho}$.*

Proof. Since $\bar{\rho}$ is irreducible and $\bar{\rho}|_{G(K(\zeta_p))}$ is reducible, we obtain $\bar{\rho} = \mathrm{Ind}_{G_L}^{G_K}\bar{\chi}$, where L is the quadratic subextension of $K(\zeta_p)/K$ and $\bar{\chi}\colon G_L \to \bar{\mathbb{F}}_p^{\times}$ is a character.

(1) Let $\mathfrak{p}$ be any prime of K dividing p. Set $D = D_{\mathfrak{p}}$ and $D' = D \cap G_L$. We have $D \neq D'$ because K is unramified at p, and so $\bar{\rho}|_D = \mathrm{Ind}_{D'}^{D}\bar{\chi}|_{D'}$. Since $\bar{\rho}|_{D'}$ contains $\bar{\chi}|_{D'}$ and $\bar{\rho}|_D$ is reducible as in the assumption, $\bar{\chi}|_{D'}$ is extended to $\bar{\chi}' = \bar{\chi}_i^{(\mathfrak{p})}$ for $i = 1$ or 2. Hence we obtain $\bar{\rho}|_D = \bar{\chi}' \oplus \bar{\chi}'\epsilon$, where $\epsilon\colon D \to D/D' \simeq \{\pm 1\}$ is the canonical quadratic character. This shows (1).

(2) Twisting $\bar{\rho}$ by a character if necessary, we may assume that $\bar{\chi}_2^{(\mathfrak{p})}$ is unramified for every $\mathfrak{p}|p$, and we will construct an ordinary $\bar{\chi}_2$-good lift of $\bar{\rho}$.

Let $\chi\colon G_L \to \bar{\mathbb{Q}}_p^{\times}$ denote the Teichmuller lift of $\bar{\chi}$, and set $\rho_1 := \mathrm{Ind}_{G_L}^{G_K}\chi$. Then ρ_1 is a lift of $\bar{\rho}$ with finite image.

We claim that ρ_1 is ordinary. Let $\mathfrak{p}$, D, and D' be as above. If $D = D'$, then $\rho_1|_D = \chi|_D \oplus \chi'|_D$ with χ' the conjugate character of χ by the generator of $\mathrm{Gal}(L/K)$. Suppose that $D \neq D'$. Then we have $\rho_1|_D = \mathrm{Ind}_{D'}^{D}\chi|_{D'}$. A similar argument to (1) shows that $\chi|_{D'}$ is extended to a character $\chi'\colon D \to \bar{\mathbb{Q}}_p^{\times}$; that is, the Teichmuller lift of $\bar{\chi}_i^{(\mathfrak{p})}$ for $i = 1$ or 2. This implies that $\mathrm{Ind}_{D'}^{D}\chi|_{D'} = \chi' \oplus \chi'\epsilon$. In both cases $D = D'$ and $D \neq D'$, the characters appearing in $\rho_1|_D$ have order prime to p, and thus they are the Teichmuller lifts of $\bar{\chi}_1^{(\mathfrak{p})}$ and $\bar{\chi}_2^{(\mathfrak{p})}$. This implies that ρ_1 is ordinary at $\mathfrak{p}$.

Since ρ_1 is an induction from a character (of finite order), a classical construction due to Hecke (for example, see [8, Theorem 7.11]) shows that ρ_1 is modular of parallel weight 1. Let f_1 be the corresponding (ordinary) Hilbert modular form of parallel weight 1. Then, a theorem of Wiles [24, Theorem 3] implies that, after replacing f_1 by its v-stabilization for each v, we can realize f_1 as a member of an ordinary p-adic analytic family. Specializing it at any weight $k \geq 2$ produces a desired automorphic lift, which proves (2). □

With the above preparations in hand, we are now ready to prove Theorem 1.6.

Proof of Theorem 1.6. Let K and E be as in Theorem 1.6. If E has semi-stable reduction at some prime dividing 7, then the assertion follows from [6, Theorem 7].

