Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$

Pierre Parent

October 8, 2003

Abstract

We give a criterion to check if, given a prime power p^r with $r > 1$, the only rational points of the modular curve $X_0^+(p^r)$ are trivial (i.e. cusps or points furnished by complex multiplication). We then prove that this criterion is verified if p satisfies explicit congruences. This applies in particular to the modular curves $X_{\mathrm{split}}(p)$, which intervene in the problem of Serre concerning uniform surjectivity of Galois representations associated to division points of elliptic curves.

1 Introduction

Let p^r be a power of a prime number p, with $r > 1$, and $X_0(p^r)$ be the classical modular curve over $\mathbb{Q}$. Let $X_0^+(p^r)$ be its quotient by the Atkin-Lehner involution. We say that a point of $X_0^+(p^r)(\mathbb{C})$ is *trivial* if it is a cusp, or if the underlying elliptic curves have complex multiplication. In this article, we state a criterion to check whether $X_0^+(p^r)(\mathbb{Q})$ is trivial (Proposition 2.3). Then we prove that this criterion is verified if p satisfies some congruences. Explicitly, set $\mathcal{A} :=$ {primes which are simultaneously a square mod 3, mod 4, mod 7, and a square mod at least five of the following: 8, 11, 19, 43, 67, 163}. Our main theorem is the following:

Theorem 1.1 *If p^r is a prime power such that $p \geq 11$, $p \notin \{13, 37\}$, and p does not belong to the above set $\mathcal{A}$, then $X_0^+(p^r)(\mathbb{Q})$ is trivial.*

This applies in particular to the modular curve $X_{\mathrm{split}}(p)$, which is isomorphic over $\mathbb{Q}$ to $X_0^+(p^2)$. This special result was our first motivation for this work, because of its relation with the following problem of Serre. Let E be an elliptic curve over a number field K without complex multiplication over $\overline{K}$. The Galois action induces a representation $\mathrm{Gal}(\overline{K}/K) \to GL(E[p]) \simeq GL_2(\mathbb{F}_p)$. In his famous article [25], Serre proved that there exists an integer C_E such that this representation is surjective if $p > C_E$. In the same paper, Serre asked if the integer C_E can be chosen to depend only on K, not on E (loc. cit., p. 299; see also [10], Introduction). This question boils down to determining whether the K-rational points of several modular curves of level p are trivial (in the above sense) for large enough p. These curves are $X_0(p)$, $X_{\mathrm{split}}(p)$, $X_{\mathrm{non-split}}(p)$, and maybe "exceptional" ones. The latter case (of exceptional curves) was ruled out by Serre (see [10], Introduction), and that $X_0(p)(\mathbb{Q})$ is made of cusps for $p > 163$ (and is trivial for $p > 37$) is a celebrated theorem of Mazur ([11]). In the case of $X_{\mathrm{split}}(p)$ and $X_{\mathrm{non-split}}(p)$, a new difficulty arises from the fact that elliptic curves over $\mathbb{Q}$ with complex multiplication always provide rational points on one of those two modular curves. From the above, our criterion for $X_{\mathrm{split}}(p)(\mathbb{Q})$ to be trivial (Proposition 2.3) is verified for $p \geq 11$, $p \notin \{13, 37\}$, that does not belong to the set $\mathcal{A}$.

The density of the p's in Theorem 1.1 is $(1 - 7.2^{-9}) \simeq 0,986...$ At the moment, we are unable to prevent a positive density of primes from escaping our methods, which use quadratic imaginary orders of trivial class number (as one guesses from the shape of $\mathcal{A}$). Still in Section 5 we indicate a procedure which could asymptotically improve this density. For general p, we also prove a quantitative result, giving explicit upper bounds for the number of non-trivial points in $X_0^+(p)(\mathbb{Q})$ (Theorem 6.1).

Our approach is based on the well-known method inaugurated by Mazur. We also make use of previous works by Momose on $X_0^+(p^r)(\mathbb{Q})$, Kolyvagin-Logachev's (or now, Kato's) theorem on the Birch and Swinnerton-Dyer conjecture, and a recent application by Merel of the graph method for $X_0(p)$ of Mestre and Oesterlé. Our criterion is in fact almost the same as Merel in [13], Proposition 4, which arose in a different context. A new tool we use is a formula of Gross, generalized by Zhang, on special values of L-functions, which allows us to describe the cotangent space of J_e (conjecturally the largest quotient of $J_0(p)$ having trivial rank on $\mathbb{Q}$) in terms of Heegner points (Proposition 4.2).

More precisely, the text is organized as follows. In Section 2, we reduce our problem to a question on $X_0(p)$'s special fiber. In Section 3, we give our criterion (Propositions 3.1 and 3.2). Section 4 concentrates on J_e's cotangent space in order to reformulate our criterion thanks to Gross formula. In the fifth section we restrict to primes satisfying the congruences of Theorem 1.1 and make an application of the graph method to build special elements making the criterion work. Finally, in Section 6 we prove our quantitative improvement (Theorem 6.1), we describe an algorithm to verify triviality of $X_0^+(p^r)(\mathbb{Q})$ for any specified prime p, and we discuss the example of $X_0^+(37^r)$. In the course of the article, we also give new elementary proofs of a result, by Ahlgren and Ono, on Weierstrass points of $X_0(p)(\overline{\mathbb{Q}})$ (Theorem 3.3), and of an equidistribution theorem for Heegner points of Vatsal (Theorem 4.3).

I am grateful to Emmanuel Kowalski for providing me the results of analytic number theory which are used in Section 6.

2 Reducing to $X_0(p)$'s bad fiber

For any positive integer N, recall that $X_0(N)$ is the modular curve over $\mathbb{Q}$ corresponding to the congruence subgroup $\Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}), c \equiv 0 \mod N\}$. This curve deprived from its cusps is the coarse moduli space over $\mathbb{Q}$ of the isomorphism classes of elliptic curves equipped with a N-isogeny. If $M|N$, we write $\pi_{N,M}\colon X_0(N) \to X_0(M)$ for the degeneracy morphism which is defined functorially as $(E, C_N) \mapsto (E, C_M)$, where $C_M := E[M] \cap C_N$. In this paper, the model of $X_0(N)$ over $\mathbb{Z}$ that we consider is the *modular* one, which is obtained by taking the normalization of $\mathbb{P}^1_{\mathbb{Z}}$ in $X_0(N)_{\mathbb{Q}}$ via the morphism $\pi_{N,1}\colon X_0(N) \to X_0(1) \simeq \mathbb{P}^1$. Models over arbitrary schemes of these modular curves will be deduced by base change. If M is a divisor of N such that M and N/M are relatively prime, we write w_M for the corresponding Atkin-Lehner involution, and $X_0^+(N) := X_0(N)/w_N$. As usual, we write $J_0(N)$ for the jacobian over $\mathbb{Q}$ of $X_0(N)$, and $J_0^-(N) := J_0(N)/(1+w_N)J_0(N)$. Models for abelian varieties will be Néron models.

