JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Sho YOSHIKAWA

Modularity of elliptic curves over abelian totally real fields unramified at 3, 5, and 7

Tome 30, n° 3 (2018), p. 729-741.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_3_729_0>

Journal de Théorie des Nombres de Bordeaux **30** (2018), 729–741

Modularity of elliptic curves over abelian totally real fields unramified at 3, 5, and 7

par Sho YOSHIKAWA

Résumé. Soit K un corps totalement réel qui est une extension abélienne finie de $\mathbb{Q}$ non ramifiée en $3, 5$ et 7. Nous prouvons que toute courbe elliptique E sur K est modulaire, en réduisant la question de modularité de E aux théorèmes de relèvement modulaire connus.

Abstract. Let K be a totally real field which is a finite abelian extension over $\mathbb{Q}$ and is unramified at 3,5, and 7. We prove that any elliptic curve E over K is modular, by reducing modularity of E to known modularity lifting theorems.

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 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. This conjecture for semi-stable elliptic curves, which was the crucial step in proving Fermat's Last Theorem, was proved by Wiles [18] and Taylor–Wiles [16]. 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

Manuscrit reçu le 17 février 2017, accepté le 18 juillet 2017.

2010 *Mathematics Subject Classification.* 11F80, 11G05, 11F41.

Mots-clefs. elliptic curves, Hilbert modular forms, Galois representations.

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 also thank Bao Le Hung for answering my question about how to use Skinner–Wiles' theorem on residually irreducible representations. Finally we thank the anonymous referee for their comments to improve the manuscript. This work is supported by the Program for Leading Graduate Schools, MEXT, Japan.

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 [15]. (The detailed proof is given in the appendix of [9], 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 this problem was brought by Freitas–Le Hung–Siksek. In their paper [5], they prove Conjecture 1.1 for any quadratic field. Based on the methods and results of loc. cit., we attack Conjecture 1.1 for certain abelian totally real fields. More precisely, the main theorem is the following:

Theorem 1.2. *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, we explain the structure of the proof of Theorem 1.2.

Firstly, we prove the following proposition, which is a complementary result of [5, Theorem 7] (see Proposition 3.2); we treat elliptic curves with additive reduction at a prime dividing $p = 5$ or 7, instead of semi-stable reduction as considered in loc. cit..

Proposition 1.3. *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 $\bar{\rho}_{E,p}$ (absolutely) irreducible, with $\bar{\rho}_{E,p}$ the mod p Galois representation defined by p-torsion points of E. Then, $\bar{\rho}_{E,p}|_{G(K(\zeta_p))}$ is absolutely irreducible, unless either of the following exceptional cases holds:*

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

Remarks 1.4.

(1) Note that, for $p \neq 2$, $\bar{\rho}_{E,p}$ is irreducible if and only if $\bar{\rho}_{E,p}$ is absolutely irreducible. This follows from the presence of the complex conjugates in G_K. So, we will omit the term "absolutely" if we do not need it.
(2) The absolute irreducibility of $\bar{\rho}_{E,p}|_{G_{K(\zeta_p)}}$ in the above proposition is very important, because under this condition we may use a powerful modularity theorem for elliptic curves; for details, see Theorem 4.1.

The proof of Proposition 1.3 will be given in Section 3. The basic strategy is the same as [5, Theorem 7]; we shall sketch it very briefly. First we look closely at the projective image of $\bar{\rho}_{E,p}(I_{\mathfrak{p}})$, where $I_{\mathfrak{p}}$ is the inertia subgroup at $\mathfrak{p}$, to find a cyclic subgroup of certain order in that projective image. Then, we show that the existence of such a cyclic subgroup forces $\bar{\rho}_{E,p}|_{G(K(\zeta_p))}$ to be absolutely irreducible; to do this, we use a description [5, Proposition 9.1] (see Theorem 3.1) of the projective image of $\bar{\rho}_{E,p}$ such that $\bar{\rho}_{E,p}|_{G(K(\zeta_p))}$ is absolutely reducible.

Since we treat the cases of additive reduction, we need to look at local mod p Galois representations more carefully than [5, Theorem 7]. The local computations are carried out in Section 2. For this local arguments, we heavily use the results of Kraus [7].

Secondly, we show the following result:

Theorem 1.5. *Let K be a totally real field in which 7 is unramified. If E is an elliptic curve over K with $\bar{\rho}_{E,7}$ irreducible, then E is modular.*

Let us sketch the proof of Theorem 1.5. By Proposition 1.3 and [5, Theorem 7] together with the modularity result [5, Theorem 2], we prove modularity of many elliptic curves with irreducible mod 7 representations. In the remaining cases where neither Proposition 1.3 nor [5, Theorem 7] can be applied, we will see that we may use another modularity lifting theorem due to Skinner–Wiles [14] to prove modularity. The detailed proof of Theorem 1.5 is given in Section 4.

We remark that Theorem 1.5 is seen as a mod 7 variant of the following theorem due to Thorne.

