Journal de Théorie des Nombres
de Bordeaux **15** (2003), 831–838

No 17-torsion on elliptic curves over cubic number fields

par Pierre PARENT

Résumé. On achève de dresser la liste des nombres premiers de torsion de courbes elliptiques sur les corps de nombres cubiques, en montrant que 17 n'en fait pas partie.

Abstract. We complete our previous determination of the torsion primes of elliptic curves over cubic number fields, by showing that 17 is not one of those.

1. Introduction

Consider, for d an integer, the set $S(d)$ of prime numbers p such that: there exists a number field K of degree d, an elliptic curve E over K, and a point P in $E(K)$ of order p. It is a well-known theorem of Mazur, Kamienny, Abramovich and Merel that $S(d)$ is finite for every d; moreover $S(1)$ and $S(2)$ are known. In [7], we tried to answer a question of Kamienny and Mazur by determining $S(3)$, and we proved $S(3) = \{2, 3, 5, 7, 11, 13$ and *may be* $17\}$. (Actually in *loc. cit.* we made for some p's the arithmetic assumption (called $(*)_p$ there) that $J_1(p)$'s winding quotient has rank 0 over $\mathbb{Q}$. This is now known to be true for every p, by Kato's almost published work ([5]).) We also proved that our techniques could not settle the case of 17. In this note, using elementary theory of formal groups as supplementary ingredient, we finally prove that 17 does not belong to $S(3)$ (Theorem 5.1).

I would like to thank Bas Edixhoven for many useful conversations, and Annie Goro for her insistance about 17.

2. Summary of known computations

We first summarize the methods and results already known. Suppose one has an elliptic curve on a cubic number field K endowed with a point of order 17 with values in K. In [7], following Mazur-Kamienny's method, we associate to these data a point $P = (p_1, p_2, p_3)$ in $X_1(17)^{(3)}(\mathbb{Z}[1/17])$ (symmetric power), such that the p_i's are generically non-cuspidal points,

Manuscrit reçu le 9 juillet 2001.

but P coincides in the fiber at 2 with a triplet of cusps P_0 in $X_1(17)^{(3)}$ above the cusp $3.\infty \in X_0(17)^{(3)}$. Then we consider the morphism F_{P_0}:

$$\begin{cases} X_1(17)^{(3)} & \to & J_1(17) & \to & J_1(17) \\ Q & \mapsto & Q - P_0 & \mapsto & t.(Q-P_0), \end{cases}$$

where t is an element of the Hecke algebra $\mathbb{T}_{\Gamma_1(17)}$ which kills the 2-torsion of $J_1(17)$. In order to derive a contradiction showing $17 \notin S(3)$, we would like to prove that for each such P_0, the above F_{P_0} is a formal immersion at the closed point $P_0(\mathbb{F}_2)$: indeed, this would imply $P = P_0$. The criterion for this formal immersion is the following (where T_n and $\langle d\rangle$ denote the n^{th} Hecke operator and d^{th} diamond operator respectively):

Proposition 2.1. *([7], Proposition 1.2) If there exists t as above such that the triplets:*

- $(t.T_1,\ t.T_2,\ t.T_3)$,
- $(t.T_1,\ t.\langle d\rangle,\ t.T_2)$, *and*
- $(t.T_1,\ t.\langle d_1\rangle,\ t.\langle d_2\rangle)$

are all $\mathbb{F}_2$-linearly independent in $\mathbb{T}_{\Gamma_1(17)} \otimes \mathbb{F}_2$ (with $1 < d, d_1, d_2 < 8$, and $d_1 < d_2$), then every morphism F_{P_0} as above is a formal immersion at $P_0(\mathbb{F}_2)$.

Recall ([7], 1.5 and 2.6) that triplets of Hecke operators $(\langle 1\rangle, \langle d_1\rangle, \langle d_2\rangle)$ here correspond to triplets of cusps with form $P_0 = p_1 + \langle d_1\rangle^{-1}p_1 + \langle d_2\rangle^{-1}p_1$; the triplets $(T_1, T_2, \langle d\rangle)$ correspond to $P_0 = 2p_1 + \langle d\rangle^{-1}p_1$; while (T_1, T_2, T_3) corresponds to $P_0 = 3p_1$. (The fact that we are working on *symmetric* products is the reason for the additive notations here.)