One defines similarly the curve $X_{\mathrm{sp.C.}}(N)$ associated to the split Cartan subgroup $\Gamma_{\mathrm{sp.C.}}(N) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}), \gamma \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \mod N\}$, and the curve $X_{\mathrm{split}}(N)$ corresponding to the normalizer of the above group: $\Gamma_{\mathrm{split}}(N) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}), \gamma \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \text{ or } \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right) \mod N\}$. The curve $X_{\mathrm{sp.C.}}(N)$ (respectively, $X_{\mathrm{split}}(N)$) parametrizes elliptic curves endowed with an ordered (respectively, unordered) pair of independent N-isogenies. There is an involution w on $X_{\mathrm{sp.C.}}(N)$ defined functorially by $(E, (A, B)) \mapsto (E, (B, A))$, such that $X_{\mathrm{split}}(N) = X_{\mathrm{sp.C.}}(N)/w$. The map $z \mapsto Nz$ on the upper half-plane induces $\mathbb{Q}$-isomorphisms $X_0(N^2) \simeq X_{\mathrm{sp.C.}}(N)$ (an "exotic" map in the language and

Katz and Mazur) and $X_{\rm split}(N) \simeq X_0(N^2)/w_{N^2}$.

We now fix a prime power p^r, $r > 1$. Let P be a point in $X_0^+(p^r)(\mathbb{Q})$ and $z \in X_0(p^r)(K)$ a lifting of P, for K a quadratic number field (or $\mathbb{Q}$, but this is possible only for $p \leq 163$ by Mazur's theorem). The point z corresponds to a couple (E, C_{p^r}) over K, by [5], Proposition VI.3.2. Set $\pi := \pi_{p^r,p}$, $x := w_p\pi(z)$ and $x_0 := \pi w_{p^r}(z) \in X_0(p)(K)$. Let $y \in J_0^-(p)(K)$ be the image of the divisor class of $(x) - (x_0)$ in $J_0(p)(K)$.

Lemma 2.1 *The point y comes from an element of $J_0^-(p)(\mathbb{Q})$.*

Proof. This is a straightforward calculation: if σ is the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$, then

$$\begin{aligned} \mathrm{cl}(y - \sigma(y)) &= \mathrm{cl}((w_p\pi(z)) - (\pi w_{p^r}(z)) - (w_p\pi w_{p^r}(z)) + (\pi(z))) \\ &= (1 + w_p)\mathrm{cl}((\pi(z)) - (\pi w_{p^r}(z))). \end{aligned}$$

□

In the following, we will also need the next result.

Lemma 2.2 (Momose) *If P belongs to $X_0^+(p^r)(\mathbb{Q})$, with $r > 1$ and $p \geq 7$, then the isogeny class of elliptic curves corresponding to P is not supersingular at p.*

Proof. This is Lemma 2.2 (ii) together with Theorem 3.2 of [18]. □

What has been done so far will allow us to reduce to the bad fiber of the smooth part $X_0(p)_{\mathbb{Z}}^{\rm sm}$ of $X_0(p)_{\mathbb{Z}}$, which we now look closer.

3 Using the graph method

Denote by S the set of supersingular invariants of elliptic curves in characteristic p, and by Δ_S the group of divisors of degree 0 with support on S. Let $\mathbb{T}$ be the subring of $\mathrm{End}(J_0(p))$ generated by the Hecke operators. The group Δ_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 p of $X_0(p)$ (see e.g. [23]). The $\mathbb{T} \otimes \mathbb{Q}$-module $\Delta_S \otimes \mathbb{Q}$ is free of rank one ([15], [14]). We can identify Δ_S, as a $\mathbb{T}$-module, with the character group of the neutral component of the fiber at p of the Néron model of $J_0(p)_{\mathbb{Q}}$, as in [15] (see also [13], section 1.4). More precisely, if $\mathcal{O}$ is the ring of integers of an extension of $\mathbb{Q}_p$, the zero-component of the special fiber of $J_0(p)$ on $\mathcal{O}$ is a (possibly trivial) quadratic twist of the torus $(\mathbb{G}_m^S/\mathbb{G}_m)$, where the latter quotient is relative to the diagonal morphism $\mathbb{G}_m \to \mathbb{G}_m^S$. Note that if $\mathcal{O}$ is ramified, the Néron model over $\mathcal{O}$ of $J_0(p)_K$ is not the base change of $J_0(p)_{\mathbb{Z}}$; however the zero components of these two schemes are canonically isomorphic, as they both represent the neutral component of the Picard functor, according to a theorem of Raynaud ([23], Théorème 2). We also remark that Δ_S can be interpreted as a cotangent space (see Remark 1 below).

If F is a number field or a p-adic field with ring of integers $\mathcal{O}_F$, and P is a F-rational point of $X_0(p)$, denote by ϕ_P the morphism from $X_0(p)_F$ to $J_0(p)_F$ which maps Q to $(Q-P)$. If P is ordinary above p, we consider the canonical extension of ϕ_P from $X_0(p)^{\mathrm{sm}}_{\mathcal{O}_F}$ to $J_0(p)_{\mathcal{O}_F}$. One sees from the above that ϕ_P may be explicitly described in any special fiber at k above p: if Q and P specialize to the same component at k, then

$$\phi_P(Q)_{\overline{k}} = (\frac{j_E - j_Q}{j_E - j_P})_{j_E \in S} \in (\mathbb{G}_m^S/\mathbb{G}_m)(\overline{k}).$$

Define the winding quotient $J_e = J_0(p)/I_e J_0(p)$ as in [12]. Denote by Φ_P the morphism obtained by composing ϕ_P with the surjection $J_0(p) \to J_e$, and extend Φ_P from $X_0(p)^{\mathrm{sm}}_{/\mathcal{O}_F}$ to J_e's Néron model on $\mathcal{O}_F$.

