SERRE’S UNIFORMITY CONJECTURE FOR ELLIPTIC CURVES WITH RATIONAL CYCLIC ISOGENIES

PEDRO LEMOS

Abstract. Let $E$ be an elliptic curve over $\mathbb{Q}$ such that $\text{End}_\mathbb{Q}(E) = \mathbb{Z}$ and which admits a non-trivial cyclic $\mathbb{Q}$-isogeny. We prove that, for $p > 37$, the residual mod $p$ Galois representation $\bar{\rho}_{E,p} : G_\mathbb{Q} \to \text{GL}_2(\mathbb{F}_p)$ is surjective.

1. Introduction

In [13], Serre famously proved that, given an elliptic curve $E$ defined over a number field $K$ without complex multiplication, there exists a prime number $p_{E,K}$ such that, for any prime $p > p_{E,K}$, the image of the residual mod $p$ Galois representation $\bar{\rho}_{E,p} : G_\mathbb{Q} \to \text{GL}_2(\mathbb{F}_p)$ attached to $E$ is the whole of $\text{GL}_2(\mathbb{F}_p)$. In the very same paper, Serre raised the following question:

Given a number field $K$, is there a prime number $p_K$ such that, for any elliptic curve $E$ over $K$ without complex multiplication, the residual mod $p$ Galois representation $\bar{\rho}_{E,p}$ is surjective onto $\text{GL}_2(\mathbb{F}_p)$, whenever $p$ is a prime larger than $p_K$?

This conjecture remains open today, but, over the last forty years, there has been a lot of progress towards a proof for $K = \mathbb{Q}$ — it is believed that, in this case, $p_K = 37$. The classification of maximal subgroups of $\text{GL}_2(\mathbb{F}_p)$ plays a central role in the general strategy used to tackle this problem: the aim is to try to show that, for $p$ large enough, there are no elliptic curves without complex multiplication for which the image of $\bar{\rho}_{E,p}$ is contained in any of these maximal subgroups. The maximal subgroups not containing $\text{SL}_2(\mathbb{F}_p)$ are the Borel subgroups, the normalisers of (split and non-split) Cartan subgroups and a few exceptional ones. The exceptional cases were treated by Serre in [14]. Mazur, in [12], treated the Borel case, exhibiting all the possible prime degrees of rational isogenies admitted by elliptic curves over $\mathbb{Q}$: for elliptic curves over $\mathbb{Q}$ without complex multiplication, the possible prime degrees of rational isogenies are $2, 3, 5, 7, 11, 13, 17$ and $37$. Finally, Bilu and Parent [1] and Bilu, Parent and Rebolledo [2] studied the case of the normaliser of a split Cartan. In [2], they proved that if $E$ is an elliptic curve over $\mathbb{Q}$ without complex multiplication, and $p \geq 11$ is a prime different from 13, then the image of $\bar{\rho}_{E,p}$ is not contained in the normaliser of a split Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$. The verification of the conjecture is thus reduced to the proof that, for $p$ large enough, the image of the mod $p$ Galois representation of any non-CM elliptic curve over $\mathbb{Q}$ is not contained in the normaliser of any non-split
Cartan subgroup of $GL_2(\mathbb{F}_p)$.

For deep reasons, this last case seems, for the moment, out of reach. However, in the direction of such a result, we prove, in this paper, the following:

**Theorem 1.1.** Let $E$ be an elliptic curve over $\mathbb{Q}$ such that $\text{End}_{\mathbb{Q}}(E) = \mathbb{Z}$. Suppose, moreover, that $E$ admits a non-trivial cyclic $\mathbb{Q}$-isogeny. Then, for $p > 37$, the residual mod $p$ Galois representation $\bar{\rho}_{E,p} : G_\mathbb{Q} \to GL_2(\mathbb{F}_p)$ is surjective.

Mazur [12] proved that if $p \geq 11$ is a prime different from 13, then any elliptic curve over $\mathbb{Q}$ with a $\mathbb{Q}$-rational $p$ isogeny has potentially good reduction at every prime $\ell > 2$. In order to prove this, Mazur introduced the concept of formal immersion, concept which will be central in our discussion. We say that a morphism $f : X \to Y$ between two schemes is a formal immersion at a point $P \in X$ if the induced morphism of completed local rings at $P$

$$\hat{f}^* : \hat{O}_{Y,f(P)} \to \hat{O}_{X,P}$$

is surjective. We will briefly describe his method.

Say that $E$ is an elliptic curve over $\mathbb{Q}$ and that $C$ is a $\mathbb{Q}$-rational subgroup of $E(\bar{\mathbb{Q}})$ of order $p$, where $p \geq 11$ is a prime different from 13. Then $(E,C)$ is a representative of an isomorphism class of pairs which, by the moduli interpretation of $X_0(p)$, corresponds to a non-cuspidal rational point $P$ of $X_0(p)$. Moreover, since $E$ is assumed to have potentially multiplicative reduction at a prime $\ell > 2$ (for simplicity, we will take $\ell$ to be different from $p$), the reduction of $P$ mod $\ell$ coincides with a cusp. By an application of the Atkin–Lehner involution if necessary, we may assume that this cusp is $\infty$. Mazur, in [11] and [12], proves two fundamental claims that make the remainder of the argument work: firstly, he proves that $J_0(p) := \text{Jac}(X_0(p))$ has a non-trivial rank 0 quotient $A$ defined over $\mathbb{Q}$; secondly, he shows that the morphism

