ON THE MODULARITY OF ELLIPTIC CURVES OVER THE CYCLOTOMIC $\mathbb{Z}_p$-EXTENSION OF SOME REAL QUADRATIC FIELDS

XINYAO ZHANG

Abstract. The modularity of elliptic curves always intrigues number theorists. Recently, Thorne had proved a marvelous result that for a prime $p$, every elliptic curve defined over a $p$-cyclotomic extension of $\mathbb{Q}$ is modular. The method is to use some automorphy lifting theorems and study non-cusp points on some specific elliptic curves by Iwasawa theory for elliptic curves. Since the modularity of elliptic curves over real quadratic was proved, one may ask whether it is possible to replace $\mathbb{Q}$ with a real quadratic field $K$. Following Thorne’s idea, we give some assumptions first and prove the modularity of elliptic curves over the $\mathbb{Z}_p$-extension of some real quadratic fields.

1. Introduction

Let $E_1$, $E_2$ be two elliptic curves given by the following Weierstrass equations.

\begin{align*}
E_1 &: y^2 + xy + y = x^3 + x^2 - 10x - 10.
E_2 &: y^2 + xy + y = x^3 + x^2 - 5x + 2.
\end{align*}

In order to state our main theorem, we give the following assumptions first.

Assumptions. Let $i = 1, 2$. Let $K$ be a real quadratic field, $p$ an odd prime satisfying

1. $K \neq \mathbb{Q}(\sqrt{5})$,
2. The Mordell-Weil group $E_i(K)$ is finite,
3. The $p$-Tate-Shafarevich group $\Sha(E_i/K)_p$ is trivial,
4. $p$ splits completely in $K$.

Our goal in this article is to prove the following result:

Theorem 1.1. Let $K$ and $p$ satisfy the Assumptions. Let $F$ be a number field contained in the cyclotomic $\mathbb{Z}_p$-extension of $K$. Let $E$ be an elliptic curve over $F$. Then $E$ is modular.

In recent years, a number of results about modularity or automorphy lifting theorems have been proved. As arithmetic consequences, the modularity of elliptic curves over some

Key words and phrases. Modularity, Iwasawa theory for elliptic curves.
specific fields can be verified. By studying non-cuspidal points on some modular curves, the following theorems had been proved:

**Theorem 1.2** ([FLHS13, Theorem 1]). Let $E$ be an elliptic curve over a real quadratic field $K$. Then $E$ is modular.

**Theorem 1.3** ([DNS20, Theorem 4]). Let $K$ be a totally real cubic number field. Let $E$ be an elliptic curve over $K$. Then $E$ is modular.

For more discussions, one can see [Hun13]. Using Iwasawa theory for elliptic curves, Thorne proved the following remarkable result:

**Theorem 1.4** ([Tho19, Theorem 1]). Let $p$ be a prime, and let $F$ be a number field which is contained in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let $E$ be an elliptic curve over $F$. Then $E$ is modular.

To prove Theorem 1.1, our strategy is to extend Thorne’s method, but there are some obstructions to study the $K_n$-points of $E_i$, where $K_n$ is the $p$-cyclotomic extension of a real quadratic field $K$ satisfying $[K_n : K] = p^n$. In Thorne’s proof, a key point is the fact that the Selmer group $\text{Sel}(E_i/\mathbb{Q})_p$ is trivial and then one can use some results in Iwasawa theory. This is the reason why we first assume that the Mordell-Weil group $E_i(K)$ is finite and the $p$-Tate-Shafarevich group $\text{III}(E_i/K)_p$ is trivial. Under these assumptions, we use some more general results in Iwasawa theory for elliptic curves to prove our result.

