Normalizers of split Cartan subgroups and supersingular elliptic curves

Loïc Merel

1. Introduction

Let us recall the following theorem of J-P. Serre ([20], result (7)).

Theorem 1 (Serre [20]). — *Let E be an elliptic curve without complex multiplication over a number field K. There exists a number $B(E,K)$ such that for any prime number $p > B(E,K)$, the image $G_{E,p}$ of $\mathrm{Gal}(\bar{K}/K)$ in the group $\mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbf{F}_p)$ of automorphisms of the $\mathbf{F}_p$-vector space formed by the p-division points of E is $\mathrm{Aut}(E[p])$ itself.*

This is the major step to prove Serre's open image theorem for elliptic curves ([20], result (1)). An explicit version of Serre's theorem is given by D. Masser and G. Wüstholz [6](see also the work of F. Pellarin [17]).

Theorem 2 (Masser-Wüstholz [6]). — *There exist absolute constants c, $\gamma \in \mathbf{Z}$ such that if p does not divide the discriminant of K, and is larger than $c\max(\{d,h\})^\gamma$, where d is the absolute degree of K and h is the Weil height of E, then $G_{E,p} = \mathrm{Aut}(E[p])$.*

Serre asked in [20], 4.3. and in [21], p. 91 whether the number $B(E,K)$ occuring in the statement of theorem 1 can be chosen independently of E. As a specific question, does the statement above hold for $K = \mathbf{Q}$ and $B(E,\mathbf{Q}) = 37$?

It was well known in the 1970's that giving an affirmative answer to Serre's question amounts to show that the image of $G_{E,p}$ is not contained in one of the following maximal subgroups of $\mathrm{Aut}(E[p])$: a Borel subgroup, the normalizer of a split Cartan subgroup, or the normalizer of a nonsplit Cartan subgroup [20].

We consider only in this paper that $K = \mathbf{Q}$. B. Mazur proved in 1978 that the image of $G_{E,p}$ is not contained in a Borel subgroup when $p > 37$ [7]. His techniques formed the foundation of most of subsequent work on Serre's problem. For reasons explained in [10], they are difficult to apply to study normalizers of nonsplit Cartan subgroups.

We will concentrate here on the normalizer of split Cartan subgroup. Mazur proved in [8], when $p = 11$ or $p \geq 17$, that there are finitely many elliptic curves E (up to $\bar{\mathbf{Q}}$-isomorphism) over $\mathbf{Q}$ such that $G_{E,p}$ is contained the normalizer of a split Cartan subgroup

of $\mathrm{Aut}(E[p])$. Denote this number by n_p. Momose, in [14], gave a bound growing linearly in p for n_p.

The purpose of the present article is twofold: to report on the recent work of P. Parent and M. Rebolledo on the study of normalizer of Cartan subgroups and to improve mildly on this very work.

First, Parent shows that n_p is bounded sublinearly in p [16], theorem 6.1. We are more interested in showing that $n_p = 0$ for almost all prime numbers p. Parent was the first to show that $n_p = 0$ for infinitely many values of p. More precisely, he established a density statement, later improved by Rebolledo (in Parent's version the density is bounded by 7.2^{-9}).

THEOREM 3 (Parent [16], Rebolledo [19]). — *The set of prime numbers p such that $n_p \neq 0$ is of density $< 5.2^{-9}$.*

As one can imagine, this set is shown by Rebolledo to be contained in a set of prime numbers given by explicit congruences and of density 5.2^{-9} [19], theorem 0.12. As a corollary, Rebolledo shows that if $n_p > 0$ then $p \geq 1873$ or $p \leq 13$.

We would like to bring attention to a certain object emerging from Rebolledo's proof. Let p be prime number > 3. Let $\mathcal{S}$ be the set of isomorphism classes of supersingular elliptic curves in characteristic p. It is known to be a finite set of cardinality $g + 1$, where g is the genus of the modular curve $X_0(p)$. Denote by w_s ($= 1$, 2 or 3) and $j(s) \in \mathbf{F}_{p^2}$ half the number of automorphisms and the j-invariant respectively of a representative of s.

Consider now the q-expansion, with coefficients in $\mathbf{F}_{p^2}(J)$, given by

$$R = \frac{1}{2}\sum_{s\in\mathcal{S}} \frac{1}{w_s}\frac{1}{J - j(s)} + \sum_{n=1}^{\infty}\sum_{s\in\mathcal{S}} \frac{c_n(s)}{J - j(s)}q^n,$$

where $c_n(s)$ is given as follows. If one writes $n = n_0 p^a$, with n_0 integer prime to p, then $c_n(s)$ is the number of subgroups C of order n_0 in a representative E of s such that E/C is isomophic to E (resp. to the conjugate E^p of E by the Frobenius substitution) when a is even (resp. odd). Rebolledo (essentially) shows that it is the q-expansion of a modular form which is of weight 2, for the congruence subgroup $\Gamma_0(p)$ and is over the base $\mathbf{F}_p(J)$. We will denote this modular form by R and call it *Rebolledo's modular form.* In fact, Rebolledo considers only the cuspidal part of R. When j in a non-supersingular invariant in $\bar{\mathbf{F}}_p$, we denote by $R(j)$ the specialization of R at j.

THEOREM 4. — *If for all ordinary j-invariants in $\mathbf{F}_p$, one has $R(j) \neq 0$, then $n_p = 0$.*

Rebolledo's version of the previous theorem is slightly weaker: her hypothesis consists in the nonvanishing of the cuspidal part of $R(j)$. She proves theorem 3 by establishing the nonvanishing of one of the first seven coefficients of the cuspidal part of $R(j)$ for prime numbers p satisfying certain congruences. It is likely, and perhaps of little interest, that theorem 3 would be improved (*i.e.* the density mentioned in the statement of theorem

3 would be lowered) by studying a few more coefficients of the cuspidal part of R. The density occuring in the statement of theorem 3 can also be improved by applying theorem 4 and studying to the first seven coefficients of R itself (see section 5). In fact, the following strengthening of theorem 4 holds (see [16]and adapt the proof of proposition 6)): if for all ordinary j-invariants in $\mathbf{F}_p$, one has $R(j) \neq 0$, then the modular curve $Y_0^+(p^n) = Y_0(p^n)/W$, where W is the Atkin-Lehner involution and n is an integer > 1, has no non-CM $\mathbf{Q}$-rational point.

The minor improvements of the work of Rebolledo and Parent we propose in this article rely on two technicalities: the consideration of the generalized (with respect to the set of cusps) jacobians of modular curves and an improvement of an integrality statement of Mazur and Momose for the j-invariants of elliptic curves E over $\mathbf{Q}$ for which there exists a prime number $p > 13$ such that $G_{E,p}$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{Aut}(E[p])$.

We fix a prime number $p > 13$ in what follows.

I would like to thank Marusia Rebolledo for her attentive reading of this article.

2. The generalized jacobian of the modular curve $X_0(p)$

Let $X_0(p)$ be the modular curve which classifies coarsely generalized elliptic curves with a cyclic subgoup of order p. It possesses two cusps denoted by 0 and ∞. Let $J_0(p)$ be the jacobian variety of $X_0(p)$. It is endowed with the action of the Hecke algebra $\mathbf{T}$ (generated by the Hecke operators T_l, for l prime number $\neq p$ and the involution W_p).

