Surjectivity of Galois representations associated with quadratic Q-curves

Samuel Le Fourn

Noname manuscript No.
(will be inserted by the editor)

Surjectivity of Galois representations associated with quadratic $\mathbb{Q}$-curves

Samuel Le Fourn

July 28, 2015

Abstract We prove in this paper an uniform surjectivity result for Galois representations associated with non-CM $\mathbb{Q}$-curves over imaginary quadratic fields, using various tools for the proof, such as Mazur's method, isogeny theorems, Runge's method and analytic estimates of sums of L-functions.

Keywords Galois representations · $\mathbb{Q}$-curves · isogeny theorems · Serre's uniformity problem · Runge's method

Mathematics Subject Classification (2000) 11G05 · 11G10 · 11G16 · 11G18

Contents

Introduction

For every elliptic curve E defined over a number field K and every prime number p, the representation

$$\rho_{E,p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(E_p) \cong \mathrm{GL}_2(\mathbb{F}_p),$$

defined by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion E_p of E, is a central object in the study of elliptic curves. Serre proved in 1972 [18] that for any elliptic curve E without complex multiplication and defined over a number field K, the representation $\rho_{E,p}$ is surjective for large enough p, the bound depending on E and K. In fact, we prove here as a side result a totally explicit version of Serre's result (Theorem 4.2) which might be of independent interest : in particular, it asserts that for any such elliptic curve E, the representation $\rho_{E,p}$ is surjective for

$$p > 10^7 [K:\mathbb{Q}]^2 \left(\max\{h_{\mathcal{F}}(E), 985\} + 4\log[K:\mathbb{Q}]\right)^2$$

not dividing the discriminant of K, where $h_{\mathcal{F}}(E)$ is the stable Faltings height of E. What is now known as "Serre's uniformity problem" is determining whether this bound can be made independent on E.

So far, little is known about this problem for general number fields. Over the field $\mathbb{Q}$, Mazur proved in 1977 [13] that for any elliptic curve E defined over $\mathbb{Q}$ without complex multiplication, the representation

Institut de Mathématiques de Bordeaux
E-mail: Samuel.Le.Fourn@math.u-bordeaux1.fr

$\rho_{E,p}$ is irreducible when $p > 37$. Recently, Bilu, Parent and Rebolledo proved that for such an E, the image of $\rho_{E,p}$ is also not contained in the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ for $p \geq 11$, $p \neq 13$.

The present work does not deal with the uniformity problem for elliptic curves defined over $\mathbb{Q}$, but for a slightly different object called $\mathbb{Q}$-curve.

Definition. Let K be a number field. An elliptic curve E defined over K is called a $\mathbb{Q}$-curve if for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the elliptic curve E^σ is isogenous to E. Its degree $d(E)$ is then the least common multiple of the minimal degrees of isogenies between E and its conjugates.

Remark. The set of $\mathbb{Q}$-curves is stable by isogeny. In particular, every elliptic curve defined over $\overline{\mathbb{Q}}$ which is isogenous to an elliptic curve defined over $\mathbb{Q}$ is a $\mathbb{Q}$-curve. To put aside this special case, we will say E is a *strict $\mathbb{Q}$-curve* if it is not isogenous to an elliptic curve defined over $\mathbb{Q}$.

For every $\mathbb{Q}$-curve E of degree d without complex multiplication and every p not dividing d, one defines in subsection 1.1 a projective representation

$$\mathbb{P}\overline{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}(E_p)$$

analogous to the representation $\rho_{E,p}$ for $\mathbb{Q}$-curves. One small difference with elliptic curves over $\mathbb{Q}$ is that the Weil pairing does not always guarantee the surjectivity of the determinant anymore (but this obstruction to surjectivity only exists when p is ramified in the field of definition of E). Therefore, we say $\mathbb{P}\overline{\rho}_{E,p}$ is quasi-surjective if $\mathbb{P}\overline{\rho}_{E,p}$ contains the projection of $\mathrm{SL}(E_p)$ into $\mathrm{PGL}(E_p)$, to ignore these questions of image of determinant.

As for modularity, Ribet proved [28], using Serre's conjectures (now proved by Khare, Kisin and Wintenberger), that the $\mathbb{Q}$-curves are exactly the modular elliptic curves, that is the elliptic curves that appear as quotients of a modular curve $X_1(N)$ for some N. The "modular machinery" therefore works for these curves too, and gives new applications for ternary diophantine equations. In fact, in a certain number of cases, one can attach to a ternary diophantine equation a Frey elliptic curve, as in the celebrated Fermat case, and this curve often happens to be a $\mathbb{Q}$-curve (see, for instance, [7] or [30]). This has been one of the motivations for the study of such objects in the recent period.

The main result of the present article is the following :

Theorem. *Let K be an imaginary quadratic field of discriminant $-D_K$.*

For every strict $\mathbb{Q}$-curve E defined over K without complex multiplication of degree $d(E)$, the representation $\mathbb{P}\overline{\rho}_{E,p}$ is surjective for every prime number $p > \max(50D_K^{1/4}\log(D_K), 2 \cdot 10^{13})$ not dividing $D_K d(E)$.

We actually give a more precise statement of this theorem in section 4.

Let us insist that this theorem does not add to our knowledge of elliptic curves over $\mathbb{Q}$ (the reader will notice the hypothesis "strict $\mathbb{Q}$-curve"). In particular, the issues arising for the nonsplit Cartan case over $\mathbb{Q}$ still hold, even if this case is solved in our context.

The theorem is entirely explicit in hope this might apply to diophantine equations, using Frey curves, but but our motivation was to give what seems to be the first instance of a surjectivity theorem for families of elliptic curves. It can even be interpreted as a "uniform big Galois image" result for families of abelian surfaces, taking Weil restriction from K to $\mathbb{Q}$ for the $\mathbb{Q}$-curves over quadratic imaginary fields.

The proof mechanism improves on [7] and is akin to that of [4]. More precisely, let K be an *imaginary quadratic field*. For the rest of the introduction, E refers to a strict $\mathbb{Q}$-curve without complex multiplication, defined over K. Here is the structure of the proof :

(***0***) Use classical knowledge on $\mathbb{Q}$-curves to reduce the problem to a question about rational points on modular curves in subsection 1.1.

(***I***) Prove that for large enough p (not depending on E), if $\mathbb{P}\overline{\rho}_{E,p}$ is not quasi-surjective, E has potentially good reduction at every prime of $\mathcal{O}_K$ (that is, $j(E) \in \mathcal{O}_K$). This follows from the classical Mazur's method, designed in [13]. From Proposition 1.1 below, this splits as follows :

$$(I) = (I)_B + (I)_{SC} + (I)_{NSC} + (I)_{Exc} \tag{1}$$

where $(I)_*$ means that for large enough p, if $\mathbb{P}\overline{\rho}_{E,p}$ is contained in a maximal subgroup of $\mathrm{PGL}(E_p)$ of the shape $(*)$, then $j(E) \in \mathcal{O}_K$, with the four possible types of maximal subgroups of $\mathrm{PGL}(E_p)$ are denoted by B for Borel subgroup, SC (resp. NSC) for the normaliser of a split (resp. nonsplit) Cartan subgroup and Exc for an exceptional subgroup.

This step improves Theorem 3.14 of [7], as with the same hypothesis, we obtain potentially good reduction everywhere for E, even for primes above 2 and 3. This improvement is crucial for Runge's method in part (II) below. The four cases are of various difficulty :

$(I)_{Exc}$ does not use Mazur's method, as $\mathbb{P}\overline{\rho}_{E,p}$ is not in the exceptional case for large enough p (see subsection 1.1, using results of [18] on the action of tame inertia).

$(I)_B$ et $(I)_{SC}$ will respectively be proved in subsections 2.1 and 2.2 with bounds independent of K, and even for elliptic curves defined over $\mathbb{Q}$ and $\mathbb{Q}$-curves over K real quadratic. The Borel and split Cartan case use results from subsections 1.2 and 1.3. Our results improve (as explained above) Propositions 3.2 and 3.4 of [7].

$(I)_{NSC}$ will be stated in subsection 2.3 and proved in the Appendix, with a bound depending on D_K and only for strict $\mathbb{Q}$-curves : we only improve quantitatively Proposition 3.6 of [7] here by using different estimates for weighted sums of L-functions.

(***II***) Use Runge's method in section 3 to get an *upper bound* of the shape

$$\log|j(E)| \leq C\sqrt{d(E)}$$

for every $\mathbb{Q}$-curve E of degree $d(E)$ defined over an imaginary quadratic field and with an integral j-invariant, where C is an absolute explicit constant.

(***III***) From Gaudron-Rémond's version of the period theorem ([9], Theorem 1.2), and the associated isogeny theorems (giving explicit and sharper versions of Masser-Wüstholz theorem [12] and Pellarin's theorem [16]), we obtain in section 4 a new explicit version of Serre's surjectivity theorem, which in turns gives us a *lower bound* of the shape

$$\log|j(E)| \geq C'\sqrt{d(E)p}$$

(and even better for Cartan cases) for every $\mathbb{Q}$-curve E of degree $d(E)$, without complex multiplication, defined over a quadratic field, whose j-invariant is integral and such that $\mathbb{P}\overline{\rho}_{E,p}$ is not quasi-surjective. Here again, the constant C' is absolute and explicit.

(***IV***) Finally, gather the previous results to obtain, for any quadratic imaginary field K, an explicit bound p_K such that for any prime number $p > p_K$ and any strict $\mathbb{Q}$-curve E of degree $d(E)$ (prime to p) over K whose representation $\mathbb{P}\overline{\rho}_{E,p}$ is not quasi-surjective, $j(E) \in \mathcal{O}_K$ and

$$C'\sqrt{d(E)p} \leq \log|j(E)| \leq C\sqrt{d(E)}$$

which is impossible for large enough p (independant of $d(E)$). Therefore, there is a bound M_K such that $\mathbb{P}\overline{\rho}_{E,p}$ is surjective for all $p > M_K$ not dividing $D_K d(E)$, and computing this bound gives us the main the theorem.

The problem of surjectivity for quadratic $\mathbb{Q}$-curves can be asked for $\mathbb{Q}$-curves on larger fields. We expect at least the $(I)_B$, $(I)_{SC}$ and $(I)_{Exc}$ parts to be feasible in the same way for any $\mathbb{Q}$-curve, giving bounds for potentially good reduction depending only on the degree of its field of definition. Moreover, Runge's method in part (II) demands that for a $\mathbb{Q}$-curve of degree d defined on K with an integral j-invariant, there are more cusps on $X_0(d)$ than there are infinite places on K (hence the "imaginary quadratic field" hypothesis), so it might be adaptable to polyquadratic fields that are not totally real. Finally, part (III) is very general and gives the same type of bounds, with constants C and C' depending only on the degree of the field of definition of the $\mathbb{Q}$-curve. Consequently, there is some hope for similar results for $\mathbb{Q}$-curves over larger fields, the thorniest issue remaining the nonsplit Cartan case.

Acknowledgements

I would like to thank my advisor, Pierre Parent, for his guidance to help me approach the topic, and patience throughout the many readings and corrections of this article. I also am very grateful to Gaël Rémond for his precious help and thorough checks and corrections, especially for the isogeny theorem presented here and its consequences.

Notations

In this article, unless stated otherwise, we denote by

p	a prime number larger than 5.
E	an elliptic curve defined over $\overline{\mathbb{Q}}$.
E^σ	the Galois conjugate of E by $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
E_n or $E[n]$	the n-torsion of E, non-canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$.
$\mathbb{T}$	the Hecke algebra for $\Gamma_0(p)$, generated over $\mathbb{Z}$ by the usual Hecke operators $T_n, n \in \mathbb{N}$.
(a, b)	the greatest common divisor of the integers a and b.

For every scheme $X = X_{\mathbb{Z}}$ over $\mathrm{Spec}\,\mathbb{Z}$, we denote by :

$X_{\mathbb{Q}}$ the generic fiber of X, considered as a variety over $\mathbb{Q}$.

$X_R := X \otimes_{\mathbb{Z}} R$ the extension of scalars from $\mathbb{Z}$ to any ring R.

$X_{\overline{\mathbb{F}_p}} := X \otimes_{\mathbb{Z}} \overline{\mathbb{F}_p}$ the geometric extension of the special fiber of X at p.

$\widetilde{X}$ the regular minimal model of X on $\mathrm{Spec}\,\mathbb{Z}$.

$\widetilde{X_R}$ the regular minimal model of X on R (generally different from $(\widetilde{X})_R$) if R is a Dedekind ring of characteristic 0.

For every abelian variety $J = J_{\mathbb{Q}}$ defined over $\mathbb{Q}$, we denote by :

$J_{\mathbb{Z}}$ the Néron model of J over $\mathbb{Z}$.

J_R the Néron model of J over any discrete valuation ring R of characteristic 0.

$J_{\overline{\mathbb{F}_p}} := J_{\mathbb{Z}} \otimes_{\mathbb{Z}} \overline{\mathbb{F}_p}$ the geometric extension of the fiber of $J_{\mathbb{Z}}$ at p.

$J(\mathbb{Q})_{\mathrm{tors}}$ the finite group of rational torsion points of J.

1 Setup of the surjectivity problem and tools for Mazur's method

1.1 $\mathbb{Q}$-curves and moduli spaces associated to the surjectivity problem

We assume throughout this article that every considered $\mathbb{Q}$-curve is without complex multiplication (which is the natural hypothesis for Serre's surjectivity problem).

Definition 1.0.1. Let K be a number field. Let E be a $\mathbb{Q}$-curve *without complex multiplication* defined over K. For every prime number p not dividing $d(E)$, the map

$$\mathbb{P}\overline{\rho}_{E,p} : \left| \begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & \mathrm{PGL}(E_p) \\ \sigma & \longmapsto & (D \longmapsto D_\sigma := \mu_\sigma(D^\sigma)) \end{array} \right.$$

for every $\mathbb{F}_p$-line D of E_p, is a projective representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathbb{P}E_p$, which does not depend on the choice of the isogenies $\mu_\sigma : E^\sigma \to E$ of degree prime to p. For a fixed embedding $K \subset \overline{\mathbb{Q}}$, the restriction of $\mathbb{P}\overline{\rho}_{E,p}$ to $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is the projectivization of the natural representation $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}(E_p)$ on p-torsion points of E.