2. **Some data**

In this section, we will give some data of $E_i$, most of which are from [LMF22].

| Information               | $E_1$                               | $E_2$                               |
|---------------------------|-------------------------------------|-------------------------------------|
| Mordell-Weil group        | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ |
| Conductor                 | 15                                  | 15                                  |
| $j$-invariant             | $\frac{111284641}{50025} = 3^{-4} \cdot 5^{-4} \cdot 13^3 \cdot 37^3$ | $\frac{1399725}{225} = 3^{-2} \cdot 5^{-2} \cdot 241^3$ |
| Reduction type            | semistable                          | semistable                          |
|                           | split multiplicative: 5             | split multiplicative: 5             |
|                           | non-split multiplicative: 3         | non-split multiplicative: 3         |
| Tamagawa product          | 8                                   | 4                                   |
| Analytic order of III     | 1                                   | 1                                   |
| Growth of $2\infty$-torsion | $\mathbb{Q}(\sqrt{5}) : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | $\mathbb{Q}(\sqrt{5}) : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ |
|                           | $\mathbb{Q}(i) : \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | $\mathbb{Q}(i, \sqrt{15}) : \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ |
Table 1. Some data of $E_i$.

From table 1, we can obtain:

**Lemma 2.1.** The Tamagawa product $\text{Tam}(E_i/K)$ is a power of 2.

*Proof.* If $E_i$ has nonsplit multiplicative reduction at some $v$, the Tamagawa factor at $v$ is either 1 or 2 (see [Sil09], Appendix C, proof of Corollary 15.2.1). If $E_i$ has split multiplicative reduction at some $v$, by Kodaira and Néron’s theorem ([Sil09], Theorem 6.1), the Tamagawa factor at $v$ is a power of 2 from the decomposition of the $j$-invariant. The lemma holds since $E_i$ is semistable. □

**Lemma 2.2.** Under our assumptions, $E_i(K)[2^\infty] = E_i(K_\infty)[2^\infty]$, where $K_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $K$.

*Proof.* Let $\overline{\rho}_{E_i,2}$ be the Galois representation associated to the Tate module $T_2E_i$. As the elements in $E_i[2]$ are $\mathbb{Q}$-rational, the image of the absolute Galois group $G_\mathbb{Q}$ is congruent to the identity element mod $2\mathbb{Z}_2$ and thus a pro-2 group. As $K$ and $K_\infty$ are both Galois extensions of $\mathbb{Q}$, the index of $G_K$ and $G_{K_\infty}$ are both a power of 2. Then the lemma holds since $p$ is an odd prime. □

**Remark 2.3.** In fact, under our assumptions, we have $E_i(\mathbb{Q})[2^\infty] = E_i(K_\infty)[2^\infty]$ from the growth of $2^\infty$-torsion of $E_i$ in number fields given above.

3. **The proof**

For a number field $F$, we denote the absolute Galois group by $G_F$. For an elliptic curve $E$ over $F$ and a rational prime $l$, let $\overline{\rho}_{E,l} : G_F \to \text{GL}_2(\mathbb{F}_l)$ be the Galois representation associated to the $l$-torsion points of $E$. Let $\zeta_l$ be a primitive $l$-th root of unity.

**Theorem 3.1** ([Tho19], Theorem 2). Let $E$ be an elliptic curve over a totally real number field $F$, and suppose that (at least) one of the following is true:

1. The representation $\overline{\rho}_{E,3}|_{G_F(\zeta_3)}$ is absolutely irreducible.
2. $\sqrt{5} \notin F$, and $\overline{\rho}_{E,5}$ is irreducible.

Then $E$ is modular.

Following [FLHS15] and [Tho19], we consider modular curves $X(s3,b5)$ and $X(b3,b5)$. The next corollary is an analogue to [Tho19, Lemma 3].
Corollary 3.2. Let $F$ be a totally real field such that $\sqrt{5} \notin F$.
1. If $E/F$ is an elliptic curve which is not modular, then $E$ determines an $F$-rational point of one of the curves $X(s3, b5), X(b3, b5)$.
2. Recall that $K$ is a real quadratic field satisfying $K \neq \mathbb{Q}(\sqrt{5})$. If $F/K$ is cyclic and $X(s3, b5)(F) = X(s3, b5)(K), X(b3, b5)(F) = X(b3, b5)(K)$, then all elliptic curves over $F$ are modular.