Let $J_0^{\#}(p)$ be the generalized jacobian of $X_0(p)$ with respect to the set of cusps. It is a semi-abelian variety over $\mathbf{Q}$ which fits into the following exact sequence of semi-abelian varieties:

$$0 \longrightarrow T \longrightarrow J_0^{\#}(p) \longrightarrow J_0(p) \longrightarrow 0,$$

where T is a torus isomorphic to the multiplicative group. Since the Hecke correspondences T_l (l prime number $\neq p$) and the involution W_p on $X_0(p)$ leave stable the set of cusps, they define endomorphisms $T_l^{\#}$ and $W_p^{\#}$ of $J_0^{\#}(p)$. They generate a ring $\mathbf{T}^{\#}$ (which is isomorphic to the ring generated by Hecke operators acting on holomorphic modular forms of weight 2 for $\Gamma_0(p)$, and to the rings generated by Hecke operators acting on $\mathrm{H}_1(X_0(p), \mathit{cusps}; \mathbf{Z})$). One has a canonical ring homomorphism $\mathbf{T}^{\#} \to \mathbf{T}$. Let $\mathcal{I}^{\#}$ be the *Eisenstein ideal* of $\mathbf{T}^{\#}$. It is defined, for instance, as the annihilator of the Eisenstein series of weight 2 for $\Gamma_0(p)$ or equivalently as the annihilator of the class of the cuspidal divisor $(0) - (\infty)$. Alternately, it is generated by the operators $T_l^{\#} - (l+1)$ (l prime number) and $W_p + 1$. The kernel of the morphism $J_0^{\#}(p) \to J_0(p)$ is the identity component of $J_0(p)^{\#}[\mathcal{I}^{\#}]$.

When I is an ideal of $\mathbf{T}^{\#}$, one gets a quotient semi-abelian variety $J_0(p)^{\#}/IJ_0(p)^{\#}$. Denote by $IJ_0(p)$ the image in $J_0(p)$ of $IJ_0(p)^{\#}$.

Consider the modular symbol $\{0, \infty\} \in \mathrm{H}_1(X_0(p)(\mathbf{C}), \mathit{cusps}; \mathbf{Z})$. It is the *winding element* of $\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathit{cusps}; \mathbf{Z})$. (Its image e in $\mathrm{H}_1(X_0(p)(\mathbf{C}); \mathbf{R})$ is in fact in $\mathrm{H}_1(X_0(p)(\mathbf{C}); \mathbf{Q})$, by the Manin-Drinfeld theorem, and is the winding element introduced

by Mazur in [7].) Denote by $I_e^\#$ the annihilator in $\mathbf{T}^\#$ of $\{0,\infty\}$. Call the semi-abelian variety $J_e^\# = J_0(p)^\#/I_e^\# J_0(p)^\#$ the *winding quotient* of $J_0(p)^\#$.

Recall that the winding quotient J_e of $J_0(p)$ is by definition the quotient abelian variety $J_0(p)/I_e J_0(p)$, where I_e is the annihilator in $\mathbf{T}$ of the winding element $e \in \mathrm{H}_1(X_0(p)(\mathbf{C}); \mathbf{Q})$ [9].

PROPOSITION 1. — *1) The ideal $I_e^\#$ is contained in $\mathcal{I}^\#$.*
2) The image by the canonical surjective ring homomorphism $\mathbf{T}^\# \to \mathbf{T}$ of $I_e^\#$ is I_e.
Proof. — Let us write, as in [9], the modular symbol $\{0,\infty\}$ as $e+b$, where e is the winding element $e \in \mathrm{H}_1(X_0(p)(\mathbf{C}); \mathbf{Q})$ and $b \in \mathrm{H}_1(X_0(p), cusps; \mathbf{Q})$ is a nonzero rational multiple of the Eisenstein element. The action of $\mathbf{T}^\#$ on $\mathrm{H}_1(X_0(p); \mathbf{Q})$ factorizes through $\mathbf{T}$. Let $t^\# \in \mathbf{T}^\#$. Denote by t the image of $t^\#$ in $\mathbf{T}$. One has $t^\{0,\infty\} = 0$ if and only if $t^\# e = 0$ and $t^\# b = 0$. Those two conditions are equivalent to $te = 0$ and $t^\# \in \mathcal{I}^\#$ respectively.

PROPOSITION 2. — *The kernel of the composed morphism $T \to J_0(p)^\# \to J_e^\#$ is a finite group scheme.*
Proof. — It suffices to show that $I_e^\# J_0(p)^\# \cap J_0(p)^\#[\mathcal{I}^\#]$ is finite or, since $I_e^\#$ is contained in $\mathcal{I}^\#$ by proposition 1, that the group scheme $\mathcal{I}^\# J_0(p)^\# \cap J_0(p)^\#[\mathcal{I}^\#]$ is finite. This is indeed the case since $\mathbf{T}^\#$ acts faithfully on $J_0(p)^\#$ and is, after $\otimes\mathbf{Q}$, a semi-simple $\mathbf{Q}$-algebra.

Denote by $\mathcal{J}_e^\#$ the Néron model (locally of finite type) over $\mathbf{Z}$ of $J_e^\#$, whose existence is established, for instance by [1]chapter 10, proposition 7 and corollary 10. Let T_e be the image of T in $J_e^\#$. It is isomorphic to the multiplicative group by proposition 2. Its Néron model $\mathcal{T}_e$ over $\mathbf{Z}$ has identity component $\mathcal{T}_e^0$ isomorphic to the multiplicative group. Consider now the identity component ${\mathcal{J}_e^\#}^0$ of $\mathcal{J}_e^\#$ and the canonical morphism $\mathcal{T}_e^0 \to {\mathcal{J}_e^\#}^0$. (Remarks of B. Poonen and K. Ribet have helped correcting an earlier version of the following proposition.)

PROPOSITION 3. — *Any section $s :$ $\mathrm{Spec}(\mathbf{Z}) \to {\mathcal{J}_e^\#}^0$ of the structural morphism is of finite order.*
Proof. — By a theorem of Kolyvagin and Logachev, the winding quotient J_e of $J_0(p)$ has finitely many $\mathbf{Q}$-rational points [5], [9]. After multiplication by a suitable integer n, the image of s vanishes in the generic fiber of J_e. Therefore ns is a section $\mathrm{Spec}\,\mathbf{Z} \to \mathcal{T}_e$. The semi-abelian scheme ${\mathcal{J}_e^\#}^0$ meets finitely many, say m, components of $\mathcal{T}_e$, whose component group is torsion free. Therefore nms is a section $\mathrm{Spec}\,\mathbf{Z} \to \mathcal{T}_e^0$ Since $\mathcal{T}_e^0$ is isomorphic to the multiplicative group over $\mathbf{Z}$, it possesses at most 2 such sections. Therefore $2nms$ is the 0-section.

Recall that $\mathcal{S}$ is the set of isomorphism classes of supersingular elliptic curves in characteristic p. The group $\mathbf{Z}[\mathcal{S}]$ is called the *supersingular module* in [19]. It is endowed with an action of $\mathbf{T}^\#$ as follows. Let m be a positive integer not in $p\mathbf{Z}$. Set $T_m^\#[s] = \sum_C [s/C]$ (where C runs through the finite group subscheme of order m of a representative E of s and s/C is the class of E/C) and $W_p^\#[s] = -[s^{(p)}]$, where $s^{(p)}$ is the conjugate of s by the Frobenius substitution in $\mathrm{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p)$. The formula $T_{mp^a} = T_m(-W_p)^a$ gives

the action of the operator T_{mp^a} for a integer > 0. The subgroup $\mathbf{Z}[\mathcal{S}]^0$ of $\mathbf{Z}[\mathcal{S}]$ formed by elements of degree 0 is a $\mathbf{T}$-module compatible with the canonical map $\mathbf{T}^\# \to \mathbf{T}$.

Let $\mathcal{X}_0(p)$ be the normalization over the j-line of the ring of rational functions of $X_0(p)$. It is a scheme over $\mathrm{Spec}(\mathbf{Z})$ whose generic fiber is $X_0(p)$. Accordingly, the open affine subscheme obtained by deleting the cusps is denoted by $\mathcal{Y}_0(p)$. Let $\mathcal{Y}_0(p)^{\mathrm{smooth}}$ be the smooth locus of $\mathcal{Y}_0(p)$ (obtained by deleting the supersingular points in the special fiber at p).