So suppose that E has additive reduction at every prime $\mathfrak{p}|7$. If $j_E = 0$, then E has complex multiplication. Thus, the Tate module of E is induced from a character, which proves that E is modular by class field theory and the automorphic induction. So we may moreover assume that $j_E \neq 0$. By Proposition 3.3 and Theorem 4.1, we have only to consider the case when E has potential good ordinary reduction at every prime $\mathfrak{p}|7$ and $\bar{\rho}_{E,7}|_{G(K(\zeta_7))}$ is absolutely reducible. In this case, we will apply Theorem 4.2 in order to prove the modularity of E.

In the following, we check that our $\rho_{E,7}\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_7)$ satisfies (i)-(v) and (a)-(c) in Theorem 4.2. First, the conditions (i)-(iv) are immediate. Also, $\rho_{E,7}$ satisfies (v) because we now assume that E has potential good ordinary reduction at every $\mathfrak{p}|7$. As K is unramified at 7, Lemma 4.3 (1) for $\bar{\rho}_{E,7}$ implies (a). Also (b) follows from Lemma 4.3 (2) for $\bar{\rho}_{E,7}$. Finally, the condition (c) is automatic under our assumption that K is unramified at 7. Therefore, Theorem 4.2 shows that E is modular. □

Remark 4.4. A similar argument does not reprove Theorem 1.7 even if K is just unramified at 5; in fact, Proposition 3.3 implies that an elliptic curve E over K with $\bar{\rho}_{E,5}|_{G(K(\zeta_5))}$ absolutely reducible must have additive potential supersingular reduction at every prime $\mathfrak{p}|5$. In such a case, the theorem of Skinner-Wiles [18] is unavailable.

Remark 4.5. In his thesis [11], Le Hung essentially shows the following; if K is a totally real field unramified at 5 and 7, and if E is an elliptic curve over K with both $\bar{\rho}_{E,p}$ $(p = 5, 7)$ irreducible, then E is modular. This follows from [11, Proposition 6.1] combined with the modularity lifting theorem due to Skinner-Wiles [18].

Remark 4.6. Very recently, S. Kalyanswamy [9] announced to prove a version of Theorem 1.6. He actually proves a new modularity theorem [9, Theorem 3.4] for certain Galois representations, and applies it to elliptic curves in [9, Theorem 4.4]. For clarity, we describe the difference between Theorem 1.6 and [9, Theorem 4.4]: Kalyanswamy considers elliptic curves over a totally real field F with $F \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$, which is weaker than the assumption that F is unramified at 7, while he also imposes an additional condition on the mod 7 Galois representations. Therefore, both Theorem 1.6 and [9, Theorem 4.4] have their own advantage.

5. Proof of the first main theorem: Theorem 1.4

For a group G, a $\mathbb{Z}[G]$-module M, and a character $s\colon G \to \{\pm 1\}$, we write M_s for the subgroup of M defined by

$$M_s = \{m \in M; m^\sigma = s_\sigma m \text{ for all } \sigma \in G\}.$$

The following lemma immediately follows from the definition of quadratic twists.

Lemma 5.1. *Let K/F be a Galois extension. Let X be an elliptic curve over F. Then, for each character $s\colon \mathrm{Gal}(K/F) \to \{\pm 1\}$, we have*

$$X(K)_s \simeq X^{(s)}(F).$$

Proof. By the definition of quadratic twists, we have an isomorphism $f\colon X \xrightarrow{\simeq} X^{(s)}$ over K which satisfies $f(P^\sigma) = s_\sigma f(P)^\sigma$ for $P \in X(K)$ and $\sigma \in G = \mathrm{Gal}(K/F)$. By the isomorphism f, the subgroup $X(K)_s \subset X(K)$ corresponds to the subgroup $X^{(s)}(F) \subset X^{(s)}(K)$. □

For a group G isomorphic to $(\mathbb{Z}/(2))^r$ with r a positive integer, let $G^\vee$ denote the group $\mathrm{Hom}(G, \{\pm 1\})$ of characters.