However we show in [7], 4.3, that some of the above triplets are *never* $\mathbb{F}_2$-independent. To be explicit, one has $\mathbb{T}_{\Gamma_1(17)} \simeq \mathbb{Z}[X]/(X-1)(X^4+1)$ (where the diamond operator $\langle 3\rangle$ is mapped to X), and if one takes as the above "t" for example the operator a_3 of [7], Proposition 1.8, one has (mod 2): $a_3.T_1 \equiv X^4+X^3+X^2+1$, $a_3.T_2 \equiv X^4+X^3$, $a_3.T_3 \equiv X^4+1$, $a_3.\langle 2\rangle \equiv X^4+X$, $a_3.\langle 3\rangle \equiv X^3+1$, $a_3.\langle 4\rangle \equiv X^4+X^3+X^2+1$, $a_3.\langle 5\rangle \equiv X^3+1$, $a_3.\langle 6\rangle \equiv X^4+X^2+X+1$, $a_3.\langle 7\rangle \equiv X^4+X^2+X+1$, $a_3.\langle 8\rangle \equiv X^4+X$. (Recall T_1 and $\langle 1\rangle$ are the identity morphism.) So one sees that the triplets which are *not* linearly independent among those we have to consider by Proposition 2.1 are precisely the $(a_3.t_1, a_3.t_2, a_3.t_3)$ with (t_1, t_2, t_3) equal to : $(T_1, T_2, \langle 4\rangle)$, $(\langle 1\rangle, \langle 2\rangle, \langle 4\rangle)$, $(\langle 1\rangle, \langle 2\rangle, \langle 8\rangle)$, $(\langle 1\rangle, \langle 3\rangle, \langle 4\rangle)$, $(\langle 1\rangle, \langle 3\rangle, \langle 5\rangle)$, $(\langle 1\rangle, \langle 4\rangle, \langle 5\rangle)$, $(\langle 1\rangle, \langle 4\rangle, \langle 6\rangle)$, $(\langle 1\rangle, \langle 4\rangle, \langle 7\rangle)$, $(\langle 1\rangle, \langle 4\rangle, \langle 8\rangle)$, $(\langle 1\rangle, \langle 6\rangle, \langle 7\rangle)$. Thus we have *a priori* 1+9 geometric situations to deal with. We can reduce that a little, because we may write a triplet $P_0 = p_1 + \langle d_1\rangle^{-1}p_1 + \langle d_2\rangle^{-1}p_1$ or $P_0 = p_2 + \langle d_1\rangle p_2 + \langle d_1.{d_2}^{-1}\rangle p_2$, or $P_0 = p_3 + \langle d_2\rangle p_3 + \langle d_2.{d_1}^{-1}\rangle p_3$ (here d^{-1} means the inverse class of d in $(\mathbb{F}_{17}^*)/(\pm 1)$). So the nine triplets above of shape $(\langle 1\rangle, \langle d_1\rangle, \langle d_2\rangle)$ actually correspond to three different geometric situations only - for each of which we will choose to consider the single triplet:

$(\langle 1\rangle, \langle 3\rangle, \langle 4\rangle)$, $(\langle 1\rangle, \langle 7\rangle, \langle 4\rangle)$ and $(\langle 1\rangle, \langle 8\rangle, \langle 4\rangle)$ respectively. Therefore, not forgetting the case "$(T_1, T_2, \langle 4\rangle)$", we are finally left with *four* geometric situations to deal with.

For each P_0 corresponding to one of those four situations, we now consider the morphisms f_{P_0}:

$$\begin{cases} X_1(17)^{(3)} & \rightarrow & J_1(17) \\ Q & \mapsto & Q - P_0. \end{cases}$$

Then [7], 1.5 implies that in order to show $17 \notin S(3)$ it is actually sufficient to prove the following two facts, for each f_{P_0}. First, this morphism is a formal immersion at $P_0(\mathbb{F}_2)$; and second, no non-cuspidal point of $X_1(17)^{(3)}(\mathbb{Z})$ is mapped by f_{P_0} to the non-trivial section of a μ_2-subscheme of $J_1(17)_{/\mathbb{Z}}$ (here μ_2 denotes the kernel of multiplication-by-two in $\mathbb{G}_{m/\mathbb{Z}}$). That each f_{P_0} is a formal immersion at $P_0(\mathbb{F}_2)$ is already proven in [7], 4.3. The verification of the second fact is the goal of what follows.

