Elliptic curves over $\mathbb{Q}_\infty$ are modular

Jack A. Thorne*

July 11, 2016

Abstract

We show that if p is a prime, then all elliptic curves defined over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ are modular.

1 Introduction

Our goal in this paper is to prove the following theorem:

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.*

By definition, the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ is the unique subfield $\mathbb{Q}_\infty$ of $\mathbb{Q}(\zeta_{p^\infty})$ with Galois group $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. It is totally real. An elliptic curve E over a number field F is said to be modular if there is a regular algebraic automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ which has the same L-function as E. This is one of several equivalent formulations; if F is totally real, then π will be generated by vectors which can be interpreted as Hilbert modular forms of parallel weight 2.

The modularity of a given elliptic curve E has many useful consequences. It implies that the L-function of E has an analytic continuation to the whole complex plane, allowing one to formulate the Birch–Swinnerton-Dyer conjecture for E unconditionally. When the order of vanishing of the L-function at the point $s = 1$ is at most 1, this conjecture is known, in its weak form, in many cases [Zha01].

The modularity of all elliptic curves over $\mathbb{Q}$ has been known since work of Wiles and Breuil, Conrad, Diamond, and Taylor [Wil95], [TW95], [CDT99], [BCDT01]. Attempts to generalize this work to fields other than $\mathbb{Q}$ have all followed Wiles' original strategy: one first proves automorphy lifting theorems. For curves satisfying the conditions of these theorems, one attempts to verify the residual automorphy. One then hopes that curves not satisfying the conditions of these theorems can be enumerated and checked explicitly to be modular.

This strategy has recently been used by Freitas, Le Hung, and Siksek to establish the modularity of all elliptic curves over real quadratic fields [FLHS15]. They use automorphy lifting theorems of Kisin to reduce the result to a calculation of real quadratic points on a finite list of modular curves; they then carry out some formidable calculations to check that these points also correspond to modular elliptic curves.

In this paper, we use an automorphy lifting theorem established recently by the author [Tho], which reduces the modularity of elliptic curves over a given totally real field F with $\sqrt{5} \notin F$ to checking the modularity of elliptic curves corresponding to rational points on two modular curves (one of which is $X_0(15)$, and the other of which is a genus 1 curve isogenous to $X_0(15)$). We then use Iwasawa theory to check that these curves acquire no new rational points in any cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Acknowledgements

This work was carried out while the author served as a Clay Research Fellow. I would like to thank James Newton and John Coates for useful conversations.

*Department of Pure Mathematics and Mathematical Statistics, Wilberforce Road, Cambridge, United Kingdom. *Email address:* thorne@dpmms.cam.ac.uk

2 The proof

If F is a number field, we write G_F for its absolute Galois group (relative to a fixed choice of algebraic closure $\overline{F}$). If $n \geq 1$ is an integer, we write $\zeta_n \in \overline{F}$ for some primitive n^{th} root of unity.

If E is an elliptic curve defined over a number field F, and p is a prime, then we write $\rho_{E,p} : G_F \to \mathrm{GL}_2(\mathbb{Z}_p)$ for the associated representation of the absolute Galois group of F on the p-adic Tate module of E, and $\overline{\rho}_{E,p} : G_F \to \mathrm{GL}_2(\mathbb{F}_p)$ for its reduction modulo p. Both of these representations are defined up to conjugation by elements of $\mathrm{GL}_2(\mathbb{Z}_p)$; the determinant of $\rho_{E,p}$ is the p-adic cyclotomic character $\epsilon : G_F \to \mathbb{Z}_p^\times$.

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.

Proof. The first part follows from results of Kisin and Langlands–Tunnell, see [FLHS15, Theorem 3]. The second part, in the case where $\overline{\rho}_{E,5}$ remains absolutely irreducible on restriction to $G_{F(\zeta_5)}$, is a consequence of the first part and the 3–5 switch of Wiles, described in *loc. cit.*. The second part in the remaining case is [Tho, Theorem 1.1]. □

Following [FLHS15, §2.2], we introduce modular curves $X(s3, b5)$ and $X(b3, b5)$. These are smooth, projective curves over $\mathbb{Q}$. Loosely speaking, for a number field K the non-cuspidal K-points of $X(s3, b5)$ correspond to isomorphism classes of elliptic curves E such that $\overline{\rho}_{E,3}(G_K)$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ and $\overline{\rho}_{E,5}(G_K)$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$ (i.e. E has a K-rational 5-isogeny). The non-cuspidal K-points of $X(b3, b5)$ correspond to isomorphism classes of curves which are endowed with a K-rational 15-isogeny.