Proposition 3.1 *Let p^r be a power of a prime $p \geq 11$ with $r > 1$. If, for every P in $X_0(p)^{\mathrm{sm}}(\mathbb{Z}_p)$, the morphism Φ_P is a formal immersion at $P(\mathrm{Spec}(\mathbb{F}_p))$, then $X_0^+(p^r)(\mathbb{Q})$ is trivial.*

Proof. Suppose one has a non-cuspidal point in $X_0^+(p^r)(\mathbb{Q})$. As in previous section, let $z \in X_0(p^r)(K)$ be one of its liftings (for K a quadratic field), $x := w_p \pi_{p^r,p}(z)$ and $x_0 := \pi_{p^r,p} w_{p^r}(z) \in X_0(p)(K)$. Lemma 2.2 gives us that x and x_0 extend to points of $X_0(p)^{\mathrm{sm}}(\mathcal{O}_K)$.

Let k be a residue field of K above p. We claim that x and x_0 specialize to the same element of $X_0(p)^{\mathrm{sm}}(k)$. Indeed, if z corresponds to (E, C_{p^r}), then x and x_0 correspond to $(E/C_p, E[p]/C_p)$ and $(E/C_{p^r}, E[p]+C_{p^r}/C_{p^r})$ respectively. The isogenies associated to the specializations at k of these points are both either radicial or étale, hence x_k and x_{0k} belong to the same component. Moreover the j-invariants of the two associated curves are conjugated by a power of Frobenius. Now [18], Theorem 3.2, says that p splits in K. Therefore $x_k = x_{0k}$.

As J_e is a quotient of $J_0^-(p)$, Lemma 2.1 says that $\Phi_{x_0}(x)$ comes from an element of $J_e(\mathbb{Q})$, which must have finite order by the Kolyvagin-Logachev theorem ([9]). As $\Phi_{x_0}(x)_k = 0_k$ and $p > 2$, a well-known specialization lemma tells us that $\Phi_{x_0}(x) = 0$. The hypothesis that Φ_{x_0} be a formal immersion at x_{0k} implies that $x = x_0$. Therefore the underlying elliptic curve has a non-trivial endomorphism. $\square$

Now for the criterion:

Proposition 3.2 *Assume $p > 2$. Let P be an element of $X_0(p)^{\mathrm{sm}}(\mathbb{Z}_p)$, with j-invariant $j_0 \mod p$. Suppose that there exists $v = (v_E)_{j_E \in S}$ in $\Delta_S[I_e]$ such that $\sum_{j_E \in S} \frac{v_E}{(j_0 - j_E)} \neq 0 \mod p$. Then the morphism Φ_P of 3.1 is a formal immersion at $P(\mathrm{Spec}(\mathbb{F}_p))$.*

Note that this is very close to [13], Proposition 4. The slight difference is that our maps Φ_P go to a quotient of $J_0(p)$, not a subvariety.

Proof. We will show that the map induced by $\Phi_{P_{\mathbb{F}_p}}$ on cotangent spaces (at $0_{\mathbb{F}_p}$ and $P_{\mathbb{F}_p}$ respectively) is nonzero. We first identify $P_{\mathbb{F}_p}$'s component with $(\mathbb{P}^1 \backslash S)$ via j-invariant.

We claim that the natural morphism: $\mathrm{Cot}(J_{e\mathbb{Z}_p}) \to \mathrm{Cot}(J_0(p)_{\mathbb{Z}_p})$ identifies $\mathrm{Cot}(J_{e\mathbb{Z}_p})$ with $\mathrm{Cot}(J_0(p)_{\mathbb{Z}_p})[I_e]$. Indeed, from the exact sequence: $0 \to I_e.J_0(p)_{\mathbb{Q}} \to J_0(p)_{\mathbb{Q}} \to J_{e\mathbb{Q}} \to 0$, one deduces a sequence of free $\mathbb{Z}_p$-modules of finite rank:

$$0 \to \mathrm{Cot}(J_{e\mathbb{Z}_p}) \to \mathrm{Cot}(J_0(p)_{\mathbb{Z}_p}) \to \mathrm{Cot}(I_e.J_0(p)_{\mathbb{Z}_p}) \to 0$$

which is exact (this comes form a theorem of Raynaud (see [11], Corollary 1.1), since $J_0(p)_{\mathbb{Z}}$ is semi-stable). At the generic fiber, $\mathrm{Cot}(J_{e\mathbb{Q}_p}) \simeq \mathrm{Cot}(J_0(p)_{\mathbb{Q}_p})[I_e]$ (see for instance [21], Proposition 4.10), therefore this isomorphism remains true on $\mathbb{Z}_p$. This is our claim.

As $J_0(p)_{\mathbb{Z}_p}$ has purely toric reduction, one has $\Delta_S \otimes \overline{\mathbb{F}}_p \simeq \mathrm{Cot}(J_0(p)_{\overline{\mathbb{F}}_p})$, and the above reads $\Delta_S[I_e] \otimes \overline{\mathbb{F}}_p \simeq \mathrm{Cot}(J_{e\overline{\mathbb{F}}_p})$. Let $\omega \in \mathrm{Cot}(J_{e\overline{\mathbb{F}}_p})$ be the invariant differential associated to the element v of the proposition. By hypothesis, the pull-back $\Phi^*_{P_{\overline{\mathbb{F}}_p}}(\omega) = \sum_{j_E \in S} \frac{v_E}{(j - j_E)} dj$ is non-zero at j_0. $\square$

Remark 1 In [13], Proposition 4, Δ_S was interpreted as a character group, while we here make use of cotangent space interpretation: denoting by Δ_e the character group of J_e^0, we have isomorphisms $\Delta_e \otimes \overline{\mathbb{F}}_p \simeq \mathrm{Cot}(J_{e\overline{\mathbb{F}}_p})$ and $\Delta_S \otimes \overline{\mathbb{F}}_p \simeq \mathrm{Cot}(J_0(p)_{\overline{\mathbb{F}}_p})$, as we already remarked. Using uniformization results for the purely toric varieties $J_0(p)_{\mathbb{Z}_p}$ and $J_{e\mathbb{Z}_p}$ one can actually prove that those isomorphisms at the special fiber remain true *globally*: if

$\mathcal{O}$ is the ring of integers of the unramified quadratic extension of $\mathbb{Q}_p$, then $\mathrm{Cot}(J_0(p)_{\mathcal{O}}) \simeq \Delta_S \otimes \mathcal{O}$, and similarly $\mathrm{Cot}(J_{e\mathcal{O}}) \simeq \Delta_e \otimes \mathcal{O} = \Delta_S[I_e] \otimes \mathcal{O}$ (see for instance [15], section 1.4.5).