3. Description of $\widehat{\mathcal{O}}_{J_1(17),0_{\mathbb{F}_2}}$

Let R be a discrete valuation ring of characteristic 0, K its fraction field. Let X be a smooth, proper, absolutly connected curve over K, of genus g. Let J be its Jacobian. Suppose $\mathcal{X}$ is a smooth model over R for X, and denote by $\mathcal{J}$ the Néron model of J over R. Suppose there exists $P_1 = \sum p_i \in \mathcal{X}^{(g)}(R)$ and $F \in \mathrm{Spec}(R)$ such that the canonical morphism $f_{P_1} : \mathcal{X}^{(g)} \rightarrow \mathcal{J}$ mapping $Q = \sum Q_i$ to $\sum Q_i - p_i$ is a formal immersion at $P_1(F)$. Then clearly the morphism: $\hat{\mathcal{O}}_{\mathcal{J},0_F} \rightarrow \hat{\mathcal{O}}_{\mathcal{X}^{(g)},P_1(F)}$ induced by f_{P_1} is an isomorphism.

Now take a basis $\{\omega_i\}_{0\leq i\leq g-1}$ of invariant differentials on J. They induce invariant differentials for the formal group law $\mathcal{F}$ on $\hat{\mathcal{O}}_{J,0_F}$. If one knows their formal expansion in a set of formal parameters $\{x_i\}_{0\leq i\leq g-1}$, it is a classical result on finite dimensional formal groups over a zero-characteristic ring that integration of these differentials provides a *formal logarithm* (or *"transformer"* in Honda's terminology) for the formal group law $\mathcal{F}$ (see [2], Theorem 1, and 1.4, Definition). We summarize this discussion as:

Proposition 3.1. *With notation as above, suppose that the morphism $f_{P_1} : \mathcal{X}^{(g)} \rightarrow \mathcal{J}$ is a formal immersion at $P_1(F)$. Suppose moreover that the invariant differentials ω_i's on J are* adapted *to the formal parameters x_i's of $\hat{\mathcal{O}}_{\mathcal{X}^{(g)},P_1(F)}$,* i.e. *there exists $L \in (K[[x_i]])^g$ such that $L = (x_0, x_1, \ldots, x_{g-1}) +$ (higher other terms) and $dL = (f_{P_1}^*\omega_0, \ldots, f_{P_1}^*\omega_{g-1})$. Then as formal series one has: $\mathcal{F}(X,Y) = L^{-1}(L(X) + L(Y))$.*