Lemma 5.2. *If G is a group isomorphic to $(\mathbb{Z}/(2))^r$ for a positive integer r and M is a $\mathbb{Z}[G]$-module, then we have $2^r M \subset \sum_{s\in G^\vee} M_s$.*

Proof. This is clear by noting that, for $m \in M$, $2^r m$ is written as

$$2^r m = \sum_{s\in G^\vee} \sum_{\sigma\in G} s_\sigma m^\sigma,$$

and that the element $\sum_{\sigma\in G} s_\sigma m^\sigma$ belongs to M_s. □

Lemma 5.3. *For $X = X_0(15)$ or $X_0(21)$ and a prime number $\ell \geq 3$, the mod ℓ Galois representation $\bar{\rho}_{X,\ell}$ is surjective.*

Proof. Recall that $X_0(15)$ (resp. $X_0(21)$) is the elliptic curve with Cremona label 15A1 (resp. 21A1). The j-invariant j_X of X is given by

$$j_X = \begin{cases} 3^{-4}\cdot 5^{-4}\cdot 13^3\cdot 37^3 & (\text{if } X = X_0(15)) \\ 3^{-4}\cdot 7^{-2}\cdot 193^3 & (\text{if } X = X_0(21)). \end{cases}$$

Thus, ℓ does not divide the exponents of 3 and 5 (resp. 3 and 7) in $j_{X_0(15)}$ (resp. $j_{X_0(21)}$). Also, by hand or by looking at the coefficients of the modular form corresponding to X, it is checked that $|X_0(15)(\mathbb{F}_7)| = |X_0(21)(\mathbb{F}_5)| = 8$; in particular, these are not divisible by ℓ. Applying [13, Proposition 21] to our X and ℓ, we see that $\bar{\rho}_{X,\ell}$ is surjective. □

Using the above two basic results, we prove the following proposition.

Proposition 5.4. *Under the assumption of Theorem 1.4, we have $X(K) = X(\mathbb{Q})$.*

Proof. Let G denote the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, which is by assumption isomorphic to $(\mathbb{Z}/(2))^r$ for a positive integer r. By Lemma 5.3, $\bar{\rho}_{X,\ell}$ for every prime $\ell \geq 3$ is in particular irreducible, and thus $X^{(s)}(\mathbb{Q})$ for $s \in G^\vee$ has only 2-power torsion points. Also, for each $s \in G^\vee$, $X^{(s)}(\mathbb{Q})$ is assumed to be of rank 0, and Lemma 5.1 implies that $X(K)_s \simeq X^{(s)}(\mathbb{Q})$. It follows that all $X(K)_s$ for $s \in G^\vee$ are killed by $[2^n]\colon X \to X$ for some positive integer n. Then, since $[2^r]X(K) \subset \sum_{s\in G^\vee} X(K)_s$ by Lemma 5.2, we have $[2^{n+r}]X(K) = 0$; that is, $X(K) \subset X[2^{n+r}](\bar{\mathbb{Q}})$. This implies that the G-module $X(K)$ can be ramified only at primes dividing $6p$. On the other hand, by the assumption that K is unramified at primes dividing $6p$, it follows that $X(K)$ is unramified everywhere. Therefore, we have $X(K) = X(\mathbb{Q})$. □

Before proceeding to the proof of Theorem 1.4, we also need to introduce certain modular curves from [6, Section 3]. For a prime number $p \neq 3$, let $X(s3, bp)$ denote the modular curve classifying elliptic curves such that $\mathrm{Im}\,\bar{\rho}_{E,3}$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ and that $\bar{\rho}_{E,p}$ is reducible. For the details of such a modular curve, we refer the reader to [6]. For the proof of Theorem 1.4, we only need the following properties of $X(s3, b5)$ and $X(s3, b7)$.

Lemma 5.5. *The following are true:*

1. *The modular curve $X(s3, b5)$ is an elliptic curve over $\mathbb{Q}$ and $X(s3, b5)$ is isogeneous to $X_0(15)$ by an isogeny of degree 2.*
2. *The modular curve $X(s3, b7)$ is isomorphic to $X_0(63)/\langle w_9\rangle$, and the curve $X_0(63)/\langle w_7, w_9\rangle$ is isomorphic to $X_0(21)$, where w_7 and w_9 are the Atkin-Lehner involutions on $X_0(63)$. In particular, $X(s3, b7)$ admits a morphism to $X_0(21)$ of degree 2.*

Proof. See [22, Proposition 4] for (1), and see [6, Proof of Lemma 1.1] for (2). □

We are now ready to prove Theorem 1.4.