Remark 2 Propositions 3.1 and 3.2 already imply that, if $J_0(p)^-$ has rank 0 over $\mathbb{Q}$ (and if there are at least two supersingular invariants j_1, j_2 in $\mathbb{F}_p$, which is true as soon as $\mathbb{Q}(\sqrt{-p})$ has class number at least 3), then $X_0^+(p^r)(\mathbb{Q})$ is trivial (see Lemma 5.1: one can take $v = [j_1] - [j_2]$). Thus we find a (slightly) different proof of Momose's main result ([18], Theorem 3.6). The limitation of this statement is that the condition on $J_0(p)^-(\mathbb{Q})$ is not true when p is too large, so Momose's result concerns a finite number of primes only. On the other hand, comparing dimensions of cotangent spaces described as rational functions spaces as in the proof of Proposition 3.2, one sees that a basis of $\mathrm{Cot}(J_{e\overline{\mathbb{Q}}_p})$ can have at most $\dim(J_0(p)) - \dim(J_e) := n$ common zeros. Using Lemma 4.2 of [17], one recovers the quantitative version of Momose's theorem ([18], Theorem 3.7): n is an upper bound for the number of non-trivial rational points of $X_0^+(p^r)(\mathbb{Q})$ (note that we use J_e instead of the Eisenstein quotient). In Section 6, we will improve such bounds.

Remark 3 We note in passing the following by-product of the above:

Theorem 3.3 *The Weierstrass points in $X_0(p)(\overline{\mathbb{Q}})$ are potentially supersingular in characteristic p.*

In [20], Ogg proved that the Weierstrass points of $X_0(p)(\mathbb{Q})$ are supersingular, and recently Ahlgren and Ono obtained the same result for $X_0(p)(\overline{\mathbb{Q}})$ (Theorem 1 of [1]). Actually their result is much more precise than ours, but their proof relies on involved computations on modular functions, whereas the following is elementary.

Proof. Call $j_0, \ldots, j_g$ the supersingular invariants in characteristic p (assuming $g \geq 2$ of course). Let $\mathcal{O}$ be the ring of integers of the quadratic unramified extension of $\mathbb{Q}_p$. Set $\omega_i := [1/(j-j_i) - 1/(j-j_0)]dj$. According to Remark 1, by lifting the ω_i's one obtains a basis of $S_2(\Gamma_0(p))_{\mathcal{O}}$. One readily computes that the Wronskian of the ω_i's is $W(j) = c\det(1/(j-j_k)^i - 1/(j-j_0)^i)_{1\leq i,k\leq g} = c\prod_{k>i}(1/(j-j_k)-1/(j-j_i))$, with $c = (-1)^{E(g/2)}(\prod_{k=1}^{g-1} k!) \neq 0$ mod p. This proves the proposition for non-cuspidal points, and a change of variable shows that cusps are not Weierstrass points neither. $\square$

4 Heegner points description of $\mathrm{Cot}_0(J_{e\mathbb{Q}_p})$

For studying formal immersion properties as above, we need to understand J_e's cotangent space at 0. It happens that this space can be entirely described in terms of Heegner points, thanks to a formula of Gross on special values of L-functions.

We first briefly recall some elements of the arithmetic of quaternion algebras underlying Gross' theory (see [6], [2], or [26], and references therein). If M is a $\mathbb{Z}$-module, define $\hat{M} := M \otimes \hat{\mathbb{Z}}$. Let B be the quaternion algebra over $\mathbb{Q}$ which is ramified precisely at p and ∞. Choose a maximal order R of B, and let $\{R_1 := R, ..., R_n\}$ be a set of maximal orders in B corresponding to representatives for $\mathrm{Cl}(B) = \hat{R}^* \backslash \hat{B}^* / B^*$ as in [6], Section 3: to a double coset $g := (g_2, g_3, \dots, g_l, \dots)$ we associate the B^*-conjugation class of the maximal order $B \cap g^{-1}\hat{R}g$. Recall that $\mathrm{Cl}(B)$ is in one-to-one correspondence with the set of supersingular invariants of elliptic curves in characteristic p: the order R_i associated to an invariant j_{E_i} is such that $R_i \simeq \mathrm{End}_{\mathbb{F}_{p^2}}(E_i)$.

If L is a quadratic number field, it embeds in B if and only if its localization at ramification primes for B is a field, *i.e.* L is a quadratic imaginary field in which p is inert or ramified. 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), let $u(-D) := \mathrm{card}(\mathcal{O}_{-D}^*/\langle \pm 1 \rangle)$, and $h_i(-D)$ be the number of optimal embeddings of $\mathcal{O}_{-D}$ in R_i modulo conjugation by R_i^*. We define the element[1] :

$$e_D := \frac{1}{2u(-D)} \sum_{i=1}^{n} h_i(-D)[R_i].$$

We consider e_D as an element of $\frac{1}{12}\mathbb{Z}^S$. If $(x_E)_{E \in S}$ is the canonical basis of $\mathbb{Q}^S$, and $w_E := \mathrm{card}(\mathrm{End}_{\overline{\mathbb{F}}_p}(E)^*/\langle \pm 1 \rangle)$, one defines a scalar product $\langle ., . \rangle$ on $\mathbb{Q}^S$ by $\langle x_E, x_{E'} \rangle = w_E . \delta_{j_E, j'_E}$ (where δ is the Kronecker symbol). The Hecke correspondences induce linear operators of $\mathbb{Z}^S$ which are self-adjoint for this product. The Eisenstein vector Eis, with coordinates $(1/w_E)_{E \in S}$ in the canonical basis, spans the orthogonal complement to $\Delta_S \otimes \mathbb{Q}$. As

[1] This element was improperly defined in [22], Section 3. The mistake came from a misinterpretation of the notations of [6], p. 167 (e_D is **not** "*the class of the divisor c_D of 3.8*" when $-D$ is not a fundamental discriminant). This did not affect our results anyway.

its name promises, Eis is an eigenvector for the Hecke endomorphism T_l with eigenvalue $l+1$ for any prime $l \neq p$. The restriction of the Hecke endomorphisms on $\Delta_S \otimes \mathbb{Q}$ gives its $\mathbb{T}$-module structure.