Denote by $\mathcal{X}_0(p)_{\mathbf{F}_p}$ the special fiber at p of $\mathcal{X}_0(p)$. It consists in two irreducible components Γ_0 (which contains the cusp 0) and Γ_∞ (which contains the cusp ∞) which intersect at the supersingular points, which are in one to one correspondence with $\mathcal{S}$, and are both isomorphic to the projective line.

Let us recall the description of the Néron model $\mathcal{J}_0^\#(p)_{\mathbf{Z}_p}$ over $\mathbf{Z}_p$ of $J_0^\#(p)$. Its special fiber is the generalized jacobian of $\mathcal{X}_0(p)_{\mathbf{F}_p}$, with respect to the cusps. The identity component $(\mathcal{J}_0^\#(p)_{/\mathbf{F}_p})^0$ of its fiber at p is a torus whose character group is canonically isomorphic, as a $\mathbf{T}^\#$-module, to $\mathbf{Z}[\mathcal{S}]$ [2], 2.3. The corresponding isomorphism associates to $\lambda = \sum_{s\in\mathcal{S}} n_s[s] \in \mathbf{Z}[\mathcal{S}]$ the character χ_λ given by the following formula. Let $\tilde{D}$ in $(\mathcal{J}_0^\#(p)_{/\mathbf{F}_p})^0$ be the class of a divisor $D = D_0 + D_\infty = \sum_P c_P[P]$, where D_0 and D_∞ are of degree 0 and supported on Γ_0 and Γ_∞ respectively but away from $\mathcal{S}$ and the cusps. Then one has

$$\chi_\lambda(\tilde{D}) = \frac{\prod_{P\in\Gamma_\infty}\prod_{s\in\mathcal{S}}(j(P)-j(s))^{c_P n_s}}{\prod_{P\in\Gamma_0}\prod_{s\in\mathcal{S}}(j(P)-j(s))^{c_P n_s}}.$$

We take note of the structure of the cotangent space of $\mathcal{J}_0^\#(p)_{/\mathbf{F}_p}$ derived from this description. Denote by χ_s the character associated to $s \in \mathcal{S}$. The map $\mathbf{F}_p[\mathcal{S}] \to \mathrm{Cot}_0(\mathcal{J}_0^\#(p)_{/\mathbf{F}_p})$ which to $[s]$ associates $d\chi_s/\chi_s$ is an isomorphism of $\mathbf{T}^\#$-modules.

Let s_0 be a section $\mathrm{Spec}(\mathbf{Z}_p) \to \mathcal{Y}_0(p)^{\mathrm{smooth}}$. Denote by P_0 the $\mathbf{Q}_p$-rational point obtained by restriction to the generic fiber and $P_{0/\mathbf{F}_p}$ the $\mathbf{F}_p$-rational point obtained by restriction to the special fiber. Denote by j_0 the (necessarily ordinary and p-adically integral) j-invariant of $P_{0/\mathbf{F}_p}$. Consider the morphism, over $\mathbf{Q}_p$, of algebraic varieties $\phi_0 : Y_0(p) \to J_0^\#(p)$ which to P associates the class of the divisor $P - P_0$. It extends to a morphism over $\mathrm{Spec}(\mathbf{Z}_p)$, still denoted by ϕ: $\mathcal{Y}_0(p)^{\mathrm{smooth}} \to \mathcal{J}_0^\#(p)$. The modular function j provides a local parameter in the neighborhood of $P_{0/\mathbf{F}_p}$. Therefore dj is a basis of the cotangent space at $P_{0/\mathbf{F}_p}$ of $\mathcal{Y}_0/\mathbf{F}_p$.

PROPOSITION 4. — *Let $\lambda = \sum_{s\in\mathcal{S}} n_s[s] \in \mathbf{Z}[\mathcal{S}]$. Let $x = d\chi_\lambda/\chi_\lambda \in \mathrm{Cot}_0(\mathcal{J}_0^\#(p)_{/\mathbf{F}_p})$. If $P_{0/\mathbf{F}_p}$ belongs to Γ_∞, one has*

$$\mathrm{Cot}(\phi)(x) = \sum_{s\in\mathcal{S}} \frac{n_s}{j_0 - j(s)}\, dj.$$

The opposite of this formula holds when $P_{0/\mathbf{F}_p}$ belongs to Γ_0.

Proof. — Assume that $P_{0/\mathbf{F}_p}$ belongs to Γ_∞. Let $P_{/\mathbf{F}_p}$ be a $\bar{\mathbf{F}}_p$-rational point of Γ_∞ of j-invariant j. The following formula follows from the description of χ_λ:

$$\chi_\lambda((P_{0/\mathbf{F}_p}) - (P_{/\mathbf{F}_p})) = \frac{\prod_{s\in\mathcal{S}}(j - j(s))^{c_P n_s}}{\prod_{s\in\mathcal{S}}(j_0 - j(s))^{c_P n_s}},$$

which has to be inverted if $P_{0/\mathbf{F}_p}$ and $P_{/\mathbf{F}_p}$ belong to Γ_0. By differentiating logarithmically, one gets the desired formula.

We study now the restriction to the special fiber of the morphism ϕ_e, over $\mathbf{Z}_p$ obtained by composing ϕ with the canonical morphism $\mathcal{J}_0^{\#}(p)_{/\mathbf{Z}_p} \to \mathcal{J}_e^{\#}{}_{/\mathbf{Z}_p}$.

COROLLARY . — *If there exists* $\lambda = \sum_{s\in\mathcal{S}} n_s[s] \in \mathbf{Z}[\mathcal{S}]$ *such that (in* $\mathbf{Z}[\mathcal{S}]$*)*

$$I_e^{\#}\lambda = 0$$

and (in $\bar{\mathbf{F}}_p[\mathcal{S}]$*)*

$$\sum_{s\in\mathcal{S}} \frac{n_s}{j_0 - j(s)} \neq 0,$$

then ϕ_e *is a formal immersion at* $P_{0/\mathbf{F}_p}$.

Proof. — One simply needs to identify $\mathrm{Cot}_0(\mathcal{J}_e^{\#}{}_{/\mathbf{F}_p})$, by functoriality of the cotangent space, with the subspace of $\mathrm{Cot}_0(\mathcal{J}_0^{\#}(p)_{/\mathbf{F}_p})$ annihilated by $I_e^{\#}$, *i.e.* with $\mathbf{F}_p[\mathcal{S}][I_e^{\#}]$. For this, it is sufficient to establish that the exact sequence of semi-abelian varieties over $\mathbf{Q}_p$

$$0 \to I_e^{\#}J_0(p)^{\#} \to J_0(p)^{\#} \to J_0^{\#} \to 0$$

extended to the following sequence of Néron models over $\mathbf{Z}_p$

$$I_e^{\#}\mathcal{J}_0(p)^{\#}_{/\mathbf{Z}_p} \to \mathcal{J}_0(p)^{\#}_{/\mathbf{Z}_p} \to \mathcal{J}_e^{\#}{}_{/\mathbf{Z}_p}$$

gives then rise, by passing to the cotangent spaces along the zero-section, to the following exact sequence of free $\mathbf{Z}_p$-modules:

$$0 \to \mathrm{Cot}_0(\mathcal{J}_e^{\#}{}_{/\mathbf{Z}_p}) \to \mathrm{Cot}_0(\mathcal{J}_0(p)^{\#}_{/\mathbf{Z}_p}) \to \mathrm{Cot}_0(I_e^{\#}\mathcal{J}_0(p)^{\#}_{/\mathbf{Z}_p}) \to 0.$$

