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

# Trivialité de $X_{\text {split }}(N)(\mathbb{Q})$ pour certaines classes de congruence de $N$ 

Pierre Parent<br>A2X, U.F.R de mathématiques et d'informatique, Université de Bordeaux I, 351, cours de la libération, 33405 Talence cedex, France<br>Received 31 October 2002; accepted after revision 30 January 2003<br>Presented by Jean-Pierre Serre


#### 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. To cite this article: P. Parent, C. R. Acad. Sci. Paris, Ser. I 336 (2003). © 2003 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS. All rights reserved.


## Résumé

Soit $N$ un nombre premier. On donne un critère permettant de vérifier si les points rationnels de la courbe modulaire $X_{\text {split }}(N)$ sont triviaux (c'est-à-dire des pointes ou des points fournis par la multiplication complexe). On montre ensuite que ce critère est satisfait si $N$ est assez grand et vérifie certaines congruences explicites. Pour citer cet article : P. Parent, C. R. Acad. Sci. Paris, Ser. I 336 (2003).
© 2003 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS. Tous droits réservés.

## 1. Introduction

For any prime number $N$, let $X_{\text {split }}(N)$ be the modular curve over $\mathbb{Q}$ corresponding to the congruence subgroup $\Gamma_{\text {split }}(N):=\left\{\left(\begin{array}{ll}a & c \\ b & d\end{array}\right) \in \operatorname{SL}_{2}(\mathbb{Z}), b \equiv c \equiv 0 \bmod N\right.$ or $\left.a \equiv d \equiv 0 \bmod N\right\}$. 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 $X_{\text {split }}(N)(\mathbb{Q})$ 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

[^0]representations furnished by division points of elliptic curves (without complex multiplication) over $\mathbb{Q}$ ([11], p. 299, [4], Introduction). Set $\mathcal{A}:=\{$ primes which are simultaneously a square $\bmod 3, \bmod 4, \bmod 7$, and a square $\bmod$ at least five of the following: $8,11,19,43,67,163\}\left(\mathcal{A}\right.$ has density $\left.7.2^{-9} \simeq 0.013 \ldots\right)$. We prove the following:

Theorem 1.1. If $N>433$ and $N \notin \mathcal{A}$, 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 $\mathbb{T}$ be the subring of $\operatorname{End}\left(J_{0}(N)\right)$ generated by the Hecke operators. Denote by $X_{0}(N)^{\mathrm{sm}}$ 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 $\mathbb{T}$, deduced for instance from the action of the Hecke correspondences on the supersingular points of the fiber at $N$ of $X_{0}(N)$. The $\mathbb{T} \otimes \mathbb{Q}$-module $\Delta_{S} \otimes \mathbb{Q}$ is free of rank one ([9,8]). We will identify $\Delta_{S}$, as a $\mathbb{T}$-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 $J_{e}=J_{0}(N) / I_{e} J_{0}(N)$ as in [5]. Set $v:=\operatorname{num}((N-1) / 2)$; it is the order of $J_{0}(N)_{\mathbb{F}_{N}}$ 's component group. If $F$ is a number field of ring of integers $\mathcal{O}_{F}$ 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 $X_{0}(N)_{F}$ to $J_{0}(N)_{F}$ 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 $X_{0}(N)_{/ \mathcal{O}_{F}}^{\mathrm{sm}}$ to the zero-component of $J_{e}$ 's Néron model on $\mathcal{O}_{F}$.

Proposition 2.1. Suppose that, for every $P$ in $X_{0}(N)^{\mathrm{sm}}(\mathbb{Z})$, the morphism $\Phi_{P}$ is a formal immersion at $P\left(\operatorname{Spec}\left(\overline{\mathbb{F}}_{N}\right)\right)$. 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 $N$-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 $(E, A)$ comes from an element of $X_{0}(N)^{\mathrm{sm}}\left(\mathcal{O}_{K}\right)$ (and $w_{N}(E, A)$ too). Moreover $N$ splits in $K$ (loc. cit., Lemma 3.2). Thus if $P:=(E / B, E[N] / B)$ ), $\Phi_{P}$ extends to a morphism from $X_{0}(N)_{/ \mathcal{O}_{K}}^{\mathrm{sm}}$ to $J_{e / \mathcal{O}_{K}}$.

The class in $J_{0}(N)$ of the divisor $\left(1-w_{N}\right)((E, A)-(E / B, E[N] / B))$ is $\mathbb{Q}$-rational. By the KolyvaginLogachev theorem, the group $J_{e}(\mathbb{Q})$ is finite $([3])$. Since $\left(1+w_{N}\right)$ belongs to $I_{e}$, one has $\left(1-w_{N}\right)((E, A)-$ $(E / B, E[N] / B))=2((E, A)-(E / B, E[N] / B))$ in $J_{e}(\mathbb{Q})$, so $\Phi_{P}(E, A)$ is torsion. Now if $k \simeq \mathbb{F}_{N}$ is any of the two residue fields of $\mathcal{O}_{K}$ 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.