$$f : X_0(p)_{\mathbb{Z}_\ell} \to A_{\mathbb{Z}_\ell},$$

defined by composing the Abel–Jacobi map $X_0(p)_{\mathbb{Z}_\ell} \to J_0(p)_{\mathbb{Z}_\ell}$ with the natural projection $J_0(p)_{\mathbb{Z}_\ell} \to A_{\mathbb{Z}_\ell}$, is a formal immersion at $\infty$, the reduction of $\infty$ to the special fibre. Here, $X_0(p)_{\mathbb{Z}_\ell}$ stands for the minimal regular model of $X_0(p)$ over $\mathbb{Z}_\ell$, and $A_{\mathbb{Z}_\ell}$ and $J_0(p)_{\mathbb{Z}_\ell}$ for the Néron models of $A$ and $J_0(p)$ over $\mathbb{Z}_\ell$. As we have seen, $P$ reduces to $\infty$, which means that $f(P)$ will reduce to 0 mod $\ell$. However, $f(P)$ is rational, and, since $A(\mathbb{Q})$ is finite, it must be a torsion point of $A$. Now, $\text{Tors} A(\mathbb{Q})$ injects, by reduction mod $\ell$, into $A(\bar{\mathbb{F}}_\ell)$. Therefore, $f(P) = 0$. Let

$$s_\infty : \text{Spec} \mathbb{Z}_\ell \to X_0(p)_{\mathbb{Z}_\ell} \quad \text{and} \quad s_P : \text{Spec} \mathbb{Z}_\ell \to X_0(p)_{\mathbb{Z}_\ell}$$

be, respectively, the sections corresponding to $\infty$ and $P$. We find that $f \circ s_\infty = f \circ s_P$. Therefore,

$$\hat{s}_\infty^* \circ \hat{f}^* = \hat{s}_P^* \circ \hat{f}^*,$$

where $\hat{s}_\infty^*$, $\hat{s}_P^*$ and $\hat{f}^*$ are the induced maps on the completed local rings at $\infty$, $P_\ell$ and 0, the mod $\ell$ reductions of $\infty$, $P$ and 0, respectively. But since $\hat{f}^*$ is surjective, this yields
$s_\infty^* = \hat{s}_p^*$, implying that $P = \infty$. However, we asserted above that $P$ is non-cuspidal, and, therefore, we have a contradiction.

We might try to apply this strategy to other modular curves, such as $X_{ns}^+(p)$. However, as it is remarked in [8], assuming the Birch and Swinnerton-Dyer conjecture, it can be shown that the Jacobian of $X_{ns}^+(p)$ does not have a non-trivial rank 0 quotient defined over $\mathbb{Q}$. Indeed, by Chen [4] (see Theorem 3.1 in section 3), the Jacobian of $X_{ns}^+(p)$ is isogenous to the Jacobian of $X_0^+(p^2) := X_0(p^2)/w_{p^2}$, and the L-functions of every weight 2 cusp form of $\text{Jac}(X_0^+(p^2))$ have sign $-1$ in their functional equations. By the Birch and Swinnerton-Dyer conjecture, every non-trivial quotient of $\text{Jac}(X_{ns}^+(p))$ will then have Mordell–Weil rank $\geq 1$. But, as we have seen, the existence of a non-trivial rank 0 quotient is necessary for Mazur’s method to work.

Nevertheless, using a result by Imin Chen [4], later generalized by de Smit and Edixhoven [9], Darmon and Merel [8] proved the following result.

**Theorem 1.2** ([8, Proposition 7.1]). Let $r = 2$ or $3$, and let $p > 3$ be a prime. There exists a non-trivial optimal quotient $A$ of the Jacobian $J_{0,ns}^+(r,p)$ of the curve $X_0(r) \times_{X(1)} X_{ns}^+(p)$ such that $A(\mathbb{Q})$ is finite. Moreover, the kernel of the canonical projection $J_{0,ns}^+(r,p) \to A$ is stable under the action of the Hecke operators $T_n$ for $n$ coprime to $p$.

With it, they were able to show the following:

**Theorem 1.3** ([8, Theorem 8.1]). Let $E$ be an elliptic curve over $\mathbb{Q}$ admitting a $\mathbb{Q}$-rational $r$-isogeny, where $r = 2$ or $3$. Suppose that there exists a prime $p > 3$ such that the image of $\bar{\rho}_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$. Then $j(E) \in \mathbb{Z}[\frac{1}{p}]$.

In fact, their methods work not only when $r = 2$ or $3$, but whenever $X_0(r)$ has genus 0; in other words, whenever $r \in \{2, 3, 5, 7, 13\}$ (subject to the condition that, in the results aforementioned, $p \notin \{2, 3, 5, 7, 13\}$). Therefore, we have the following theorem:

**Theorem 1.4.** Set $\Sigma := \{2, 3, 5, 7, 13\}$. Let $E$ be an elliptic curve over $\mathbb{Q}$ admitting a $\mathbb{Q}$-rational $r$-isogeny, for some $r \in \Sigma$. Suppose that there exists a prime $p \notin \Sigma$ such that the image of $\bar{\rho}_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$. Then $j(E) \in \mathbb{Z}[\frac{1}{p}]$.