We specialize these remarks to the case which is of interest to us. Take $P_1 := \sum_{0\leq k\leq 4} \langle 3\rangle^{-k}\infty \in X_1(17)^{(5)}(\mathbb{Z})$. In this case, one sees as in [7], 2.6 that the morphism f_{P_1} is a formal immersion at every $P_1(\mathbb{F}_l)$, $l \neq 17$ a prime. (This is because the elements $X^k, 0 \leq k \leq 4$ are obviously $\mathbb{F}_l$-linearly independent in $\mathbb{T}_{\Gamma_1(17)} \otimes \mathbb{F}_l$.) If q is the formal parameter $\exp(2i\pi\tau)$ of $X_1(17)$ at ∞, one gets a formal parameter $x_k := \langle 3^k \rangle^* q$ at $\langle 3 \rangle^{-k}\infty$, and a set $(x_0, \ldots, x_4)$ of parameters of $X_1(17)^{(5)}$ at P_1. This gives: $\hat{\mathcal{O}}_{X_1(17)^{(5)}, P_1(\mathbb{F}_l)} = \mathbb{Z}_l[[x_0, \ldots, x_4]]$, and this ring is in turn isomorphic *via* f_{P_1} to $\hat{\mathcal{O}}_{J_1(17), 0_{\mathbb{F}_l}}$. The module $H^0(X_1(17)_{/\mathbb{Z}_2}, \Omega_{X_1(17)_{/\mathbb{Z}_2}})$ is isomorphic to $\mathrm{Cot}_0(J_1(17)_{/\mathbb{Z}_2})$ (cotangent space at the 0-section), and this is the $\mathbb{Z}_2$-dual of the Hecke algebra. We recall $\mathbb{T}_{\Gamma_1(17)} \simeq \mathbb{Z}[X]/(X-1)(X^4+1)$; *via* this isomorphism, $\langle 3 \rangle$ is mapped to X, and T_2 is $-X^3+X^2-1$ (see [7], 4.3. These are the only computational data we will use below). Choose as a $\mathbb{Z}_2$-basis of the cotangent space the dual basis of $\{1, X, X^2, X^3, X^4\}$: call it $\{f_0, f_1, \ldots, f_4\}$. Denote by $\{\omega_0, \ldots, \omega_4\}$ the corresponding invariant differentials on $J_1(17)_{/\mathbb{Z}_2}$: for any integer m, if we write the m^{th} Hecke operator $T_m = \sum_{i=0}^4 a_i(T_m)X^i$ in $\mathbb{T}_{\Gamma_1(17)}$, the q-expansion at the cusp ∞ of the (pull-back on $X_1(17)_{/\mathbb{Z}}$ of the) chosen ω_i's are $f_P^*(\omega_i) = f_i dq = \sum_{n=1}^{\infty} a_i(T_n) q^n (dq/q)$. Hence the Fourier expansions at P_1 of these pull-backs on $X_1(17)^{(5)}_{/\mathbb{Z}_2}$ are

$$f_{P_1}^*(\omega_i) = \sum_{j=0}^{4} \sum_{n=1}^{+\infty} a_i(X^j T_n) x_j^n (dx_j/x_j).$$

It means that the ω_i's are adapted to our choice of formal parameters, and with the above data one readily computes that the formal logarithm associated to the x_i's is

$$\begin{aligned}\mathrm{Log}(x_0, \ldots, x_4) &= \sum_{n \geq 1} \frac{1}{n} \sum_{j=0}^{4} x_j^n (a_0(X^j.T_n), a_1(X^j.T_n), \ldots, a_4(X^j.T_n)) \\ &= (x_0, x_1, x_2, x_3, x_4) + \frac{1}{2}(-x_0^2 - x_2^2, -x_1^2 + x_2^2 - x_3^2, x_0^2 - x_2^2 + x_3^2 - x_4^2, \\ &\qquad -x_0^2 + x_1^2 - x_3^2 + x_4^2, -x_1^2 - x_4^2) + O(.^3)\end{aligned}$$

(where, now and then, "$O(.^n)$" means "terms of degree at least n"). Note that $(a_0(X^j.T_n), a_1(X^j.T_n), \ldots, a_4(X^j.T_n))$ is the row vector of the coordinates of the element $X^j.T_n$ with respect to the basis $\{1, X, \ldots, X^4\}$ of $\mathbb{T}_{\Gamma_1(17)}$. We will use this fact below.

Remark. Thanks to the work of Cartier, Honda, Deninger and Nart, one already knows a description of the formal groups over $\mathbb{Z}$ of $J_0(N)^{\text{new}}$ (or $J_1(N)^{\text{new}}$), given by (roughly speaking) a formal logarithm provided by "integration of L-series of the abelian variety, whose coefficients are the Hecke operators" (see [2], [1], and references therein). In our precise case, it gives exactly the same formal group law as ours. But Honda's proof is much more complicated than what we did, and anyway, it does not give explicit parameters to work with. Indeed his theorem only insures the existence of parameters for which the formal logarithm has the above shape, and this is not sufficient for our purpose as should be clear below.

4. Subschemes isomorphic to μ_2

We now use the above description of $J_1(17)$'s formal group at 2 to control its 2-torsion.

