Yoshikawa *Res. Number Theory* (2016) 2:8
DOI 10.1007/s40993-016-0060-8

Research in Number Theory

RESEARCH Open Access

On the modularity of elliptic curves over a composite field of some real quadratic fields

Sho Yoshikawa*

*Correspondence:
yoshi@ms.u-tokyo.ac.jp
Graduate School of Mathematical Sciences, The University of Tokyo, 3-8-1, Komaba, Meguro-Ku, Tokyo 153-8914, Japan

Abstract

Let K be a composite field of some real quadratic fields. We give a sufficient condition on K such that all elliptic curves over K are modular.

1 Introduction

For an elliptic curve E over a totally real field K, we say that E is modular if there exists a Hilbert modular form f over K of parallel weight 2 which satisfies the equality

$$L(E, s) = L(f, s).$$

The original Shimura-Taniyama conjecture asserts that any elliptic curve over $\mathbb{Q}$ is modular. This conjecture was proved in the celebrated works by Wiles [11], Taylor–Wiles [8], and Breuil–Conrad–Diamon–Taylor [1]. The Shimura-Taniyama conjecture has a natural generalization to the totally real field setting:

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. However, it has been difficult to prove the modularity of *all* elliptic curves over a fixed field. A few years ago, Le Hung and Freitas-Le Hung-Siksek brought a breakthrough in the problem of modularity of elliptic curves:

Theorem 1.2 ([3, Theorem 1]) *Let K be a real quadratic number field. Then, any elliptic curve over K is modular.*

Also, using the results in [9] and in Iwasawa theory for elliptic curves, Thorne recently proved the following theorem:

Theorem 1.3 ([10, 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.*

In this paper, we prove some special cases of Conjecture 1.1 by making use of methods in [3]. Before stating our main theorem, we introduce a notation and give a remark. For

Springer Open

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 $\tilde{s}\colon \mathrm{Gal}(\bar{F}/F) \to \mathrm{Gal}(K/F) \xrightarrow{s} \{\pm 1\}$. 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 [3] (Magma scripts are available at http://arxiv.org/abs/1310.7088). The main theorem of this paper is the following:

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 $6p$. We furthermore assume that, for each character $s\colon \mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\}$, the Mordell-Weil group $X^{(s)}(\mathbb{Q})$ is of rank 0. Then, any elliptic curve over K is modular.*

In contrast to the case of cyclic field extensions as considered in [9], we consider here certain extensions which are far from cyclic ones. We prove Theorem 1.4 in the next section. It is motivated from the proof of [3, Lemma 1.1] and is outlined as follows: By [3, Theorem 2], an elliptic curve which is not yet proved to be modular defines a point of a certain modular curve. We show that the point of the modular curve is actually a rational point or a real quadratic point, both of which corresponds to a modular elliptic curve.

After the proof of Theorem 1.4, we also discuss how often the hypotheses of Theorem 1.4 are likely to hold.

2 Proof of 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

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

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

Lemma 2.1 *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 isomorhic to $(\mathbb{Z}/(2))^r$ with r a positive integer, let $G^\vee$ denote the group $\mathrm{Hom}(G, \{\pm 1\})$ of characters.

Lemma 2.2 *Let 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. □

For an elliptic curve E over a field K and a prime number ℓ, let $\bar{\rho}_{E,\ell}\colon \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ denote the mod ℓ Galois representation attached to the ℓ-torsion points of E.

Lemma 2.3 *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 [6, 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 2.4 *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 2.3, $\bar{\rho}_{X,\ell}$ 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 2.1 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 2.2, we have $[2^{n+r}]X(K) = 0$; that is, $X(K) \subset X[2^{n+r}](\bar{\mathbb{Q}})$. This implies that 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 $X(K) = X(\mathbb{Q})$. □

We note the following modularity theorem, which is a consequence of a theorem of Langlands–Tunnel and modularity switching arguments.

Theorem 2.5 ([3, Theorem 2]) *Let E be an elliptic curve over a totally real field K. If $p = 3, 5$, or 7, and if the restriction of $\bar{\rho}_{E,p}$ to $\mathrm{Gal}(\bar{K}/K(\zeta_p))$ is absolutely irreducible, then E is modular.*

For mod 5 (resp. mod 7) representations, we can relax the hypothesis in Theorem 2.5 under the assumption that the base field is unramified at 5 (resp. 7).

Theorem 2.6 *Let $p = 5$ or 7 and K be a totally real field unramified at p. If E is an elliptic curve over K such that the mod p Galois representation $\bar{\rho}_{E,p}$ is (absolutely) irreducible, then E is modular.*

Proof The case $p = 5$ is proved in [9] by Thorne. He in fact obtains a slightly stronger result: we only need to assume that $\sqrt{5} \notin K$ instead of the unramifiedness of 5 in K. The case $p = 7$ is proved in [12] by the author. □

Before proceeding to the proof of Theorem 1.4, we also need to introduce a certain modular curve from [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 nomalizer 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 [3]. For the proof of Theorem 1.4, we only need the following properties of $X(s3, b5)$ and $X(s3, b7)$.

