Triviality of $X_{\text{split}}(N)(\mathbb{Q})$ for certain congruence classes of $N$

Pierre Parent

Abstract

We give a criterion to check if, given a prime number $N$, the only rational points of the modular curve $X_{\text{split}}(N)$ are trivial (i.e., cusps or points furnished by complex multiplication). We then prove that this criterion is verified for large enough $N$ satisfying some explicit congruences.

1. Introduction

For any prime number $N$, let $X_{\text{split}}(N)$ be the modular curve over $\mathbb{Q}$ corresponding to the congruence subgroup $\Gamma_{\text{split}}(N) := \{ \left( \begin{array}{cc} a & c \\ b & d \end{array} \right) \in \text{SL}_2(\mathbb{Z}), \ b \equiv c \equiv 0 \mod N \text{ or } a \equiv d \equiv 0 \mod N \}$. This curve deprived from its cusps is the coarse moduli space over $\mathbb{Q}$ of the isomorphism classes of elliptic curves equipped with an unordered pair of independent $N$-isogenies. We say a point of $X_{\text{split}}(N)(\overline{\mathbb{Q}})$ is trivial if it is a cusp, or if the isomorphism class of elliptic curves defined by it has complex multiplication over $\overline{\mathbb{Q}}$. The goal of this Note is to make progress in the problem of showing that, if $N$ is large enough, $X_{\text{split}}(N)$ has only trivial rational points. It is known that this result would be a step toward an affirmative answer to Serre’s question about uniform surjectivity of the Galois...

E-mail address: Pierre.Parent@math.u-bordeaux.fr (P. Parent).
representations furnished by division points of elliptic curves (without complex multiplication) over \( \mathbb{Q} \) ([11], p. 299, [4], Introduction). Set \( \mathcal{A} := \{ \text{primes which are simultaneously a square mod } 3, \text{mod } 4, \text{mod } 7, \text{and a square mod at least five of the following: } 8, 11, 19, 43, 67, 163 \} \) (\( \mathcal{A} \) has density 7.2\(^{-9} \approx 0.013 \ldots \)). We prove the following:

**Theorem 1.1.** If \( N > 433 \) and \( N \not\in \mathcal{A} \), then \( X_{\text{split}}(N)(\mathbb{Q}) \) is trivial.

At the moment we are unable to prevent a positive density of primes from escaping our method, which uses quadratic imaginary orders of trivial class number. We hope to overcome this problem in the future.

2. The criterion

Let \( S \) be the set of supersingular invariants of elliptic curves in characteristic \( N \), and denote by \( \Delta_S \) the group of divisors of degree 0 with support on \( S \). Let \( \mathcal{T} \) be the subring of \( \text{End}(J_0(N)) \) generated by the Hecke operators. Denote by \( X_0(N)^{\text{sm}} \) the smooth part of the regular minimal model of \( X_0(N) \) over \( \mathbb{Z} \). The group \( \Delta_S \) is endowed with an action of the ring \( \mathcal{T} \), deduced for instance from the action of the Hecke correspondences on the supersingular points of the fiber at \( N \) of \( X_0(N) \). The \( \mathcal{T} \otimes \mathbb{Q} \)-module \( \Delta_S \otimes \mathbb{Q} \) is free of rank one ([9,8]). We will identify \( \Delta_S \), as a \( \mathcal{T} \)-module, with the character group of the neutral component of the fiber at \( N \) of the Néron model of \( J_0(N) \), as in [9]. Define the winding quotient \( J_e := J_0(N) / J_0(N)(\mathbb{Q}) \) as in [5]. Set \( v := \text{num}(N - 1)/2 \); it is the order of \( J_0(N)_{\text{ss}}'s \) component group. If \( F \) is a number field of \( \mathbb{Q} \)-rational points and \( P \) is a \( F \)-rational point of \( X_0(N) \), denote by \( \Phi_P \) the morphism over \( F \) obtained by composing the morphism from \( X_0(N)_{\mathbb{Q}} \) to \( J_0(N)_{\mathbb{Q}} \) which maps \( Q \) to \( v(Q - P) \) with the canonical surjection \( J_0(N) \rightarrow J_e \). If \( P \) is ordinary above \( N \), we consider the canonical extension of \( \Phi_P \) (deduced from the universal property of Néron models) from \( X_0(N)^{\text{sm}}_{/\mathbb{Q}} \) to the zero-component of \( J_e's \) Néron model on \( \mathbb{Q} \).