Proof of Theorem 1.4. Let p, $X = X_0(3p)$, and K be as in the statement of Theorem 1.4.

Suppose we are given an elliptic curve E over K. We show that E is modular. Because of Theorem 1.6 and Theorem 1.7, we only have to consider the case where $\bar{\rho}_{E,3}|_{\mathrm{Gal}(\bar{K}/K(\zeta_3))}$ is absolutely reducible and $\bar{\rho}_{E,p}$ is reducible. In such a case, E defines a K-point of X or $X(s3, bp)$ by [6, Proposition 4.1, Corollary 10.1].

Suppose first that E defines a K-point of X. Proposition 5.4 implies that the j-invariant of E is a rational number, and so there exists a solvable Galois extension of K over which E becomes isomorphic to an elliptic curve defined over $\mathbb{Q}$ (For this, see the proof of [15, III, Proposition 1.4. (b)].) Hence E is modular by [2, Theorem A] and the solvable base change theorem.

Next we consider the case where E defines a K-point $P = P_E$ of $X(s3, bp)$. By Lemma 5.5, we have a morphism $f_p \colon X(s3, bp) \to X$ of degree 2. By Proposition 5.4, $\mathrm{Gal}(K/\mathbb{Q})$ acts on the fiber $f_p^{-1}(f_p(P))$. Since $f_p^{-1}(f_p(P))$ consists of 2 points, the kernel of this action is a subgroup in $\mathrm{Gal}(K/\mathbb{Q})$ of index at most 2. It follows that P must be a rational point or a real quadratic point of X. Similarly to the previous paragraph, [2, Theorem A], [6, Theorem 1], and the base change theorem show that E is modular. This completes the proof. □

6. On the hypotheses of Theorem 1.4

Let the notation be as in Theorem 1.4. We discuss here how many totally real fields K are expected to satisfy the hypotheses of Theorem 1.4; We heuristically expect that, for each positive integer r, there are infinitely many K with $[K : \mathbb{Q}] = 2^r$ satisfying the condition of Theorem 1.4.

To explain this, we first note the following theorem on the description of local root numbers of an elliptic curve. For an elliptic curve E over a local or global field K, we write $w(E/K)$ for the root number of E.

Theorem 6.1. [4, Theorem 3.1] *Let E be an elliptic curve over a local field K_v. Then,*

(1) *$w(E/K_v) = -1$ if $v|\infty$ or E has split multiplicative reduction.*
(2) *$w(E/K_v) = 1$ if E has either good or nonsplit multiplicative reduction.*
(3) *$w(E/K_v) = (\frac{-1}{k})$ if E has additive potentially multiplicative reduction, and the residue field k of K_v has characteristic $p \geq 3$. Here, $(\frac{-1}{k}) = 1$ (resp. -1) if $-1 \in (k^\times)^2$ (resp. otherwise).*
(4) *$w(E/K_v) = (-1)^{\lfloor \mathrm{ord}_v(\Delta)|k|/12 \rfloor}$, if E has potentially good reduction, and the residue field k of K_v has characteristic $p \geq 5$. Here, Δ is the minimal discriminant of E, and $\lfloor x \rfloor$ is the greatest integer $n \leq x$.*

Using Theorem 6.1, we calculate the global root numbers of quadratic twists of an elliptic curve that we are interested in. Although such a result must be known under a more general assumption, the proof in our simpler setting should be more elementary and straightforward.

Corollary 6.2. *Let E be a semi-stable elliptic curve over $\mathbb{Q}$ with the odd conductor N, and $d \equiv 1 \bmod 4$ be a square-free positive integer prime to N. Then, we have $w(E^{(d)}/\mathbb{Q}) = \big(\frac{d}{N}\big) w(E/\mathbb{Q})$, where $E^{(d)}$ denotes the quadratic twist of E by d and $\big(\frac{\cdot}{N}\big)$ is the Jacobi symbol.*

Proof. Note that $E^{(d)}$ has the conductor d^2N because $d \equiv 1 \bmod 4$. Let p be a prime number.