Noting that the semi-abelian varieties involved are semi-stable, we could proceed in a general way like the proof of Corollary 1.1 of proposition 1.3 in [8](which is based on proposition 1.1 of Raynaud which applies to semi-abelian varieties). We will content ourselves with arguments appropriate to our specific situation. It is enough to show that we have an exact sequence of finite flat group schemes over $\mathbf{Z}_p$

$$0 \to (I_e^{\#}\mathcal{J}_0^{\#}(p))_{/\mathbf{Z}_p}[p^n]^0 \to \mathcal{J}_0^{\#}(p)_{/\mathbf{Z}_p}[p^n]^0 \to \mathcal{J}_e^{\#}{}_{/\mathbf{Z}_p}[p^n]^0 \to 0,$$

where n is any integer > 0 and the superscript 0 indicates the identity component. By [8], proof of proposition 1.3 and application of proposition 1.1, if suffices to show that, for any integer $n \geq 0$ one has $J_0(p)^{\#}[p^n]^0 \cap (I_e^{\#}J_0(p)^{\#})[p^n] \subset (I_e^{\#}J_0(p)^{\#})[p^n]^0$. To show this, one notes that $T[p^n]$ is a direct factor as a group scheme in $J_0(p)^{\#}[p^n]$: since p is not an Eisenstein prime, one has $J_0(p)^{\#}[p^n] = T[p^n] \oplus (\mathcal{I}^{\#}J_0(p)^{\#})[p^n]$. Since $I_e^{\#}J_0(p)^{\#}$ is an abelian subvariety of the abelian variety $\mathcal{I}^{\#}J_0(p)^{\#}$ (proposition 1), proposition 1.3 of

[8]applies and $(\mathcal{I}^{\#}J_0(p)^{\#})[p^n]^0 \cap (I_e^{\#}J_0(p)^{\#})[p^n] = (I_e^{\#}J_0(p)^{\#})[p^n]^0$. It remains to establish the inclusion

$$(T[p^n]^0 \oplus (\mathcal{I}^{\#}J_0(p)^{\#})[p^n]^0) \cap (I_e^{\#}J_0(p)^{\#})[p^n] \subset (\mathcal{I}^{\#}J_0(p)^{\#})[p^n]^0 \cap (I_e^{\#}J_0(p)^{\#})[p^n].$$

Write $a \in (T[p^n]^0 \oplus (\mathcal{I}^{\#}J_0(p)^{\#})[p^n]^0) \cap (I_e^{\#}J_0(p)^{\#})[p^n]$ as $b + c$ where $b \in T[p^n]^0$ and $c \in (\mathcal{I}^{\#}J_0(p)^{\#})[p^n]^0$. Since $(I_e^{\#}J_0(p)^{\#})[p^n] \subset (\mathcal{I}^{\#}J_0(p)^{\#})[p^n]$, $b = a - c$ belongs to $(\mathcal{I}^{\#}J_0(p)^{\#})[p^n]$ whose intersection with $T[p^n]$ is trivial. Therefore $b = 0$ and $a \in (\mathcal{I}^{\#}J_0(p)^{\#})[p^n]^0$, which implies the desired inclusion.

The Eisenstein $\mathcal{E}$ element of $\mathbf{Q}[\mathcal{S}]$ is given by the formula

$$\mathcal{E} = \sum_{s \in \mathcal{S}} \frac{1}{w_s}[s].$$

It is of degree $(p-1)/12$ by Eichler's mass formula [3]and generate the $\mathbf{Q}$-line formed by the annihilator of $\mathcal{I}^{\#}$ in $\mathbf{Q}[\mathcal{S}]$. For $x \in \mathbf{Z}[\mathcal{S}]$ call $x^0 = x - \frac{12\deg(x)}{p-1}\mathcal{E} \in \mathbf{Q}[\mathcal{S}]$ the cuspidal projection of x.

PROPOSITION 5. — *One has $I_e^{\#}x = 0$ if and only if $I_e x^0 = 0$.*
Proof. — Since $I_e^{\#} \subset \mathcal{I}^{\#}$ and $\mathcal{I}^{\#}\mathcal{E} = 0$, one has $I_e^{\#}x = I_e^{\#}x^0 = I_e x^0$.

3. Integrality of the j-invariant

As an easy application of the techniques he invented to study the rational points of $X_0(p)$, Mazur proved in [8], corollary 4.8 the integrality away from 2, p and primes congruent to $\pm 1 \pmod p$ in theorem 5 below. This was extended to the integrality away from 2 by Momose in [14], proposition 3.1. Moreover Momose, relying on [7]has proved theorem 5 when $p \equiv 1 \pmod 8$ [14], corollary (3.6). We slightly improve on their work (without making any use of the generalized jacobian).

THEOREM 5. — *Let E be an elliptic curve over $\mathbf{Q}$ without complex multiplication Suppose that $G_{E,p}$ is contained the normalizer of a split Cartan subgroup of* $\mathrm{Aut}(E[p])$. *Then $j(E) \in \mathbf{Z}$.*
Proof. — We follow a standard approach. After Momose's work, it remains to establish the integrality of $j(E)$ at the prime 2. Suppose $j(E) \notin \mathbf{Z}$. Then E does not have potentially good reduction at 2. It does possess a $\mathbf{Q}$-rational pair $\{A, B\}$ of cyclic subgroups of order p.

Let us recapitulate the situation from the modular point of view (see [14], section 1 for details). Consider the modular curve $Y_{\mathrm{s}}(p)$ (resp. $Y_{\mathrm{s}}(p)^+$) over $\mathbf{Q}$ which classifies coarsely elliptic curves with an ordered pair (resp. a pair) (A, B) of cyclic subgroups of order p and $X_{\mathrm{s}}(p)$ (resp. $X_{\mathrm{s}}^+(p)$) the compactification of $Y_{\mathrm{s}}(p)$ (resp. $Y_{\mathrm{s}}(p)^+$)obtained by adding two (resp. one) $\mathbf{Q}$-rational cusps 0 and ∞ (resp. ∞) and $p-1$ (resp. $(p-1)/2$) cusps which are rational over the cyclotomic field $\mathbf{Q}(\mu_p)$ (resp. $\mathbf{Q}(\mu_p)^+$). The curve $X_{\mathrm{s}}(p)$

is a covering of degree 2 of $X_{\rm s}^+(p)$. The triple (E, A, B) defines a $\mathbf{Q}$-rational point P_0^+ of $X_{\rm s}^+(p)$ and therefore a K-rational point P_0 of $Y_{\rm s}(p)$, where K is a quadratic extension of $\mathbf{Q}$. The curve $X_{\rm s}(p)$ is isomorphic to $X_0(p^2)$; since $Y_0(p^2)(\mathbf{Q})$ consists of CM points for $p > 7$ [8], the point P_0 is not $\mathbf{Q}$-rational.

Let $\mathcal{X}_{\rm s}(p)$ (resp. $\mathcal{X}_{\rm s}(p)^+$) be the normalization over the projective j-line of $X_{\rm s}(p)$ (resp. $X_{\rm s}^+(p)$). It is a scheme over $\mathrm{Spec}\,(\mathbf{Z})$ whose generic fiber is $X_{\rm s}(p)$ (resp. $X_{\rm s}^+(p)$). The point P_0^+ extends to a section $s_0^+ : \mathrm{Spec}\,(\mathbf{Z}) \to \mathcal{X}_{\rm s}^+(p)$. The specialisation at 2 of s_0^+ is one of the cusps of $\mathcal{X}_{\rm s}^+(p)$, since $j(E)$ is not 2-integral. It is the cusp ∞ (since the residue field at any prime above 2 of $\mathbf{Q}(\mu_p)^+$ is of degree > 2 over $\mathbf{F}_2$).