**Proposition 2.1.** Suppose that, for every \( P \) in \( X_0(N)^{\text{sm}}(\mathbb{Z}) \), the morphism \( \Phi_P \) is a formal immersion at \( P(\text{Spec}(\overline{\mathbb{F}}_N)) \). Then \( X_{\text{split}}(N)(\mathbb{Q}) \) is trivial.

**Proof.** Suppose \( (E, [A, B]) \) corresponds to a non-cuspidal point of \( X_{\text{split}}(N) \) with values in \( \mathbb{Q} \), where \( E \) is a rational elliptic curve endowed with a rational unordered pair of independent \( \mathbb{Q} \)-isogenies \( A, B \). We will show that \( E \) has complex multiplication. Galois action on the set \([A, B]\) factorises through the Galois group of a quadratic number field \( K \). The Néron model of \( E \) is ordinary at \( N \) ([10], Corollary 1.4), so \((E, A, E/B, E[N]/B), \Phi_P \) extends to a morphism from \( X_0(N)^{\text{sm}}_{/\mathbb{Q}} \) to \( J_e/\mathbb{Q}_K \).

The class in \( J_0(N) \) of the divisor \((1 - w_N)((E, A) - (E/B, E[N]/B)) \) is \( \mathbb{Q} \)-rational. By the Kolyvagin–Logachev theorem, the group \( J_e(\mathbb{Q}) \) is finite ([13]). Since \((1 + w_N) \) belongs to \( I_e \), one has \((1 - w_N)((E, A) - (E/B, E[N]/B)) = 2((E, A) - (E/B, E[N]/B)) \) in \( I_e(\mathbb{Q}) \), so \( \Phi_P(E, A) \) is torsion. Now if \( k \simeq \mathbb{F}_N \) is any of the two residue fields of \( \mathbb{Q}_K \) at \( N \), Proposition 3.3 of [10] asserts that \( \Phi_P(E, A)_k = 0_k \), and a well-known specialization lemma gives us that \( \Phi_P(E, A) = 0 \). The hypothesis that \( \Phi_P \) be a formal immersion at \((E, A)_k \) implies \( (E, A) = (E/B, E[N]/B) \). Therefore \( E \) has a nontrivial endomorphism. \( \square \)

**Proposition 2.2.** Suppose that, for every \( j \) in \( \mathbb{F}_N \setminus S \), there exists \( v = (v_E)_{j \in S} \) in \( \Delta_S[I_e] \) such that \( \sum_{j \in S} v_E(j - j_E) \neq 0 \). Then for each ordinary \( P \), the morphism \( \Phi_P \) of 2.1 is a formal immersion at \( P(\text{Spec}(\overline{\mathbb{F}}_N)) \).

(Note this is very close to [6], Proposition 4; see also [7]. The slight difference is that our maps \( \Phi_P \) go to a quotient of \( J_0(N) \), not a subvariety.) To prove Proposition 2.2, we need the following lemma, which one can prove by using the rigid-analytic description of \( J_0(N)_{/\mathbb{Q}_N} \) (a variety with purely toric reduction), and by interpreting the character group as a cotangent space as in [9], 1.4.5.
Lemma 2.3. Let $\Delta_r$ be the character group of $J^0_{e,F_N}$. The natural map $\Delta_r \to \Delta_S$ extends to an isomorphism: $\Delta_r \cong (\Delta_S \otimes \mathbb{Z}(N))[I_e]$, where $\mathbb{Z}(N)$ is the localization of $\mathbb{Z}$ at $N$.