Proof. The first assertion is a consequence of Theorem 3.1 and \[FLHS15\], Proposition 4.1. The second part follows from the first one, Theorem 1.2 and base change for $GL_2$ (see \[Lan80\]). □

Proposition 3.3 \((\text{Tho19}, \text{Proposition 4})\). The modular curves $X(b3, b5), X(s3, b5)$ are isomorphic over $\mathbb{Q}$ to $E_1, E_2$, respectively.

Remark 3.4. $E_1$ and $E_2$ are elliptic curves of Cremona label $15A1$ and $15A3$, respectively. See \[Cre97\].

Lemma 3.5. Let $l$ be an odd prime. Under our assumptions, we have $E_i(\mathbb{Q})[l^\infty] = E_i(K_\infty)[l^\infty]$.

Proof. Considering the Galois representation $\bar{\rho}_{E,i} : G_\mathbb{Q} \to GL_2(\overline{\mathbb{F}}_l)$, we know that $\bar{\rho}_{E,i}$ is surjective (see \[Tho19\], proof of Theorem 5 or \[Yos16\], Lemma 2.3). If $K_\infty$ has an $l$-torsion point, then the order of $\bar{\rho}_{E,i}|_{G_{K_\infty}}$ is a factor of $l(l - 1)$. Since $[K : \mathbb{Q}] = 2$ and $K_\infty$ is the $\mathbb{Z}_l$-extension of $K$, the index of $\bar{\rho}_{E,i}|_{G_{K_\infty}}$ in $GL_2(\overline{\mathbb{F}}_l)$ is either $p^n$ or $2p^n$ for some $n$. It is known that the order of the finite group $GL_2(\overline{\mathbb{F}}_l)$ is $l(l + 1)(l - 1)^2$, so we have $(l + 1)(l - 1) | 2p^n$. The only possibility is $p = 2$, but it is against our assumptions. □

Corollary 3.6. Under our assumptions, the $p$-Selmer group $Sel(E_i/K_\infty)_p$ is trivial.

Proof. It is a direct consequence of Lemma 3.5. □

To prove the next proposition, we will use Iwasawa theory. We denote a generator of the characteristic ideal of the Pontryagin dual of the Selmer group $Sel(E_i/K_\infty)_p$ by $f_{E_i}$. Let the $\lambda$-invariant $\lambda_{E_i}$ be the $\mathbb{Z}_p$-corank of $Sel(E_i/K_\infty)_p$.

Proposition 3.7. Under our assumptions, we have $E_i(K) = E_i(K_\infty)$.

Proof. By Lemma 2.2 and Lemma 3.5, we just need to prove that $E_i(K_\infty)$ is finite. Since $p$ splits completely in $K$, we can divide the proof into three cases.
Case 1. \( E_i \) has good ordinary reduction at all primes lying above \( p \).

In this case, we have the formula \([\text{Gre99}, \text{Theorem 4.1}]\):

\[
f_{E_i}(0) \sim \left( \prod_{v \text{ bad}} c_v^{(p)} \right) \left( \prod_{v \mid p} \left| \tilde{E}_{i,v}(\mathbb{F}_v) \right| \right)^2 |\text{Sel}(E_i/K)_p| / |E_i(K)_p|^2.
\]

Here \( a \sim b \) when \( a \) and \( b \) have the same \( p \)-adic valuation, the highest power of \( p \) dividing the Tamagawa factor \( c_v \) at \( v \) is \( c_v^{(p)} \), and \( \mathbb{F}_v \) is the residue field at \( v \).

As \( |E_i(\mathbb{Q})| = 8 \), if \( p \) divides \( |E_i(\mathbb{F}_p)| \), then \( 8p \) divides \( |E_i(\mathbb{F}_p)| \) and it contradicts the Hasse bound. Since \( p \) splits completely in \( K \), we have \( p \nmid |\tilde{E}_{i,v}(\mathbb{F}_v)_p| \). By Lemma 2.1 and Corollary 3.6, \( f_{E_i}(0) \) is a \( p \)-adic unit and \( \lambda_{E_i} = 0 \). Hence, \( E_i(K_{\infty}) \) is finite.

Case 2. \( E_i \) has multiplicative reduction at all primes lying above \( p \).