Let W be the involution of $X_{\rm s}(p)$ defined by exchanging subgroups of order p. (It coincides with the Fricke involution when one identifies $X_{\rm s}(p)$ with $X_0(p^2)$.)

Consider now the morphism $g : X_{\rm s}(p) \to J_0(p)$ which to $P = (E, A, B)$ associates the class of the divisor $(E, A) - (E/B, E[p]/B)$. One has $g \circ W = -W_p g$. By the universal property of the Néron model, g extends to a morphism over $\mathrm{Spec}\,(\mathcal{O}_K)$: $\mathcal{X}_{\rm s}^{\rm smooth}(p) \to \mathcal{J}_0(p)$, which we still denote by g, where $\mathcal{X}_{\rm s}^{\rm smooth}(p)$ is the smooth locus of $\mathcal{X}_{\rm s}(p)$, which is obtained again by deleting the supersingular points in the special fiber at p [14]. The point P_0 extends to $\mathcal{X}_{\rm s}^{\rm smooth}(p)$ [14], (*i.e.* the elliptic curve E is not supersingular at p).

One get a K-rational point $g(P) - W_p g(P)$ of $J_0(p)$, which is in fact $\mathbf{Q}$-rational, since P_0 is not $\mathbf{Q}$-rational.

Our method diverges from from the ones employed by Mazur and Momose here. Instead of considering a quotient of $J_0(p)$, we consider an abelian subvariety.

In [7], theorem (2), Mazur has shown that the abelian variety $J_0(p)$ contains a subgroup isomorphic to μ_2 if and only if $p \equiv 1 \pmod 8$. This observation has enabled Momose to prove theorem 5, when $p \equiv 1 \pmod 8$. Curiously, in the case when p is not $\equiv 1 \pmod 8$, it provides also the key argument to prove the theorem.

Let $t \in \mathbf{T}$ such that $tI_e = 0$. Then the abelian variety $tJ_0(p)$ is isogenous to an abelian subvariety of the winding quotient of $J_0(p)$, therefore it has finitely many rational points (by a theorem of Kolyvagin and Logachev [5], more details can be found in [15]and [11]). Moreover, since $1 + W_p \in I_e$, the point $tg(P)$ is $\mathbf{Q}$-rational. Consequently, the point $tg(P_0)$ of $J_0(p)$ has finite order. When $p > 13$, one has $I_e \neq \mathbf{T}$ (see for instance [11], proposition 8) therefore one can find $t \neq 0$ such that $tI_e = 0$. Moreover t can be taken as 2-adically maximal, *i.e.* such that $t \notin 2\mathbf{T}$. Therefore, there exists $t \in \mathbf{T} - 2\mathbf{T}$ such that $tI_e = 0$.

Since $g \circ W = W_p \circ g$, the morphism g_t obtained by composing g with multiplication by t in $J_0(p)$ factorises through $X_{\rm s}^+(p)$. Denote by g_t^+ the morphism $X_{\rm s}^+ \to J_0(p)$ thus obtained. It satisfies $g_t(P_0) = g_t^+(P_0^+) = tg(P_0)$. By universal property of the Néron model, one gets a morphism over $\mathrm{Spec}\,(\mathbf{Z})$: $\mathcal{X}_{\rm s}^{+\rm smooth}(p) \to \mathcal{J}_0(p)$, which we still denote by g, where $\mathcal{X}_{\rm s}^{+\rm smooth}(p)$ is the smooth locus of $\mathcal{X}_{\rm s}^+(p)$.

Since s_0^+ and the ∞-section coincide in the fiber at 2 of $\mathcal{X}_{\rm s}^+(p)$, the points $tg(P_0)$ and $tg(\infty)$ extend to points in the Néron model $\mathcal{J}_0(N)$ of $J_0(N)$, which coincide in the fiber at 2. Therefore the point $tg(P_0) - tg(\infty)$ is of finite order in the generic fiber of $J_0(p)$ and vanishes in the fiber at 2. By a theorem of Raynaud [18], since the ramification index of $\mathbf{Q}_2$ over $\mathbf{Q}_2$ is $1 = 2 - 1$, the point $tg(P_0)$ is 0 in the generic fiber or is of order 2 and belongs to a subgroup isomorphic to μ_2. Our hypothesis that $p \equiv 1 \pmod 8$ makes the existence of such a subgroup impossible, as noted above. Hence, we have shown that

$g_t^+(P_0^+) = g_t^+(\infty)$. Since P_0^+ and ∞ coincide in the fiber at 2 of $X_{\mathrm{s}}^+(p)$, we derive that g_t^+ is not a formal immersion at the point ∞ in the fiber at 2 of $X_{\mathrm{s}}^+(p)$, *i.e* the cotangent map $\mathrm{Cot}(g_t^+)$ deduced from g_t^+ is not surjective.

This cotangent map has been described by Mazur [8], Lemma 2.1: using the theory of the Tate curve, one identifies, as a $\mathbf{T}$-module, $\mathrm{Cot}_{0_{\mathbf{F}_2}}(\mathcal{J}_0(p))$ with $\mathrm{Hom}(\mathbf{T}, \mathbf{F}_2)$ and $\mathrm{Cot}_{\infty_{\mathbf{F}_2}}(\mathcal{X}_{\mathrm{s}}(p))$ with $\mathbf{F}_2$ in such a way that $\mathrm{Cot}(g)(\psi) = \psi(T_1)$. Therefore one has $\mathrm{Cot}(g_t)(\psi) = \psi(t)$. Since $t \notin 2\mathbf{T}$, there exists $\psi \in \mathrm{Hom}(\mathbf{T}, \mathbf{F}_2)$ such that $\psi(t) \neq 0$. This establishes the surjectivity of $\mathrm{Cot}(g_t)$.

To obtain the surjectivity of $\mathrm{Cot}(g_t^+)$, one simply remarks that the cotangent map of the canonical morphism $\pi : \mathcal{X}_{\mathrm{s}}(p) \to \mathcal{X}_{\mathrm{s}}^+(p)$ is an isomorphism of $\mathbf{F}_2$-vector spaces at the point ∞ in the fiber at 2 [14], proof of proposition 2.5. Therefore, since $g_t = g_t^+ \circ \pi$, one gets the surjectivity of $\mathrm{Cot}(g_t^+)$.

Remarks. 1) Take note of the complementarity between the techniques of Mazur, which tend to show that $G_{E,p}$ is large when $j(E)$ is not integral and those of diophantine approximation, like those who give rise to the theorem of Masser-Wüstolz above, which deal typically with elliptic curves with integral j invariant.

2) It seems possible to treat the cases where $p \equiv 1 \pmod 8$ by the above method as well, without resorting to Momose's trick. One has to show that the point tP does not belong to a subgroup isomorphic to μ_2. For that one can make use of [7], chapter 3, proposition 4.2, to show that tP does not belong to such a group in the fiber at p of $\mathcal{J}_0(p)$ and therefore in the generic fiber.

4. Proof of theorem 3

The proofs of the theorems of Parent and Rebolledo use a slightly weaker form (which requires the element x below to belong to $\mathbf{Z}[\mathcal{S}]^0$) of the following statement (which is similar to conditions expressed and used in [11]and [12]).

PROPOSITION 6. — *Suppose that, for any ordinary j-invariant in $\mathbf{F}_p$, there exists $x = \sum_{s\in\mathcal{S}} n_s[s] \in \mathbf{Z}[\mathcal{S}]$ such that, in $\mathbf{Z}[\mathcal{S}]$,*

$$I_e^{\#} x = 0$$

and, in $\mathbf{F}_{p^2}[\mathcal{S}]$,

$$\sum_{s\in\mathcal{S}} \frac{n_s}{j - j(s)} \neq 0,$$

then $n_p = 0$.