Now let f be a newform of weight 2 for $\Gamma_0(p)$. If $-D$ is a quadratic imaginary discriminant as above, we write ε_D for the non-trivial quadratic character associated to $\mathbb{Q}(\sqrt{-D})$, and $f \otimes \varepsilon_D$ for the twist of f by ε_D. Let $(\Delta_S \otimes \overline{\mathbb{Q}})^f$ be the $\mathbb{T}_{\overline{\mathbb{Q}}}$-eigenspace associated to f, let $e_{f,D}$ be the component of e_D on $(\Delta_S \otimes \overline{\mathbb{Q}})^f$, and write $(.,.)$ for the Petersson product. Extend $\langle .,. \rangle$ to $\overline{\mathbb{Q}}^S$ by bilinearity. Gross' formula which is of interest to us here is the following.

Theorem 4.1 **(Gross**, *generalized by* **Zhang)** *If D is prime to p, one has*

$$L(f,1)L(f \otimes \varepsilon_D, 1) = \frac{(f,f)}{\sqrt{D}} \langle e_{f,D}, e_{f,D} \rangle.$$

Proof. In [6], Corollary 11.6, the formula is proven for prime discriminants. A more general form can be found in [3], Theorem 1.1, and the above statement comes from [27], Theorem 1.3.2, or [28], Theorem 7.1. □

Proposition 4.2 *Set $A := \{$prime-to-p imaginary quadratic discriminants$\}$. Let $\mathcal{E}$ be the $\mathbb{Q}$-vector subspace of $\Delta_S \otimes \mathbb{Q}$ spanned by the orthogonal projections (relatively to $\langle \cdot, \cdot \rangle$) of the elements e_D, for $D \in A$. Then $\mathcal{E} = (\Delta_S[I_e] \otimes \mathbb{Q})$.*

Proof. If x is an element of $\overline{\mathbb{Q}}^S$, write $\overline{x}$ for the orthogonal projection of x on $\Delta \otimes \overline{\mathbb{Q}}$ with respect to $\langle \cdot, \cdot \rangle$. We first claim that $\mathcal{E}$ is a $\mathbb{T}_{\mathbb{Q}}$-submodule of $\Delta_S \otimes \mathbb{Q}$, which is generated by the $\overline{e_l}$'s with $-l$ running through the fundamental imaginary quadratic discriminants which are prime to p. For $-D \in A$, $q \neq p$ a prime, and $n \geq 1$, a formula of [2], paragraph 2.4 provides the induction relation $\overline{e}_{q^{n+2}D} = T_q.\overline{e}_{q^{n+1}D} - q.\overline{e}_{q^n D}$. Together with the other formulae on the "behaviour under norms" of Heegner points in loc. cit., this gives our claim.

In order to prove $\mathcal{E} = (\Delta_S[I_e] \otimes \mathbb{Q})$, we may tensorize both sides of this equality with $\overline{\mathbb{Q}}$. Let f be a newform of weight 2 for $\Gamma_0(p)$. Gross-Zhang's formula implies that if $-D$ is a prime-to-p discriminant such that the component $e_{f,D}$ of e_D in $(\Delta_S \otimes \overline{\mathbb{Q}})^f$ is non-zero, then $L(f,1) \neq 0$. In that case, it follows from the definition of J_e that $I_e.f = 0$, so $I_e.e_{f,D} = 0$. This proves that $\mathcal{E} \otimes \overline{\mathbb{Q}}$ is included in $\Delta_S[I_e] \otimes \overline{\mathbb{Q}}$. For the reverse inclusion, we remark that for any newform f in $S_2(\Gamma_0(p))$, a (refinement of a) theorem of Waldspurger furnishes infinitely many prime-to-p D's such that $L(f\otimes\varepsilon_D,1)\neq 0$ (see [8]). Therefore if $L(f,1)\neq 0$, then $e_{f,D}\neq 0$, and we may choose an idempotent element t in $\mathbb{T}_{\overline{\mathbb{Q}}}$ such that $t.\overline{e_D}=e_{f,D}$. □

Remark 4 Before going further, we remark that the above furnishes an elementary proof of the following equidistribution results on Heegner points, which was first proved by Vatsal using arguments from graph theory (see [26], Theorem 1.5). We write $h_E(l^{2n}D)$ for the component of $e_{l^{2n}D}$ on the element $[R_E]$ of the set $S(\simeq \mathrm{Cl}(B))$ of supersingular primes in characteristic p, and we denote by $w(e_{l^{2n}D}) := \sum_{E\in S} h_E(l^{2n}D)$ and $w(\mathrm{Eis}) := \sum_{E\in S} 1/w_E(= (p-1)/12)$ the weight of $e_{l^{2n}D}$ and Eis, respectively.

Theorem 4.3 (Vatsal) *Let $-D$ be a fundamental quadratic imaginary discriminant such that $(\frac{-D}{p})\neq 1$. Let $l\neq p$ be a prime. Then $e_{l^{2n}D}$ is equidistributed as n tends to infinity, and more precisely*

$$\frac{1}{w(e_{l^{2n}D})}e_{l^{2n}D}=\frac{1}{w(\mathrm{Eis})}\mathrm{Eis}+O(l^{-n/2}).$$

Proof. From Eichler formula: $w(e_{l^{2n}D})=(1-\left(\frac{-l^{2n}D}{p}\right))h(-l^{2n}D)$ (see e.g. [6], p. 122), we find that $w(e_{l^{2n}D})$ is proportionnal to l^n. As in the proof of Proposition 4.2, one has the induction relation $\overline{e}_{l^{2(n+2)}D}=T_l.\overline{e}_{l^{2(n+1)}D}-l.\overline{e}_{l^{2n}D}$ (at least for $n\geq 1$). Decomposing $\overline{e}_{l^{2n}D}=\sum_f \nu_n(f)$ in $\Delta_S\otimes\overline{\mathbb{Q}}$ as a sum of eigenvectors for the Hecke algebra, the recursion relation shows that the weight of each $\nu_n(f)$ can be written as $\lambda_{D,f}.l^{n/2}\cos(n.\tau_f)$, for some real $\lambda_{D,f}$ and τ_f (recall that the polynomial $X^2-a_l(f)X+l$, where $a_l(f)$ is T_l's eigenvalue on f, is real). This completes the proof of the theorem. □

Notice that Ph. Michel proved another equidistribution result: if I is the set of *fundamental* quadratic imaginary orders, then again every sequence of e_D's, $D\in I$, tends to Eis as D increases (see [16], Theorem 10).