To put aside the problem of surjectivity of determinant (entirely described by the degrees of the isogenies $\mu_\sigma : E^\sigma \to E$, as the reader can check using Weil pairing), we make the following definition.

Definition 1.0.2. Let E be a $\mathbb{Q}$-curve and p a prime number not dividing $d(E)$. The representation $\mathbb{P}\overline{\rho}_{E,p}$ is quasi-surjective if its image contains $\mathrm{PSL}(E_p)$ (it is then $\mathrm{PSL}(E_p)$ or $\mathrm{PGL}(E_p)$).

The following proposition (see [18], § 2.4 to 2.6) is a consequence of Dickson's theorem on maximal subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$ and justifies the equality (1) in the introduction.

Proposition 1.1. *Let p be a prime number and K be a number field. Let E be a $\mathbb{Q}$-curve without complex multiplication, defined over K and of degree prime to p. If $\mathbb{P}\overline{\rho}_{E,p}$ is not quasi-surjective, its image is included in one of the four following types of groups :*

- *A Borel subgroup of $\mathrm{PGL}(E_p)$, which means $\mathbb{P}\overline{\rho}_{E,p}$ leaves invariant an $\mathbb{F}_p$-line C_p (Borel case).*

• *The normaliser of a split Cartan subgroup of* $\mathrm{PGL}(E_p)$*, which means* $\mathbb{P}\overline{\rho}_{E,p}$ *leaves globally stable a pair* $\{A_p, B_p\}$ *of distinct* $\mathbb{F}_p$*-lines (split Cartan case).*

• *The normaliser of a nonsplit Cartan subgroup of* $\mathrm{PGL}(E_p)$*, which means* $\mathbb{P}\overline{\rho}_{E,p}$ *is included in the normaliser of a copy of* ${\mathbb{F}_{p^2}}^*$ *in* $\mathrm{GL}(E_p)$*.*

• *An exceptional subgroup of* $\mathrm{PGL}(E_p)$*,that is, a copy of* $\mathfrak{A}_4$*,* $\mathfrak{A}_5$ *or* $\mathfrak{S}_4$ *in* $\mathrm{PGL}(E_p)$ *(exceptional case).*

The exceptional case is immediately solved, using well-known results of [18] on the action of tame inertia of E_p.

Proposition 1.2. *Let* K *be a number field and* E *an elliptic curve over* K*. For every prime number* $p > 30[K : \mathbb{Q}] + 1$*, the image of* $\mathbb{P}\rho_{E,p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{PGL}(E_p)$ *is not contained in an exceptional subgroup* $\mathcal{A}_4$*,* $\mathcal{A}_5$ *or* $\mathcal{S}_4$*.*

To any $\mathbb{Q}$-curve E for which $\mathbb{P}\overline{\rho}_{E,p}$ is not quasi-surjective, we can associate a point on a moduli scheme, as we will now explain. In characteristic zero, giving an isogeny on E amounts to giving its kernel (up to isomorphism), hence we will not make (unless necessary) the difference between an isogeny and its kernel in the following.

• The scheme $X_0(N)$ is, for any integer $N \geq 1$, the compactified coarse moduli space over $\mathbb{Z}$ parametrising the isomorphism classes of couples (E, C_N) with E an elliptic curve and C_N a cyclic isogeny of degree N of E. Its generic fiber $X_0(N)_{\mathbb{Q}}$ is the modular curve corresponding to the congruence subgroup $\Gamma_0(N)$.

• The scheme $X_0^*(N)$ is, for any integer $N \geq 1$, the quotient of $X_0(N)$ by its whole group of Atkin-Lehner involutions $\{w_d; d|N, (d, N/d) = 1\}$. A noncuspidal point of $X_0^*(N)(\mathbb{Q})$ is a set of isogenous elliptic curves stable by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, hence the set of conjugates of one or more isogenous $\mathbb{Q}$-curves. This justifies the following definition borrowed to [26].

Definition 1.2.1. Let d be a squarefree positive integer. We call *central* $\mathbb{Q}$*-curve of degree* d every $\mathbb{Q}$-curve of degree d obtained from a point of $X_0^*(d)(\mathbb{Q})$.

The next proposition (reformulated from the Theorem of [26] with elements of its proof) allows us to see $X_0^*(N)$ as a sort of moduli space for $\mathbb{Q}$-curves of degree N.

Proposition 1.3. *For every* $\mathbb{Q}$*-curve* E *without complex multiplication defined over* K*, there exists an isogeny* $E \to E'$ *of degree dividing* $d(E)$ *towards a central* $\mathbb{Q}$*-curve* E' *defined over* K *and of squarefree degree* $d|d(E)$*.*

If E and E' are two $\mathbb{Q}$-curves isogenous by an isogeny of degree m, we readily see that $\mathbb{P}\overline{\rho}_{E,p}$ and $\mathbb{P}\overline{\rho}_{E',p}$ are isomorphic for any prime p not dividing m. Therefore, with help of Proposition 1.3, the problem of quasi-surjectivity of $\mathbb{P}\overline{\rho}_{E,p}$ for any $\mathbb{Q}$-curve E without complex multiplication of degree d prime to p boils down to the same problem for central $\mathbb{Q}$-curves of degree d and p not dividing d. Hence, *from now on and until the end of this article, we assume that every considered* $\mathbb{Q}$*-curve is a central* $\mathbb{Q}$*-curve of squarefree degree* d *without complex multiplication.*

Let us finish with the useful moduli spaces for our problem.

• The scheme $X_{\mathrm{split}}(p)$ is, for any prime p, the compactified coarse moduli scheme over $\mathbb{Z}$ parametrising the isomorphism classes of couples $(E, \{A_p, B_p\})$ with E an elliptic curve and A_p, B_p nonisomorphic isogenies of degree p of E. Its generic fiber $X_{\mathrm{split}}(p)_{\mathbb{Q}}$ is the modular curve corresponding to the congruence subgroup

$$\Gamma_{\mathrm{split}}(p) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}), \gamma \equiv \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \text{ or } \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \mod p \right\}.$$

• The scheme $X_{\mathrm{nonsplit}}(p)$ is, for any prime p, the compactified coarse moduli scheme over $\mathbb{Z}$ parametrising the isomorphism classes of couples (E, α_p) with E an elliptic curve and α_p a copy of $\mathbb{F}_{p^2}$ in the endomorphism ring of the group scheme E_p. Its generic fiber $X_{\mathrm{nonsplit}}(p)_{\mathbb{Q}}$ is the modular curve corresponding to one/any congruence subgroup $\Gamma_{\mathrm{nonsplit}}(p)$ which is the pullback of the normaliser of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ in $\mathrm{SL}_2(\mathbb{Z})$.

If now p is a prime number and d a squarefree integer prime to p, we define (as in [7]) the schemes

$$X_0^s(d; p) := X_0(d) \times_{X(1)} X_{\mathrm{split}}(p), \qquad X_0^{ns}(d; p) := X_0(d) \times_{X(1)} X_{\mathrm{nonsplit}}(p).$$

These two schemes and $X_0(dp)$ are endowed with an involution w_d which becomes the Fricke involution on $X_0(d)$ by the forgetful functors towards $X_0(d)$. Functorially :

$$\begin{array}{rcccc} w_d(E,C_d,C_p) & = & (E/C_d, E_d/C_d, C_p/C_d) & \text{on} & X_0(dp), \\ w_d(E,C_d,\{A_p,B_p\}) & = & (E/C_d, E_d/C_d, \{A_p/C_d, B_p/C_d\}) & \text{on} & X_0^s(d;p), \\ w_d(E,C_d,\alpha) & = & (E/C_d, E_d/C_d, \alpha/C_d) & \text{on} & X_0^{ns}(d;p), \end{array}$$

where, for a structure H on E_p, H/C_d means the transport of H on E/C_d by the isogeny $E \to E/C_d$ (for C_p, it is $(C_p + C_d)/C_d$ in E/C_d for example).

Assume now that K is a quadratic field with automorphism σ. Let E be a $\mathbb{Q}$-curve of degree d defined over K such that $\mathbb{P}\overline{\rho}_{E,p}$ is not surjective. The kernel of a minimal isogeny $E \to E^\sigma$ is called C_d. In the Borel case, $\mathbb{P}\overline{\rho}_{E,p}$ stabilises some subgroup C_p of order p of E_p, therefore $P = (E, C_d, C_p)$ is a K-rational point on $X_0(dp)$ such that

$$P^\sigma = w_d \cdot P$$

(because we assumed E is a central $\mathbb{Q}$-curve). Similarly, in the split Cartan case (resp. nonsplit Cartan case), we associate to E a point P on $X_0^s(d;p)(K)$ (resp. $X_0^{ns}(d;p)(K)$) such that $P^\sigma = w_d \cdot P$. For more details on this, see ([7], Proposition 2.2 and above).

1.2 Formal immersions and Mazur's method

Let us now recall a key proposition for Mazur's method here.

Proposition 1.4. *Let K be a number field and λ be a nonzero prime ideal of $\mathcal{O}_K$ above ℓ. We call $\mathcal{O}_\lambda$ the localised ring of $\mathcal{O}_K$ at λ and $\mathbb{F}_\lambda = \mathcal{O}_K/\lambda$.*

Let X be an algebraic curve defined over $\mathbb{Q}$ with a proper model $X_\mathbb{Z}$ on $\operatorname{Spec}\mathbb{Z}$, A an abelian variety defined on $\mathbb{Q}$ with Néron model $A_\mathbb{Z}$ on $\mathbb{Z}$, and $f : X \to A$ a morphism defined over $\mathbb{Q}$. It naturally extends to a morphism $f_\mathbb{Z} : X_\mathbb{Z}^{\text{smooth}} \to A_\mathbb{Z}$ by the universal mapping property of Néron models. Now, suppose there are two points x and y of $X(K)$ such that :

- *The points x and y have the same reduction modulo λ, and it belongs to $X_\mathbb{Z}^{\text{smooth}}$.*
- *The morphism $f_\mathbb{Z}$ is a formal immersion at $x_\lambda = y_\lambda$.*
- *The point $f(y) - f(x)$ is $\mathbb{Q}$-rational and torsion in $A(\mathbb{Q})$.*

Then, if $\ell > 2$, $x = y$. If $\ell = 2$, either $x = y$ or $f(y) - f(x)$ is a 2-torsion point in $A(\mathbb{Q})$ generating a copy of the finite group scheme μ_2 in $A_\mathbb{Z}$.

Proof. Let us suppose first that $\ell > 2$. By hypothesis, $z = f(y) - f(x) \in A(\mathbb{Q})_{tors}$. As $e = 1 < \ell - 1$, according to the specialisation lemma of Raynaud ([14], Proposition 1.1), the order of z is the same as the order of its reduction z_ℓ in $A_\mathbb{Z}(\mathbb{F}_\ell)$. Here, we have

$$z_\ell = z_\lambda = f_\mathbb{Z}(y)_\lambda - f_\mathbb{Z}(x)_\lambda = f_\mathbb{Z}(y_\lambda) - f_\mathbb{Z}(x_\lambda) = 0,$$

because $x_\lambda = y_\lambda$. Therefore, $z = 0$ and $f(y) = f(x)$. As f is a formal immersion at $x_\lambda = y_\lambda$, this implies $x = y$. In the case $\ell = 2$, we do not have $e < \ell - 1$ anymore, but thanks to Proposition 4.6 of [13], we know that z is either 0 or a 2-torsion point in $A(\mathbb{Q})$ generating a copy of μ_2 in $A_\mathbb{Z}$. When z is 0, the proof of the previous case works as well. □

Remark 1.4.1. The main difference with Proposition 3.1 of [7] is that the latter one did not deal with the case $\ell = 2$ or the fact that z is defined over $\mathbb{Q}$ while x and y are defined over a bigger field (which will be the case here). For the case $\ell = 2$, we will need to rule out the case when $f(y) - f(x)$ is 2-torsion in $A(\mathbb{Q})$ to prove Proposition 2.3. In our study, $f(y) - f(x)$ belongs to the cuspidal subgroup C of $J_0(p)(\mathbb{Q})$, and we know ([13], Proposition 11.11) its Zariski closure indeed contains a μ_2 when it is of even order. This is why we actually need the analysis of the components group of the jacobian (see proof of Lemma 2.2).

We recall the following classical result on the Albanese morphism from $X_0(p)$ to $J_0(p)$ (easily obtained from the q-expansion principle), fundamental for Mazur's method.

Proposition 1.5. *Let $p = 11$ ou $p > 13$ be a prime number. Let $\mathbb{T}$ be the Hecke subalgebra of $\mathrm{End}_{\mathbb{Q}}(J_0(p))$ generated over $\mathbb{Z}$ by the Hecke operators $T_n, n \in \mathbb{N}^*$. Let $\phi : X_0(p)_{\mathbb{Q}} \to J_0(p)_{\mathbb{Q}}$ be the Albanese morphism sending ∞ to 0 and $\phi_{\mathbb{Z}} : X_0(p)_{\mathbb{Z}}^{\mathrm{smooth}} \to J_0(p)_{\mathbb{Z}}$ its extension by Néron mapping property. For every $t \in \mathbb{T}$ and every prime ℓ, $t \circ \phi_{\mathbb{Z}}$ is a formal immersion at $\infty_{\mathbb{F}_\ell} \in X_0(p)(\mathbb{F}_\ell)$ if and only if $t \notin \ell\mathbb{T}$.*

1.3 Eisenstein quotient and components group of the jacobian

The Eisenstein ideal $\mathcal{I}$ of $\mathbb{T}$ (defined in [13]) is the ideal $\mathcal{I} := \langle 1 + \ell - T_\ell, 1 + w_p, l \in \mathcal{P}_p \rangle$, with $\mathcal{P}_p$ the set of prime numbers different from p. The Eisenstein quotient $\widetilde{J}(p)$ is the quotient of $J_0(p)$ by the abelian subvariety generated by $\gamma_{\mathcal{I}}.J_0(p)_{\mathbb{Q}}$, with $\gamma_{\mathcal{I}} = \bigcap_{n\in\mathbb{N}} \mathcal{I}^n$. It is defined over $\mathbb{Q}$, and benefits the following properties (in particular, it is the first historical example of a nontrivial rank zero quotient of $J_0(p)$).