Proposition 4.1. *There are exactly two elements in* $\widehat{J_0(17)}(\mathbb{Z}_2)[2]$*, and two in* $\widehat{J_1(17)}(\mathbb{Z}_2)[2]$*. More precisely, choose as formal parameter on* $\widehat{J_0(17)}$ *the parameter at infinity* $q := \exp(2i\pi\tau)$ *on* $X_0(17)(= J_0(17))$*, and on* $\widehat{J_1(17)}$ *take the formal parameters* $(x_0, \dots, x_4)$ *of section 3. Then if* $q_0 \in 2.\mathbb{Z}_2$ *is* q*'s value for the non-trivial element of* $\widehat{J_0(17)}(\mathbb{Z}_2)[2]$*, then* $(q_0, 0, 0, 0, q_0)$ *is the non-trivial element of* $\widehat{J_1(17)}(\mathbb{Z}_2)[2]$*.*

Before showing this proposition we need the following elementary generalization of Hensel's lemma, whose proof we give for lack of references.

Lemma 4.2. *Let* R *be a complete discrete valuation ring with uniformizer* π*,* Q *an element of* R^N *for some integer* N*, and* $f : R^N \to R^N$ *an analytic map. Suppose that for an integer* $m \geq 0$ *one has:*

(1) $Df(Q) = \pi^m.\alpha$*, with* α *an element of* $\mathrm{GL}_N(R)$*, and*
(2) $f(Q) \equiv 0 \mod \pi^{2m+1}$.

Then there exists an unique q *in* R^N *such that* $q \equiv Q \mod \pi^{m+1}$ *and* $f(q) = 0$*.*

Proof of the lemma. Consider the following induction proposition, for $n \geq 2m+1$: "There exists q_n such that $q_n \equiv Q \mod \pi^{m+1}$ and $f(q_n) \equiv 0 \mod \pi^n$; such a q_n is unique $\mod \pi^{n-m}$". That it is true for $n = 2m+1$, taking $q_{2m+1} = Q$, comes from the hypotheses of the proposition. Assume it is true for $n \geq 2m+1$. Define $q_{n+1} = q_n + \pi^{n-m}\varepsilon_n$ for some ε_n in R^N. One writes the Taylor expansion:

$$\begin{aligned}
f(q_{n+1}) &= f(Q) + Df(Q)(q_{n+1}-Q) + \Delta_2 f(Q)(q_{n+1}-Q)^2 + \cdots + \\
&\quad + \Delta_n f(Q)(q_{n+1}-Q)^n \mod \pi^{n+1} \\
&= (f(Q) + Df(Q)(q_n - Q) + \Delta_2 f(Q)(q_n-Q)^2 + \cdots + \\
&\quad + \Delta_{n-1} f(Q)(q_n-Q)^{n-1}) \\
&\quad + Df(Q)(q_{n+1}-q_n) + \Delta_n f(Q)(q_n-Q)^n \mod \pi^{n+1} \\
&= \pi^n(A_n + \alpha.(\varepsilon_n) + (1/\pi^n)\Delta_n f(Q)(q_n-Q)^n) \mod \pi^{n+1},
\end{aligned}$$

where A_n is defined by the relation:

$$\pi^n A_n = f(Q) + Df(Q)(q_n - Q) + \cdots + \Delta_{(n-1)} f(Q)(q_n-Q)^{n-1},$$

using induction hypothesis. As α is supposed to be invertible, one gets from the above that there is an unique $\varepsilon_n \mod \pi$ such that $f(q_{n+1}) = 0 \mod \pi^{n+1}$. $\square$

Remark. It is elementary to deduce from the preceeding lemma that to detect p-torsion in a commutative finite dimensional formal group over a p-adic ring with ramification index e, it suffices to "compute the solutions" mod (π^{e+1}) which lift mod (π^{2e+1}).

Proof of the proposition. Recall $J_0(17)_{/\mathbb{Z}}$ is an elliptic curve, and the Fourier expansion of its newform is $(q - q^2 + O(q^3))(dq/q)$. Hence, following the preceeding section, one readily computes that the multiplication-by-two map in the formal group $\widehat{J_0(17)}$ is given by: $2 * q = 2q + q^2 + O(q^3)$. There is one non-trivial solution mod 4 of $2q + q^2 = 0 \mod 8$. Therefore lemma 4.2 insures us that this solution lifts, a unique way, to an element q_0 of $\mathbb{Z}_2$. (In this case we already knew that there is exactly one $\mathbb{Z}$-closed immersion $\mu_2 \hookrightarrow J_0(17)$, from classical results of Mazur ([6], III (1.1) & (1.3)).