Proposition 2.2. Suppose that, for every $j$ in $\mathbb{F}_{N^{2}} \backslash S$, there exists $v=\left(v_{E}\right)_{j_{E} \in S}$ in $\Delta_{S}\left[I_{e}\right]$ such that $\sum_{j_{E} \in S} v_{E} /\left(j-j_{E}\right) \neq 0$. Then for each ordinary $P$, the morphism $\Phi_{P}$ of 2.1 is a formal immersion at $P\left(\operatorname{Spec}\left(\overline{\mathbb{F}}_{N}\right)\right)$.
(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 $\Delta_{e}$ be the character group of $J_{e}^{0}{ }_{/ \mathbb{F}_{N}}$. The natural map $\Delta_{e} \rightarrow \Delta_{S}$ extends to an isomorphism: $\Delta_{e} \otimes \mathbb{Z}_{(N)} \simeq\left(\Delta_{S} \otimes \mathbb{Z}_{(N)}\right)\left[I_{e}\right]$, 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 $X_{0}(N)^{\mathrm{sm}}\left(\overline{\mathbb{F}}_{N}\right)$. We have to show that the map induced by $\Phi_{{\overline{\mathbb{F}}_{N}}}$ on cotangent spaces (at $0_{\overline{\mathbb{F}}_{N}}$ and $P_{\overline{\mathbb{F}}_{N}}$ respectively) is nonzero. Identify $P_{\overline{\mathbb{F}}_{N}}$ 's component with $\left(\mathbb{P}^{1} \backslash S\right)_{\overline{\mathbb{F}}_{N}}$ via $j$-invariant. Let $v$ be the element as in the proposition and $\chi$ be the character of $J_{0}(N) \frac{\mathbb{F}}{N}$ 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 $\Psi: X_{0}(N) \frac{\mathbb{F}}{N}^{\mathrm{sm}} \rightarrow J_{0}(N)_{\overline{\mathbb{F}}_{N}}^{0} \rightarrow \mathbb{G}_{m, \overline{\mathbb{F}}_{N}}$, which maps a point $Q$ to $\chi\left(\nu\left(Q-P_{\overline{\mathbb{F}}_{N}}\right)\right.$ ), factorizes through $\Phi_{P_{\bar{F}_{N}}}$. Therefore it is sufficient to show that the cotangent map deduced from $\Psi$ is nonzero. Now if we restrict $\Psi$ on $P_{\overline{\mathbb{F}}_{N}}$ 's component, then we see that on structural sheaves $\Psi^{\sharp}(j)=\prod_{j_{E} \in S}\left(j_{E}-j\right)^{v \cdot v_{E}}$ ([9], 1.4.4, Proposition 16), therefore $\left(\mathrm{d} \Psi^{\sharp}\left(j_{P_{\mathbb{F}_{N}}}\right) / \Psi^{\sharp}\left(j_{P_{\mathbb{F}_{N}}}\right)\right) \neq 0$.

## 3. Using Gross' formula

We recall the theory of Gross $([2,12])$. If $M$ is a $\mathbb{Z}$-module, define $\widehat{M}:=M \otimes \widehat{\mathbb{Z}}$. 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 $\left\{R_{1}:=R, \ldots, R_{n}\right\}$ be a set of maximal orders in $B$ corresponding to representatives for $\mathrm{Cl}(B)=\widehat{R}^{*} \backslash \widehat{B}^{*} / B^{*}$ as in [2], Section 3. Recall that $\mathrm{Cl}(B)$ can be identified with the set of supersingular invariants of elliptic curves in characteristic $N$. The order $R_{i}$ associated to an invariant $j_{E_{i}}$ is such that $R_{i} \simeq \operatorname{End}_{\mathbb{F}_{N^{2}}}\left(E_{i}\right)$.

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 $\mathcal{O}$ of $L$, a morphism of algebras $\sigma: L \hookrightarrow B$, and a maximal order $\mathcal{R}$ of $B$, the pair ( $\sigma, \mathcal{R}$ ) is said to be an optimal embedding of $\mathcal{O}$ in $\mathcal{R}$ if $\sigma(L) \cap \mathcal{R}=\sigma(\mathcal{O})$. If $d$ is a negative integer, let $h(d)$ be the class number of the quadratic order $\mathcal{O}_{d}$ with discriminant $d$ (if it exists), and $h_{i}(d)$ be the number of optimal embeddings of $\mathcal{O}_{d}$ in $R_{i}$ modulo conjugation by $R_{i}^{*}$. For any (positive) integer $D$, we define the element:

$$
e_{D}:=\frac{1}{2} \sum_{i=1}^{n}\left(\sum_{-D=d a^{2}} \frac{1}{u(d)} h_{i}(d)\right)\left[R_{i}\right],
$$