Proposition 1.6. *Let $p = 11$ or $p > 13$ be a prime number. Let $n = \mathrm{num}(\frac{p-1}{12})$. Let C be the cuspidal subgroup of $J_0(p)(\mathbb{Q})$, generated by $\mathrm{cl}([0] - [\infty])$.*

(a) The rational torsion of $J_0(p)$ is exactly C, and it is a cyclic subgroup of order n ([13], Theorem 1.2 p.142 and Proposition 11.1).

(b) The canonical projection $J_0(p) \to \widetilde{J}(p)$ is defined over $\mathbb{Q}$ and induces a bijection between $C = J_0(p)(\mathbb{Q})_{tors}$ and $\widetilde{J}(p)(\mathbb{Q})$ which is therefore a cyclic subgroup of order n ([13], Corollary 1.4 p.143).

(c) The Eisenstein ideal is exactly the kernel of the map $t \mapsto t.\,\mathrm{cl}([0]-[\infty])$ from $\mathbb{T}$ to C, which induces an isomorphism $\mathbb{T}/\mathcal{I} \to \mathbb{Z}/n\mathbb{Z}$ ([13], Proposition 11.1). In particular, when $t = 1 \mod \mathcal{I}$, t acts as the identity on C.

It is crucial for the proofs of Propositions 2.3 and 2.6 for prime ideals above 2 to cancel $\gamma_{\mathcal{I}}$ by "good elements of $\mathbb{T}$". The following lemma will allow us to do so.

Lemma 1.7. *For every prime number ℓ, there exists a Hecke operator $t \in \mathbb{T}\backslash\ell\mathbb{T}$ such that $t = 1 \mod \mathcal{I}$ and $t \cdot \gamma_{\mathcal{I}} = 0$. Moreover, for such a $t \in \mathbb{T}$, $t \cdot (1 + w_p) = 0$.*

Proof. As $\mathbb{T}$ is a noetherian ring, by Artin-Rees lemma, we have $\mathcal{I} \cdot \gamma_{\mathcal{I}} = \gamma_{\mathcal{I}}$. Hence, by Nakayama's lemma, $\gamma_{\mathcal{I}}$ is cancelled by some element $t \in \mathbb{T}$ congruent to 1 mod $\mathcal{I}$. For a fixed prime ℓ, we can even choose such a t not in $\ell\mathbb{T}$: if ℓ divides n, this is automatic because of Proposition 1.6 (c), otherwise we can choose an integer ℓ' prime to ℓ but congruent to $\ell \mod n$. Then, for k such that $t \in \ell^k\mathbb{T}\backslash\ell^{k+1}\mathbb{T}$, the operator $t' = (\ell'/\ell)^k t \in \mathbb{T}\backslash\ell\mathbb{T}$ but is still congruent to $1 \mod \mathcal{I}$ while cancelling $\gamma_{\mathcal{I}}$. Finally, such a $t \in \mathbb{T}$ automatically cancels $(1 + w_p)$ under the previous conditions, because the Eisenstein quotient is a quotient of the minus part of the jacobian $J_0(p)$ ([13], Chapter 2, Proposition 17.10). □

We need to describe the components group of the special fiber of $J_0(p)_R$, which is made possible by Theorem 9.6.1 of [20]. In short, if R is a discrete valuation ring of mixed characteristic with fraction field K and perfect residual field k, and Φ is the group of irreducible components of $J_0(p)_R \otimes \overline{k}$, this theorem gives a description of Φ by generators $(\mathcal{C})$, and relations given by the irreducible components of $\widetilde{X_0(p)_R}$ (the minimal regular model of $X_0(p)$ over R) and their intersection numbers, and this description is compatible with the reduction morphism from $J_0(p)(K)$ to $J_0(p)_R \otimes \overline{k}$.

A first application of this to $J_0(p)_{\mathbb{Z}}$ gives the following results ([13], Theorem 10 and Appendix).

Proposition 1.8. *Let $p = 11$ or $p > 13$ be a prime number and $n = \mathrm{num}\left(\frac{p-1}{12}\right)$. Let $\phi : X_0(p)_{\mathbb{Q}} \to J_0(p)_{\mathbb{Q}}$ be the Albanese morphism sending ∞ to 0.*

(a) Reduction modulo p of the cuspidal subgroup $C = \langle \mathrm{cl}([0] - [\infty]) \rangle$ induces an isomorphism from C to the group of components Φ of $J_0(p)_{\mathbb{Z}} \otimes \overline{\mathbb{F}_p}$.

(b) For every point $Q \in J_0(p)(\mathbb{Q})$, we define $\rho(Q) \in \mathbb{Z}/n\mathbb{Z}$ the image of Q by

$$J_0(p)(\mathbb{Q}) \to J_0(p)_{\mathbb{Z}}(\overline{\mathbb{F}_p}) \to \Phi \cong C \cong \mathbb{Z}/n\mathbb{Z}.$$

Then, for every point $P \in Y_0(p)(\mathbb{Q})$:

- *If E has potentially ordinary or multiplicative reduction modulo p, $\rho(\phi(P)) = 0$ if C_p defines a separable isogeny modulo p, and $\rho(\phi(P)) = 1$ otherwise.*
- *If E has potentially supersingular reduction modulo p, either $p = -1 \mod 4$, $j(E) = 0 \mod p$ and $\rho(\phi(P)) = 1/2$, or $p = -1 \mod 3$, $j(E) = 1728 \mod p$ and $\rho(\phi(P)) = 1/3$ or $2/3$.*

The idea underlying (b) of Proposition is that $\rho \circ \phi(X_0(p)(\mathbb{Q}))$ is small, and in particular it does not not the unique nontrivial 2-torsion point of C for $p = 11$ or $p > 13$. This is the same idea that we will use in a more general analysis in Lemma 2.2

Let R be a complete discrete valuation ring of characteristic 0, with fraction field K and residual field k that we assume perfect of characteristic p. Let π be a uniformizer of R, v be the normalised valuation on K and $e = v(p)$ the absolute ramification of R.

The following result of Edixhoven (section 3 of the Appendix of [2]) generalises Theorem 1.1 of the Appendix of [13].

Proposition 1.9. (a) *The scheme $X_0(p)_R$ is smooth over R outside its supersingular points in the special fiber.*

(b) *The geometric special fiber $X_0(p)_{\overline{k}}$ is made up with two copies of $\mathbb{P}^1(\overline{k})$ (which are also its irreducible components) crossing transversally at supersingular elliptic curves : the first one, called Z, parametrises elliptic curves endowed with their Frobenius isogeny, and the second one, called Z', parametrises elliptic curves endowed with their Vershiebung isogeny.*

(c) *Let s be a supersingular point of $X_0(p)_R \otimes_R \overline{k}$ corresponding to a couple (E, C_p) with E an elliptic curve over $\overline{k}$ and C_p a p-isogeny of E. We call width of s the integer $k_s = |\mathrm{Aut}(E, C_p)|/2$. The scheme $X_0(p)_R$ is nonregular at s if and only if $ek_s > 1$. More precisely, the local completed ring of $X_0(p)_R$ at s is isomorphic to $R[[X, Y]]/(XY - \pi^{ek_s})$.*

If $p \neq 2, 3$, then $k_s > 1$ implies that $j(E) = 0$, $k_s = 3$ and $p = -1 \mod 3$, or $j(E) = 1728$, $k_s = 2$ and $p = -1 \mod 4$.

(d) *The geometric fiber $(\widetilde{X_0(p)_R})_{\overline{k}}$ of the minimal regular model over R is therefore obtained by blowing up in $X_0(p)_{\overline{k}}$ every nonregular point s to a chain of $ek_s - 1$ projective lines. These projective lines, as Cartier divisors, have auto-intersection -2.*

For the following proposition on components group, we need some notations. First, we can suppose $e > 1$ because the case $e = 1$ is dealt with Proposition 1.8. Therefore, every supersingular point s in the special fiber *is* nonregular. To provide some intuition on the proof, we define (as in the Appendix of [2]) the dual graph $\widetilde{G}$ associated to $\widetilde{X_0(p)_{R\overline{k}}}$: its vertices are the irreducible components of $(\widetilde{X_0(p)_R})_{\overline{k}}$ and an edge links two vertices if and only if the two components intersect. Thanks to Theorem 9.6.1 of [20], the problem therefore becomes a problem on $\widetilde{G}$: compute the abelian group Φ given by generators (its vertices) and relations (the image of the laplacian operator on the graph).

We define $\mathcal{S}$ (resp. $\mathcal{S}'$) the set of cardinality S (resp. S') of supersingular points of $X_0(p)_{\overline{k}}$ (resp. supersingular points with j-invariant different from 0 and 1728). We also define $I = 1$ if the elliptic curve with j-invariant 1728 is supersingular in k, 0 otherwise and $R = 1$ if the elliptic curve with j-invariant 0 is supersingular, 0 otherwise, so that

$$S = S' + I + R \quad \text{and} \quad S' + \frac{I}{2} + \frac{R}{3} = \frac{p-1}{12}. \tag{2}$$

from ([25], Theorem $V.4.1$ (c)).

For every $s \in \mathcal{S}$, we call $\mathcal{C}_s$ the path of length ek_s between the points Z and Z' associated to $s \in \mathcal{S}$ in $\widetilde{G}$, due to the blowup of s in $\widetilde{X_0(p)_R}$. In case s is of j-invariant 1728 (resp. 0), we also call it $\mathcal{E}$ (resp. $\mathcal{G}$). We order the points of $\widetilde{G}$ (that is, the components of $\widetilde{X_0(p)_R} \times \overline{k}$) on every one of these paths in the following way : we call $C_{s,0} = Z'$, $C_{s,1} = C_s$ the unique point of $\mathcal{C}_s$ linked to Z', $C_{s,2}$ the point of $\mathcal{C}_s$ linked to C_s not yet named, and so on until $C_{s,ek_s} = Z$. If s is of j-invariant 1728 (resp. 0), we call $E = \mathcal{C}_{s,1}$ (resp. $G = \mathcal{C}_{s,1}$) to remain consistent with notations of the Appendix of [13] (where $F = \mathcal{C}_{s,2}$ with $j(s) = 0$).

We use for every irreducible component C the notation

$$\overline{C} = [C] - [Z']$$

as Z' is the component where reduces the cusp ∞, our choice of base point for the Albanese morphism. The following lemma simplifies the presentation of Φ.

Lemma 1.10. *Let $\mathcal{C}_s$ be the path of length ek_s between Z and Z' associated to s in $\widetilde{G}$. In the group Φ, for every $i \in [|0, ek_s|]$,*

$$\overline{C_{s,i}} = i\overline{C_{s,1}} = i\overline{C_s}$$

In particular,

$$\overline{Z} = ek_s\overline{C_s}.$$

Proof. It is true by definition for $i = 0$ and 1. For every $i \in [|1, m-1|]$, the relation given by the laplacian operator on $\widetilde{G}$ at $C_{s,i}$ is

$$-2\overline{C_{s,i}} + \overline{C_{s,i-1}} + \overline{C_{s,i+1}} = 0.$$

The lemma follows by double induction on i. □

The group Φ is therefore the abelian group generated by $\overline{Z}$ and the $\overline{C_s}$, $s \in \mathcal{S}$, and the relations

$$\begin{array}{rl} -S\overline{Z} + (2e-1)I\overline{E} + (3e-1)R\overline{G} + \sum_{s\in\mathcal{S}'}(e-1)\overline{C_s} = 0 & (Z) \\ I\overline{E} + R\overline{G} + \sum_{s\in\mathcal{S}'}\overline{C_s} = 0 & (Z') \\ \forall s \in \mathcal{S}', \quad \overline{Z} = e\overline{C_s}, & (C_s) \end{array}$$

with additional relations

$$\begin{array}{ll} \overline{Z} = 2e\overline{E} & (E) \\ \overline{Z} = 3e\overline{G} & (G) \end{array}$$

whenever E or G exist (the name of these relations corresponding to the point where the laplacian operator is applied). Adding to (Z) the relation $-(e-1)(Z')$, we get a new relation

$$-S\overline{Z} + eI\overline{E} + 2eR\overline{G} = 0 \qquad (Z).$$

that we use in replacement of the previous relation (Z). Let us now give the description of the components group Φ.

Proposition 1.11. *Let $p = 11$ or $p > 13$ be a prime number and $n = \mathrm{num}\left(\frac{p-1}{12}\right)$. With previous notations :*

(a) The group of irreducible components Φ of $J_0(p)_R \times \overline{k}$ is non-canonically of the form

$$\Phi \cong (\mathbb{Z}/ne\mathbb{Z}) \times (\mathbb{Z}/e\mathbb{Z})^{S-2}.$$

(b) The cuspidal subgroup C of $J_0(p)(\mathbb{Q})$ reduces injectively in Φ, with $\overline{Z}$ being the reduction of $\mathrm{cl}([0]-[\infty])$. *Hence, $\langle\overline{Z}\rangle$ is of order n and we identify it with $\mathbb{Z}/n\mathbb{Z}$ in the following.*

(c) There is an exact sequence of $\mathbb{Z}/e\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z}/e\mathbb{Z} \xrightarrow{\Delta} (\mathbb{Z}/e\mathbb{Z})^S \xrightarrow{\alpha} \Phi/\langle\overline{Z}\rangle \longrightarrow 0$$

with $\Delta : \lambda \mapsto \lambda \cdot \sum_{s\in S}[C_s]$ and $\alpha : \sum_{s\in S}\lambda_s[C_s] \mapsto \sum_{s\in S}\lambda_s\overline{C_s}$.