Proof of Proposition 2.2. Suppose $P_{\mathbb{F}_N}$ is an element of $X_0(N)^{\text{sm}}(\overline{\mathbb{F}}_N)$. We have to show that the map induced by $\Phi_{P_{\mathbb{F}_N}}$ on cotangent spaces (at $0_{\mathbb{F}_N}$ and $P_{\mathbb{F}_N}$ respectively) is nonzero. Identify $P_{\mathbb{F}_N}$’s component with $(\mathbb{P}^1 \setminus S)_{\mathbb{F}_N}$ via $j$-invariant. Let $v$ be the element as in the proposition and $\chi$ be the character of $J_0(N)_0^{0,F_N}$ associated to $v$.

After multiplication of $v$ by a prime-to-$N$ rational integer, if necessary, Lemma 2.3 allows us to suppose that the morphism $\Psi : X_0(N)^{\text{sm}}_{\mathbb{F}_N} \to J_0(N)_{\mathbb{F}_N} \to \mathbb{G}_{m,\mathbb{F}_N}$, which maps a point $Q$ to $\chi(v(Q - P_{\mathbb{F}_N}))$, factorizes through $\Phi_{P_{\mathbb{F}_N}}$. Therefore it is sufficient to show that the cotangent map deduced from $\Psi$ is nonzero. Now if we restrict $\Psi$ on $P_{\mathbb{F}_N}$’s component, then we see that on structural sheaves $\Psi^\ast(j) = \prod_{j \in S}(j - j)^{\ast\ast}$, therefore $(d\Psi^\ast(j_{P_{\mathbb{F}_N}})/\Psi^\ast(j_{P_{\mathbb{F}_N}})) \neq 0$. □

3. Using Gross’ formula

We recall the theory of Gross ([2,12]). If $M$ is a $\mathbb{Z}$-module, define $\hat{M} := M \otimes \mathbb{Q}$. Let $B$ be the quaternion algebra over $\mathbb{Q}$ which is ramified precisely at $N$ and $\infty$. Choose a maximal order $R$ of $B$, and let $(R_1 := R, \ldots, R_n)$ be a set of maximal orders in $B$ corresponding to representatives for $\text{Cl}(B) = \mathbb{R}^\ast \setminus \mathbb{R}^\ast/B^\ast$ as in [2, Section 3]. Recall that $\text{Cl}(B)$ can be identified with the set of supersingular invariants of elliptic curves in characteristic $N$. The order $R_i$ associated to an invariant $j_{xE}$ is such that $R_i \cong \text{End}_{\mathbb{Q}(E)}(E)_{\mathbb{Q}(E)}$.

If $L$ is a quadratic number field, $L$ embeds in $B$ if and only if its localization at ramification primes for $B$ is a field. Then, for an order $O$ of $L$, a morphism of algebras $\sigma : L \hookrightarrow B$, and a maximal order $R$ of $B$, the pair $(\sigma, R)$ is said to be an optimal embedding of $O$ in $R$ if $\sigma(L) \cap R = \sigma(O)$. If $f$ is a negative integer, let $h(f)$ be the class number of the quadratic order $O_d$ with discriminant $d$ (if it exists), and $h_i(d)$ be the number of optimal embeddings of $O_d$ in $R_i$; modulo conjugation by $R^\ast$. For any (positive) integer $D$, we define the element:

$$\epsilon_D := \frac{1}{2} \sum_{i=1}^n \left( \sum_{-D = da^2} \frac{1}{u(d)} h_i(d) \right)[R_i],$$

where $u(d) = (\text{card}(O_d^\ast))/2$; we consider it as an element of $\left(\frac{1}{\mathbb{Q}}\right)^S$. Finally, if $(x_E)_{E \in S}$ is the canonical basis of $\mathbb{Q}^S$, one defines a scalar product $\langle \cdot, \cdot \rangle$ on $\mathbb{Q}^S$ by $\langle x_E, x_{E'} \rangle = (\text{card}(\text{End}_{\mathbb{Q}(E)}(E^\ast))/2) \cdot \delta_{j_{x_E}, j_{x_{E'}}}$ (where $\delta$ is the Kronecker symbol).