Theorem 1.6 ([17, 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.*

Finally, in Section 5, we complete the proof of Theorem 1.2. Let K be a totally real field as in Theorem 1.2 and E be an elliptic curve over K. We want to show that E is modular. If $\bar{\rho}_{E,5}$ or $\bar{\rho}_{E,7}$ is irreducible, then modularity of E follows from Theorem 1.5 or Theorem 1.6, so that we may assume that E has reducible mod 5 and mod 7 representations. In this case, by an elementary group-theoretic argument, we show that a quadratic twist of E will be semi-stable at all primes dividing 3. Then, we can use another modularity theorem [4] due to Freitas to prove modularity of E.

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, $I = I_F$ 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 image of $\bar{\rho}_{E,p}|_I$. The results obtained here will be used to prove Proposition 1.3 in the next section. In this section, we only consider elliptic curves having additive reduction. More precisely, we consider the following three cases; additive potential multiplicative reduction, additive potential good ordinary reduction, or additive potential good supersingular reduction. In each of the following subsections, we treat these three cases separately, and we heavily use the results of Kraus in [7]. 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*

$$\bar{\rho}_{E,p}|_I \simeq \begin{pmatrix} \omega_1^{\frac{p+1}{2}} & * \\ 0 & \omega_1^{\frac{p-1}{2}} \end{pmatrix}. \tag{2.1}$$

Proof. See [7, Proposition 10]. □

Since the projective image of (2.1) is of the form $\left(\begin{smallmatrix} \omega_1 & * \\ 0 & 1 \end{smallmatrix}\right)$, 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* [7]*. Then, the restriction of $\bar{\rho}_{E,p}$ to the inertia subgroup I is of the form*

$$\bar{\rho}_{E,p}|_I \simeq \begin{pmatrix} \omega_1^{1-\alpha} & * \\ 0 & \omega_1^{\alpha} \end{pmatrix}. \tag{2.2}$$

Proof. See [7, Proposition 1]. □

The projective image of (2.2) is of the form $\left(\begin{smallmatrix}\omega_1^{1-2\alpha} & * \\ 0 & 1\end{smallmatrix}\right)$, 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.

1. *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.*
2. *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*

$$\bar{\rho}_{E,p}|_I \otimes \mathbb{F}_{p^2} \simeq \begin{pmatrix} \omega_2^{\alpha}{\omega'_2}^{p-\alpha} & 0 \\ 0 & {\omega'_2}^{\alpha}\omega_2{}^{p-\alpha} \end{pmatrix}. \tag{2.3}$$

Here, $\alpha = (p+1)v(\Delta)/12$ is an integer as noted in [7, Proposition 2].

Proof. The part (1) is a consequence of [7, Lemme 2, Proposition 4]. The part (2) follows directly from [7, Proposition 2, Lemme 2]. □

From the case (1) 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 (2.3) 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; the proof of Proposition 1.3

In this section, we apply the results in the previous section to prove the following proposition:

Proposition 1.3. *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 $\bar{\rho}_{E,p}$ (absolutely) 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 $\mathfrak{p}$.*

Before proving this proposition, we give a few facts. 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 ([5, 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 obtained the following result.

Proposition 3.2 ([5, 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 semi-stable at $\mathfrak{p}$ and suppose that $\bar{\rho}_{E,p}$ is irreducible. Then, $\bar{\rho}_{E,p}|_{G(K(\zeta_p))}$ is absolutely irreducible.*

As noted in the introduction, Proposition 1.3 treats elliptic curves with additive reduction at a prime above $p = 5$ or 7, while Proposition 3.2 considers those with semi-stable reduction at such a prime.

Proof of Proposition 1.3. 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:

Case (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.

Case (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 $v_{\mathfrak{p}}(\Delta) \equiv 1 \bmod 3$. 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 $j_E = 1728A^3/\Delta$.

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

If the condition (1) 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 (2) 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 $v_{\mathfrak{p}}(\Delta) \equiv 2 \bmod 3$ can be rephrased as $v_{\mathfrak{p}}(j_E) \equiv 1 \bmod 3$.
- 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 1.3. □

4. Proof of Theorem 1.5

First we recall Theorem 1.5 stated in the introduction:

Theorem 1.5. *Let K be a totally real field in which 7 is unramified. If E is an elliptic curve over K with $\bar{\rho}_{E,7}$ irreducible, then E is modular.*

To prove Theorem 1.5, 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 ([5, 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 [14], we will state the modified version as corrected in [12, Theorem 1].

As [12] 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 some character ψ of finite order, where χ_p is the p-adic cyclotomic character, and
(v) for each prime $\mathfrak{p}|p$ of K,

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

with $\psi_2^{(\mathfrak{p})}|_{I_\mathfrak{p}}$ having finite order.

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 ([12, Theorem 1]). *Suppose that $\rho\colon G_K \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$ satisfies* (i)–(v) *above. Let $\bar{\rho}^{ss}$ denote the semi-simplification of a mod p reduction of ρ. Suppose also that*

(1) *$\bar{\rho}^{ss}$ is irreducible and $D_{\mathfrak{p}}$-distinguished for all $\mathfrak{p}|p$;.*
(2) *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 $\mathfrak{p}|p$;*
(3) *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 (1) and (2) 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) *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 $\bar{\rho}|_D = \mathrm{Ind}_{D'}^{D}\chi|_{D'}$. 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 that $\bar{\rho}$ is D-distinguished.