Lemma 3. *Let F be a totally real field such that $\sqrt{5} \notin F$.*

1. *If E is an elliptic curve over F which is not modular, then E determines an F-rational point of one of the curves $X(s3, b5)$, $X(b3, b5)$.*
2. *If $F/\mathbb{Q}$ is cyclic and $X(s3, b5)(F) = X(s3, b5)(\mathbb{Q})$, $X(b3, b5)(F) = X(b3, b5)(\mathbb{Q})$, then all elliptic curves over F are modular.*

Proof. The first part is a consequence of Theorem 2 and [FLHS15, Proposition 4.1]. The second part is a consequence of the first part, the modularity of all elliptic curves over $\mathbb{Q}$, and cyclic base change for GL_2 [Lan80]. □

We can make these modular curves explicit:

Proposition 4. *The curve $X(b3, b5)$ is isomorphic over $\mathbb{Q}$ to the elliptic curve*

$$E_1 : y^2 + xy + y = x^3 + x^2 - 10x - 10$$

of Cremona label 15A1. The curve $X(s3, b5)$ is isomorphic over $\mathbb{Q}$ to the elliptic curve

$$E_2 : y^2 + xy + y = x^3 + x^2 - 5x + 2$$

of Cremona label 15A3. Both curves have group of rational points isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. They are related by an isogeny of degree 2.

Proof. See [FLHS15, Lemmas 5.6, 5.7]. □

By Lemma 3, the proof of Theorem 1 is therefore reduced to the following result:

Theorem 5. *Let p be a prime, let $i \in \{1,2\}$, and let $\mathbb{Q}_\infty$ denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Then $E_i(\mathbb{Q}_\infty) = E_i(\mathbb{Q})$.*

Proof. We just treat the case of $E = E_1$, since the other case is extremely similar (because E_1, E_2 are related by a 2-isogeny). We first show $E(\mathbb{Q}_\infty)^{\mathrm{tors}} = E(\mathbb{Q})$ by studying the Galois representations of E. It is known that the Galois representation $\rho_{E,l} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_l)$ is surjective for all primes $l \geq 3$. (For example, this can be shown using [Ser72, Proposition 21] and the fact that E has minimal discriminant 15^4.) It follows that for any prime $l \geq 3$, we have $E(\mathbb{Q}_\infty)[l^\infty] = 0$. To address the 2-power torsion, we appeal to the calculation by Rouse and Zureick-Brown of the image $\rho_{E,2}(G_{\mathbb{Q}})$ [RZB15]. They show that this subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ is the pre-image of the subgroup $G \subset \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ which is (up to conjugation) generated by the following matrices[1]:

$$G = \left\langle \begin{pmatrix} 5 & 4 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 5 \end{pmatrix} \right\rangle.$$

This group has order 16. In particular, $\rho_{E,2}(G_{\mathbb{Q}})$ is a pro-2 group, and if $p > 2$ then $\rho_{E,2}(G_{\mathbb{Q}_\infty}) = \rho_{E,2}(G_{\mathbb{Q}})$ and hence $E(\mathbb{Q}_\infty)[2^\infty] = E(\mathbb{Q})[2^\infty]$. If $p = 2$, then $\rho_{E,2}(G_{\mathbb{Q}_\infty}) = \{g \in \rho_{E,2}(G_{\mathbb{Q}}) \mid \det(g)^2 = 1\}$. We calculate that the subgroup of G consisting of matrices with determinant ± 1 is given by

$$H = \left\langle \begin{pmatrix} 5 & 4 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 4 & 5 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 5 & 4 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \right\rangle.$$

We have $(\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z})^H = (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z})^G$, and this easily implies that $E(\mathbb{Q}_\infty)[2^\infty] = E(\mathbb{Q})[2^\infty]$ in this case also. (We checked these group-theoretic calculations using Magma [BCP97].) Since the group $E(\mathbb{Q}_\infty)^{\mathrm{tors}}$ is the product of its l-primary components, we have now shown it to be equal to $E(\mathbb{Q})$.

We now show that the group $E(\mathbb{Q}_\infty)$ is finite, using results in Iwasawa theory. Since we already know $E(\mathbb{Q}_\infty)^{\mathrm{tors}} = E(\mathbb{Q})$, this will prove the theorem. Calculations of Greenberg [Gre99, p. 136] in the case $p = 2$ show that the 2-adic λ-invariant of E is trivial, hence $E(\mathbb{Q}_\infty)$ is finite. We can therefore assume that $p \geq 3$. It is known (cf. the tables in [Cre97] or [LMF]) that the L-function of E satisfies $L(E,1)/\Omega_E = 1/8$. The product $\mathrm{Tam}(E)$ of the Tamagawa numbers of E is equal to 8.