In particular, $e \cdot \Phi = \langle\overline{Z}\rangle$, and we get

$$\begin{array}{rl} \forall s \in \mathcal{S}', \forall i \in [|1, e-1|], e.\overline{C_{s,i}} = i & \\ \forall i \in [|1, 2e-1|], e.\overline{E_i} = i/2 & \text{if } p = -1 \mod 4 \\ \forall i \in [|1, 3e-1|], e.\overline{G_i} = i/3 & \text{if } p = -1 \mod 3 \\ \sum_{s\in\mathcal{S}}\overline{C_s} = 0 & \text{in} \Phi \end{array}$$

Proof. We only compute Φ in the case $p = 11 \mod 12$ so that $I = R = 1$, the other cases being simpler but similar. We replace $\overline{Z}$ by $2e\overline{E}$ thanks to relation (E), and for every $s \in \mathcal{S}'$ we make the variable changes

$$\overline{C'_s} := \overline{C_s} - 2\overline{E} \quad \text{and} \quad \overline{G'} := \overline{G} + (2S-3)\overline{E}.$$

The relations become

$$\begin{array}{rl} e(6S-7)\overline{E} + 2e\overline{G'} = 0 & (Z)' \\ \overline{G'} + \sum_{s\in\mathcal{S}'}\overline{C'_s} = 0 & (Z')' \\ \forall s \in \mathcal{S}', e.\overline{C'_s} = 0 & (C_s)' \end{array}$$

As $p = 11 \mod 12$, $6S - 7 = 6S' + 5 = (p-1)/2 = n$ by the mass formula of (2), and $(Z)'$ is equivalent to $en\overline{E} = 0$ with help of the other relations. Hence, $\overline{G'}$ is generated by the other generators, and the relations $(C_s)', s \in \mathcal{S}'$ and $(Z)'$ are diagonal, which gives us the announced isomorphism of (a). Via this isomorphism, we have

$$\begin{aligned}\overline{Z} &= (2e, 0, \cdots, 0)\\ \overline{E_i} &= (i, 0 \cdots, 0)\\ \overline{G_i} &= (-(2S'+1)i, -i, \cdots, -i)\\ \overline{C_{s,i}} &= (2i, 0, \cdots, 0, i, 0, \cdots, 0) \quad (s \in \mathcal{S}')\end{aligned}$$

and this readily gives us (b) and (c). □

2 Application of Mazur's method

2.1 Borel case

Let p be a fixed prime and d be a squarefree positive integer prime to p. The scheme $X_0(dp)_{\mathbb{Z}}$ is smooth outside its supersingular points in characteristic dividing dp, in particular every cusp reduces in the smooth part modulo every prime number ℓ. If r is the number of prime factors of d, $X_0(dp)_{\mathbb{Q}}$ has 2^{r+1} cusps on which the Atkin-Lehner group acts transitively. As d and p are coprime, the cusps of $X_0(dp)_{\mathbb{Q}}$ are in bijection via forgetful functors $X_0(dp)_{\mathbb{Q}} \to X_0(d)_{\mathbb{Q}}$ and $X_0(dp)_{\mathbb{Q}} \to X_0(p)_{\mathbb{Q}}$ with couples of cusps of $X_0(d)_{\mathbb{Q}}$ and $X_0(p)_{\mathbb{Q}}$. Via this correspondance, the Atkin-Lehner involutions $w_{d'}, d'|d$ on $X_0(dp)_{\mathbb{Q}}$ leave unchanged the component of the cusp in $X_0(p)_{\mathbb{Q}}$ and w_p leaves unchanged the component in $X_0(d)_{\mathbb{Q}}$. We call ∞^{dp} (resp. ∞^d, ∞^p) the usual infinity cusp of $X_0(dp)_{\mathbb{Q}}$ (resp. $X_0(d)_{\mathbb{Q}}$, $X_0(p)_{\mathbb{Q}}$).

Definition 2.0.1. We denote by $\pi_{dp,p} : X_0(dp)_{\mathbb{Q}} \to X_0(p)_{\mathbb{Q}}$ the "forgetting d-structure" morphism and by $\phi : X_0(p)_{\mathbb{Q}} \to J_0(p)_{\mathbb{Q}}$ the Albanese morphism sending ∞^p to 0. The morphism $g : X_0(dp)_{\mathbb{Q}} \to J_0(p)_{\mathbb{Q}}$ is defined by $g := \phi \circ \pi_{dp,p} + \phi \circ \pi_{dp,p} \circ w_d$. Functorially, we have

$$g(E, C_d, C_p) = \mathrm{cl}([E, C_p] + [E/C_d, C_p/C_d] - 2[\infty^p]).$$

For every $t \in \mathbb{T}$, we note $g_t = t \circ g$.

Proposition 2.1. *Let $p = 11$ or $p > 13$ be a prime number, and ℓ be a prime number (possibly equal to p). For every $t \in \mathbb{T}$, the morphism $(g_t)_{\mathbb{Z}} : X_0(dp)^{\mathrm{smooth}}_{\mathbb{Z}} \to J_0(p)_{\mathbb{Z}}$ extending g_t by Néron mapping property is a formal immersion at $\infty^{dp}_{\mathbb{F}_\ell}$ if and only if $t \notin \ell\mathbb{T}$.*

Proof. Fix $t \in \mathbb{T}$ and $g'_t = t \circ \phi \circ \pi$ so that $g_t = g'_t + g'_t \circ w_d$. As w_d permutes cusps of $X_0(dp)_{\mathbb{Q}}$ above $\infty^p \in X_0(p)$, $g'_t(\infty^{dp}) = g'_t \circ w_d(\infty^{dp}) = 0$. The residual fields of the points $\infty^{dp}_{\mathbb{F}_\ell}$ and $0_{\mathbb{F}_\ell}$ are both $\mathbb{F}_\ell$ as ∞^{dp} and $0 \in J_0(p)$ cusps are $\mathbb{Q}$-rational, so we only have to check the induced maps on cotangent spaces. Notice $w_d(\infty^{dp})$ is a cusp of $X_0(dp)_{\mathbb{Q}}$ not above ∞^d, therefore $(\pi_{dp,p})_{\mathbb{C}} : X_0(dp)_{\mathbb{C}} \to X_0(p)_{\mathbb{C}}$ is ramified at this cusp (because $X_0(d)_{\mathbb{C}} \to X(1)_{\mathbb{C}}$ is ramified at any cusp but ∞^d). Hence the cotangent map of $g'_t \circ w_d$ is zero at section $\infty^{dp}_{\mathbb{Z}}$ and the cotangent map of g_t at $\infty^{dp}_{\mathbb{Z}}$ is the cotangent map of g'_t. Finally the cotangent map of $(\pi_{dp,p})_{\mathbb{Z}}$ at section $\infty^{dp}_{\mathbb{Z}}$ is an isomorphism so the cotangent map of g'_t at $\infty^{dp}_{\mathbb{F}_\ell}$ is surjective if and only if $t \notin \ell\, T$ by Proposition 1.5, which concludes the proof by the usual formal immersion criterion. □

The following lemma is essential for the case $\ell = 2$.

Lemma 2.2. *Let $p = 11$ or $p > 13$ be a prime number, $n = \mathrm{num}((p-1)/12)$ and K be a quadratic field with ramification degree e over p. Let E be a central $\mathbb{Q}$-curve of degree d defined over K such that $\mathbb{P}\overline{\rho}_{E,p}$ is reducible, and P the corresponding point of $X_0(dp)(K)$. Then $g(P)$ belongs to $J_0(p)(\mathbb{Q})$, and with the*

retraction $\rho : J_0(p)(\mathbb{Q}) \to \mathbb{Z}/n\mathbb{Z}$ defined at Proposition 1.8, the possible values of $\rho(g(P))$ are the following :

	$p = 1 \mod 12$	$p = 5 \mod 12$	$p = 7 \mod 12$	$p = 11 \mod 12$
$e = 1$	0,2	$0,1,2,\frac{2}{3},\frac{4}{3}$	0,1,2	$0,1,2,\frac{2}{3},\frac{4}{3}$
$e = 2$	0,1,2	$0,1,2,\frac{1}{3},\frac{2}{3},\frac{4}{3},\frac{5}{3}$	$0,1,2,\frac{1}{2},\frac{3}{2}$	$0,1,2,\frac{1}{3},\frac{1}{2},\frac{2}{3},\frac{4}{3},\frac{3}{2},\frac{5}{3}$

In particular, this image cannot be the unique 2-torsion point of the cuspidal subgroup C unless $p = 17$ or 41.

Proof. First, $g(P) \in J_0(p)(K)$ because g is $\mathbb{Q}$-rational, and for σ the nontrivial automorphism of K,

$$g(P)^\sigma = \phi \circ \pi_{dp,p}(P^\sigma) + \phi \circ \pi_{dp,p} \circ w_d(P^\sigma) = \phi \circ \pi_{dp,p}(w_d \cdot P) + \phi \circ \pi_{dp,p}(P) = g(P)$$

by construction of P (see subsection 1.1), hence $g(P)$ indeed belongs to $J_0(p)(\mathbb{Q})$. Fix a prime ideal $\mathfrak{P}$ of K above p and define Φ the group of components of the special fiber of $J_0(p)_{\mathcal{O}_{K\mathfrak{P}}}$. We read $\rho(g(P))$ via reduction modulo $\mathfrak{P}$, using Propositions 1.8 and 1.11 (and their notations). Notice that $\pi_{dp,p}(P)$ and $\pi_{dp,p}(w_d \cdot P)$ represent elliptic curves which are isogenous of degree prime to p on $X_0(p)$. Consequently, their stable reduction type modulo $\mathfrak{P}$ (ordinary with separable isogeny, ordinary with unseparable isogeny, supersingular) is the same. This remark done, we use the Proposition 1.11 to compute the different possibilities :

• If p is unramified in $\mathcal{O}_K$, we are in the étale case of the Proposition, and the possible values of the reduction of $g(P)$ in Φ are then $2\overline{Z'} = 0$, $2\overline{Z} = 2$, $2\overline{E} = 1$, $2\overline{G} = 2/3$, $4\overline{G} = 4/3$ and $3\overline{G} = 1$ (when $\overline{E}$ or $\overline{G}$ exist). This proves the first line.

• If p is ramified in $\mathcal{O}_K$, we are in case $e = 2$ of the Proposition, and the possible values of the reduction of $g(P)$ in Φ are then $2\overline{Z'} = 0$, $2\overline{Z} = 2$, $2\overline{E_1} = 1/2$, $2\overline{E_2} = 1$, $2\overline{E_3} = 3/2$, $\overline{E_1} + \overline{E_3} = 1$, $2\overline{G_1} = 1/3$, $2\overline{G_2} = 2/3, \ldots, 2\overline{G_5} = 5/3$ (and other possibilities that do not give new values). Finally, for every $s \in \mathcal{S}'$, $2\overline{C_{s,1}} = 1$.

For the application of the result, $\mathbb{Z}/n\mathbb{Z}$ admits a nontrivial 2-torsion point if and only if 2 divides n, which is possible only when $p = 1 \mod 8$, and then this torsion point is $n/2$. Suppose $\rho(g(P))$ is equal to $n/2$. From the table, if $p = 1 \mod 12$, it means $(p-1)/12$ divides 1,2 or 4, whence $p = 13$. If $p = 5 \mod 12$, it means $(p-1)/4$ divides $1, 2, 4, 8$ or 10, whence $p = 17$ or $p = 41$. □

Proposition 2.3. *Let K be a quadratic field and E a $\mathbb{Q}$-curve of squarefree degree d defined over K. If for $p \geq 11$, $p \neq 13, 17, 41$ prime not dividing d, the representation $\mathbb{P}\overline{\rho}_{E,p}$ is reducible, E has potentially good reduction at every prime ideal of $\mathcal{O}_K$.*

Proof. Let $P \in X_0(dp)(K)$ be the point associated to E. From Lemma 2.2, we know that $g(P) \in J_0(p)(\mathbb{Q})$. Let λ be a prime ideal of $\mathcal{O}_K$ above ℓ, and suppose E has potentially multiplicative reduction at λ. As the Atkin-Lehner involutions group acts transitively and $\mathbb{Q}$-rationally on the cusps of $X_0(dp)$, we can and will assume that $P_\lambda = \infty_\lambda^{dp} = \infty_\ell^{dp} \in X_0(dp)_{\mathbb{Z}}(\mathbb{F}_\ell)$. In particular, P_λ is in the smooth part of $X_0(dp)_{\mathbb{Z}}$. We choose $t \in \mathbb{T}\backslash\ell\mathbb{T}$ cancelling the ideal $\gamma_{\mathcal{I}}$ and congruent to 1 modulo $\mathcal{I}$ (see Lemma 1.7 and above for notations). The $\mathbb{Q}$-rational morphism $t : J_0(p)_{\mathbb{Q}} \to J_0(p)_{\mathbb{Q}}$ cancels on $\gamma_{\mathcal{I}} \cdot J_0(p)$, therefore it factors through $\widetilde{J}(p)$ and sends the $\mathbb{Q}$-rational point $g(P)$ on a $\mathbb{Q}$-rational torsion point of $J_0(p)$ because $\widetilde{J}(p)$ is of rank zero. It allows us to apply Proposition 1.4 to $x = P$, $y = \infty^{dp}$, $X = X_0(dp)_{\mathbb{Q}}$, $A = J_0(p)_{\mathbb{Q}}$ and g_t (the latter being a formal immersion by Proposition 2.1). In the case $\ell > 2$, we obtain $P = \infty^{dp}$, which is a contradiction, therefore E has potentially good reduction modulo λ. In the case $\ell = 2$, as $t = 1 \mod \mathcal{I}$, $\rho(g_t(P)) = \rho(g(P))$ (Proposition 1.6 (c)), therefore $g_t(P)$ is not the non-trivial 2-torsion point of $J_0(p)(\mathbb{Q})$ by Lemma 2.2. So $P = \infty^{dp}$ in this case too, which is a contradiction, hence E has potentially good reduction modulo λ for every prime ideal λ of $\mathcal{O}_K$. □

2.2 Split Cartan case

Let p be a prime number and d be a squarefree positive integer prime to p. As in [7], we define $X_{\text{sp.Car.}}(p)_{\mathbb{Z}}$ the compactified coarse moduli scheme over $\mathbb{Z}$ parametrising the triples (E, A_p, B_p) with A_p, B_p nonisomorphic p-isogenies of E and $X_0^{\text{sC}}(d;p)_{\mathbb{Z}} := X_0(d) \times_{X(1)} X_{\text{sp.Car.}}(p)_{\mathbb{Z}}$. These schemes are proper over

$\operatorname{Spec}\mathbb{Z}$, and there is a natural involution

$$w : (E, C_d, A_p, B_p) \to (E, C_d, B_p, A_p)$$

so that the quotient $X_0^{\mathrm{sC}}(d;p)_{\mathbb{Z}}/\langle w\rangle$ is the scheme $X_0^s(d;p)_{\mathbb{Z}}$ defined in subsection 1.1. As for Borel case, the "forgetting d-structure" and "forgetting p-structure" morphisms induce a bijection between cusps of $X_0^{\mathrm{sC}}(d;p)_{\mathbb{Q}}$ (resp. $X_0^s(d;p)_{\mathbb{Q}}$) and couples of cusps of $X_0(d)_{\mathbb{Q}}$ and cusps of $X_{\mathrm{sp.Car.}}(p)_{\mathbb{Q}}$ (resp. of $X_{\mathrm{split}}(p)_{\mathbb{Q}}$) because d is prime to p. Henceforth, we will note (c, c') the unique cusp of $X_0^{\mathrm{sC}}(d;p)_{\mathbb{Q}}$ (resp. $X_0^s(d;p)_{\mathbb{Q}}$) above the cusps $c \in X_0(d)_{\mathbb{Q}}$ and $c' \in X_{\mathrm{sp.Car.}}(p)_{\mathbb{Q}}$ (resp. $c' \in X_{\mathrm{split}}(p)$). The scheme $X_0^{\mathrm{sC}}(d;p)_{\mathbb{Z}}$ is smooth in characteristics prime to dp. In characteristic ℓ dividing d, its singular points correspond to supersingular elliptic curves over $\overline{\mathbb{F}_\ell}$. In characteristic p, $X_0^{\mathrm{sC}}(d;p)_{\overline{\mathbb{F}_p}}$ (resp. $X_{\mathrm{sp.Car.}}(p)_{\overline{\mathbb{F}_p}}$) is made up with three irreducible components which parametrise the quadruples (E, C_d, A_p, B_p) (resp. (E, A_p, B_p)) such that respectively :

- The isogeny A_p is unseparable (Z component).
- The isogeny B_p is unseparable (Z' component).
- Neither A_p nor B_p are unseparable (W component).