where $u(d)=\left(\operatorname{card}\left(\mathcal{O}_{d}^{*}\right)\right) / 2$; we consider it as an element of $\frac{1}{12} \mathbb{Z}^{S}$. Finally, if $\left(x_{E}\right)_{E \in S}$ is the canonical basis of $\mathbb{Q}^{S}$, one defines a scalar product $\langle\cdot, \cdot\rangle$ on $\mathbb{Q}^{S}$ by $\left\langle x_{E}, x_{E^{\prime}}\right\rangle=\left(\operatorname{card}\left(\operatorname{End}_{\overline{\mathbb{F}}_{N}}(E)^{*}\right) / 2\right) \cdot \delta_{j_{E}, j_{E}^{\prime}}$ (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 $\varepsilon_{D}$ the (nontrivial) quadratic character associated to $\mathbb{Q}(\sqrt{-D})$, and $f \otimes \varepsilon_{D}$ the twist of $f$ by $\varepsilon_{D}$. Let $\left(\Delta_{S} \otimes \overline{\mathbb{Q}}\right)^{f}$ be the $\mathbb{T}_{\overline{\mathbb{Q}}}$-eigenspace associated to $f, e_{f, D}$ be the component of $e_{D}$ on $\left(\Delta_{S} \otimes \overline{\mathbb{Q}}\right)^{f},(\cdot, \cdot)$ be the Petersson product, and extend $\langle\cdot, \cdot\rangle$ to $\overline{\mathbb{Q}}^{S}$.

Theorem 3.1 (Gross). One has $L(f, 1) L\left(f \otimes \varepsilon_{D}, 1\right)=\frac{(f, f)}{\sqrt{D}}\left\langle e_{f, D}, e_{f, D}\right\rangle$.
(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 $\langle\cdot, \cdot\rangle)$ of the elements $e_{D} \otimes 1$ for $D \in \mathbb{N}$. Then:
(1) $E \subseteq\left(\Delta_{S} \otimes \mathbb{Q}\right)\left[I_{e}\right]$;
(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 $\mathbb{F}_{N^{2}} \backslash S$.

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 $\Delta_{S} \otimes \mathbb{Q}$ 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 $j \mapsto \sum_{j_{E} \in S} v_{E} /\left(j_{E}-j\right)$ is nowhere zero on each component of $X_{0}(N)\left(\overline{\mathbb{F}}_{N}\right)$ '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 $N \equiv-1 \bmod 4$, define $v:=e_{16}-3 e_{4}$. Else, if $N$ is not a square modulo $p$ for some $p \in\{3,7\}$, set $v:=e_{4 p}-(u(-p)+1) e_{p}$. 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 3.2.

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 $\sum_{i=1}^{n} h_{i}(d)$ 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 $\mathcal{O}$ with trivial class group may be lifted to the $j$-invariant of an elliptic curve over $\mathbb{Q}$ which has complex multiplication by $\mathcal{O}$. 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 $\bmod N$.

## References

[1] M. Bertolini, H. Darmon, A rigid Gross-Zagier formula and arithmetic applications, Ann. of Math. (2) 146 (1997) 111-147. With an appendix by B. Edixhoven.
[2] B. Gross, Heights and the special values of $L$-series, in: Canadian Math. Soc. Conference Proceedings, Vol. 7, American Mathematical Society, Providence, RI, 1987, pp. 115-187.
[3] V.A. Kolyvagin, D.Yu. Logachev, Finiteness of the Shafarevich-Tate group and the group of rational points for some modular Abelian varieties, Leningrad Math. J. 1 (5) (1990).
[4] B. Mazur, Rational isogenies of prime degree, Invent. Math. 44 (1978) 129-162.
[5] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math. 124 (1996) 437-449.
[6] L. Merel, Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques, avec un appendice de E. Kowalski et Ph. Michel, Duke Math. J. 110 (1) (2001) 81-119.
[7] L. Merel, W.A. Stein, The field generated by the points of small prime order on an elliptic curve, Internat. Math. Res. Notices 20 (2001) 1075-1082.
[8] J.-F. Mestre, La méthode des graphes : exemples et applications, in: Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields, Katata, 1986, Nagoya University, Nagoya, 1986, pp. 217-242.
[9] J.-F. Mestre, J. Oesterlé, Courbes elliptiques de conducteur premier, Manuscript.
[10] F. Momose, Rational points on the modular curves $X_{\text {split }}(p)$, Compositio Math. 52 (1984) 115-137.
[11] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259-331.
[12] V. Vatsal, Uniform disribution on Heegner points, Invent. Math. 148 (1) (2002) 1-46.


[^0]:    E-mail address: Pierre.Parent@math.u-bordeaux.fr (P. Parent).

    1631-073X/03/\$ - see front matter © 2003 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS. Tous droits réservés. doi:10.1016/S1631-073X(03)00078-5