The proof of this theorem is essentially the same as the one presented by Darmon and Merel [8] for Theorem 1.3. Section 3 will provide an outline of it, the details being referred to [8].

There are essentially two steps in the proof of Theorem 1.1. The first one is to prove that, under the conditions of Theorem 1.4, we can actually conclude that $j(E) \in \mathbb{Z}$. The second
one consists, firstly, in noting that, for \( p > 37 \), the image of the mod \( p \) Galois representation of any non-CM elliptic curve over \( \mathbb{Q} \) will be either contained in the normaliser of a non-split Cartan subgroup of \( \text{GL}_2(\mathbb{F}_p) \), or will be the whole of \( \text{GL}_2(\mathbb{F}_p) \); and, secondly, in checking that, for \( r \in \{2, 3, 5, 7, 13\} \), the non-CM elliptic curves corresponding to the rational points of \( X_0(r) \) with integral \( j \)-invariant have surjective mod \( p \) Galois representations. Separately, we check the same thing for the non-cuspidal rational points of \( X_0(11), X_0(17) \) and \( X_0(37) \). This will yield the theorem.

**Notation.** We will denote the normaliser of a split Cartan subgroup of \( \text{GL}_2(\mathbb{F}_p) \) by \( N_{sp} \), and the normaliser of a non-split Cartan subgroup by \( N_{ns} \). The quotients \( X(p)/N_{sp} \) and \( X(p)/N_{ns} \) will be abbreviated to \( X^+_{sp}(p) \) and \( X^+_{ns}(p) \), respectively. Moreover, we will denote the fibre product \( X_0(r) \times_{X(1)} X^+_{sp}(p) \) by \( X^+_{0,sp}(r,p) \), and, similarly, the fibre product \( X_0(r) \times_{X(1)} X^+_{ns}(p) \) by \( X^+_{0,ns}(r,p) \).

**Acknowledgements.** I would like to thank Samir Siksek for all his helpful advice and suggestions. Also, I want to thank the referee for the useful comments and corrections. Finally, I would like to express my gratitude to the EPSRC for the financial support.

2. Proof of Theorem 1.1

One of the fundamental observations of this paper is the following improvement of Theorem 1.4:

**Proposition 2.1.** Set \( \Sigma := \{2, 3, 5, 7, 13\} \). Let \( E \) be an elliptic curve over \( \mathbb{Q} \) admitting a \( \mathbb{Q} \)-rational \( r \)-isogeny for some \( r \in \Sigma \). Suppose that there exists a prime \( p \notin \Sigma \) such that the image of \( \bar{\rho}_{E,p} \) is contained in the normaliser of a non-split Cartan subgroup of \( \text{GL}_2(\mathbb{F}_p) \). Then \( j(E) \in \mathbb{Z} \).

This proposition is actually a corollary of the following result.

**Proposition 2.2.** Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) and \( p \geq 5 \) a prime number such that \( \bar{\rho}_{E,p}(G_\mathbb{Q}) \) is contained in the normaliser of a non-split Cartan subgroup of \( \text{GL}_2(\mathbb{F}_p) \). Then, for any prime \( \ell \not\equiv \pm 1 \pmod{p} \), the elliptic curve \( E \) has potentially good reduction at \( \ell \).

**Proof.** Suppose \( \bar{\rho}_{E,p}(G_\mathbb{Q}) \) is contained in the normaliser \( N_{ns} \) of a non-split Cartan subgroup \( C_{ns} \) of \( \text{GL}_2(\mathbb{F}_p) \). Let \( \ell \) be a prime of potentially multiplicative reduction. For the remainder of this proof, we will write \( E \) for \( E_{\mathbb{Q}_\ell} \), the elliptic curve obtained from \( E \) by extension of scalars to \( \mathbb{Q}_\ell \). Also, we fix an embedding \( \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell \), which amounts to a choice of decomposition subgroup \( G_{\mathbb{Q}_\ell} \hookrightarrow G_\mathbb{Q} \) over \( \ell \).

Since \( E \) has potentially multiplicative reduction, it is a quadratic twist of a Tate curve \( E_q, q \in \mathbb{Q}_\ell^\times \). Let \( \psi \) be the quadratic character associated to this twist (\( \psi \) may well be the trivial character). Then \( \bar{\rho}_{E,p} \cong \bar{\rho}_{E_q,p} \otimes \psi \). Since we have

\[
\bar{\rho}_{E_q,p} \sim \begin{pmatrix} \chi_q & * \\ 0 & 1 \end{pmatrix},
\]

one of the fundamental observations of this paper is the following improvement of Theorem 1.4:
Proof of Proposition 2.1. Let \( p > \) prime number. Then we already know, due to Theorem 1.4, that the eigenvalues of \( \bar{\rho}_{E,p} \) reduction for any two elliptic curves over \( \mathbb{Q} \) satisfy the conditions of Proposition 2.2. It follows that \( \chi_p \) surjects onto \( \mathbb{F}_p^\times \), which forces \( p \not\equiv 1, 3 \pmod{4} \).