In this case, we have the formula \([\text{Gre99}, \text{pp. 92-93}]\):

\[
f_{E_i}(0) \sim \left( \prod_{v \mid p} l_v \right) \left( \prod_{v \text{ bad}} c_v^{(p)} \right) |\text{Sel}(E_i/K)_p| / |E_i(K)_p|^2
\]

If \( E_i \) has non-split multiplicative reduction at \( v \), we can take \( l_v = 2 \). If \( E_i \) has split multiplicative reduction at \( v \), we can take

\[
l_v = \frac{\log_p(N_{K_v/Q_p}(q_{E_i}^{(v)}))}{\text{ord}_p(N_{K_v/Q_p}(q_{E_i}^{(v)}))} \cdot \frac{[K_v \cap Q_p^{unr} : Q_p]}{2p[K_v \cap Q_p^{cyc} : Q_p]}
\]

Here \( q_{E_i} \) is the Tate period, and \( Q_p^{unr} \) and \( Q_p^{cyc} \) are the maximal unramified extension and the cyclotomic \( \mathbb{Z}_p \)-extension of \( Q_p \), respectively. From \([\text{Tho19}, \text{proof of Theorem 5}]\), we know that \( \frac{\log_p(N_{K_v/Q_p}(q_{E_i}^{(v)}))}{\text{ord}_p(N_{K_v/Q_p}(q_{E_i}^{(v)}))} \) lies in \( p\mathbb{Z}_p^\times \) since \( p \) splits completely in \( K \). By Lemma 2.1 and Corollary 3.6 and the formula, \( E_i(K_{\infty}) \) is finite.

Case 3. \( E_i \) has good supersingular reduction at all primes lying above \( p \).

In this case, our assertion follows from \([\text{IP06}, \text{Theorem 5.1}]\) as \( a_p = 0 \) under our assumptions.

\( \square \)

Theorem 1.1 follows from Corollary 3.2 and Proposition 3.7.

At last, we give some data from \([\text{LMF22}]\).
From table 2, we can find many real quadratic fields and infinitely many odd primes satisfying our assumptions.

**Acknowledgements.** The author would like to express appreciation to his supervisor Professor Takeshi Saito for his comments and suggestions. Also, the author would like to thank Professor Jack Thorne and Dr. Sho Yoshikawa for some helpful communications.
References

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[DNS20] Maarten Derickx, Filip Najman, and Samir Siksek. Elliptic curves over totally real cubic fields are modular. *Algebra & Number Theory*, 14(7):1791–1800, 2020.

[FLHS15] Nuno Freitas, Bao V. Le Hung, and Samir Siksek. Elliptic curves over real quadratic fields are modular. *Inventiones mathematicae*, 201(1):159–206, 2015.

[Gre99] Ralph Greenberg. Iwasawa theory for elliptic curves. *Arithmetic theory of elliptic curves (Cetraro, 1997)*, pages 51–144. Springer, Berlin, 1999.

[Hun13] Bao V. Le Hung. Modularity of some elliptic curves over totally real fields. Preprint. arXiv:1309.4134, 2013.

[IP06] Adrian Iovita and Robert Pollack. Iwasawa theory of elliptic curves at supersingular primes over \( \mathbb{Z}_p \)-extensions of number fields. *Journal für die Reine und Angewandte Mathematik*, 2006(598):71–103, 2006.

[Lan80] Robert P. Langlands. *Base change for GL(2)*. Number 96. Princeton University Press, 1980.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. [http://www.lmfdb.org](http://www.lmfdb.org) 2022.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[Tho19] Jack A. Thorne. Elliptic curves over \( \mathbb{Q}_\infty \) are modular. *Journal of the European Mathematical Society*, 21(7):1943–1948, 2019.

[Yos16] Sho Yoshikawa. On the modularity of elliptic curves over a composite field of some real quadratic fields. *Research in Number Theory*, 2(1):1–6, 2016.

Graduate School of Mathematical Sciences, University of Tokyo, Komaba, Meguro, Tokyo 153-8914, Japan

Email address: zhangxy96@g.ecc.u-tokyo.ac.jp