If $p \geq 3$ is a prime of good ordinary reduction for E, then by [Gre99, Proposition 3.8], to show $E(\mathbb{Q}_\infty)$ is finite it is enough to show that $\mathrm{Sel}_p(E) = Ш(E)[p]$ is trivial and $a_p \not\equiv 1 \bmod p$. We have $a_p \equiv 1 \bmod p$ if and only if p divides the order of the group $E(\mathbb{F}_p)$. If this happens then $8p$ divides $\#E(\mathbb{F}_p)$, which contradicts the Hasse bound $|a_p| \leq 2\sqrt{p}$. The triviality of $\mathrm{Sel}_p(E)$ follows from results of Kato and the fact that $L(E,1)/\Omega_E$ is a p-adic unit, see [Kat04, Theorem 17.4] or [SU14, Theorem 3.35] for a convenient reference. If p is a prime of good supersingular reduction, then the finiteness of $E(\mathbb{Q}_\infty)$ follows from results of Kato and Kurihara [Kur02, Theorem 0.1] and the fact that $L(E,1)/\Omega_E$ is a p-adic unit.

It remains to treat the primes $p = 3, 5$ of bad reduction of E. In either case, it follows from [Ski, Theorem C] and the fact that $L(E,1)/\Omega_E$ is a p-adic unit that $\mathrm{Sel}_p(E)$ is trivial. We will use this to show that the characteristic ideal $(f_E(T))$ of the p^∞-Selmer group of E is the unit ideal of the Iwasawa algebra $\Lambda = \mathbb{Z}_p[\![T]\!]$, which will imply the finiteness of $E(\mathbb{Q}_\infty)$. It suffices to show that $f_E(0)$ is a p-adic unit.

It follows from the discussion on [Gre99, pp. 92–93] that if E has non-split multiplicative reduction, then this is a consequence of the fact that the Tamagawa number of E, the cardinality of the group $\mathrm{Sel}_p(E)$, and the cardinality of the torsion subgroup of $E(\mathbb{Q})$, are all prime to p. This takes care of the case $p = 3$. In the remaining case of split multiplicative reduction (thus $p = 5$), the same discussion shows that we'll be done if we can show that the $\mathcal{L}$-invariant $\mathcal{L}_E = \frac{\log_p q_E}{\mathrm{ord}_p q_E}$ has p-adic valuation 1. The j-invariant of E is

$$j_E = \frac{111284641}{50625} = 3^{-4}5^{-4}13^3 37^3 = 5^{-4} + 2 \times 5^{-3} + 4 + O(5),$$

implying that

$$q_E = 5^4 + 3 \times 5^5 + O(5^6), \ \log_p q_E \equiv 3 \times 5 + O(5^2),$$

hence $\mathcal{L}_E = 2 \times 5 + O(5^2)$. (In the original version of this paper, we did these calculations using `sage` [S$^+$13]. We thank the anonymous referee for pointing out that in this case they could also easily be done by hand.) This completes the proof. □

[1] See `http://users.wfu.edu/rouseja/2adic/X187d.html`.

References

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over **Q**: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[CDT99] Brian Conrad, Fred Diamond, and Richard Taylor. Modularity of certain potentially Barsotti-Tate Galois representations. *J. Amer. Math. Soc.*, 12(2):521–567, 1999.

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

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

[Gre99] Ralph Greenberg. Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 51–144. Springer, Berlin, 1999.

[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, (295):ix, 117–290, 2004. Cohomologies p-adiques et applications arithmétiques. III.

[Kur02] Masato Kurihara. On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I. *Invent. Math.*, 149(1):195–224, 2002.

[Lan80] Robert P. Langlands. *Base change for* GL(2), volume 96 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, N.J., 1980.

[LMF] The LMFDB Collaboration. The L-functions and Modular Forms Database. `http://www.lmfdb.org`.

[RZB15] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Research in Number Theory*, 1(12), 2015.

[S$^+$13] W. A. Stein et al. *Sage Mathematics Software (Version 5.9)*. The Sage Development Team, 2013. `http://www.sagemath.org`.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ski] Christopher Skinner. Multiplicative reduction and the cyclotomic main conjecture for GL_2. Preprint, avaiable at `http://arxiv.org/abs/1407.1093`.

[SU14] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[Tho] Jack A. Thorne. Automorphy of some residually dihedral Galois representations. To appear in Math. Annalen.

[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[Zha01] Shouwu Zhang. Heights of Heegner points on Shimura curves. *Ann. of Math. (2)*, 153(1):27–147, 2001.