Now, note that \( C_{ns} \), as a subgroup of \( \text{GL}_2(\mathbb{F}_{p^2}) \), is conjugate to the subgroup
\[
(2.1) \quad \left\{ \begin{pmatrix} a & 0 \\ 0 & a^p \end{pmatrix} : a \in \mathbb{F}_{p^2}^\times \right\} \subseteq \text{GL}_2(\mathbb{F}_{p^2})
\]
Since \([N_{ns} : C_{ns}] = 2\), we have \( \bar{\rho}_{E,p}(\sigma)^2 \in C_{ns} \), for all \( \sigma \in G_{Q_\ell} \). Also, since \( \psi \) is quadratic, the eigenvalues of \( \bar{\rho}_{E,p}(\sigma)^2 \) are \( \chi_p(\sigma)^2 \) and 1. It then follows from \((2.1)\) that \( \chi_p(\sigma)^2 = 1 \), for all \( \sigma \in G_{Q_\ell} \). If \( \ell = p \), then we know that \( \chi_p \) surjects onto \( \mathbb{F}_p^\times \), which forces \( p \leq 3 \). If \( \ell \neq p \), then we have \( \ell^2 \equiv 1 \pmod{p} \).

Proof of Proposition 2.7. Let \( E \) be an elliptic curve and \( p \) a prime as in the statement of the proposition. Then we already know, due to Theorem 1.4, that \( j(E) \in \mathbb{Z}[\frac{1}{p}] \). Note that \( E \) and \( p \) satisfy the conditions of Proposition 2.2. It follows that \( E \) has potentially good reduction at \( p \). Therefore, \( j(E) \in \mathbb{Z} \).

With Proposition 2.1 proven, we have the most important ingredients for the proof of the main result of this paper.

Proof of Theorem 2.1. Let \( E \) be an elliptic curve over \( \mathbb{Q} \) without CM which admits a cyclic \( \mathbb{Q} \)-rational isogeny, which we may assume to be of prime degree \( r \). By Mazur [12], we have \( r \in \{2, 3, 5, 7, 11, 13, 17, 37\} \). Suppose, for the sake of contradiction, that there exists a prime number \( p > 37 \) such that \( \bar{\rho}_{E,p}(G_{\mathbb{Q}}) \neq \text{GL}_2(\mathbb{F}_p) \). For each prime number \( r \), define
\[
S_r = \{ j(P) : P \in X_0(r)(\mathbb{Q}) \}.
\]
We will distinguish two cases: we can either have \( r \in \{2, 3, 5, 7, 13\} \), or \( r \in \{11, 17, 37\} \). For \( r = 11, 17 \), the modular curve \( X_0(r) \) is an elliptic curve over \( \mathbb{Q} \) of rank 0; and for \( r = 37 \), \( X_0(r) \) is a curve of genus 2 whose Jacobian has rank 0. This makes it easy to determine the rational points of \( X_0(r) \) for \( r \in \{11, 17, 37\} \), which are, in fact, known. From [6 p. 98], we obtain
\[
S_{11} = \{-11 \cdot 13^3, -2^{15}, -11^2\};
\]
\[
S_{17} = \left\{ -\frac{17^2 \cdot 101^3}{2}, -\frac{17 \cdot 373^3}{2^{17}} \right\};
\]
\[
S_{37} = \{-7 \cdot 137^3 \cdot 2083^3, -7 \cdot 11^3\}.
\]
Therefore, if \( r \in \{11, 17, 37\} \), the \( j \)-invariant of \( E \) is one of the values in \( S_{11} \cup S_{17} \cup S_{37} \). Since any two elliptic curves over \( \mathbb{Q} \) without CM and with the same \( j \)-invariant are related by a quadratic twist, the surjectivity of \( \bar{\rho}_{E,p} \) only depends on the \( j \)-invariant. The LMFDB [10] provides a long list of elliptic curves over \( \mathbb{Q} \), together with information about the surjectivity of the mod \( p \) Galois representations attached to them, such as the largest non-surjective prime — which is computed using an algorithm of Sutherland [15]. For each of the seven values in \( S_{11} \cup S_{17} \cup S_{37} \), we found an elliptic curve over \( \mathbb{Q} \) in this database.
with this \( j \)-invariant, we verified that \(-2^{15}\) is the only CM \( j \)-invariant, and checked that the largest non-surjective prime of each of the other six \( j \)-invariants is \( \leq 37 \). Therefore, if an elliptic curve \( E \) defined over \( \mathbb{Q} \) without CM admits a \( \mathbb{Q} \)-rational isogeny of degree \( r \in \{11, 17, 37\} \), then the image of \( \bar{\rho}_{E,p} \) is \( \text{GL}_2(\mathbb{F}_p) \) for all \( p > 37 \).

Keeping up with the notation introduced at the beginning of this proof, we suppose that \( r \in \{2, 3, 5, 7, 13\} \). Now, \( X_0(r) \) is a smooth curve of genus 0 with rational points (the cusps, for instance), which means that \( X_0(r) \) will have infinitely many rational points. Therefore, we will not be able to use the same strategy we applied to treat the case \( r \in \{11, 17, 37\} \). Instead, we are going to start by showing that if \( \bar{\rho}_{E,p}(G_{\mathbb{Q}}) \neq \text{GL}_2(\mathbb{F}_p) \), then \( j(E) \in \mathbb{Z} \). This result, together with Proposition \ref{proposition2.1}, yields \( j(E) \in \mathbb{Z} \).