Cusps above $\infty^p \in X_{\mathrm{sp.Car.}}(p)$ reduce in component Z, cusps above $0^p \in X_{\mathrm{sp.Car.}}(p)$ reduce in component Z', and all the others reduce to component W, which is of multiplicity $p-1$. Hence, the nonrational cusps do not reduce to smooth points. Considering the quotient morphism $X_0^{\mathrm{sC}}(d;p)_{\mathbb{Z}} \to X_0^s(d;p)_{\mathbb{Z}}$ (resp. $X_{\mathrm{sp.Car.}}(p)_{\mathbb{Z}} \to X_{\mathrm{split}}(p)_{\mathbb{Z}}$), the components Z and Z' identify in the fiber at p to form a component called Z_0, the other irreducible component being the image of the component W (still noted W).

We need preparatory results inspired from [15]. We also owe this article the original idea for the following formal immersion, that [7] adapted for $\mathbb{Q}$-curves.

Proposition 2.4. *Let E be an elliptic curve defined over a number field K and $p > 2[K:\mathbb{Q}]+1$ be a prime number such that the image of $\rho_{E,p}$ is in the normaliser of a split Cartan subgroup of $\mathrm{GL}(E_p)$. Let $P = (E, \{A_p, B_p\})$ be the corresponding K-rational point of $X_{\mathrm{split}}(p)$, and K' an extension of degree two of K over which A_p and B_p are defined. Then, for any prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ above p :*

(a) The elliptic curve E does not have potentially supersingular reduction at $\mathfrak{P}$.

(b) The reduction modulo $\mathfrak{P}$ of P in $X_{\mathrm{split}}(p)_{\mathbb{F}_p}$ does not belong to the W component.

(c) For every prime ideal $\mathfrak{P}'$ of $\mathcal{O}_{K'}$ above $\mathfrak{P}$, the reductions modulo $\mathfrak{P}'$ of (E, A_p) and $(E/B_p, E_p/B_p)$ belong to the same irreducible component of $X_0(p)_{\mathcal{O}_{\mathfrak{P}'}} \times \overline{\mathbb{F}_p}$.

Proof. Let $p \geq 5$ be a prime number and $\mathfrak{P}'$ be a prime ideal of $\mathcal{O}' = \mathcal{O}_{K'}$ above p. The $\mathrm{Gal}(\overline{\mathbb{Q}}/K')$-modules E_p, A_p and B_p define group schemes over K' noted $(E_p)_{K'}$, $(A_p)_{K'}$ and $(B_p)_{K'}$ such that

$$(E_p)_{K'} \cong (A_p)_{K'} \oplus (B_p)_{K'}. \tag{3}$$

Passing to Zariski closure in Néron model of E over $\mathcal{O}'$, we obtain group schemes $(E_p)_{\mathcal{O}'}$, $(A_p)_{\mathcal{O}'}$ and $(B_p)_{\mathcal{O}'}$ extending the group schemes over K'. As the absolute ramification index e' of p in $\mathcal{O}_{K'}$ is smaller that $2[K:\mathbb{Q}] < p-1$, we know by Raynaud's specialisation lemma (Theorem 3.3.3 and Corollary 3.3.4 of [17]) that

$$(E_p)_{\mathcal{O}'} \cong (A_p)_{\mathcal{O}'} \oplus (B_p)_{\mathcal{O}'}.$$

Furthermore, as $e' < p+1$ again, the finite group schemes $(A_p)_{\mathcal{O}'}$ and $(B_p)_{\mathcal{O}'}$ are constant or isomorphic to μ_p. This already proves (a) because if E is potentially supersingular, $(E_p)_{\mathcal{O}'}$ contains a group scheme α_p. Furthermore, $(E_p)_{\mathcal{O}'}$ is not étale since it has at most p $\overline{\mathbb{F}_p}$-rational points while being of rank p^2. Therefore, $(A_p)_{\mathcal{O}'}$ or $(B_p)_{\mathcal{O}'}$ is not étale, hence isomorphic to μ_p. This proves (b). Finally, the $\mathrm{Gal}(\overline{\mathbb{Q}}/K')$-modules isomorphism $A_p \to E_p/B_p$ given by (3) extends (as $e' < p-1$ again) to an isomorphism $(A_p)_{\mathcal{O}'} \cong (E_p/B_p)_{\mathcal{O}'}$. Hence, they are simultaneously constant or isomorphic to μ_p. As E is not potentially supersingular, the component to which belongs the reduction of (E, A) in $X_0(p)_{\mathcal{O}'} \times \overline{\mathbb{F}_p}$ is Z or Z', and entirely determined by the nature (étale or not) of A, hence the two points (E, A_p) and $(E/B_p, E_p/B_p)$ reduce to the same component.

□

Recall $\phi : X_0(p)_{\mathbb{Q}} \to J_0(p)_{\mathbb{Q}}$ is the Albanese morphism sending ∞^p to 0.

Definition 2.4.1. Let p be a prime number. We note $\pi : X_0^{\mathrm{sC}}(d;p)_{\mathbb{Q}} \to X_0(p)_{\mathbb{Q}}$ the forgetful morphism that sends (E, C_d, A_p, B_p) to (E, A_p). The map $h : X_0^{\mathrm{sC}}(d;p)_{\mathbb{Q}} \to J_0(p)_{\mathbb{Q}}$ is defined by $h := \phi \circ \pi - \phi \circ w_p \circ (\pi \circ w) + \phi \circ \pi \circ w_d - \phi \circ w_p \circ (\pi \circ w \circ w_d)$. Functorially, we have

$$h(E, C_d, A_p, B_p) = \mathrm{cl}\left([E, A_p] - [E/B_p, E_p/B_p] + [E/C_d, A_p/C_d] - [E/(B_p + C_d), E_p/(B_p + C_d)]\right).$$

Furthermore, $h \circ w = -w_p \circ h$ where w_p is the endomorphism of $J_0(p)_{\mathbb{Q}}$ corresponding to Atkin-Lehner involution w_p on $X_0(p)_{\mathbb{Q}}$. For every $t \in \mathbb{T}$, we define $h_t = t \circ h$. Hence, if $t(1 + w_p) = 0$, $h_t \circ w = h_t$ so that h_t factors through the projection $X_0^{\mathrm{sC}}(d;p)_{\mathbb{Q}} \to X_0^s(d;p)_{\mathbb{Q}}$ in a $\mathbb{Q}$-rational morphism $h_t^+ : X_0^s(d;p)_{\mathbb{Q}} \to J_0(p)_{\mathbb{Q}}$.

Remark 2.4.1. The sum h' of the first two terms of h give the good candidate for elliptic curves over $\mathbb{Q}$ (see [4]). As in Borel case, the generalisation to $\mathbb{Q}$-curves relies in the consideration of $h' + h' \circ w_d$.

Proposition 2.5. *Let ℓ be a prime number and $t \in \mathbb{T}$.*

The morphism $(h_t)_{\mathbb{Z}} : X_0^{\mathrm{sC}}(d;p)^{\mathrm{smooth}} \to J_0(p)_{\mathbb{Z}}$ extending h_t by Néron mapping property is a formal immersion at the cusp $(\infty, \infty)_{\mathbb{F}_\ell}$ of $X_0^{\mathrm{sC}}(d;p)_{\mathbb{F}_\ell}$ if and only if $t \notin \ell\mathbb{T}$. If $t(1 + w_p) = 0$, the same condition holds for $(h_t)_{\mathbb{Z}}^+ : X_0^s(d;p)^{\mathrm{smooth}} \to J_0(p)_{\mathbb{Z}}$ to be a formal immersion at the cusp $(\infty, \infty)_{\mathbb{F}_\ell}$ of $X_0^s(d;p)_{\mathbb{F}_\ell}$.

Proof. We define $\psi : X_0^{\mathrm{sC}}(d;p)_{\mathbb{Q}} \to X_0(dp)_{\mathbb{Q}}$ as the "forgetting B_p"-morphism that sends (E, C_d, A_p, B_p) to (E, C_d, A_p). With the definitions of the Borel case, $\pi = \pi_{dp,p} \circ \psi$ and $h = g \circ \psi + g \circ w_p \circ \psi \circ w$. As $\psi((\infty, \infty)) = \infty^{dp} = w_p \circ \psi \circ w(\infty, \infty)$, the cotangent map of $h_{\mathbb{Z}}$ at section $(\infty, \infty)_{\mathbb{Z}}$ is the sum of the cotangent maps of $(g \circ \psi)_{\mathbb{Z}}$ and $(g \circ w_p \circ \psi \circ w)_{\mathbb{Z}}$. Notice that ψ is ramified of degree p at $(\infty, \infty)_{\mathbb{Z}}$ (as it can be checked out on corresponding Riemann surfaces), so that $g \circ \psi$ is. Hence, the cotangent map of $h_{\mathbb{Z}}$ is the cotangent map of $(g \circ w_p \circ \psi \circ w)_{\mathbb{Z}}$. Furthermore, we readily see that $g \circ w_p = w_p \circ g + 2\,\mathrm{cl}([0] - [\infty^p])$, so $(h_t)_{\mathbb{Z}}$ is a formal immersion at $(\infty, \infty)_{\mathbb{F}_\ell}$ if and only if $(g_t \circ \psi \circ w)_{\mathbb{Z}}$ is, because w_p is an automorphism of $J_0(p)_{\mathbb{Z}}$. But the cotangent map of $(\psi \circ w)_{\mathbb{Z}} : X_0^{\mathrm{sC}}(d;p)_{\mathbb{Z}} \to X_0(p)_{\mathbb{Z}}$ at the section $(\infty, \infty)_{\mathbb{Z}}$ is an isomorphism (see [15], Proof of Proposition 2.5), whence the result for $(h_t)_{\mathbb{Z}}$ by Proposition 2.1. The result follows for $(h_t)_{\mathbb{Z}}^+$ as (∞, ∞) is not a fixed point of w. □

We can now prove our result in split Cartan case.

Proposition 2.6. *Let K be a quadratic field. For every prime number $p = 11$ or $p > 13$, if E is a $\mathbb{Q}$-curve of degree d prime to p defined over K, the image of $\mathbb{P}\overline{\rho}_{E,p}$ is in the normaliser of a split Cartan subgroup of $\mathrm{PGL}(E_p)$, then E has potentially good reduction at every prime ideal of $\mathcal{O}_K$.*

Proof. Let $P \in X_0^s(d;p)(K)$ be the point associated to E. For any $t \in \mathbb{T}$ such that $t(1 + w_p) = 0$, h_t^+ is a $\mathbb{Q}$-rational morphism so $h_t^+(P) \in J_0(p)_{\mathbb{Q}}(K)$. If we call σ the automorphism of K,

$$h_t^+(P)^\sigma = h_t^+(P^\sigma) = h_t^+(w_d.P) = h_t^+(P)$$

because $h \circ w_d = h$ by construction, so that $h_t^+(P)$ is $\mathbb{Q}$-rational.

Now, if we also suppose that t cancels $\gamma_{\mathcal{I}}$ and $t = 1 \mod \mathcal{I}$ (see Lemma 1.7 and above for notations), then $h_t^+(P) = 0$. Indeed, it is a torsion point of $J_0(p)$ because the Eisenstein quotient has rank zero. Taking any prime $\mathfrak{P}$ of $\mathcal{O}_K$ above p, by Proposition 2.4 we know that P reduces modulo $\mathfrak{P}$ in the smooth part of $X_0^s(d;p)_{\mathbb{Z}}$ (by (a) and (b)), and that $({h_t}^+)_{\mathbb{Z}}(P_{\mathfrak{P}})$ is 0 in the group of components Φ of $J_0(p)_{\mathcal{O}'} \times \overline{\mathbb{F}'_{\mathfrak{P}}}$ (by (c)). Therefore, $h_t^+(P) = 0$ as reduction from the cuspidal subgroup C to Φ is injective (Proposition 1.11 (b)). We can now apply Mazur's method.