- If $p \nmid dN$, then both $E^{(d)}$ and E have good reduction at p and thus $w(E/\mathbb{Q}_p) = w(E^{(d)}/\mathbb{Q}_p) = 1$ by Theorem 6.1 (2).
- If $p|d$, then $E^{(d)}$ has additive potentially good reduction at p and it acquires good reduction over the quadratic extension $\mathbb{Q}_p(\sqrt{d})$ of $\mathbb{Q}_p$. Thus, by Theorem 6.1 (4), $w(E^{(d)}/\mathbb{Q}_p) = (-1)^{\lfloor p/2 \rfloor}$, which is equal to 1 (resp. -1) for $p \equiv 1 \bmod 4$ (resp. $p \equiv 3 \bmod 4$).
- Suppose here that $p|N$. Thus, E and $E^{(d)}$ have multiplicative reduction at p. Take a minimal Weierstrass equation
$$y^2 = f(x)$$
of E over $\mathbb{Q}_p$, where $f(x) \in \mathbb{Z}_p[x]$ is a monic polynomial of degree 3. Write $\mathbb{F}_p$ as the union of the subsets
$$\begin{aligned} S_0 &= \{x \in \mathbb{F}_p; f(x) = 0\} \\ S^+ &= \{x \in \mathbb{F}_p; \Big(\frac{f(x)}{p}\Big) = 1\} \\ S^- &= \{x \in \mathbb{F}_p; \Big(\frac{f(x)}{p}\Big) = -1\}. \end{aligned}$$
In particular, we have $|E(\mathbb{F}_p)| = |S_0| + 2|S^+| + 1$. Note that, for an elliptic curve X over $\mathbb{Q}_p$ with bad reduction,
$$p + 1 - |X(\mathbb{F}_p)| = \begin{cases} 0 & \text{if } X \text{ has additive reduction.} \\ 1 & \text{if } X \text{ has split multiplicative reduction.} \\ -1 & \text{if } X \text{ has non-split multiplicative reduction.} \end{cases}$$
If $\big(\frac{d}{p}\big) = 1$, then we have $|E^{(d)}(\mathbb{F}_p)| = |S_0| + 2|S^+| + 1 = |E(\mathbb{F}_p)|$, and hence E has (non-)split multiplicative reduction if and only if so does $E^{(d)}$. If $\big(\frac{d}{p}\big) = -1$, then we have $|E^{(d)}(\mathbb{F}_p)| = |S_0| + 2|S^-| + 1 = 2p + 2 - |E(\mathbb{F}_p)|$, and hence E has split (resp. non-split) multiplicative reduction if and only if $E^{(d)}$ has non-split (resp. split) multiplicative reduction. Summarizing these arguments and Theorem 6.1 (1), (2), we obtain $w(E^{(d)}/\mathbb{Q}_p) = \big(\frac{d}{p}\big) w(E/\mathbb{Q}_p)$ for every $p|N$.
- Also, $w(E/\mathbb{R}) = w(E^{(d)}/\mathbb{R}) = -1$ by Theorem 6.1 (1).

Taking the products of the local root numbers over all places of $\mathbb{Q}$, we obtain the desired formula. □

Let $r \geq 2$ be an integer and d_1,...,d_r be square-free positive integers satisfying the following conditions:

- $(d_1, ..., d_r, 3p) = 1$,
- $d_i \equiv 1 \bmod 4$ for $i = 1, ..., r$, and
- $\big(\frac{d_i}{3p}\big) = 1$ for $i = 1, ..., r$.

Here, recall that $3p$ is the conductor of X, and note that there are infinitely many choices of such r-tuples $(d_1, ..., d_r)$. The field $K := \mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_r})$ is unramified at every prime dividing $6p$. Also, Corollary 6.2 shows that $w(X^{(s)}/\mathbb{Q}) = w(X/\mathbb{Q})$ for any $s\colon \mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\}$. Since $\operatorname{rank} X = 0$, the parity conjecture for our X therefore predicts that $\operatorname{rank} X^{(s)}$ for any s is even. The Goldfeld conjecture [7] suggests that, for an elliptic curve over $\mathbb{Q}$, most of its quadratic twists of even (resp. odd) rank would be of rank 0 (resp. 1). Thus, it seems reasonable to expect that the fields $K = \mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_r})$ for most $(d_1, ..., d_r)$ satisfy the hypotheses in Theorem 1.4, although the two conjectures do *not* imply that this is actually true.