This would be of no use for us if \( S_r \cap \mathbb{Z} \) were infinite; but it turns out that, for \( r \in \{2, 3, 5, 7, 13\} \), this set is finite. In order to prove this, we can directly compute these sets, and that is what we will do now.

For an appropriate choice of local coordinate \( t \) on \( X_0(r) \cong \mathbb{P}^1_{\mathbb{Q}} \), the \( j \)-invariant map is explicitly given by a map of the form

\[
t \mapsto \frac{f(t)}{t},
\]

where \( f(t) \in \mathbb{Z}[t] \) is a monic polynomial of degree \( r + 1 \) and non-zero constant term. The values of \( f(t) \) can be found in the following table:

| \( r \) | \( f(t) \) |
|---|---|
| 2 | \((t + 16)^4\) |
| 3 | \((t + 27)(t + 3)^4\) |
| 5 | \((t^2 + 10t + 5)^4\) |
| 7 | \((t^2 + 5t + 1)^2(t^2 + 13t + 49)\) |
| 13 | \((t^4 + 7t^3 + 20t^2 + 19t + 1)^4(t^2 + 5t + 13)\) |

For \( r = 2, 3 \), they are easy to check (see \cite{[3]} pp. 179-180\}); for \( r = 5, 7, 13 \), we refer to \cite{[7]} p. 54. If \( t \) corresponds to a \( \mathbb{Q} \)-point in \( X_0(r) \), then we can write \( t = a/b \), where \( a, b \in \mathbb{Z} \), \( b > 0 \) and \( \gcd(a, b) = 1 \). Now, if the \( j \)-invariant of this point is integral, we have

\[
\frac{b^{r+1}f(a/b)}{ab^r} \in \mathbb{Z}.
\]
Therefore, $b \mid b^r f(a/b)$. But $b^{r+1} f(a/b) = a^{r+1} + bG(a,b)$, where $G \in \mathbb{Z}[s,t]$ is a homogeneous polynomial. Since $\gcd(a,b) = 1$, we must have $b = 1$. Hence, $t \in \mathbb{Z}$ and $t$ must divide the constant term of $f(t)$. Substituting $t$ in $f(t)/t$ by all integers that divide the constant term of $f(t)$, we obtain $S_r \cap \mathbb{Z}$:

\[ S_2 \cap \mathbb{Z} = \{-3^3 \cdot 5^3, -2^2 \cdot 7^3, -2^4 \cdot 3^3, -2^6, 0, 2^7, 2^6 \cdot 3^3, 2^4 \cdot 5^3, 2^{11}, 2^2 \cdot 3^6, 2^7 \cdot 3^3, 17^3, 2^6 \cdot 5^3, 2^5 \cdot 7^3, 2^6 \cdot 3^3 \cdot 5^3, 2^4 \cdot 17^3, 2^3 \cdot 31^3, 2^3 \cdot 3^3 \cdot 11^3, 2^2 \cdot 3^6 \cdot 7^3, 2^2 \cdot 5^3 \cdot 13^3, 2 \cdot 127^3, 2 \cdot 3^3 \cdot 43^3, 3^3 \cdot 5^3 \cdot 17^3, 257^3\};
\]

\[ S_3 \cap \mathbb{Z} = \{-2^4 \cdot 11^6 \cdot 13, -2^{15} \cdot 3 \cdot 5^3, -2^4 \cdot 3^2 \cdot 13^3, -2^4 \cdot 13, 0, 2^4 \cdot 3^3, 2^8 \cdot 7, 2^4 \cdot 3^3 \cdot 5, 2^8 \cdot 3^3, 2^4 \cdot 3^3 \cdot 5^3, 2^8 \cdot 3^2 \cdot 7^3, 2^4 \cdot 3 \cdot 5 \cdot 41^3, 2^8 \cdot 7 \cdot 61^3\};
\]

\[ S_5 \cap \mathbb{Z} = \{-2^6 \cdot 719^3, -2^6 \cdot 5 \cdot 19^3, 2^6 \cdot 2^6 \cdot 5^2, 2^{12}, 2^{12} \cdot 5^2, 2^{12} \cdot 5 \cdot 11^3, 2^{12} \cdot 211^3\};
\]

\[ S_7 \cap \mathbb{Z} = \{-3^3 \cdot 37 \cdot 719^3, -3^3 \cdot 5^3, 3^3 \cdot 37, 3^2 \cdot 7^4, 3^3 \cdot 5^3 \cdot 17^3, 3^2 \cdot 7 \cdot 2647^3\};
\]

\[ S_{13} \cap \mathbb{Z} = \{-2^6 \cdot 3^2 \cdot 4079^3, 2^6 \cdot 3^2, 2^{12} \cdot 3^3, 19, 2^{12} \cdot 3^3 \cdot 19 \cdot 991^3\}. \]

Resorting once again to the elliptic curve database of the LMFDB\cite{LMFDB}, we verified that the largest non-surjective prime of each of the non-CM $j$-invariants in

\[(S_2 \cup S_3 \cup S_5 \cup S_7 \cup S_{13}) \cap \mathbb{Z}\]

is not larger than 37. This concludes the proof of Theorem\cite{1}. \hfill \Box

**Remark.** During the proof of Theorem\cite{1} we computed the sets $S_r \cap \mathbb{Z}$, for $r \in \{2, 3, 5, 7, 13\}$, using an explicit description of the $j$-invariant map. There is, however, a nice proof of the finiteness of the sets $S_r \cap \mathbb{Z}$, pointed out to me by Samir Siksek. Since this proof is interesting in its own right, we include it here.