Proof. — Let E be an elliptic curve over $\mathbf{Q}$ without complex multiplication. Suppose that $G_{E,p}$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{Aut}(E[p])$. Then E possesses a $\mathbf{Q}$-rational pair $\{A, B\}$ of cyclic subgroup of order p. By theorem 5, E has potentially good reduction everywhere, in particular at p. We know also, since $p > 7$, that the the groups A and B are K-rational, where K is a quadratic extension of $\mathbf{Q}$, without being $\mathbf{Q}$-rational. Let $\mathcal{O}_K$ be the ring of integers of K.

We use the basic setup of the proof of theorem 5, and proceed in a similar way, with a few differences: a) the fiber at p, and not the fiber at 2, of the modular curve will be the subject of our attention, b) the only modular curve that we will consider is $X_0(p)$ and c) we will make use of the generalized jacobian $J_0^{\#}(p)$ of $X_0(p)$.

The pairs (E, A) and $(E/B, E[p]/B)$ give rise to two K-rational points P_1 and P_2 of the modular curve $Y_0(p)$. Since $j(E) \in \mathbf{Z}$ (theorem 5), those points extend to sections $\mathrm{Spec}(\mathcal{O}_K) \to \mathcal{Y}_0(p)$. If $P_1 = P_2$, E has an endomorphism of degree p which necessarily comes from complex multiplication and a contradiction has been reached.

Momose provides the following informations: E has potentially good reduction at p, p splits in K and the the Néron models of the elliptic curves E and E/B, as well as the subgroups A et $E[p]/B$ coincide in the fibers at p [14], Lemma 1.3. Therefore the points P_1 and P_2 coincide in the special fiber at (a prime of K above) p of $\mathcal{Y}_0(p)$.

Consider the morphism $\phi^{\#}$: $Y_0(p) \to J_0^{\#}(p)$ which to P associates the class of the divisor $(P) - (P_1)$ and the canonical morphism $J_0^{\#}(p) \to J_e^{\#}$. Denote by $\phi_e^{\#}$ the composition of these morphisms. It extends to a morphism over $\mathrm{Spec}(\mathcal{O}_K)$, still denoted by $\phi_e^{\#}$: $\mathcal{Y}_0(p) \to \mathcal{J}_e^{\#}$, where $\mathcal{J}_e^{\#}$ is the Néron model of $J_e^{\#}$ over $\mathbf{Z}$.

The class of the divisor $(P_1)-(P_2)$ is *a priori* K-rational in $J_e^{\#}$. Since the involution W_p acts as -1 on $J_e^{\#}$ and exchanges P_1 and P_2 and since the nontrivial element of $\mathrm{Gal}(K/\mathbf{Q})$ exchanges P_1 and P_2, the image in $J_e^{\#}$ of the class of $(P_1) - (P_2)$ is $\mathbf{Q}$-rational, *i.e.* the image in $J_e^{\#}$ of $\phi^{\#}(P_1) - \phi^{\#}(P_2)$ is $\mathbf{Q}$-rational.

As noted above, the points P_1 and P_2 extend to sections $\mathrm{Spec}(\mathcal{O}_K) \to \mathcal{Y}_0(p)$. Therefore the class of the divisor $(P_1) - (P_2)$, as well as its image $\phi_e^{\#}(P_1) - \phi_e^{\#}(P_2)$ in ${\mathcal{J}_e^{\#}}^0$ extend to sections $\mathrm{Spec}(\mathcal{O}_K) \to {\mathcal{J}_0}^{\#}(p)$ belonging to the identity component (over $\mathcal{O}_K$). Since $\phi_e^{\#}(P_1) - \phi_e^{\#}(P_2)$ is $\mathbf{Q}$-rational and $\mathcal{J}_e^{\#}$ is a semi-stable semi-abelian variety, $\phi_e^{\#}(P_1) - \phi_e^{\#}(P_2)$ extends to a section $\mathrm{Spec}(\mathbf{Z}) \to {\mathcal{J}_e^{\#}}^0$. By application of proposition 3, it is of finite order in the generic fiber . In the special fiber at p, this section vanishes, therefore, since $p > 2$, it vanishes also in the generic fiber of $\mathcal{J}_e^{\#}$.

We have obtained the following two assertions: the element $\phi_e(P_1) - \phi_e(P_2)$ is zero and the points P_1 and P_2 coincide in the fiber at p of $\mathcal{Y}_0(p)$. By the argument of [8], corollary 4.3, at least one of the following two statements is true: (a) the morphism $\phi_e^{\#}$ is not a formal immersion at $\pi = P_{1/\mathbf{F}_p} = P_{2/\mathbf{F}_p}$ or (b) one has $P_1 = P_2$.

By the corollary of proposition 4, (which we apply after embedding the ring $\mathcal{O}_K$ in $\mathbf{Z}_p$) the hypotheses of the proposition imply that $\phi_e^{\#}$ is a formal immersion at π. We have to conclude that $P_1 = P_2$, a contradiction.

5. The formulas of Gross-Zhang and Gross-Kudla

Let us return to the first condition imposed on x in proposition 6. To maximize the odds that the second condition is satisfied, one would like to choose $x \in \mathbf{Z}[\mathcal{S}]$ such that x is an annihilator of $I_e^{\#}$ (and p-adically maximal). In the terminology used for elements in the homology group $\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathit{cusps}, \mathbf{Z})$, such an x could be called a winding element. In $\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathit{cusps}, \mathbf{Z})$, a winding element is given quite explicitly by the modular symbol $\{0, \infty\}$. This is why it seems natural to ask whether an element in $\mathbf{Z}[\mathcal{S}]$ whose

annihilator in $\mathbf{T}^{\#}$ is $I_e^{\#}$ can be explicitly expressed. I do not know any such expression for a winding element. The formulas of Gross-Zhang and Gross-Kudla provide infinite families of elements which satisfy the first condition of proposition 6, *i.e.* whose annihilator in $\mathbf{T}^{\#}$ contains $I_e^{\#}$.

Let us begin with the formula of Gross-Zhang. Let D be an integer > 0. Denote by $h(-D)$ the class number of the quadratic field $\mathbf{Q}(\sqrt{-D})$ and by $u(-D)$ half the number of units of the ring of integers $\mathcal{O}_{-D}$ of $\mathbf{Q}(\sqrt{-D})$. The maximal orders of the quaternion algebra ramified at ∞ and p coincide with the elements of $\mathcal{S}$: R_s contains the endomorphism ring (over $\bar{\mathbf{F}}_p$) of a representant of s. Denote them by $(R_s)_{s\in\mathcal{S}}$. For $s \in \mathcal{S}$, let $h_s(-D)$ be the number of embeddings of the ring $\mathcal{O}_{-D}$ in R_s.

$$e_D = \frac{1}{2u(-D)} \sum_{s\in\mathcal{S}} h_s(-D)[s] \in \mathbf{Z}[\frac{1}{6}][\mathcal{S}].$$

Recall that $\mathbf{Z}[\mathcal{S}]$ is endowed with a pairing $< .,. >$ given by $< s, s' >= 0$ except when $s = s'$, then $< s, s >= w_s$ (s, $s' \in \mathcal{S}$). The Hecke algebra is symmetric for this pairing.

THEOREM 6 (Gross [3], Zhang [22][23]). — *Let f be a newform of weight 2 for $\Gamma_0(p)$. Let χ_D be the quadratic character modulo D. One has*

$$L(f,1)L(f,\chi_D,1) = \frac{(f,f)}{\sqrt{D}} < \mathbf{1}_f e_D, \mathbf{1}_f e_D >$$

where $(.,.)$ is the Petersson scalar product, and where $\mathbf{1}_f$ is the idempotent of $\mathbf{T}\otimes\mathbf{C}$ such that $\mathbf{1}_f f = f$.