Suppose there is a prime ideal λ of $\mathcal{O}_K$ (above the prime number ℓ) such that E has potentially multiplicative reduction at λ. Then P reduces at a cusp c modulo λ, hence is in the smooth part of $X_0^s(d;p)_{\mathbb{Z}}$ (this is obvious when λ is not above p, and we just explained why it is true when λ is above p). Actually, this cusp must be a cusp above $\infty_{\mathbb{F}_\ell} \in X_{\mathrm{split}}(p)_{\mathbb{F}_\ell}$. Indeed, if $\ell = p$, this is what we just proved as the other cusps are not in the smooth part (Proposition 2.4), and if $\ell \neq p$, simple computation shows that the image of a cusp c of $X_0^{\mathrm{sC}}(d;p)_{\mathbb{Q}}$ not above ∞ or $0 \in X_{\mathrm{sp.Car.}}(p)_{\mathbb{Q}}$ by h is $2\,\mathrm{cl}([0] - [\infty])$. For $t \in \mathbb{T}$ as above, as $h_t^+(P) = 0$ and the Zariski closure $C_{\mathbb{Z}}$ of C in $J_0(p)_{\mathbb{Z}}$ is étale outside 2 (eg by Raynaud's Theorem 3.3.3 [17]), if $\ell > 2$, it prevents P from reducing at c modulo λ (unless $n = 1$ or

2, impossible when $p = 11$ or $p > 13$), and for $\ell = 2$, it is only possible when n divides 4 which is also impossible for $p > 23$. Now we know P reduces modulo λ at a cusp above $\infty_{\mathbb{F}_\ell} \in X_{\text{split}}(p)_{\mathbb{Z}}$. After applying an Atkin-Lehner involution $w_{d'}$, $d'|d$, we can suppose that P reduces modulo λ at $(\infty, \infty)_{\mathbb{F}_\ell}$. Take now $t \in \mathbb{T}\backslash \ell\mathbb{T}$ still satisfying the previous conditions by Lemma 1.7, so we can apply Proposition 2.5. As $h_t^+(P) = 0$, there is no problem with the case $\ell = 2$ here, and we obtain $P = (\infty, \infty)$, which is a contradiction. Therefore, E has potentially good reduction at every prime ideal λ. □

2.3 Nonsplit Cartan case

In this subsection, we do not provide any qualitative improvement on the third section of [7], but a quantitative one. The next proposition is the algebraic part of section 3 of *loc. cit.*, which uses Mazur's method and relies on the existence of a rank zero quotient on a twisted jacobian (using crucially the results of Kolyvagin and Logachev). Small characteristic issues can be easily ruled out for $p \geq 7$ in this case (see proof of Proposition 3.9 of [7]).

Proposition 2.7 ([7], proof of Proposition 3.6)**.** *Let K be an imaginary quadratic number field of discriminant $-D_K$, χ_K the associated Dirichlet character and $d > 1$ a squarefree positive integer.*

Let $p \geq 7$ be a prime number not dividing dD_K. If there exists an eigenform $f \in S_2(\Gamma_0(p^2))^{\text{new}}$ such that $w_p \cdot f = f$ and $L(f \otimes \chi_K, 1) \neq 0$, then for every strict $\mathbb{Q}$-curve E of degree d defined over K such that the image of $\mathbb{P}\overline{\rho}_{E,p}$ is included in the normaliser of a nonsplit Cartan subgroup of $\mathrm{PGL}(E_p)$, E has potentially good reduction at every prime ideal of $\mathcal{O}_K$.

Thanks to this Proposition and using the same type of analytic estimates as in [7], we obtain in the Appendix the following result :

Proposition 2.8. *Let K be an imaginary quadratic field of discriminant $-D_K$.*

Let $p > 50D_K^{1/4}\log(D_K)$ be a prime number not dividing D_K. If E is a $\mathbb{Q}$-curve defined over K, of degree coprime with p, without complex multiplication and such that the image of $\mathbb{P}\overline{\rho}_{E,p}$ is in the normaliser of a nonsplit Cartan subgroup of $\mathrm{PGL}(E_p)$, then E has potentially good reduction at every prime ideal of $\mathcal{O}_K$.

3 Runge's method

Runge's method can be used on a modular curve X to bound the absolute logarithmic height of j-invariants of S-integral points on X, where S is a set of places of the number field K containing the infinite places, of cardinality smaller than the number of Galois orbits of cusps of X. In this article, our application of Runge's method will be a very simple case : K is an imaginary quadratic field $X = X_0(p)$ with p a fixed prime number, and S contains one single element : the euclidean norm on $\mathcal{O}_K$. We define

$$X_0(p)(\mathcal{O}_K) := \{P \in X_0(p)(K), j(P) \in \mathcal{O}_K\}.$$

Our goal is to explicitly bound the j-invariant of elements of $X_0(p)(\mathcal{O}_K)$. We denote by

$\mathcal{H}$ the Poincaré upper half plane.

$\mathcal{D}$ the fundamental domain of $\mathcal{H}$ for the action of $\mathrm{SL}_2(\mathbb{Z})$ bounded by the geodesic triangle $\{0, 1, \infty\}$

$q_\tau := \exp(2i\pi\tau)$ for any $\tau \in \mathcal{H}$ (the τ index will be omitted if τ is obvious).

$q_\tau^r := \exp(2i\pi r\tau)$ for any rational number r.

Finally, for sake of precision, we denote c_∞ (resp. c_0) the cusp of $X_0(p)$ which is the image of ∞ (resp. 0) by the canonical projection $\pi : \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) \to X_0(p)$. Notice that the Runge's method will be applied for p dividing the degree of a $\mathbb{Q}$-curve, so our result has to hold for any prime p.

For general Runge's method, we need some knowledge about modular units (see [3] for a general exposition in the case of modular curves), but in our case we will just use one, defined as follows.

Definition 3.0.1. Let p be a fixed prime number. The holomorphic function g on $\mathcal{H}$ is defined for all $\tau \in \mathcal{H}$ by

$$g(\tau) = \frac{\Delta(\tau)}{\Delta(p.\tau)} = q_\tau^{1-p} \prod_{\substack{n=1 \\ (p,n)=1}}^{+\infty} (1-q_\tau^n)^{24}.$$

where Δ is the discriminant modular form on $\mathcal{H}$. This is the quotient of two modular forms of weight 12 on $\Gamma_0(p)$, hence it defines a modular function U on $X_0(p)$.

The modular function U benefits the following properties :

Proposition 3.1. *(a) For every $\tau \in \mathcal{H}$:*

$$g(-1/\tau) = p^{12} g^{-1}(\tau/p) = p^{12} q^{(p-1)/p} \prod_{n=1}^{\infty} \left(\frac{1-q^n}{1-q^{n/p}}\right)^{24}.$$

(b) For w_p the Atkin-Lehner involution of $X_0(p)$, $U \circ w_p = p^{12} U^{-1}$.
(c) The divisor of U on $X_0(p)$ is supported by cusps, more precisely

$$\mathrm{div}(U) = (p-1)([c_0] - [c_\infty]).$$

(d) The function U is a $\mathbb{Q}$-rational function on $X_0(p)$ which is integral over $\mathbb{Z}[j]$.

Proof. The assertion (a) implies (b) because for every $\tau \in \mathcal{H}$ of image P in $X_0(p)$, $g(\tau) = U(P)$ and $-1/(p\tau)$ has image $w_p(P)$ by definition. To prove (a), we only write that for every $\tau \in \mathcal{H}$, by definition of g,

$$g(-1/\tau) = \frac{\Delta(-1/\tau)}{\Delta(-p/\tau)} = \frac{\tau^{12}\Delta(\tau)}{p^{-12}\tau^{12}\Delta(\tau/p)} = p^{12} g^{-1}(\tau/p),$$

because Δ is a modular form of weight 12 on $\mathrm{SL}_2(\mathbb{Z})$. Next, the discriminant modular form does not cancel on $\mathcal{H}$, therefore the divisor of U is indeed supported by the two cusps c_∞ and c_0. The q-expansion of g at ∞ shows that the order of the pole of U at c_∞ is $(p-1)$, and the order at c_0 is necessarily the opposite, which proves (c). The modular function U is $\mathbb{Q}$-rational on $X_0(p)$ as a quotient of two $\mathbb{Q}$-rational modular forms of weight 12 on $X_0(p)$. Only the integrality remains to be proved. Recall that

$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(p) \cup \bigcup_{k \in \mathbb{Z}} \Gamma_0(p) \cdot \begin{pmatrix} 0 & 1 \\ -1 & -k \end{pmatrix} \tag{4}$$

Indeed, for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, either $\gamma \cdot \infty = \gamma' \cdot \infty$ with $\gamma' \in \Gamma_0(p)$, and in this case $\gamma \in \Gamma_0(p)$ because the stabiliser of the cusp ∞ in $\mathrm{SL}_2(\mathbb{Z})$ is contained in $\Gamma_0(p)$, or $\gamma \cdot \infty = \gamma' \cdot 0$ with $\gamma' \in \Gamma_0(p)$. The matrix $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ sends ∞ to 0, so we can write

$$(\gamma' w)^{-1} \gamma = \pm \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

for some integer k, as $(\gamma' w)^{-1} \gamma \cdot \infty = \infty$. This proves (4). From this equation, we know that for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the q-expansion of $g_{|\gamma}$ (that is, the image of g by the usual right action of $\mathrm{SL}_2(\mathbb{Z})$ on functions on $\mathcal{H}$) is a formal series in $q_\tau^{1/p}$ with algebraic integer coefficients. Indeed, if $\gamma \in \Gamma_0(p) \cdot \begin{pmatrix} 0 & 1 \\ -1 & -k \end{pmatrix}$,

$$g_{|\gamma}(\tau) = g(-1/(\tau+k)) = p^{12} e^{2i\pi(p-1)k/p} {q_\tau}^{(p-1)/p} \prod_{n=1}^{\infty} \left(\frac{1-q_\tau^n}{1-e^{2i\pi nk/p} q_\tau^{n/p}}\right)^{24}$$

by (a), so this q_τ-expansion has coefficients in $\mathbb{Z}[e^{2i\pi/p}] \subset \overline{\mathbb{Z}}$. Hence, from Lemma 2.1 of [23] (Chapter 2.2), we know that U is integral on $\mathbb{Z}[j]$. □

Remark 3.1.1. This proof is somewhat elementary, but the reader will notice that we only reproved some well-known results of the theory of modular units (which is far more general) for U. Actually, with the notations of ([23], Chapter 2),

$$g := \prod_{a=1}^{p-1} g_{(\frac{a}{p},0)}^{12p},$$

and with results of the same chapter, we recover all the results of the previous Proposition except (b). A consequence of (b) is that $p^{12}U^{-1}$ is integral over $\mathbb{Z}[j]$, and it seems that the theory of modular units would only have predicted that $p^{12p}U^{-1}$ is (see [3]).

Lemma 3.2. *For every $P \in Y_0(p)(\mathcal{O}_K)$, $U(P)$ is a nonzero element of $\mathcal{O}_K$ such that*

$$0 \leq \log|U(P)| \leq 12\log p.$$

Proof. As U is $\mathbb{Q}$-rational and integral over $\mathbb{Z}[j]$ (Proposition 3.1 (d)), $U(P) \in \mathcal{O}_K$ and is nonzero because U does not cancel on $Y_0(p)$. The same thing is true for $w_p \cdot P$: indeed, $w_p \cdot P \in Y_0(p)(\mathcal{O}_K)$ because w_p is $\mathbb{Q}$-rational and $w_p \cdot P$ represents an elliptic curve isogenous to the elliptic curve represented by P, so $j(w_p \cdot P) \in \mathcal{O}_K$ too. Therefore, $U \circ w_p(P) = p^{12}U^{-1}(P) \in \mathcal{O}_K$. As K is an imaginary quadratic field, for every nonzero element $\alpha \in \mathcal{O}_K$, $\log|\alpha| \geq 0$, hence

$$0 \leq \log|U(P)| \leq 12\log p.$$

□

We define the involution w on $\mathcal{H}$ by $w(\tau) = -1/\tau$ and the function g_0 on $\mathcal{H}$ by $g_0 := g \circ w$.

The following lemma, that we call "locating near cusps lemma" allows us to reduce Runge's method to computation with the two functions g and g_0.

Lemma 3.3. *For every point $P \in Y_0(p)(\mathbb{C})$, there exists $\tau \in \mathcal{D} + \mathbb{Z}$ such that τ or $-1/\tau$ is above P by the canonical projection $\mathcal{H} \to Y_0(p)(\mathbb{C})$. In the first case, we say P is near c_∞, and then $j(P) = j(\tau)$ and $U(P) = g(\tau)$. In the second case, we say P is near c_0, and then $j(P) = j(\tau)$ and $U(P) = g_0(\tau)$.*

Proof. Let $P \in Y_0(p)(\mathbb{C})$. Choose a lift $\tau_0 \in \mathcal{H}$ of P. There exists $\beta \in \mathrm{SL}_2(\mathbb{Z})$ such that $\beta \cdot \tau_0 = \tau_1 \in \mathcal{D}$. This τ_1 is not above P anymore unless $\beta \in \Gamma_0(p)$ (in this case, choose $\tau = \tau_1$ in the lemma, and P is near c_∞). Suppose now $\beta \notin \Gamma_0(p)$. From (4), we can write

$$\beta^{-1} = \gamma \cdot w \cdot \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

for some $k \in \mathbb{Z}$ and $\gamma \in \Gamma_0(p)$, $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Hence, $\tau = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \cdot \tau_1 \in \mathcal{D} + \mathbb{Z}$, and $w.\tau = \gamma^{-1} \cdot \tau_0$ is above P. In this case, we say P is near c_0. □

We now need a lemma for precise estimates of q-expansions of g and g_0.

Lemma 3.4. *For every $r \in]0,1[$ and every $q \in \mathbb{C}$ such that $|q| \leq r$,*

$$\sum_{n=1}^{+\infty} |\log|1-q^n|| \leq \frac{-\log(1-r)}{r(1-r)}|q|.$$

For every $q \in \mathbb{C}$ such that $|q| < 1$,

$$\sum_{n=1}^{+\infty} |\log|1-q^n|| \leq \frac{\pi^2}{6\log|q^{-1}|}.$$

Proof. The first inequality is a straightforward consequence of the triangular inequality and the maximum principle. The second one can be found in the proof of Lemma 3.5 of [3]. □

We obtain from this lemma nontrivial bounds on g and g_0.