In the same way, one computes that on $\widehat{J_1(17)}_{/\mathbb{Z}_2}$ one has:

$$2 * (x_0, x_1, x_2, x_3, x_4) = \begin{pmatrix} 2x_0 + x_0^2 + x_2^2 \\ 2x_1 + x_1^2 - x_2^2 + x_3^2 \\ 2x_2 - x_0^2 + x_2^2 - x_3^2 + x_4^2 \\ 2x_3 + x_0^2 - x_1^2 + x_3^2 - x_4^2 \\ 2x_4 + x_1^2 + x_4^2 \end{pmatrix} + O(.^3).$$

Let Q be a point of order 2 in $\widehat{J_1(17)}(\mathbb{Z}_2)$; the map "multiplication by 2 for the formal group law of $\widehat{J_1(17)}$", and Q, satisfy the hypothesis of the above lemma for $\mathbb{Z}_2$, $N = 5$ and $m = 1$, which implies moreover that Q is determined by its value mod 4. To determine the possible values mod 4 of points killed by 2 in the formal group, we just have to solve the equation $2 * (x_0, x_1, x_2, x_3, x_4) = 0 \mod 8$. There are two solutions (among those which are zero mod 2, of course): the trivial one and $(2, 0, 0, 0, 2) \mod 4$. Thus there is a unique non-trivial element of order 2 in $\widehat{J_1(17)}(\mathbb{Z}_2)$. *A fortiori*, there is at most one subscheme isomorphic to μ_2 of $J_1(17)/\mathbb{Z}$. (Actually, we will explain below (final remark) the reason for one can conclude that $J_1(17)_{/\mathbb{Z}}$ does not admit any closed subgroup scheme isomorphic to μ_2 at all.)

Now as we saw at the end of section 3, we have:

$$\begin{aligned} \mathrm{Log}(x, 0, 0, 0, x) &= \sum_{n \geq 1} \frac{1}{n} x^n \mathrm{coord.}((X^4 + 1).T_n) \\ &= \sum_{n \geq 1} \frac{x^n}{n} \mathrm{coord.}((X^4 + 1)((X - 1)Q_n + R_n)) \end{aligned}$$

where Q_n and R_n are respectively the quotient and the rest of the Euclidean division of T_n by $(X-1)$. The integer R_n is equal to the n^{th} Hecke operator in $\mathbb{T}_{\Gamma_0(17)}$, which we write T_n^0, and as $(X^4+1)(X-1)=0$ in $\mathbb{T}_{\Gamma_1(17)}$, we may rewrite the above equation as:

$$\begin{aligned}\operatorname{Log}(x,0,0,0,x) &= \sum_{n\geq 1}\frac{1}{n}T_n^0 x^n(1,0,0,0,1)\\ &= [\log_{J_0(17)}(x)](1,0,0,0,1)\end{aligned}$$

where $\log_{J_0(17)}$ denotes the formal logarithm of $\widehat{J_0(17)}$ associated to the parameter q. Writing $\oplus$ and $\tilde{+}$ for the formal group law of $\widehat{J_1(17)}$ and $\widehat{J_0(17)}$ respectively, and V for the vector $(1,0,0,0,1)$, one has:

$$\begin{aligned}(a,0,0,0,a)\oplus(b,0,0,0,b) &= \operatorname{Exp}((\log_{J_0(17)}(a)+\log_{J_0(17)}(b)).V)\\ &= \operatorname{Exp}(\log_{J_0(17)}(a\tilde{+}b).V)\\ &= (a\tilde{+}b,0,0,0,a\tilde{+}b).\end{aligned}$$

But we proved that there is a unique non-trivial q_0 in $\widehat{J_0(17)}(\mathbb{Z}_2)[2]$. Therefore the only non-trivial element of $\widehat{J_1(17)}(\mathbb{Z}_2)[2]$ is $(q_0,0,0,0,q_0)$. $\square$