7. Proof of the second main theorem: Theorem 1.5

For the proof of Theorem 1.5, we need another modularity theorem due to Freitas [5]. This theorem essentially follows from [17], [18], and Theorem 4.1.

Theorem 7.1. [5, Theorem 6.3] *Let K be an abelian totally real field where 3 is unramified. Let E be an elliptic curve over K semistable at all primes $\mathfrak{p}|3$. Then, E is modular.*

Also, we note a well-known result on a torsion version of Neron-Ogg-Shafarevich criterion of good reduction.

Lemma 7.2. [14, Corollary 2 of Theorem 2] *Let F be a local field, E an elliptic curve over F with potential good reduction, and $m \geq 3$ an integer relatively prime to the residual characteristic of F.*

(a) *The inertia group of $F(E[m])/F$ is independent of m.*
(b) *The extension $F(E[m])/F$ is unramified if and only if E has good reduction.*

Now we are ready to prove Theorem 1.5.

Proof of Theorem 1.5. Let K be as in Theorem 1.5 and E an elliptic curve over K. Our goal is to prove that E is modular. By Theorem 1.6 and Theorem 1.7, we may assume that both $\bar{\rho}_{E,5}$ and $\bar{\rho}_{E,7}$ are reducible; that is, $\bar{\rho}_{E,p}$ for $p = 5, 7$ factors through a Borel subgroup $B(\mathbb{F}_p)$. Note that $B(\mathbb{F}_5)$ (resp. $B(\mathbb{F}_7)$) is of order $4^2 \cdot 5$ (resp. $6^2 \cdot 7$).

In this situation, we claim that a suitable quadratic twist of E becomes semi-stable at every prime $\mathfrak{p}|3$ of K. So let $\mathfrak{p}$ be a prime of K dividing 3.

If $E_{\mathfrak{p}} = E \otimes K_{\mathfrak{p}}$ is semi-stable, then its quadratic twist $E_{\mathfrak{p}}^{(a)}$ by any unit $a \in O_{K_{\mathfrak{p}}}^*$ is also semi-stable, because $E_{\mathfrak{p}}$ and $E_{\mathfrak{p}}^{(a)}$ become isomorphic over an unramified extension $K_{\mathfrak{p}}(\sqrt{a})$ of $K_{\mathfrak{p}}$.

Suppose next that $E_{\mathfrak{p}}$ has additive potential good reduction. Then, by Lemma 7.2, the actions of the inertia subgroup $I_{\mathfrak{p}} \subset G_{K_{\mathfrak{p}}}$ on $E[5]$ and $E[7]$ factor through the same nontrivial quotient $I'_{\mathfrak{p}}$. This implies that $|I'_{\mathfrak{p}}|$ divides $\gcd(4^2 \cdot 5, 6^2 \cdot 7) = 4$, and hence $I'_{\mathfrak{p}}$ is tame (and so cyclic) of order dividing 4. Since the 2-Sylow subgroups of $B(\mathbb{F}_7)$ are of order 4 and not cyclic, $I'_{\mathfrak{p}}$ must be of order 2. Because $\det \bar{\rho}_{E,p}$ is trivial on $I_{\mathfrak{p}}$ if $p \neq 3$, we see that $I'_{\mathfrak{p}}$ acts on $E[p]$ $(p = 5, 7)$ via ± 1. It follows that the quadratic twist of $E_{\mathfrak{p}}$ by any uniformizer of $K_{\mathfrak{p}}$ has good reduction by Lemma 7.2 (b).

Finally, suppose that $E_{\mathfrak{p}}$ has additive potential multiplicative reduction. In this case, using [15, C, Theorem 14.1], we see that the quadratic twist of $E_{\mathfrak{p}}$ by any uniformizer of $K_{\mathfrak{p}}$ has multiplicative reduction.