(2). See [1, Lemma 5.1.2]. □

With the above preparations in hand, we are now ready to prove Theorem 1.5.

Proof of Theorem 1.5. Let K and E be as in Theorem 1.5. If E has semi-stable reduction at some prime dividing 7, then the assertion follows from [5, 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 1.3 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 (1)–(3) 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 (1). Also (2) follows from Lemma 4.3(2) for $\bar{\rho}_{E,7}$. Finally, the condition (3) 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 1.6 even if K is just unramified at 5; in fact, Proposition 1.3 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 [14] is unavailable.

Remark 4.5. In his thesis [8], 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 [8, Proposition 6.1] combined with the modularity lifting theorem due to Skinner–Wiles [14].

Remark 4.6. Recently, S. Kalyanswamy [6] announced to prove a version of Theorem 1.5. He actually proves a new modularity theorem [6, Theorem 3.4] for certain Galois representations, and applies it to elliptic curves in [6, Theorem 4.4]. For clarity, we describe the difference between Theorem 1.5 and [6, 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 1.5 and [6, Theorem 4.4] have their own advantage.

5. Proof of the second main theorem: Theorem 1.2

In this last section, we finally prove the following theorem:

Theorem 1.2. *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.*

For the proof of Theorem 1.2, we need another modularity theorem due to Freitas [4]. This theorem essentially follows from [13], [14], and Theorem 4.1.

Theorem 5.1 ([4, Theorem 6.3]). *Let K be an abelian totally real field where 3 is unramified. Let E be an elliptic curve over K semi-stable 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 5.2 ([10, 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.*

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

Now we are ready to prove Theorem 1.2.

Proof of Theorem 1.2. Let K be as in Theorem 1.2 and E an elliptic curve over K. Our goal is to prove that E is modular. By Theorem 1.5 and Theorem 1.6, 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 5.2, 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 5.2 (2).

Finally, suppose that $E_{\mathfrak{p}}$ has additive potential multiplicative reduction. In this case, using [11, 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 5.1 implies that $E^{(d)}$ is modular. Since modularity of elliptic curves is invariant under quadratic twists, it follows that E is modular. □

References

[1] P. B. Allen, "Modularity of nearly ordinary 2-adic residually dihedral Galois representations", *Compos. Math.* **150** (2014), no. 8, p. 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. Am. Math. Soc.* **14** (2001), p. 843-939.

[3] K. Buzzard, "Potential modularity - a survey", `https://arxiv.org/abs/1101.0097`, 2010.

[4] N. Freitas, "Recipes to Fermat-type equations of the form $x^r + y^r = Cz^p$", *Math. Z.* **279** (2015), no. 3-4, p. 605-639.

[5] N. Freitas, B. V. Le Hung & S. Siksek, "Elliptic Curves over Real Quadratic Fields are Modular", *Invent. Math.* **201** (2015), no. 1, p. 159-206.

[6] S. Kalyanswamy, "Remarks on automorphy of residually dihedral representations", `https://arxiv.org/abs/1607.04750`, 2016.

[7] A. Kraus, *Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique*, Dissertationes Mathematicae, vol. 364, Instytut Matematyczny Polskiej Akademi Nauk, 1997.

[8] B. V. Le Hung, "Modularity of some elliptic curves over totally real fields", `https://arxiv.org/abs/1309.4134`, 2013.

[9] J. Nekovář, "On the parity of ranks of Selmer groups. IV", *Compos. Math.* **145** (2009), no. 6, p. 1351-1359.

[10] J.-P. Serre & J. Tate, "Good Reduction of Abelian Varieties", *Ann. Math.* **88** (1968), no. 3, p. 492-517.

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer, 1986, xii+400 pages.

[12] C. Skinner, "Nearly ordinary deformation of residually dihedral representations", preprint.

[13] C. Skinner & A. Wiles, "Residually reducible representations and modular forms", *Publ. Math., Inst. Hautes Étud. Sci.* **89** (1999), p. 5-126.

[14] ———, "Nearly ordinary deformations of irreducible residual representations", *Ann. Fac. Sci. Toulouse, Math.* **10** (2001), no. 1, p. 185-215.

[15] R. Taylor, "Remarks on a conjecture of Fontaine and Mazur", *J. Inst. Math. Jussieu* **1** (2002), no. 1, p. 125-143.

[16] R. Taylor & A. Wiles, "Ring-theoretic properties of certain Hecke algebras", *Ann. Math.* **141** (1995), no. 3, p. 553-572.

[17] J. Thorne, "Automorphy of some residually dihedral Galois representations", *Math. Ann.* **364** (2016), no. 1-2, p. 589-648.

[18] A. Wiles, "Modular elliptic curves and Fermat's Last Theorem", *Ann. Math.* **141** (1995), no. 3, p. 443-551.

Sho Yoshikawa
Gakushuin University,
Department of Mathematics,
1-5-1, Mejiro, Toshima-ku, Tokyo, Japan
E-mail: `yoshikawa@math.gakushuin.ac.jp`