**Proposition 2.4.** Let $p$ be a prime number. Then the set $S_p \cap \mathbb{Z}$ is finite.

**Proof.** If the genus of $X_0(p)$ is at least 1, then it is known that there are only finitely many points in $X_0(p)(\mathbb{Q})$. Therefore, we may assume that the genus of $X_0(p)$ is 0, i.e., that $p \in \{2, 3, 5, 7, 13\}$.

Fix an isomorphism $\psi : \mathbb{P}^1_{\mathbb{Z}[\frac{1}{p}]} \to X_0(p)_{\mathbb{Z}[\frac{1}{p}]}$ over $\mathbb{Z}[\frac{1}{p}]$, and choose projective coordinates in such a way that $(0 : 1)$ is mapped to the cusp 0 and $(1 : 0)$ to the cusp $\infty$. The $j$-invariant map is then a morphism

\[ j : \mathbb{P}^1_{\mathbb{Z}[\frac{1}{p}]} \to \mathbb{P}^1_{\mathbb{Z}[\frac{1}{p}]} \]

mapping $(1 : 0)$ and $(0 : 1)$ to $(1 : 0)$. For a point in $X_0(p)$ to have integral $j$-invariant, it is necessary that its image under the $j$-invariant map does not intersect $(1 : 0)$ in any special fibre of $\mathbb{P}^1_{\mathbb{Z}[\frac{1}{p}]}$. Therefore, such a point must not intersect $(0 : 1)$ nor $(1 : 0)$ in any special fibre of $\mathbb{P}^1_{\mathbb{Z}[\frac{1}{p}]} \cong X_0(p)_{\mathbb{Z}[\frac{1}{p}]}$. This means that it must be of the form $(p^k : 1)$, for some $k \in \mathbb{Z}$.

Consider now $X_0(p)(\mathbb{C}_p)$ and $\mathbb{P}^1(\mathbb{C}_p)$ equipped with the $p$-adic topology. Consider the $\mathbb{Q}$-isomorphism between $X_0(p)$ and $\mathbb{P}^1_{\mathbb{Q}}$ obtained by restricting the isomorphism of the paragraph above to the general fibres. Let $B$ be the open ball of radius 1/p centered
at the point \((1 : 0)\) of \(\mathbb{P}^1(\mathbb{C}_p)\); the integral points of \(\mathbb{P}^1(\mathbb{C}_p)\) lie outside of \(B\). Since our isomorphism between \(X_0(p)\) and \(\mathbb{P}^1_{\mathbb{Q}}\) and the \(j\)-invariant morphism \(j : X_0(p)(\mathbb{C}_p) \to \mathbb{P}^1(\mathbb{C}_p)\) are \(p\)-adically continuous, \(U := j^{-1}(B)\) is an open subset of \(\mathbb{P}^1(\mathbb{C}_p)\) containing \((1 : 0)\) and \((0 : 1)\). Clearly, among the points \((p^k : 1), k \in \mathbb{Z}\), only finitely many lie outside of \(U\). This concludes the proof of the lemma. \(\square\)

3. Sketch Proof of Theorem 1.4

As the title indicates, the purpose of this section is to provide a sketch proof of Theorem 1.4. The proof is, mutatis mutandis, the same as the proof of [8, Theorem 8.1], and the details of what follows can be found in [8].

Let \(r\) be an integer in the set \(\{1, 2, 3, 5, 7, 13\}\), and \(p\) a prime not in there. Write \(d : X_0(rp^2) \to X_0(rp)\) for the degeneracy map that, at the level of \(\bar{\mathbb{Q}}\)-points, is given by 
\[(E, C) \mapsto (E, C[rp]).\]
By pull-back, we obtain a homomorphism \(d^* : \text{Pic}(X_0(rp)) \to \text{Pic}(X_0(rp^2))\). Let \(\pi : X_0(rp^2) \to X_0(r) \times_{X_0(1)} X_0^+(p^2)\) be the projection morphism. For ease of notation, we will denote the curve \(X_0(r) \times_{X_0(1)} X_0^+(p^2)\) by \(X_0^+(rp^2)\). Consider the homomorphism
\[\pi_* \circ d^* : \text{Pic}(X_0(rp)) \to \text{Pic}(X_0^+(rp^2)).\]
We define the \(p\)-old part of \(\text{Pic}(X_0^+(rp^2))\) to be
\[\text{Pic}(X_0^+(rp^2))^{p\text{-old}} := \pi_* \circ d^* (\text{Pic}(X_0(rp))),\]
and an element of \(\text{Pic}(X_0^+(rp^2))^{p\text{-old}}\) is called a \(p\)-old divisor.

The \(p\)-new part is defined as the following quotient:
\[\text{Pic}(X_0^+(rp^2))^{p\text{-new}} := \text{Pic}(X_0^+(rp^2))/\text{Pic}(X_0^+(rp^2))^{p\text{-old}}.\]
When \(r = 1\), we shorten \(p\)-old and \(p\)-new to old and new, respectively.