By the Chinese remainder theorem, we find an element $d \in K$ such that, for each prime $\mathfrak{p}|3$ of K,

$$v_{\mathfrak{p}}(d) = \begin{cases} 0 & (\text{if } E \text{ is semi-stable at } \mathfrak{p}) \\ 1 & (\text{if } E \text{ has additive reduction at } \mathfrak{p}). \end{cases}$$

For such a d, the above argument shows that the quadratic twist $E^{(d)}$ of E by d is semi-stable at every prime $\mathfrak{p}|3$ of K, and hence the claim follows. Now Theorem 7.1 implies that $E^{(d)}$ is modular. Since modularity of elliptic curves is invariant under quadratic twists, it follows that E is modular. □

Acknowledgements

I would like to express my deepest gratitude to my advisor Professor Takeshi Saito for a number of helpful suggestions and for his constant encouragement. Without his help, this work could not be possible. I am grateful to Professor Ken Ono for informing me of some references on the rank of quadratic twists. I also thank Bao Le Hung for answering my question about how to use Skinner-Wiles' theorem on residually irreducible representations. This work is supported by the Program for Leading Graduate Schools, MEXT, Japan.

References

[1] P. B. Allen, *Modularity of nearly ordinary 2-adic residually dihedral Galois representations*, Compositio Mathematica 150. 08 (2014), 1235-1346.

[2] C.Breuil, B.Conrad, F.Diamond, R.Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843-939.

[3] K. Buzzard, *Potential modularity - a survey*, available at https://arxiv.org/abs/1101.0097.

[4] T. Dokchitser, V. Dokchitser, *On the Birch-Swinnerton quotients modulo squares*, Annals of Mathematics **172** (2010), 567-596.

[5] N. Freitas, *Recipes for Fermat-type equation of the form $x^r + y^r = Cz^p$*, Mathematische Zeitschrift 279 (2015), no. 3-4, 605-639.

[6] N. Freitas, B. Le Hung, S. Siksek, *Elliptic Curves over Real Quadratic Fields are Modular*, Inventiones Mathematicae 201 (2015), 159-206.

[7] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Lecture Notes in Math. 751, Springer, Berlin, 1979, 108-118.

[8] S. S. Gelbart, *Automorphic forms on adele groups*, No. 83. Princeton University Press, 1975.

[9] S. Kalyanswamy, *Remarks on automorphy of residually dihedral representations*, preprint, available at https://arxiv.org/abs/1607.04750

[10] A. Kraus, *Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique*, Warszawa: Instytut Matematyczny Polskiej Akademi Nauk, 1997.

[11] B. Le Hung, *Modularity of some elliptic curves over totally real fields*, available at http://arxiv.org/abs/1309.4134.

[12] J. Nekovář, *On the parity of ranks of Selmer groups. IV*, Compos. Math. 145 (2009), no. 6, 13511359, With an appendix by Jean-Pierre Wintenberger.

[13] J. -P. Serre, *Propriétés galoisienne des points d'ordre fini des courbes elliptiques*, Inventiones mathematicae, Volume: 15 (1971/1972), 259-331.

[14] J. -P. Serre, J. Tate, *Good Reduction of Abelian Varieties*, Annals of Mathematics, Second Series, Volume 88, Issue 3 (1968), 492-517.

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer,-Verlag (1986).

[16] C. Skinner, *Nearly ordinary deformation of residually dihedral representations*, preprint.

[17] C. Skinner, A. Wiles, *Residually reducible representations and modular forms*, Publications mathématiques de l' I.H.É.S., tome 89 (1999), 5-126.

[18] C. Skinner, A. Wiles, *Nearly ordinary deformations of irreducible residual representations*, Annales de la Faculte des sciences de Toulouse : Mathematiques (2001) Volume: 10, Issue: 1, page 185-215.

[19] R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu 1 (2002), no. 1, 125143.

[20] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics **141** (1995), no. 3, 553-572.

[21] J. Thorne, *Automorphy of some residually dihedral Galois representations*, Mathematische Annalen 364 (2016), No. 1-2, pp. 589-648.

[22] J. Thorne, *Elliptic curves over $\mathbb{Q}_\infty$ are modular*, Preprint.

[23] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics **141** (1995), no. 3, 443-551.

[24] A. Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. 94 (1988), no. 3, 529-573.