Proposition 3.5. *For every $\tau \in \mathcal{D} + \mathbb{Z}$,*

$$|\log|g(\tau)| + (p-1)\log|q_\tau|| \leq 25|q_\tau|.$$
$$|\log|g_0(\tau)| - \frac{p-1}{p}\log|q_\tau|| \leq \frac{4\pi^2 p}{\log|q_\tau^{-1}|} + 12\log(p).$$

Proof. Using the q-expansion of g and Lemma 3.4 with $r = 0.005$, we have

$$|\log|g_\infty(\tau)| + (p-1)\log|q_\tau|| = 24\left|\sum_{\substack{n\geq 1\\(p,n)=1}} \log|1-q_\tau^n|\right| \leq -24\frac{\log(0.995)}{0.995\cdot 0.005}|q_\tau| \leq 25|q_\tau|$$

because $|q_\tau| \leq 0.005$ when $\tau \in \mathcal{D} + \mathbb{Z}$. For the bound with g_0, we use the other inequality of Lemma 3.4 with q-expansion of g_0 and obtain

$$|\log|g_0(\tau)| - \frac{p-1}{p}\log|q_\tau| - 12\log(p)| = 24\left|\sum_{\substack{n\geq 1\\(p,n)=1}} \log|1-q_\tau^{n/p}|\right| \leq \frac{4\pi^2}{\log|q_\tau^{-1/p}|} = \frac{4\pi^2 p}{\log|q_\tau^{-1}|}.$$

□

Finally, we recall an inequality for the j-invariant (extracted from Corollary 2.2 (*iii*) of [3]).

Proposition 3.6. *For every $\tau \in \mathcal{D} + \mathbb{Z}$, if $|j(\tau)| > 3500$, then $\log|j(\tau)| \leq \log|q_\tau^{-1}| + \log(2)$.*

We can now state our bound on the j-invariant.

Proposition 3.7. *Let K be an imaginary quadratic field. For every prime number p and every point $P \in Y_0(p)(\mathcal{O}_K)$,*

$$\log|j(P)| < 2\pi\sqrt{p} + 6\log(p) + 8.$$

Proof. Let τ be a point of $\mathcal{D}+\mathbb{Z}$ associated to P by the "locating near cusps lemma". If we have $\log|j(P)| < 2\pi\sqrt{p}$, there is nothing to prove. If not, $|j(\tau)| > 3500$ hence $\log|j(\tau)| \leq \log|q_\tau^{-1}| + \log(2)$ by Proposition 3.6. We now have to bound $|q_\tau^{-1}|$. If P is near c_∞, we have $\log|g(\tau)| = \log|U(P)| \leq 12\log p$ by Lemma 3.2. By Proposition 3.5, we obtain

$$\log|q_\tau^{-1}| \leq \frac{25|q_\tau| + 12\log p}{p-1} \leq 2\pi\sqrt{p} \tag{5}$$

after a little analysis (as $|q_\tau| \leq 0.005$ here). If P is near c_0, $\log|g_0(\tau)| = \log|U(P)| \geq 0$ by Lemma 3.2. By Proposition 3.5, we obtain this time

$$\left(\frac{p-1}{p}\right)\log|q_\tau^{-1}| \leq \frac{4\pi^2 p}{\log|q_\tau^{-1}|} + 12\log(p),$$

hence

$$\log|q_\tau^{-1}| \leq \frac{2\pi p}{\sqrt{p-1}} + \frac{6p\log(p)}{(p-1)} \leq 2\pi\sqrt{p} + 6\log(p) + 7 \tag{6}$$

because $p \geq 2$, after a small analysis on the remaining terms. In each case, (5) or (6) gives us the result. □

4 Isogeny theorems and end of the proof

We now use isogeny theorems from [9] to complete the proof and obtain completely explicit bounds. These theorems use the notion of stable Faltings height $h_{\mathcal{F}}$ (see [9], subsection 2.3 for details), but we recall that for every elliptic curve E defined over a number field K,

$$h_{\mathcal{F}}(E) \leq \frac{1}{12} h(j(E)) + 2.38 \tag{7}$$

with h the absolue logarithmic height of $j(E) \in K$, that is,

$$h(j(E)) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M} \max(0, \log(|j(E)|_v))$$

where M is the set of places of K : see Lemma 7.9 of [9]. The different normalisations for Faltings height in [9] have to be taken into account : with the notations of this article, $h(E) = h_{\mathcal{F}}(E) + \log(\pi)/2$, so we obtain the constant 2.38 instead of 2.95, but this does not matter for the following, as we round up to 3.

The following result is proved in [9] in part 7.3, but is not stated this way. We explain why after its statement.

Proposition 4.1 ([9], part 7.3)**.** *Let E be an elliptic curve without complex multiplication and B an abelian surface both defined over the number field K. Let $\psi : B \to E \times E$ be an isogeny defined over K. Suppose (hypothesis $(*)$) that for every embedding $\sigma : K \to \mathbb{C}$, if $\Omega_{E,\sigma}$ and $\Omega_{B,\sigma}$ are the period lattices of E and B with respect to this embedding, $\mathrm{d}\psi(\Omega_{B,\sigma})$ (which is a sublattice of $\Omega_{E,\sigma}^2$) contains an element (ω_1, ω_2) of $\Omega_{E,\sigma}$ which is a $\mathbb{Z}$-basis of $\Omega_{E,\sigma}$. Then,*

$$\deg(\psi) \leq 10^7 [K:\mathbb{Q}]^2 (\max\{h_{\mathcal{F}}(E), 985\} + 4\log[K:\mathbb{Q}])^2.$$

Proof. The bound given here is exactly the bound of Theorem 1.4 of [9], because the computation is almost exactly the same. Consider some isogeny $\psi : B \to E \times E$ satisfying hypothesis $(*)$ above. For every embedding σ, there is a canonical norm $\|\cdot\|_\sigma$ (coming from a principal polarization of E) on the tangent space $t_{E,\sigma}$, which contains $\Omega_{E,\sigma}$. We fix an embedding σ_0 such that there is a basis (ω_1, ω_2) of $\Omega_{E,\sigma}$ which is minimal amongst all minimal bases for all possible period lattices $\Omega_{E,\sigma}$. This means that

$$\|\omega_1\|_{\sigma_0} = \max_{\sigma} \min_{\substack{\omega \in \Omega_{E,\sigma} \\ \omega \neq 0}} \|\omega\|_\sigma$$

and $\omega_2 = \tau\omega_1$ with τ in the Siegel fundamental domain (so that $y = \mathrm{im}(\tau)$ is minimal amongst all choices of embeddings and minimal bases for these embeddings). This choice of σ_0 to minimise y is the same as in part 7.3 of [9]. We now identify all considered abelian varieties with their scalar extensions to $\mathbb{C}$ via this embedding σ_0, and therefore omit all further mention to the embeddings in the notation. We can compose ψ by an isomorphism of $E \times E$ so that $d\psi(\Omega_E)$ contains the basis (ω_1, ω_2) previously chosen, because we assumed hypothesis $(*)$. We then consider $A = E \times E \times B$ and a period $\omega = (\omega_1, \omega_2, \chi)$ of $\Omega_E^2 \times \Omega_B$, with $\chi \in \Omega_B$ such that $\mathrm{d}\psi(\chi) = (\omega_1, \omega_2)$. The minimal abelian subvariety A_ω of A containing ω in its tangent space is then

$$A_\omega = \{(\psi(z), z), z \in B\}.$$

Indeed, the inclusion $A_\omega \subset \{(\psi(z), z), z \in B\}$ is clear and the projection from A_ω to $E \times E$ is a subvariety of $E \times E$ containing (ω_1, ω_2) in its period lattice. As E is an elliptic curve without complex multiplication, the endomorphism ring of $E \times E$ is $M_2(\mathbb{Z})$, therefore no strict abelian subvariety of $E \times E$ contains (ω_1, ω_2) in its tangent space. This proves that the dimension of A_ω is at least 2, hence the equality above. The abelian variety A_ω is canonically isomorphic to B and the projection to $E \times E$ is an isogeny of degree Δ. Everything is in place, and from now on, we can repeat the computation of part 7.3 of [9] to obtain the bound of the proposition. There are only two small differences to be noticed : first, the embedding σ_0 can be real or complex, and the bound can change if σ_0 is real as part 7.3 uses that σ_0 is complex to improve slightly on the bound. To avoid this issue, we consider $K' = K(i)$ and go back from the start with K' instead of K. This sticks with the proof of part 7.3 as here also, an extension of degree at most 2 of K was needed. Second, the computation of the slopes in Lemma 7.6 of [9] is slightly different, but using only that B is isogenous to $E \times E$ with degree Δ will give the exact same bound. □

For our results on $\mathbb{Q}$-curves, we will prove the following result that gives an explicit version of Serre's surjectivity theorem, as stated by Masser-Wüstholz in [11].

Theorem 4.2. *Let E be an elliptic curve defined over the number field K without complex multiplication. We define $\mathcal{B}$ (resp. $\mathcal{C}$) a set of prime numbers p such that the image of $\rho_{E,p}$ is included in a Borel subgroup (resp. the normaliser of a Cartan subgroup, split or nonsplit) of $\mathrm{GL}(E_p)$. Then, the following inequality holds :*

$$\prod_{p\in\mathcal{B}} p \prod_{q\in\mathcal{C}} \frac{q^2}{4} \leq 10^7 [K:\mathbb{Q}]^2 \left(\max\{h_{\mathcal{F}}(E), 985\} + 4\log[K:\mathbb{Q}] + 4|\mathcal{C}|\log(2)\right)^2.$$

In particular, the Galois representation $\rho_{E,p}$ is surjective for every prime number

$$p > 10^7 [K:\mathbb{Q}]^2 \left(\max\{h_{\mathcal{F}}(E), 985\} + 4\log[K:\mathbb{Q}]\right)^2$$

not dividing the discriminant of K.

First, we prove a technical lemma to help us prove our isogeny ψ satisfies $(*)$.

Lemma 4.3. *Let p be a prime number, V be an $\mathbb{F}_p$-vector space of dimension 2 and $\underline{v}$ be a basis of V. Then, for $g \in \mathrm{GL}(V)$, the quadratic form*

$$Q : x \longmapsto \det_{\underline{v}}(x, g.x)$$

is surjective in $\mathbb{F}_p$ if g is semisimple and not an homothety.

Proof. First, if g is simple, Q does not have any isotropic vector, and is therefore surjective (looking at its expression in an orthonormal basis). In the other cases, as for every $x, y \in V$ and any bases $\underline{v}$ and $\underline{v'}$,

$$\det_{\underline{v'}}(x,y) = \det_{\underline{v'}}(\underline{v}) \cdot \det_{\underline{v}}(x,y)$$

from the properties of determinant, two quadratic forms Q built from two different choices of bases are proportional. Therefore, Q is surjective if and only if it is surjective for one/any other choice of basis. We assumed g is semisimple but not simple, therefore there is a basis $\underline{v} = (v_1, v_2)$ in which g is diagonal with distinct eigenvalues λ and μ. In this basis, the expression of Q is simply, for $x = x_1 v_1 + x_2 v_2$,

$$Q(x) = (\mu - \lambda) x_1 x_2,$$

hence Q is surjective. □

We can now prove Theorem 4.2.

Proof. We begin with the first inequality and will explain afterwards how it implies the effective version of Serre's surjectivity theorem. Let us fix K' an extension of K of degree $2^{|\mathcal{C}|}$ such that for every $q \in \mathcal{C}$, the image of $\rho_{E,q}$ restricted to $\mathrm{Gal}(\overline{K}/K')$ is included in a Cartan subgroup. Define $n_{\mathcal{B}} = \prod_{p\in\mathcal{B}} p$ and $n_{\mathcal{C}} = \prod_{q\in\mathcal{C}} q$. Then the proposition to prove is equivalent to

$$n_{\mathcal{B}} n_{\mathcal{C}}^2 \leq 10^7 [K':\mathbb{Q}]^2 \left(\left(\max\{h_{\mathcal{F}}(E), 985\} + 4\log[K':\mathbb{Q}]\right)\right)^2.$$

Therefore, we only need to find an abelian variety B and an isogeny $\psi : B \to E \times E$ both defined over K', and such that ψ has degree $n_{\mathcal{B}} n_{\mathcal{C}}^2$, satisfying the hypothesis $(*)$ of Proposition 4.1. For every $p \in \mathcal{B}$, we choose C_p an $\mathbb{F}_p$-line fixed by $\rho_{E,p}$ and define $G_p = C_p \times E[p]$, which is a subgroup of $E[p]^2$ of cardinality p^3. For every $q \in \mathcal{C}$, we choose an element g_q of the associated Cartan subgroup which is not an homothety (notice such an element is always semisimple). Then, we consider $G_q := \{(x, g_q \cdot x), x \in E[q]\} \subset E[q]^2$. This group is of cardinality q^2 and stable by the diagonal action of the Cartan subgroup (as Cartan subgroups are commutative), hence defined over K' in $E \times E$ by hypothesis. We now consider

$$G = \bigoplus_{p\in\mathcal{B}} G_p \oplus \bigoplus_{q\in\mathcal{C}} G_q \subset E[n_{\mathcal{B}} n_{\mathcal{C}}]^2.$$

This is a group of order $n_{\mathcal{B}}^3 n_{\mathcal{C}}^2$, defined over K' by hypothesis. We consider the quotient abelian variety $B = (E \times E)/G$ and the quotient morphism $\varphi : E \times E \to B$ with kernel G. As G is contained in $E[n_{\mathcal{B}} n_{\mathcal{C}}]^2$, there exists an isogeny $\psi : B \to E \times E$ such that

$$\psi \circ \varphi = [n_{\mathcal{B}} n_{\mathcal{C}}],$$

that is, the multiplication by $n_{\mathcal{B}} n_{\mathcal{C}}$ on $E \times E$. This isogeny is defined over K', and by degree multiplicativity, we find $\deg(\psi) = n_{\mathcal{B}} n_{\mathcal{C}}^2$. Hence, we only have to prove now that ψ satisfies $(*)$.

Let $\sigma : K' \to \mathbb{C}$ be an embedding. We now prove hypothesis $(*)$ for ψ and σ. For this embedding, E is naturally identified with the quotient of its tangent space $t_{E,\sigma}$ by its period lattice $\Omega_{E,\sigma}$ (we then omit further reference to σ here). If π is the projection $t_E \times t_E \to E \times E$, the lattice $\Omega = \pi^{-1}(G)$ of τ_E^2 defines a quotient abelian variety $t_E \times t_E / \Omega$ that is isomorphic to B. With these embeddings, we have the commutative diagram

$$\begin{array}{ccccc} t_E \times t_E & \xrightarrow{\mathrm{Id}} & t_E \times t_E & \xrightarrow{n_{\mathcal{B}} n_{\mathcal{C}}} & t_E \times t_E \\ \downarrow{\scriptstyle \pi} & & \downarrow & & \downarrow{\scriptstyle \pi} \\ E \times E & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & E \times E. \end{array}$$

Therefore, it remains to prove that $\Omega' = n_{\mathcal{B}} n_{\mathcal{C}} \Omega \subset \Omega_E \times \Omega_E$ contains a basis of Ω_E. Choose a basis (e_1, e_2) of Ω_E.