Denote by $e_D^0 \in \mathbf{Q}[\mathcal{S}]$ the cuspidal projection of e_D.

COROLLARY (Parent [16]). — *One has $I_e e_D^0 = 0$ (and therefore $I_e^{\#} e_D = 0$ in $\mathbf{Z}[\mathcal{S}]$).*

Parent proves his version of theorem 3 by studying $\iota_j(e_D^0)$ for a few values of D and showing that those values can not all be zero for p belonging to a set of prime numbers of density $1 - 7.2^{-9}$.

Let m be an integer > 0. Consider

$$y_m = \sum_{s\in\mathcal{S}} c_m(s)[s] \in \mathbf{Z}[\mathcal{S}]$$

where $c_m(s)$ is defined in the introduction.

Rebolledo observes $L(f,1)$ is a factor of $L(f\otimes h\otimes h, 2)$ when f and h are newforms. A precise expression due to Gross and Kudla relates the L-function of such triple product of newforms to $\mathbf{Z}[\mathcal{S}]$ [4].

Let

$$\Delta_3 = \sum_{s\in\mathcal{S}} \frac{1}{w_s}[s]^{\otimes 3} \in \mathbf{Q}[\mathcal{S}]^{\otimes 3}.$$

THEOREM 7 (Gross-Kudla [4]). — *Let f and h be newforms of weight 2 for $\Gamma_0(p)$. One has*

$$L(f,1)L(f\otimes \mathrm{Sym}^2 h,2)=\frac{(f\otimes h\otimes h, f\otimes h\otimes h)^{\otimes 3}}{4\pi p} < \mathbf{1}_f\otimes \mathbf{1}_h\otimes \mathbf{1}_h\Delta_3, \mathbf{1}_f\otimes \mathbf{1}_h\otimes \mathbf{1}_h\Delta_3 >^{\otimes 3}$$

where $(.,.)^{\otimes 3}$ is the tensor cube of the Petersson scalar product, and where $< .,. >^{\otimes 3}$ is the tensor cube of the pairing of $\mathbf{Z}[\mathcal{S}]$.

We remarked already that the pairing $< .,. >$ is a linear map on $\mathbf{Z}[\mathcal{S}]^{\otimes 2}$ which factorizes through $\mathbf{Z}[\mathcal{S}]^{\otimes_{\mathbf{T}} 2}$. Therefore it makes sense to compose a Hecke operator $T_m^{\#}$ with $< .,. >$ on $\mathbf{Z}[\mathcal{S}]^{\otimes 2}$. Rebolledo observes that

$$y_m = (1\otimes < .,. > \circ T_m^{\#})(\Delta_3)$$

and deduce the following from the formula of Gross and Kudla (where $y_m^0 \in \mathbf{Q}[\mathcal{S}]$ is the cuspidal part of y_m).

COROLLARY (Rebolledo [19]). — *One has $I_e y_m^0 = 0$ (and therefore $I_e^{\#} y_m = 0$ in $\mathbf{Z}[\mathcal{S}]$).*

In fact the elements considered by Parent and Rebolledo are related by a simple linear formula, which provides a second proof of the corollary of theorem 7 as a consequence of the corollary of theorem 6.

PROPOSITION 7 (Rebolledo [19]). — *One has*

$$y_m = \epsilon_m \mathcal{E} + \sum_{s,d,4m-s^2=dr^2} e_d,$$

where s and d run through the integers and where $\epsilon_m = 1$ if m is a square and $\epsilon_m = 0$ otherwise.

Let ι_J be the group homomorphism $\mathbf{Z}[\mathcal{S}] \to \mathbf{F}_{p^2}(J)$ given by the formula

$$\iota_J(\sum_{s\in\mathcal{S}} n_s[s]) = \sum_{s\in\mathcal{S}} \frac{n_s}{J-j(s)}.$$

For $j \in \bar{\mathbf{F}}_p$ distinct from all supersingular j-invariant, denote by $\iota_j(\sum_{s\in\mathcal{S}} n_s[s])$ the specialization at j of $\iota_J(\sum_{s\in\mathcal{S}} n_s[s])$.

Since $\iota_j(y_m)$ is the m-th coefficient of the series $R(j)$, theorem 4 follows from proposition 6, corollary of theorem 7 and proposition 5. Let us give an idea of the proof of theorem 3, and a bit more. In particular, one has $n_p = 0$ as soon as $\iota_j(y_2) \neq 0$.

A calculation of Mestre and Oesterlé gives

$$\iota_j(y_2) = \frac{a}{j-1728} + \frac{2b}{j+3375} + \frac{c}{j-8000},$$

where a, b, $c \in \{0,1\}$ and $a = 1$ (resp. $b = 1$, resp. $c = 1$) if and only if the prime number p is inert of ramified in the quadratic field $\mathbf{Q}(\sqrt{-1})$ (resp. $\mathbf{Q}(\sqrt{-7})$, resp. $\mathbf{Q}(\sqrt{-2})$) *i.e.* if and only if $p \equiv 3 \pmod 4$ (resp. $p \equiv 3$, 5 ou 6 $\pmod 7$, resp. $p \equiv 5$ ou 7 $\pmod 8$)) [13], [19]. Moreover, by studying the image by ι_j of a few elements of $\mathbf{Z}[\mathcal{S}]^0$ obtained as linear combinations of the e_D's, Parent shows that when p is not a square modulo 7 or 4 then the hypotheses of proposition 6 are satisfies [16]. The study of $\iota_j(y_2)$ improves this slightly by establishing that these hypotheses are satisfied when p is not congruent to 1 modulo 8. (This congruence is not in the list of congruences for p which imply that $n_p = 0$ obtained by Parent and Rebolledo, and therefore yields an improvement of theorem 3: for instance $n_{10333} = 0$.)

6. Rebolledo's modular form

We make first more precise a statement contained in Rebolledo's thesis.

Proposition 8 (Rebolledo [19]). — *The q-expansion*

$$\sum_{m=1}^{\infty} \iota_J(y_m) q^m$$

is, except for the constant term, the q-expansion of a modular form of weight two for $\Gamma_0(p)$ over $\mathbf{F}_p(J)$, which we call Rebolledo's modular form *and denote by R.*
Proof. — The element y_m is given as follows:

$$y_m = \sum_{s \in \mathcal{S}} \frac{1}{w_s} < s, T_m^{\#} s > [s] \in \mathbf{Z}[\frac{1}{6}][\mathcal{S}].$$

We adopt here the most naive definition for modular form (of weight 2 for $\Gamma_0(p)$) over a ring A: it is an element of the A-module obtained by extending the scalar to A from the $\mathbf{Z}$-module formed by holomorphic modular forms having integral q-expansion. Up to the constant term, the q-expansion $\sum_{m=1}^{\infty} a_m q^m$ are preciseley those for which there is a group homomorphisms ψ: $\mathbf{T}^{\#} \to A$ satisfying $\psi(T_m^{\#}) = a_m$ (m integer > 0).

There is a group homomorphism : $\mathbf{T}^{\#} \to \mathbf{F}_{p^2}(J)$ given by $\psi_j(t) = \iota_J(\sum_{s \in \mathcal{S}} < s, ts > [s])$. We observe that $(\sum_{s \in \mathcal{S}} < s, ts > [s])$ is anti-invariant by W_p, which implies that $\iota_J(\sum_{s \in \mathcal{S}} < s, ts > [s])$ is $\mathbf{F}_p$-rational. Therefore the q-expansion $\sum_{m=1}^{\infty} \psi_J(T_m^{\#}) q^m$ is, except for the constant term, the q-expansion of a modular form of weight two for $\Gamma_0(p)$ over $\mathbf{F}_p(J)$.