As the homomorphisms \(d^*\) and \(\pi_*\) preserve degrees of divisors, this whole discussion can be reproduced in terms of the Jacobian varieties of \(X_0(p), X_0(rp^2)\) and \(X_0^+(p^2)\). We then obtain the old and new parts of \(\text{Jac}(X_0^+(p^2))\), which are abelian varieties in their own right.

In [4], Chen proved the following result:

**Theorem 3.1 ([4, Theorem 1]).** The Jacobian of \(X_{\text{ns}}^+(p)\) is isogenous to the new part of the Jacobian of \(X_0^+(p^2)\).

However, his proof, making use of the Selberg trace formula, was not constructive. It was later proven by Chen [5] that a construction by Darmon and Merel [8], that we now reproduce, is, in fact, an explicit construction of Chen’s isogeny.
In order to describe this construction, we will introduce and recall some notation. Recall that we set $N_{sp}$ to be the normaliser of a split Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$, and $N_{ns}$ the normaliser of a non-split Cartan subgroup. Also, denote by $B^+$ and $B^-$ the subgroups of $\text{GL}_2(\mathbb{F}_p)$ consisting of upper triangular matrices and lower triangular matrices, respectively. Define

$$X'(p) := X(p)/(N_{sp} \cap N_{ns}).$$

For $r \in \{1, 2, 3, 5, 7, 13\}$, there are two natural projections associated to $X_0(r) \times X(1) X'(p)$:

$$X_0(r) \times X(1) X'(p) \rightarrow X'_{0,sp}(r,p) \quad \text{and} \quad X_0(r) \times X(1) X'(p) \rightarrow X'_{0,ns}(r,p).$$

We obtain a correspondence $X'_{0,sp}(r,p) \rightrightarrows X'_{0,ns}(r,p)$, which gives rise to a homomorphism

$$\phi : \text{Jac}(X'_{0,sp}(r,p)) \rightarrow \text{Jac}(X'_{0,ns}(r,p)).$$

Since we have an isomorphism between $X^+_sp(p)$ and $X^+_0(rp^2)$, we can substitute $\text{Jac}(X^+_{0,sp}(r,p))$ by the Jacobian of $X^+_0(rp^2)$ in the homomorphism $\phi$. Moreover,

**Lemma 3.2** ([8] Lemma 6.2 (a)). Under $\phi$, the image of the $p$-old part of $\text{Jac}(X^+_0(rp^2))$ is trivial.

**Proof.** Define the $p$-old part of $\text{Pic}(X^+_{0,ns}(r,p))$ as the image of

$$p^* : \text{Pic}(X_0(r)) \rightarrow \text{Pic}(X^+_{0,ns}(r,p)),$$

the pull-back of the projection to $X_0(r)$. Since $X_0(r)$ has genus 0, the $p$-old part of $\text{Jac}(X^+_{0,ns}(r,p))$ is trivial. Therefore, in order to prove the lemma, we only need to show that the image under $\phi$ of an old divisor is an old divisor.

Under our isomorphism between $X^+_{0,sp}(r,p)$ and $X^+_0(rp^2)$, an old divisor in $X^+_{0,sp}(r,p)$ has an inverse image in $X_0(r) \times X(1) X(p)$ which is the image of a $B^+$ and a $B^-$-invariant divisor. Since

$$N_{ns}B^+ = N_{ns}B^- = \text{GL}_2(\mathbb{F}_p),$$

the image in $X^+_{0,ns}(r,p)$ of such a divisor is $\text{GL}_2(\mathbb{F}_p)$-invariant, meaning that it must be an old divisor of $X^+_{0,ns}(r,p)$.

We then obtain a homomorphism

$$\text{Jac}(X^+_0(rp^2))^{p\text{-new}} \rightarrow \text{Jac}(X^+_{0,ns}(r,p)),$$

which, by Chen [5], is precisely Chen’s isogeny. Moreover, it follows from this explicit description that if $n \geq 1$ is an integer coprime to $p$, then Chen’s isogeny commutes with the Hecke operators $T_n$. Summing up,

**Theorem 3.3** ([8] Theorem 6.1). If $r \in \{1, 2, 3, 5, 7, 13\}$, there is an isogeny between $J^+_{0,ns}(r,p)$ and $\text{Jac}(X^+_0(rp^2))^{p\text{-new}}$ which, for any integer $n \geq 1$ coprime to $p$, commutes with the action of $T_n$.

The existence of such an isogeny is of fundamental importance to prove
Theorem 3.4 ([8, Proposition 7.1]). Let $r \in \{2, 3, 5, 7, 13\}$ and let $p$ be a prime number not in there. There exists a non-trivial optimal quotient $A$ of $J_{0,\text{ns}}^+(r, p)$, defined over $\mathbb{Q}$, such that $A(\mathbb{Q})$ is finite. Moreover, if $n \geq 1$ is an integer coprime to $p$, the kernel of the canonical projection $J_{0,\text{ns}}^+(r, p) \to A$ is stable under the Hecke operators $T_n$.