5 End of proof of Theorem 1.1

The results of previous section show that the v's of Proposition 3.2 can be exhibited as linear combinations, with weight zero, of Gross vectors e_D's. The following lemmas illustrate the simplest case of such v's.

Lemma 5.1 *If there exists v in the subspace $\mathcal{E}$ of Proposition 4.2 such that, in the canonical basis of $\mathbb{Q}^S$, v has exactly two non-zero components, then (a multiple of) v satisfies the hypothesis of Proposition 3.2 for every P in $X_0(p)^{\mathrm{sm}}(\mathbb{Z}_p)$.*

Proof. One may suppose that the two non-trivial components of v are ± 1, and the function $j \mapsto \sum_{j_E \in S} \frac{v_E}{(j_E - j)}$ is clearly nowhere zero on the relevant component of $X_0(p)(\overline{\mathbb{F}}_p)$'s ordinary locus. □

Lemma 5.2 *Suppose that p does not belong to the set $\mathcal{A}$ of Theorem 1.1, and $p > 997$. If p is not a square modulo l for some $l \in \{3, 4, 7\}$, set $v := e_{4l} - u(-l)e_l$. Else, if p is a non-square modulo two distinct elements q and r of $\{8,\ 11,\ 19,\ 43,\ 67,\ 163\}$, set $v := e_q - e_r$. Then v satisfies the conditions of Lemma 5.1.*

Proof. It is sufficient 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 non-zero. As in the proof of Theorem 4.3, Eichler formula gives that $\sum_{i=1}^{n} h_i(d)$ is equal to $(1 - \left(\frac{d}{p}\right))h(d)$ if p^2 does not divide d, and 0 if it does. The discriminants involved in the lemma all have class number one, so this formula implies that the support of v in S has zero or two elements (notice that if p is inert in $\mathcal{O}_d$, the factor $2 = (1 - \left(\frac{d}{p}\right))$ in Eichler formula corresponds to the fact that the optimal embeddings associated to $\mathcal{O}_d$ are "counted twice", one for each orientation. Note also 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 non-trivial. Each element of S 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 $\mathbb{Q}$ having complex multiplication by $\mathcal{O}$. The list of these thirteen invariants is well-known (see for instance [24]); if $p > 997$, they are all distinct mod p. □

End of proof of Theorem 1.1 If $p > 997$, we combine Proposition 3.1, Proposition 3.2, Lemma 5.1 and Lemma 5.2. If $11 \leq p \leq 997$, $p \notin \{13, 37\}$, one checks that one can still build a v, as in Lemma 5.2, making our method work. (Notice that the cases $p \leq 300$ follow from Theorem 0.1 of [18], apart from few possible exceptions (151, 199, 227, 277) which are easily ruled out by hand with our techniques.) □

6 Algorithm, upper bounds and example

We end by making some algorithmic and numerical remarks.

First, the above methods can clearly be extended to the case where p does belong to the set $\mathcal{A}$ of Theorem 1.1, i.e. p is inert in at most one quadratic imaginary order of class number one. Indeed, if δ is any integer, call E_δ the finite set of prime-to-p quadratic imaginary discriminants with class number at most δ. For $d \in E_\delta$, let $H_d(X) := \prod(X - j_{\mathcal{O}_d}) \in \mathbb{Z}[X]$ be the class polynomial, whose roots run through the singular moduli of elliptic curves with complex multiplication by $\mathcal{O}_d$. If there is no common root (in $\mathbb{C}$) to a certain set of polynomials $\mathcal{H}_{d_1,d_2} := h(d_1)H_{d_1}(X){H_{d_2}}'(X) - h(d_2){H_{d_1}}'(X)H_{d_2}(X)$, for some d_1's and d_2's in E_δ, then for large enough p, these polynomials have no common root mod p neither. For each δ, one may then look for a lower bound C_δ such that if $p \geq C_\delta$ and p satisfies appropriate congruences (asserting that p remains prime in sufficiently many orders with class number $\leq \delta$), then one can conclude that $X_0^+(p^r)(\mathbb{Q})$ is trivial, for any $r > 1$. This way, one could make the density of such "good" primes p growing, though of course this method will not lead to the conjectured optimal statement (i.e. Theorem 1.1 without congruences conditions).

On the other hand, given a *fixed* prime p, our methods obviously furnish an algorithm possibly - probably - showing the triviality of $X_0^+(p^r)(\mathbb{Q})$: one just have to look at allowed class polynomials. This algorithm is illustrated below with the curve $X_0^+(37^r)$ (in a case however where one can *not* conclude). We shall notice that in practice this algorithm is not easy to use because class polynomials, having huge coefficients, are hard to compute.

The above still has the following quantitative consequence.

Theorem 6.1 *For any $\varepsilon > 0$, there exists $K(\varepsilon) > 0$ such that, if $r > 1$ is an integer,*

$$\mathrm{card}(X_0^+(p^r)(\mathbb{Q})) < K(\varepsilon)p^{1/8+\varepsilon}.$$

Assuming the Riemann Hypothesis for Dirichlet L-functions, one obtains the bounds $\mathrm{card}(X_0^+(p^r)(\mathbb{Q})) \ll (\log p)^{1+\varepsilon}$.

Proof. Applying the techniques of [17], Section 4, for bounding the number of non-trivial rational points, we see that we need only determine an upper bound for the minimal number of roots of relevant polynomials $\mathcal{H}_{d_1,d_2}$ (see also Remark 2). So we look for small quadratic imaginary discriminants d_1, d_2 such that p is inert in $\mathcal{O}_{d_1}$ and $\mathcal{O}_{d_2}$. By Theorem 1.1 we may suppose

$p \equiv 1 \mod 4$. Proposition 6.3 below shows that, given $\varepsilon > 0$, there exists $C(\varepsilon) > 0$ and two fundamental discriminants d_1 and d_2 as above which are relatively prime and less than $C(\varepsilon)p^{1/4+\varepsilon}$. This means that for all $\varepsilon > 0$ there exists $K(\varepsilon)$ such that the degree of $\mathcal{H}_{d_1,d_2}$ is less than $K(\varepsilon)p^{1/8+\varepsilon}$, by the Brauer-Siegel theorem. Now the fact that $\mathcal{H}_{d_1,d_2}$ be non-zero mod p (if $p \gg 0$) follows from [7], Corollary 1.6.