5. End of proof

Theorem 5.1. *With notations of section 1, we have: $S(3)=\{2,3,5,7,11,13\}$.*

Proof. Recall from sections 1 and 2 that there are four situations to consider, which we called $(\langle 1\rangle,\langle 3\rangle,\langle 4\rangle)$, $(\langle 1\rangle,\langle 8\rangle,\langle 4\rangle)$, $(\langle 1\rangle,\langle 7\rangle,\langle 4\rangle)$, and $(T_1,T_2,\langle 4\rangle)$: we want to show that the morphism $f_{P_0}: X_1(17)^{(3)}\to J_1(17)$ corresponding to each situation does not map a non-cuspidal "point" (q_1,q_2,q_3) to the generator $(q_0,0,0,0,q_0)$ of $\widehat{J_1(17)}(\mathbb{Z}_2)[2]$.

From the previous section, we see that the morphism $\Phi: X_1(17)^{(2)}\to J_1(17)$, normalized such that $\infty+\langle 4\rangle^{-1}\infty$ is mapped to 0, sends the "point" (q_0,q_0) (with the same notations as in section 4, propositio 4.1) to the 2-torsion generator of $\widehat{J_1(17)}(\mathbb{Z}_2)$. Now one has a factorization:

$$\Phi: X_1(17)^{(2)}\xrightarrow{\Phi_{P_0}} X_1(17)^{(3)}\xrightarrow{f_{P_0}} J_1(17)$$

for each of the four f_{P_0}'s above, where $\Phi_{P_0}(Q_1+Q_2)=(Q_1+Q_2+P_i)$, with $P_i=\langle 3\rangle^{-1}\infty$, or $\langle 8\rangle^{-1}\infty$, or $\langle 7\rangle^{-1}\infty$, or ∞, respectively. As each f_{P_0} is a formal immersion at $(\Phi_{P_0}(P+\langle 4\rangle^{-1}P))(\mathbb{F}_2)$, one sees that $\Phi_{P_0}(q_0,q_0)$ is the only point of $\widehat{X_1(17)^{(3)}}(\mathbb{Z}_2)$ which is mapped to the 2-torsion generator of $\widehat{J_1(17)}(\mathbb{Z}_2)$, and clearly it is a cuspidal point (*i.e.* it does not come from a triplet of non-cuspidal points of the curve's generic fiber). Therefore it is not built by Mazur's method from an elliptic curve with a 17-torsion point over a cubic number field, as explained in section 2. □

Remark. As we noticed in section 4, the above implies that $J_1(17)$ has no μ_2-subscheme over $\mathbb{Z}$. Indeed, the curve $X_1(17)$ is not hyperelliptic over $\mathbb{C}$ ([3]), so one can check that the morphisms: $X_1(17)^{(2)} \to J_1(17)$ are closed immersions over ($\mathbb{C}$ hence over) $\mathbb{Q}$. Now the point of $X_1(17)^{(2)}(\mathbb{Z}_2)$ which is mapped to the non-trivial 2-torsion point of $J_1(17)(\mathbb{Z}_2)$ as above can not be rational, for Kamienny showed 17 does not belong to $S(2)$ (see [4]). Of course this provides an alternate (and somewhat indirect) end of proof that 17 does not belong to $S(3)$.

References

[1] C. Deninger, E. Nart, *Formal groups and L-series.* Comment. Math. Helvetici **65** (1990), 318–333.

[2] T. Honda, *On the theory of commutative formal groups.* J. Math. Soc. Japan **22** (1970), 213–246.

[3] N. Ishii, F. Momose, *Hyperelliptic modular curves.* Tsukuba J. Math. **15** *no.* **2** (1991), 413–423.

[4] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields.* Duke Math. J. **53** *no.* **1** (1986), 157–162.

[5] K. Kato, *p-adic Hodge theory and values of zeta-functions of modular forms.* To appear in Astérisque.

[6] B. Mazur, *Modular curves and the Eisenstein ideal.* Publications mathématiques de l'I.H.E.S. **47** (1977), 33–186.

[7] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques.* Ann. Inst. Fourier **50** (2000), 723–749.

Pierre Parent
A2X
UFR mathématiques et informatique
Université de Bordeaux 1
351, cours de la libération
33 405 Talence Cedex, France
E-mail : Pierre.Parent@math.u-bordeaux.fr