It is interesting to look at the constant term of the modular form R. It is given by the following formula. I am indebted to M. Rebolledo for having corrected me on the constant term of the formula. Note that she has established the formula independently by a different argument.

PROPOSITION 9. — *The constant term of the q-expansion of R is equal to*

$$\frac{1}{2}\iota_J(\mathcal{E}) = \frac{1}{2}\sum_{s\in\mathcal{S}} \frac{1}{w_s}\frac{1}{J-j(s)} \in \mathbf{F}_p(J).$$

Proof. — One has $y_m = y_m^0 + d_m\mathcal{E}$ in $\mathbf{Q}[\mathcal{S}]$, where d_m is the ratio of the degree of y_m by the degree of $\mathcal{E}$. By Eichler's mass formula [3], the degree of $\mathcal{E}$ is $(p-1)/12$.

Let R^0 (denoted by $\mathbf{g}_j$ in [19]) be the cusp form of weight 2 for $\Gamma_0(p)$ over $\mathbf{F}_{p^2}(J)$ given by the q-expansion

$$R^0 = \sum_{m=1}^{\infty} \iota_j(y_m^0)q^m.$$

Therefore one has

$$R = R^0 + \iota_J(\mathcal{E})T,$$

where T is the modular form whose m-th coefficient of the q-expansion is d_m. Since the degree of y_m is the trace of the Hecke operator $T_m^{\#}$ (operating on $\mathbf{Z}[\mathcal{S}]$), and since $T_m^{\#}$ acts as $\sigma_1^{(p)}(m)$ on $\mathbf{Z}[\mathcal{S}]/\mathbf{Z}[\mathcal{S}]^0$, one has

$$d_m = d_m^0 + \frac{12}{p-1}\sigma_1^{(p)}(m)$$

where $\sigma_1^{(p)}(m)$ is the sum of the divisors of m which are prime to p and where d_m^0 is the trace of T_m (operating on $\mathbf{Z}[\mathcal{S}]^0$) divided by the degree of $\mathcal{E}$.

Consider the Eisenstein series E of weight 2 for $\Gamma_0(p)$ given by the q-expansion

$$E = \frac{p-1}{24} + \sum_{m=1}^{\infty} \sigma_1^{(p)}(m)q^m$$

and the modular form

$$T^0 = \sum_{m=1}^{\infty} d_m^0 q^m.$$

Indeed T^0 is a cusp form since the trace is a linear form on $\mathbf{T}$. One has

$$R = R^0 + \iota_J(\mathcal{E})T^0 + \frac{12}{p-1}\iota_J(\mathcal{E})E.$$

Since R^0 and T^0 are cusp forms, the constant coefficient of R is equal to $\frac{12}{p-1}\iota_J(\mathcal{E})$ times the constant coefficient of E, *i.e.*

$$\frac{1}{2}\iota_J(\mathcal{E}) = \frac{1}{2}\iota_J(\sum_{s\in\mathcal{S}} \frac{1}{w_s}[s]) = \frac{1}{2}\sum_{s\in\mathcal{S}} \frac{1}{w_s}\frac{1}{J-j(s)}.$$

One derives a weak, but non-trivial, criterion for the nonvanishing of R, which is, as far as I know, of little use.

Corollary . — *If the rational function*

$$F(J) = \sum_{s \in \mathcal{S}} \frac{1}{w_s} \frac{1}{J - j(s)} \in \mathbf{F}_p(J)$$

does not vanish, one has $R \neq 0$. *Therefore, if* $F(j) \neq 0$ *(*$j \in \mathbf{F}_p$ *and* $j \notin \mathcal{S}$*), one has* $n_p = 0$.

The preceding corollary tells us that the singular locus of the supersingular polynomial

$$\prod_{s \in \mathcal{S}} (J - j(s))^{6/w_s} \in \mathbf{F}_p(J)$$

(the derivative of this polynomial is equal to six times the numerator of $F(j)$) is the locus of cuspidality of R. This observation motivates us to ask whether Rebolledo's modular can be defined by purely geometric means (*i.e.* without mentioning any q-expansion).

References

[1] Bosch, S.; Lütkebohmert, W.; Raynaud, M. *Néron models.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 21. Springer-Verlag, Berlin, 1990.

[2] de Shalit, E.*On certain Galois representations related to the modular curve* $X_1(p)$. *Compositio Math. 95 (1995), no. 1, 69–100.*

[3] Gross, B. *Heights and the special values of L-series.* Number theory (Montreal, Que., 1985), 115–187, CMS Conf. Proc., 7, Amer. Math. Soc., Providence, RI, 1987.

[4] Gross, B.; Kudla, S. *Heights and the central critical values of triple product L-functions.* Compositio Math. 81 (1992), no. 2, 143–209.

[5] Kolyvagin, V. A.; Logachëv, D. Yu. *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties.* Algebra i Analiz 1 (1989), no. 5, 171–196; translation in Leningrad Math. J. 1 (1990), no. 5, 1229–1253.

[6] Masser, D. W.; Wüstholz, G. *Galois properties of division fields of elliptic curves.* Bull. London Math. Soc. 25 (1993), no. 3, 247–254.

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

[8] Mazur, B. *Rational isogenies of prime degree* (with an appendix by D. Goldfeld). Invent. Math. 44 (1978), no. 2, 129–162.

[9] Merel, L. *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Invent. Math. 124 (1996), no. 1-3, 437–449.

[10] Merel, L. *Arithmetic of elliptic curves and Diophantine equations.* Les XXèmes Journées Arithmétiques (Limoges, 1997). J. Théor. Nombres Bordeaux 11 (1999), no. 1, 173–200.

[11] Merel, L. *Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques.* With an appendix by E. Kowalski and P. Michel. Duke Math. J. 110 (2001), no. 1, 81–119.

[12] Merel, L.; Stein, W. *The field generated by the points of small prime order on an elliptic curve.* Internat. Math. Res. Notices 2001, no. 20, 1075–1082.
[13] Mestre, J-F., Oesterlé, J. *Courbes elliptiques de conducteur premier.* Unpublished manuscript.
[14] Momose, F. *Rational points on the modular curves* $X_{\mathrm{split}}(p)$. Compositio Math. 52 (1984), no. 1, 115–137.
[15] Parent, P. *Torsion des courbes elliptiques sur les corps cubiques.* Ann. Inst. Fourier (Grenoble) 50 (2000), no. 3, 723–749.
[16] Parent, P. *Towards the triviality of* $X_0^+(p^r)(\mathbf{Q})$ *for* $r > 1$. Compos. Math. 141 (2005), no. 3, 561–572.
[17] Pellarin, F. *Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques.* Acta Arith. 100 (2001), no. 3, 203–243
[18] Raynaud, M. *Schémas en groupes de type* $(p, \dots, p)$. Bull. Soc. Math. France 102 (1974), 241–280.
[19] Rebolledo, M. *Module supersingulier et points rationnels des courbes modulaires*, Thèse, Université Pierre et Marie Curie, 2004.
[20] Serre, J-P. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. 15 (1972), no. 4, 259–331
[21] Serre, J-P. *Points rationnels des courbes modulaires* $X_0(N)$ *[d'après Barry Mazur].* Séminaire Bourbaki, 30e année (1977/78), Exp. No. 511, pp. 89–100, Lecture Notes in Math., 710, Springer, Berlin, 1979.
[22] Zhang, S-W. *Gross-Zagier formula for* GL_2. Asian J. Math. 5 (2001), no. 2, 183–290.
[23] Zhang, S-W. *Gross-Zagier formula for* GL(2). II. Heegner points and Rankin L-series, 191–214, Math. Sci. Res. Inst. Publ., 49, Cambridge Univ. Press, Cambridge, 2004.