Sketch proof. As we have seen, there is an isogeny between $J_{0,\text{ns}}^+(r, p)$ and $\text{Jac}(X_0^+(rp^2))^{p\text{-new}}$ which commutes with the Hecke operators $T_n$ whenever $n$ is coprime to $p$. Thus, we are reduced to prove the result for $\text{Jac}(X_0^+(rp^2))^{p\text{-new}}$. Note that $\text{Jac}(X_0^+(rp^2))^{\text{new}}$ is an optimal quotient of $\text{Jac}(X_0^+(rp^2))^{p\text{-new}}$. Given an optimal quotient $B$ of $J_{0\text{new}}^+(N)$, and writing $p: J_{0\text{new}}^+(N) \to B$ for the canonical projection, we know, by a result of Ribet (see, for example, section 2 of [12]), that $\ker p$ is stable under the action of Hecke operators. Therefore, the same will be true for any optimal quotient of $\text{Jac}(X_0^+(rp^2))^{\text{new}}$. Hence, we only need to show that $\text{Jac}(X_0^+(rp^2))^{\text{new}}$ has a non-trivial optimal quotient with only finitely many rational points.

Consider the geodesic in $H^*$ that connects 0 to $\infty$ and the path $e$ it defines in $X_0^+(rp^2)$. According to the Drinfeld–Manin theorem, $e \in H_1(X_0^+(rp^2), \mathbb{Q})$. Moreover, it is fixed under complex conjugation. Hence, $e \in H_1(X_0^+(rp^2), \mathbb{Q})^+$. Write $e'$ for the image of $e$ in $H_1(\text{Jac}(X_0^+(rp^2))^{\text{new}}(\mathbb{C}), \mathbb{Q})^+$, and $I_e$ for $\text{Ann}_{\mathbb{Z}_\ell}(e')$. Set now

$$A := \text{Jac}(X_0^+(rp^2))^{\text{new}}/I_e \text{Jac}(X_0^+(rp^2))^{\text{new}}.$$ 

It remains to prove that $A$ is non-trivial and that $A(\mathbb{Q})$ is a finite set. For the proof of these two claims, we refer to the paper of Darmon and Merel [8].

We are now in position to apply a variant of the argument by Mazur that was described in the introduction. For details, we refer, once again, to [8]. In a very informal way, the proof goes as follows. It can be proven that, for any prime $\ell \equiv \pm 1 \pmod{p}$, the composition of the maps $X_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell} \to J_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell}$ and $J_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell} \to A_{\mathbb{Z}_\ell}$ is a formal immersion at $\infty_\ell$, where $\infty \in X_{0,\text{ns}}^+(r, p)$ is one of the cusps. If $E$ is an elliptic curve as in the statement of the theorem, then it gives rise to a $\mathbb{Q}$-rational point $P$ in $X_{0,\text{ns}}^+(r, p)$. If it were the case that $j(E) \notin \mathbb{Z}[\frac{1}{p}]$, then there would exist a prime $\ell \neq p$ dividing the denominator of $j(E)$. Therefore, the $\mathbb{Z}_\ell$-section corresponding to the point $P$ would intersect a cusp (which we may assume to be $\infty$) on the special fibre over $\ell$. Since all the cusps of $X_{0,\text{ns}}^+(r, p)$ are only defined over $\mathbb{Q}(\zeta_p)^+$, we conclude that $\ell \equiv \pm 1 \pmod{p}$. It can be proven that the image of $P$ in $A$ is torsion (see [8 Lemma 8.3.]). In a manner similar to the one presented in the introduction, it is now easy to derive a contradiction from the conjunction of this and the fact that the composition of the maps $X_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell} \to J_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell}$ and $J_{0,\text{ns}}^+(r, p)_{\mathbb{Z}_\ell} \to A_{\mathbb{Z}_\ell}$ is a formal immersion at $\infty_\ell$.

References

[1] Yuri Bilu and Pierre Parent, Serre’s uniformity problem in the split cartan case, Annals of Mathematics 173 (2011), 569–584.
[2] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+ (p')$,* Ann. Inst. Fourier (Grenoble) 63 (2013), no. 3, 957–984. MR 3137477

[3] B. J. Birch, *Some calculations of modular relations*, Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, 1972), Springer, Berlin, 1973, pp. 175–186. Lecture Notes in Mathematics, Vol. 320. MR 0332658

[4] Imin Chen, *The jacobians of non-split cartan modular curves*, Proceedings of the London Mathematical Society 77 (1998), no. 1, 1–38.

[5] ———, *On relations between Jacobians of certain modular curves*, J. Algebra 231 (2000), no. 1, 414–448. MR 1779608

[6] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. MR 1628193

[7] S. R. Dahmen, *Classical and modular methods applied to diophantine equations*, Ph.D. thesis, Universiteit Utrecht, 2008.

[8] Henri Darmon and Loic Merel, *Winding quotients and some variants of Fermat’s last theorem*, J. Reine Angew. Math. 490 (1997), 81–100.

[9] Bart de Smit and Bas Edixhoven, *Sur un résultat d’Imin Chen*, Mathematical Research Letters 7 (2000), no. 2, 147–153.

[10] The LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org, 2016, [Online; accessed 11 November 2016].

[11] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978). MR 488287

[12] B. Mazur and D. Goldfeld, *Rational isogenies of prime degree*, Inventiones mathematicae 44 (1978), no. 2, 129–162 (English).

[13] Jean-Pierre Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Inventiones mathematicae 15 (1971), no. 4, 259–331 (French).

[14] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 644559

[15] Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma 4 (2016), e4, 79. MR 3482279

University of Warwick, Mathematics Institute, Coventry, UK

E-mail address: lemos.pj@gmail.com