Under the Riemann Hypothesis, the second assertion of Proposition 6.3 furnishes the other upper bound of the theorem. □

We finally illustrate these methods in the particular case $p = 37$. The curve $X_0(37)$ has been studied by many authors, including Momose in the context of our problem (see [17], paragraph 5). It has genus 2, and the supersingular polynomial in characteristic 37 is $(j-8)(j^2-6j-6)$. The "plus" and the "minus" parts of $S_2(\Gamma_0(37))$ are both non-trivial, so $\dim(J_e(37)) = 1$. Calling α and β the supersingular invariants in $\mathbb{F}_{37^2} \backslash \mathbb{F}_{37}$, we write $S = (8, \alpha, \beta)$. The class polynomials H_d's of degree 1 such that 37 is inert in $\mathcal{O}_d$ (for instance, $H_8(X) = X - 8000$) must all be congruent to $X - 8 \mod 37$ (and this can be readily checked). This gives $e_8 = (1, 0, 0)$ in $\mathbb{Q}^S$, ordering S as above. It is a general fact that the vector space in $\mathbb{Q}^S$ generated by the Gross vectors e_D's always contains the Eisenstein vector (indeed, this vector belongs to the closure of the space spanned by the e_D's, by the equidistribution results of Section 4). In the case of $X_0(37)$ this can also be directly checked from the fact that $H_{23}(X) = X^3 + 3491750.X^2 - 5151296875.X + 23375^3$ is congruent to $(X-8)(X^2-6X-6) \mod 37$, so $e_{23} = \mathrm{Eis} = (1, 1, 1)$ in $\mathbb{Q}^S$. Therefore the space $\mathcal{E}$ of Proposition 4.2 for $p = 37$ is generated by $3e_8 - e_{23} = (2, -1, -1)$, and

$$\omega_- := (\frac{2}{j-8} - \frac{1}{j-\alpha} - \frac{1}{j-\beta})dj = 10\frac{(j-6)}{(j-8)(j^2-6j-6)}dj$$

forms a basis of $\mathrm{Cot}(J_e(37)_{\mathbb{F}_{37}})$. Hence on each component of $X_0(37)^{\mathrm{sm}}_{\mathbb{F}_{37}}$, there is exactly one point at which the natural morphism to $J_e(37)_{\mathbb{F}_{37}}$ is not a formal immersion. All we can conclude about $X_0^+(37^r)(\mathbb{Q})$ is that it contains at most one non-trivial point. (Note that in [17], paragraph 5, Momose proves further results on $X_0^+(37^2)(\mathbb{Q})$.)

6.2 Appendix: a proposition of analytic number theory

The aim of this subsection is to briefly expose the results from analytic number theory which are used in the proof of Theorem 6.1. All the material here is an adaptation of a letter from E. Kowalski.

Proposition 6.3 *Let p be a prime number, $p \equiv 1 \mod 4$. For all $\varepsilon > 0$, there exists $C(\varepsilon) > 0$ and two fundamental quadratic imaginary discriminants $-d_1$ and $-d_2$, which are relatively prime, such that $\left(\frac{-d_1}{p}\right) = \left(\frac{-d_2}{p}\right) = -1$, and $d_1 < d_2 \leq C(\varepsilon)p^{(1/4)+\varepsilon}$.*

Assuming the Riemann Hypothesis for Dirichlet L-functions, there exists an absolute $C > 0$ and two different prime numbers l_1 and l_2, congruent to $3 \mod 4$, such that $\left(\frac{-l_1}{p}\right) = \left(\frac{-l_2}{p}\right) = -1$, and $l_1 < l_2 \leq C(\log p)^2$.

We shall give the proof of the first (unconditional) assertion only, which is a fairly straightforward consequence of the Burgess inequality for character sums [4], in the following form.

Lemma 6.4 *Let χ modulo q be a primitive character which is non-trivial, where q is cubefree. Given $\varepsilon > 0$, there exists $C_1(\varepsilon)$ and $\delta(\varepsilon) > 0$ such that, for all $x \geq q^{1/4+\varepsilon}$ and for all $y \leq x$, one has*

$$\Big|\sum_{n \leq y} \chi(n)\Big| \leq C_1(\varepsilon) x^{1-\delta(\varepsilon)}.$$

Proof of the lemma. According to [4], Theorem 2, for all integers $r \geq 1$ and for all $\varepsilon' > 0$ there exists $D(\varepsilon', r) > 0$ such that $\left|\sum_{n \leq y} \chi(n)\right| \leq D(\varepsilon', r) y^{1-1/r} q^{((r+1)/4r^2)+\varepsilon'} \leq D(\varepsilon', r) x^{1-1/r} q^{((r+1)/4r^2)+\varepsilon'}$. Given $\varepsilon > 0$, this shows that, if $x \geq q^{1/4+\varepsilon}$, taking r large enough and ε' small enough with respect to ε, one can choose $\delta(\varepsilon) > 0$ such that

$$x^{-1/r} q^{(r+1)/4r^2+\varepsilon'} \leq x^{-\delta(\varepsilon)},$$

whence the lemma. □

Proof of the proposition (first assertion). For $x \geq 1$, let $N(x)$ be the set of integers $d \leq x$ such that $\left(\frac{-d}{p}\right) = \left(\frac{d}{p}\right) = -1$. Let $M(x) = |N(x)|$. One has

$$M(x) = \frac{1}{2}\sum_{d\leq x}\Big(1 - \Big(\frac{d}{p}\Big)\Big),$$

assuming $x < p$ for simplicity. Fix $\varepsilon > 0$. From Lemma 6.4, there exists $C_1(\varepsilon)$ and $\delta(\varepsilon) > 0$ such that

$$\Big|\sum_{d\leq x}\Big(\frac{d}{p}\Big)\Big| \leq C_1(\varepsilon)x^{1-\delta(\varepsilon)}$$

if $x \geq p^{1/4+\varepsilon}$. Therefore

$$|M(x) - \tfrac{x}{2}| \leq C_2(\varepsilon)x^{1-\delta(\varepsilon)}.$$

Taking $x \geq p^{1/4+\varepsilon}$, $x^{\delta(\varepsilon)} > 4C_2(\varepsilon)$, and $x > 4$, one obtains $M(x) > 1$. Note that the preceeding conditions can be written $x \geq C_3(\varepsilon)p^{1/4+\varepsilon}$. Let ℓ be the smallest element of $N(x)$. It is necessarily prime by multiplicativity. If $\ell \equiv 3 \mod 4$, set $d_1 = \ell$, otherwise set $d_1 = 4\ell$: then $-d_1$ is a fundamental discriminant. Now let $N_3(x)$ be the subset of integers $d \in N(x)$ such that $d \equiv 3 \mod 4$ and d is prime to ℓ. Set $M_3(x) := |N_3(x)|$. If $N_3(x)$ is not empty, it clearly contains an element d_2 such that $-d_2$ is a fundamental discriminant. To complete the proof of the proposition it is therefore sufficient to show that $M_3(x) > 1$ if $x \gg p^{(1/4)+\varepsilon}$. One writes:

$$M_3(x) = \sum_{d\leq x,\,(d,\ell)=1} \frac{1}{4}\Big(\varepsilon_2(d) - \chi_4(d)\Big)\Big(1 - \Big(\frac{d}{p}\Big)\Big)$$

where ε_2 is the trivial character modulo 2 and χ_4 is the non-trivial character modulo 4. Using Möbius function, this reads:

$$M_3(x) = \sum_{e|\ell}\mu(e)\sum_{d\leq x/e}\frac{1}{4}\Big(\varepsilon_2(de) - \chi_4(de)\Big)\Big(1 - \Big(\frac{de}{p}\Big)\Big).$$

We estimate the four terms obtained by expanding the inner sum. The first one is

$$S_1 = \frac{1}{4}\sum_{e|\ell}\mu(e)\varepsilon_2(e)\sum_{d\leq x/e}\varepsilon_2(d) = \frac{x}{8}\Big(1 - \frac{\varepsilon_2(\ell)}{\ell}\Big) + O(1),$$

and the second one is

$$S_2 = -\frac{1}{4}\sum_{e|\ell}\mu(e)\chi_4(e)\sum_{d\le x/e}\chi_4(d) = O(1),$$

so

$$S_1 + S_2 = \frac{x}{8}\Big(1 - \frac{\varepsilon_2(\ell)}{\ell}\Big) + O(1).$$

The latter terms are

$$S_3 = -\frac{1}{4}\sum_{e|\ell}\mu(e)\varepsilon_2(e)\Big(\frac{e}{p}\Big)\sum_{d\le x/e}\varepsilon_2(d)\Big(\frac{d}{p}\Big),$$
$$S_4 = \frac{1}{4}\sum_{e|\ell}\mu(e)\chi_4(e)\Big(\frac{e}{p}\Big)\sum_{d\le x/e}\chi_4(d)\Big(\frac{d}{p}\Big).$$

Applying Lemma 6.4 again gives us

$$|S_3| + |S_4| \le C_4(\varepsilon)x^{1-\delta(\varepsilon)}$$

for $x \ge (4p)^{1/4+\varepsilon}$, and matching up those estimates one obtains the proof of the proposition. □

References

[1] *S. Ahlgren, K. Ono*, Weierstrass points on $X_0(p)$ and supersingular j-invariants, Math. Ann. **325** (2003), 355-368.

[2] *M. Bertolini, H. Darmon*, Heegner points on Mumford-Tate curves, Invent. Math. **126** (1996), 413-456.

[3] *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.

[4] *D.A. Burgess*, On character sums and L-series II, Proc. London Soc. (3) **13** (1963), 524-536.

[5] *P. Deligne, M. Rapoport*, Les schémas de modules de courbes elliptiques, Vol. II of the Proceedings of the International Summer School on modular functions, Antwerp (1972), LNM 349, Berlin-Heidelberg-New-York: Springer 1973.

[6] *B. Gross*, Heights and the special values of L-series, Canadian Math. Soc. Conference Proceedings **7**, Amer. Math. Soc., Providence (1987), 115-187.

[7] *B. Gross, D. Zagier*, On singular moduli, J. Reine Angew. Math. **355** n. **1** (1985), 11-29.

[8] *J. Hoffstein, W. Luo*, Nonvanishing of L-series and the combinatorial sieve, with an appendix by D. E. Rohrlich, Math. Res. Lett. **4** n. **2-3** (1997), 425-444.

[9] *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., Vol. **1**, number **5** (1990), 1229-1253.

[10] *B. Mazur*, Modular curves and the Eisenstein ideal, Publ. math. I.H.E.S. **47** (1977), 33-186.

[11] *B. Mazur*, Rational Isogenies of Prime Degree, Invent. Math. **44** (1978), 129-162.

[12] *L. Merel*, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math. **124** (1996), 437-449.

[13] *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** n. **1** (2001), 81-119.

[14] *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), 217-242.

[15] *J.-F. Mestre, J. Oesterlé*, Courbes elliptiques de conducteur premier, manuscript.

[16] *Ph. Michel*, The subconvexity problem for Rankin-Selberg L functions and Equidistribution of Heegner points, to appear in Ann. of Math.

[17] *F. Momose*, Rational points on the modular curves $X_{\mathrm{split}}(p)$, Compositio Math. **52** (1984), 115-137.

[18] *F. Momose*, Rational points on the modular curves $X_0^+(p^r)$, J. Fac. Sci. Univ. Tokyo, Sect. IA, Math. **33** (1986), 441-446.

[19] *F. Momose*, Rational points on the modular curves $X_0^+(N)$, J. Math. Soc. Japan, vol. **39** n. **2** (1987), 269-286.

[20] *A. Ogg*, On the Weierstrass points of $X_0(N)$, Illinois J. Math. **29** (1978), 31-35.

[21] *P. Parent*, Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, J. Reine Angew. Math. **506** (1999), 85-116.

[22] *P. Parent*, Triviality of $X_{\mathrm{split}}(N)(\mathbb{Q})$ for certain congruence classes of N, C. R. Acad. Sci. Paris, Ser. **I 336** (2003), 377-380.

[23] *M. Raynaud*, Jacobiennes des courbes modulaires et opérateurs de Hecke, Astérisque **196-197** (1991), 9-25.

[24] *J.-P. Serre*, Complex multiplication, *in* Algebraic Number Theory, J. W. S. Cassels and A. Frölich ed., Academic Press, 1967.

[25] *J.-P. Serre*, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259-331.

[26] *V. Vatsal*, Uniform distribution on Heegner points, Invent. Math., **148** (2002), n. **1** 1-46.

[27] *Sh.-W. Zhang*, Gross-Zagier formula for GL_2, Asian J. Math. **5** (2001), 183-290.

[28] *Sh.-W. Zhang*, Gross-Zagier formula for GL_2 II, preprint (2002).