Now let $f$ be a newform of weight 2 for $\Gamma_0(N)$. For $D$ a positive integer as above, call $\epsilon D$ the (nontrivial) quadratic character associated to $\mathbb{Q}((\sqrt{-D}))$, and $f \otimes \epsilon D$ the twist of $f$ by $\epsilon D$. Let $(\Delta_S \otimes \mathbb{Q})^f$ be the $\mathbb{Q}_S$-eigenspace associated to $f$, $\epsilon_f$ be the component of $\epsilon_D$ on $(\Delta_S \otimes \mathbb{Q})^f$, $(\cdot, \cdot)$ be the Petersson product, and extend $(\cdot, \cdot)$ to $\mathbb{Q}^S$.

Theorem 3.1 (Gross). One has $L(f, 1)L(f \otimes \epsilon D, 1) = \frac{U(f)}{D^2} (\epsilon_f, \epsilon_f, \epsilon_f)$.

(See [2] Corollary 11.6. Actually, in [2] the formula is proven only if $D$ is the discriminant of a maximal order; see [1], Theorem 1.1, for a proof in a more general case.) This formula allows us to reduce the proof of Theorem 1.1 to the verification of next lemma’s elementary condition (2).

Lemma 3.2. Let $E$ be the sub-$\mathbb{T} \otimes \mathbb{Q}$-module of $\Delta_S \otimes \mathbb{Q}$ generated by the orthogonal projections (relatively to $(\cdot, \cdot)$) of the elements $\epsilon_D \otimes 1$ for $D \in \mathbb{N}$. Then:

1. $E \subseteq (\Delta_S \otimes \mathbb{Q})[I_e]$;
2. if there exists $v \in E$ which has exactly two nonzero integer components in the canonical basis of $\mathbb{Q}^S$, then $v$ satisfies the hypothesis of Proposition 2.2 for every $j$ in $\overline{\mathbb{F}}_N^\ast \setminus S$. 


Proof. If $e_{f,D} \neq 0$, Gross’ formula implies that $L(f, 1) \neq 0$, and in that case $I_e \cdot f = 0$, implying $I_e \cdot e_{f,D} = 0$. Since the projection of $e_D$ on $\Delta \otimes \mathbb{Q}$ is $\sum f e_{f,D}$ (where $f$ runs through the newforms), one concludes that $I_e \cdot e_D = 0$ and therefore (1) is true. To prove (2), we use Proposition 2.1, and Proposition 2.2 with $v$ (whose two nonzero components may be supposed to be $\pm 1$): the function $j \mapsto \sum_{j \in S} v_E/(j_E - j)$ is nowhere zero on each component of $X_0(N)(\overline{\mathbb{F}}_N)$’s ordinary locus, for the supersingular invariants are all distinct. □

Matching all this up, we can conclude the proof of Theorem 1.1 with the following.

Lemma 3.3. Suppose that $N > 433$. If $N \equiv -1 \mod 4$, define $v := e_{16} - 3 e_4$. Else, if $N$ is not a square modulo $p$ for some $p \in \{3, 7\}$, set $v := e_p - (u(p) + 1)e_p$. Else, if $N$ is a nonsquare modulo two distinct elements $p$ and $q$ of $\{8, 11, 19, 43, 67, 163\}$, set $v := e_p - e_q$. Then $v$ verifies the conditions of Lemma 2.

Proof. It suffices to check that the $v$’s of the lemma have no more than two coordinates in the canonical basis of $\mathbb{Z}^S$, and are nonzero. Eichler proved that $\sum_{n=1}^{N} h_1(d)$ is equal to $(1 - (d/N))h(d)$ if $N^2$ does not divide $d$, and 0 if it does (see e.g. [2], p. 122). This implies that the support of $v$ in $S$ has zero or two elements. (Note that $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-7})$ each have several orders with class number one: this explains the particular role that the discriminants $-4$, $-3$ and $-7$ play in our statement.) Now we prove $v$ is nontrivial. Each vertex of the graph corresponding to a maximal order $R_i$ in which there is an optimal embedding of an order $O$ with trivial class group may be lifted to the $j$-invariant of an elliptic curve over $\mathbb{Q}$ which has complex multiplication by $O$. The list of these invariants is well-known; for $N > 433$, each pair of those we consider in the definition of the $v$’s are made of distinct elements mod $N$. □

References