Lemma 2.7 *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 [10, Proposition 4] for (1), and see [3, Proof of Lemma 1.1] for (2). □

We are now ready to prove Theorem 1.4.

Proof of Theorem 1.4 Let p, X, 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 2.5 and Theorem 2.6, 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 [3, Proposition 4.1, Corollary 10.1].

Suppose first that E defines a K-point of X. Then Proposition 2.4 implies that, after a suitable base change by a solvable Galois extension, E becomes actually defined over $\mathbb{Q}$, and hence E is modular (by [1, 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 2.7, we have a morphism $f_p\colon X(s3, bp) \to X$ of degree 2. By Proposition 2.4, $\mathrm{Gal}(K/\mathbb{Q})$ 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, [1, Theorem A], [3, Theorem 1], and the base change theorem show that E is modular. This completes the proof. □

Let again 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 2.8 [2, 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 2.8, we calculate, in an elementary way, the global root numbers of quadratic twists of an elliptic curve that we are interested in.

Corollary 2.9 *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 $w(E^{(d)}/\mathbb{Q}) = \left(\frac{d}{N}\right) w(E/\mathbb{Q})$, where $E^{(d)}$ denotes the quadratic twist of E by d and $\left(\frac{\cdot}{N}\right)$ 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 2.8 (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 2.8 (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

  $$\begin{aligned} S_0 &= \{x \in \mathbb{F}_p; f(x) = 0\} \\ S^+ &= \left\{x \in \mathbb{F}_p; \left(\frac{f(x)}{p}\right) = 1\right\} \\ S^- &= \left\{x \in \mathbb{F}_p; \left(\frac{f(x)}{p}\right) = -1\right\}. \end{aligned}$$

  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 $\left(\frac{d}{p}\right) = 1$, 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 $\left(\frac{d}{p}\right) = -1$, 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 2.8 (1), (2), we obtain $w(E^{(d)}/\mathbb{Q}_p) = \left(\frac{d}{p}\right) w(E/\mathbb{Q}_p)$ for every $p|N$.
- Also, $w(E/\mathbb{R}) = w(E^{(d)}/\mathbb{R}) = -1$ by Theorem 2.8 (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 $d_1,\ldots,d_r$ 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
- $\left(\frac{d_i}{3p}\right) = 1$ for $i = 1, ..., r$.

Here, recall that $3p$ is the conductor of X, and note that there 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 2.9 shows that $w(X^{(s)}/\mathbb{Q}) = w(X/\mathbb{Q})$ for any $s\colon \mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\}$. Since $\mathrm{rank}\, X = 0$, the parity conjecture for our X therefore predicts that $\mathrm{rank}\, X^{(s)}$ for any s is even. The Goldfeld conjecture [4] 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.

Remark 2.10 After the author wrote up this paper, 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 [5]. Unfortunately, such fields are not constructed in an explicit way. On the other hand, our result Theorem 1.4 gives explicit conditions on totally real fields over which any elliptic curve is modular, although it does not seem easy to show the existence of infinitely many fields satisfying the hypotheses of Theorem 1.4.

Acknowledgements
The author is especially grateful to his advisor Professor Takeshi Saito for a number of helpful suggestions to improve the arguments in this paper. He would like to thank Professor Ken Ono for informing the author of some references on the rank of quadratic twists. His thanks also go to Bao Le Hung and anonymous referees for helpful comments. This work was supported by the Program for Leading Graduate Schools, MEXT, Japan.

Received: 21 July 2016 Accepted: 27 September 2016
Published online: 24 November 2016

References

1. Breuil, C., Conrad, B., Diamond, F., Taylor, R.: On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. J. Am. Math. Soc. **14**, 843–939 (2001)
2. Dokchitser, T., Dokchitser, V.: On the Birch–Swinnerton quotients modulo squares. Ann. Math. **172**, 567–596 (2010)
3. Freitas, N., Le Hung, B., Siksek, S.: Elliptic curves over real quadratic fields are modular. Invent. Math. **201**, 159–206 (2015)
4. Goldfeld, D.: Conjectures on elliptic curves over quadratic fields. Lecture Notes in Mathematics, vol. 751. Springer, Berlin (1979)
5. Le Hung, B.: Modularity of some elliptic curves over totally real fields, http://arxiv.org/abs/1309.4134
6. Serre, J.P.: Propriétés galoisienne des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1971)
7. Skinner, C., Wiles, A.: Nearly ordinary deformations of irreducible residual representations. Annales de la Faculte des sciences de Toulouse: Mathematiques **10**(1), 185–215 (2001)
8. Taylor, R., Wiles, A.: Ring-theoretic properties of certain Hecke algebras. Ann. Math. **141**(3), 553–572 (1995)
9. Thorne, J.: Automorphy of some residually dihedral Galois representations, Preprint
10. Thorne, J.: Elliptic curves over $\mathbb{Q}_\infty$ are modular, Preprint
11. Wiles, A.: Modular elliptic curves and Fermat's last theorem. Ann. Math. **141**(3), 443–551 (1995)
12. Yoshikawa, S.: On the modularity of elliptic curves with a residually irreducible representation, https://arxiv.org/abs/1606.06597