Now, consider the image of Ω' in $(\Omega_E / p\Omega_E)^2$ for $p \in \mathcal{B} \cup \mathcal{C}$. Notice that after multiplication by $1/p$, this image identifies with a subgroup of $((\Omega_E/p)/(\Omega_E))^2$, that is, $E[p]^2$. From the definitions of Ω and Ω', the image of Ω'/p in $E[p]^2$ is $((n_{\mathcal{B}} n_{\mathcal{C}})/p)G_p = G_p$ (the prime-to-p part of Ω is mapped to Ω_E^2 when multiplied by $n_{\mathcal{B}} n_{\mathcal{C}}/p$). A canonical $\mathbb{F}_p$-basis of $E[p]^2$ is $\pi(e_1/p, e_2/p)$ and we now identify $E[p]$ to ${\mathbb{F}_p}^2$ with this choice of basis.

For $p \in \mathcal{B}$, we choose a nonzero vector $(a, b) \in C_p$. Then, we fix (c, d) such that $ad - bc = 1 \mod p$. Therefore, the vector $((a, b), (c, d))$ belongs to G_p and is of determinant 1 in the canonical basis $\pi(e_1/p, e_2, p)$.

For $q \in \mathcal{C}$, by Lemma 4.3, we can choose $x \in E[q]$ such that $\det_{\pi(e_1/q, e_2, q)}(x, g_q \cdot x) = 1$. Therefore, the subgroup G_q of $E[q]^2$ contains an element of determinant 1 in the canonical basis $\pi(e_1/q, e_2, q)$.

We just proved that for every $p \in \mathcal{B}$, there exists a matrix $\gamma_p = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p)$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \overline{e_1} \\ \overline{e_2} \end{pmatrix} \in \Omega'/(p\Omega_E)^2$$

The specialisation morphism $\mathrm{SL}_2(\mathbb{Z}) \to \prod_{p \in \mathcal{B} \cup \mathcal{C}} \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is known to be surjective ([24], Chapter XIII, Exercise 18) , therefore there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\gamma \cdot \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} \in \Omega' + (n_{\mathcal{B}} n_{\mathcal{C}}) \Omega_E^2 \subset \Omega',$$

because Ω contains Ω_E^2. Such an element $\gamma \cdot (e_1, e_2)$ is by construction a basis of Ω_E, therefore Ω' contains a basis of Ω_E. This concludes the proof of the first inequality of the theorem.

Now, this result implies the surjectivity theorem in the following way : take p a prime number such that $\rho_{E,p}$ is not surjective, not dividing the discriminant of K. Then, the image of $\rho_{E,p}$ is included in a Borel subgroup, the normaliser of a Cartan subgroup, or an exceptional subgroup. In the Borel case, we obtain $p \leq 10^7 [K : \mathbb{Q}]^2 (\max\{h_{\mathcal{F}}(E), 985\} + 4 \log[K : \mathbb{Q}])^2$. In the Cartan case, we obtain $p \leq 2 \cdot 10^{3.5} [K : \mathbb{Q}] (\max\{h_{\mathcal{F}}(E), 985\} + 4 \log[K : \mathbb{Q}] + 4 \log(2))$. In the exceptional case, we have $p \leq 30[K : \mathbb{Q}] + 1$ by Proposition 1.2. The maximum of these three bounds is obtained for the Borel case, and it gives us the effective surjectivity theorem. □

Remark 4.3.1. Some papers, such as [5], give other (nonexplicit) versions of Serre's surjectivity theorem, but based on the conductor N_E of E. Note however, that by [5], Theorem 3 (which assumes the degree conjecture...), our result implies that for E defined over $\mathbb{Q}$, one would have surjectivity for $p \gg \log(N_E)^2$.

This gives us our direct application for $\mathbb{Q}$-curves.

Corollary. *Let E be a $\mathbb{Q}$-curve without complex multiplication, of squarefree degree $d(E)$ over a quadratic field K.*

If $\mathbb{P}\overline{\rho}_{E,p}$ is reducible for some prime p not dividing d,

$$d(E)p \leq 10^7[K:\mathbb{Q}]^2(\max\{h_{\mathcal{F}}(E), 985\} + 4\log[K:\mathbb{Q}])^2$$

If $\mathbb{P}\overline{\rho}_{E,p}$ has image in the normaliser of a Cartan subgroup for some prime p not dividing d,

$$d(E)p^2 \leq 4 \cdot 10^7[K:\mathbb{Q}]^2(\max\{h_{\mathcal{F}}(E), 985\} + 4\log(2[K:\mathbb{Q}]))^2.$$

We can now state the main theorem in detail.

Theorem 4.4. *Let K be an imaginary quadratic field of discriminant $-D_K$. For every strict $\mathbb{Q}$-curve E defined over K with degree $d(E)$ and every prime number p coprime with $d(E)$,*

- *If $p \geq 2 \cdot 10^{13}$, the representation $\mathbb{P}\overline{\rho}_{E,p}$ is not included in a Borel subgroup.*
- *If $p \geq 10^7$ the representation $\mathbb{P}\overline{\rho}_{E,p}$ is not included in the normaliser of a split Cartan subgroup.*
- *If $p \geq \max(10^7, 50D_K^{1/4}\log(D_K))$ and does not divide D_K, the representation $\mathbb{P}\overline{\rho}_{E,p}$ is not included in the normaliser of a nonsplit Cartan subgroup.*
- *If $p \geq 67$, the representation $\mathbb{P}\overline{\rho}_{E,p}$ is not included in an exceptional subgroup.*

Proof. The exceptional case is solved by Proposition 1.2. For the other cases, we use Propositions 2.3, 2.6 and 2.8 to know that with the given bounds, if $\mathbb{P}\overline{\rho}_{E,p}$ is included in one of the three types of maximal subgroups, $j(E) \in \mathcal{O}_K$. Consider now d_0 the smallest prime divisor of d. We use Runge's method in $X_0(d_0)(\mathcal{O}_K)$ (Proposition 3.7) to obtain

$$\log|j(E)| \leq 2\pi\sqrt{d_0} + 6\log(d_0) + 8.$$

As $j(E) \in \mathcal{O}_K$ and K is imaginary quadratic, $h_{\mathcal{F}}(E) \leq (\log|j(E)|)/12 + 3$ by (7). Computing with the previous Corollary and the Runge bound above, we finally obtain the theorem. □

Some comments are in order about the different steps of the proof here. First, about Mazur's method, we suspect that it can be used for any central $\mathbb{Q}$-curve over any number field in Borel and split Cartan cases, giving bounds depending only on the degree of this field (but maybe growing exponentially in this degree). Indeed, both proofs in theses cases mainly rely on the fact that $X_0(d) \to X(1)$ is unramified at ∞ and ramified at 0, but it is actually ramified at *every* cusp of $X_0(d)$ different from ∞, so we could make use of all Atkin-Lehner involutions group and obtain a formal immersion satisfying the good conditions. Furthermore, all the theoretical work is done for the analysis of components group by Proposition 1.11, although a precise equivalent of Lemma 2.2 for a general number field is likely to be hard to write. About the nonsplit Cartan case, it is not completely clear for now what happens, but Ellenberg's trick might be applied for some (but not all) bigger number fields.

Regarding Runge's method, because for a central $\mathbb{Q}$-curve of degree d, with d having r prime factors, the number of rational cusps of $X_0(d)$ is 2^r, which is also the expected degree of the field of definition K of E. Therefore, for Runge's condition to hold, we need K not to be a totally real number field. The exponent on d we should expect to bound $\log|j(E)|$ is not known for now (but it may be $1/2$ as in the quadratic case).

We would also like to point out that up until now, if we know about infinite families of quadratic $\mathbb{Q}$-curves of degrees 2,3,5,7 or 11 over quadratic fields (see for instance [10] for parametrisations), examples on bigger fields turn out to be more rare. Of course, for reasons of genus, when the degree d is too large, there is only a finite number of $\mathbb{Q}$-curves of degree d but the limit has not been precisely computed yet.

5 Appendix : Analytic estimates of weighted sums of L-functions

The aim of this appendix is to prove Proposition 2.8. We fix an imaginary quadratic field K of discriminant $-D$ and χ_K (often shortened in χ) its quadratic character. Thanks to Proposition 2.7 (we use the same notations), we only have to find, for every $p > 50D^{1/4}\log(D)$ not dividing D, an eigenform $f \in S_2(\Gamma_0(p))^{new}$ such that $w_p \cdot f = f$ and $L(f \otimes \chi_K, 1) \neq 0$.

For every positive integers m, N and every vector space $V \subset S_2(\Gamma_0(N))$, we denote by a_m and L_χ the linear forms defined on V by

$$a_m : f \mapsto a_m(f), \quad L_\chi : f \mapsto L(f \otimes \chi_K, 1).$$

We recall that $S_2(\Gamma_0(N))^+$ (resp. $S_2(\Gamma_0(N))^-$)) is the space of modular forms of $S_2(\Gamma_0(N))$ such that $w_N \cdot f = f$ (resp. $w_N \cdot f = -f$). We also denote by $S_2(\Gamma_0(N))^{old}$ (resp. $S_2(\Gamma_0(N))^{new}$) the space of old (resp. new) modular forms of $S_2(\Gamma_0(N))$. The scalar product of a_m and L_χ on a vector space $V \subset S_2(\Gamma_0(N))$ is

$$(a_m, L_\chi)_V := \sum_{f \in \mathcal{F}_V} \overline{a_m(f)} L(f \otimes \chi_K, 1),$$

where $\mathcal{F}_V$ is any Petersson-orthonormal basis of V. This will be shortened in $(a_m, L_\chi)_N$ (resp. $(a_m, L_\chi)_N^{new}$, $(a_m, L_\chi)_N^{old}$, $(a_m, L_\chi)_N^{+,new}$, $(a_m, L_\chi)_N^{+}$, $(a_m, L_\chi)_N^{-}$) for $V = S_2(\Gamma_0(N))$ (resp.

$S_2(\Gamma_0(N))^{new}$, $S_2(\Gamma_0(N))^{old}$, $S_2(\Gamma_0(N))^{+,new}$, $S_2(\Gamma_0(N))^{+}$, $S_2(\Gamma_0(N))^{-}$), and similarly with $(a_m, a_n)_V$. We will prove the following result which immediately implies Proposition 2.8.

Proposition 5.1. *For every imaginary quadratic field K with discriminant $-D$ and Dirichlet character χ, and every prime number $p > 50D^{1/4}\log(D)$ not dividing D,*

$$(a_1, L_\chi)_{p^2}^{+,new} \neq 0.$$

For any positive integer M and any eigenform $g \in S_2(\Gamma_0(M))$, the L-function of g admits a meromorphic continuation over $\mathbb{C}$ and

$$L(g,1) = \begin{cases} 4\pi \int_{1/\sqrt{M}}^{+\infty} g(iu)du \text{ if } g_{|w_M} = -g. \\ 0 \qquad\qquad\qquad\quad \text{if } \ g_{|w_M} = g \end{cases} \tag{8}$$

Moreover, if f is a modular form in $S_2(\Gamma_0(N))$ with N prime to D, $f \otimes \chi_K \in S_2(\Gamma_0(D^2N))$ and

$$(f \otimes \chi)_{|w_{D^2N}} = \chi(-N)(f_{|w_N} \otimes \chi) \tag{9}$$

(for more details, see ([21], § I.5)). Hence, for an eigenform $f \in S_2(\Gamma_0(p^2))^+$, the sign of the functional equation of $L(f \otimes \chi)$ is $-\chi(-p^2) = 1$ because $\chi(-1) = -1$: this is where we need K to be imaginary to ensure that the twisting actually changes the sign of the functional equation for L. In the real quadratic case, we expect from Birch and Swinnerton-Dyer conjecture that there is no nontrivial rank zero quotient of the jacobian of $X_{\text{nonsplit}}(p^2)$, because $J(X_{\text{nonsplit}}(p^2))$ is isogenous over $\mathbb{Q}$ to $J_0(p^2)^{+,new}$ [19]. In our situation, twisting reverts the sign of the functional equation, so $(a_1, L_\chi)_{p^2}^{-} = 0$ and

$$(a_1, L_\chi)_{p^2}^{new} = (a_1, L_\chi)_{p^2}^{+,new} = (a_1, L_\chi)_{p^2} - \frac{p}{p^2-1}(a_1, L_\chi)_p + \frac{\chi(p)}{p^2-1}(a_p, L_\chi)_p \tag{10}$$

from Lemma 3.12 of [7] and its proof. The idea is that $(a_1, L_\chi)_{p^2}$ is close to 4π in modulus when p is large enough compared to D, whereas the remaining term is close to 0. From (10), we only need to estimate $(a_m, L_\chi)_N$ for $m = 1, N = p^2$ (case (1)), $m = 1, N = p$ (case (2)) and $m = N = p$ (case (3)) with $p \geq 7$ prime not dividing D (the reader should mind throughout the estimates).

For an estimate of $(a_m, L_\chi)_N$, we will use Petersson's trace formula ([22], Proposition 14.5) in a restricted version of Akbary ([29], Theorem 3). For this, we define for every integers m, n, c the Kloosterman sum

$$S(m,n;c) := \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} e^{2i\pi(mv + n\overline{v})/c}$$

where for every $v \in (\mathbb{Z}/c\mathbb{Z})^*$, $\overline{v}$ is the inverse of v.

Next proposition is a reformulation of Akbary's trace formula in weight 2 case.

Proposition 5.2. *Let m, n, N be three positive integers and $\varepsilon = \pm 1$. We have*

$$\frac{1}{2\pi\sqrt{mn}}(a_m, a_n)_N^+ = \delta_{mn} 2\pi \sum_{\substack{c>0 \\ N|c}} c^{-1} S(m,n;c) J_1\left(\frac{4\pi\sqrt{mn}}{c}\right) - \frac{2\pi\varepsilon}{\sqrt{N}} \sum_{\substack{d>0 \\ (d,N)=1}} d^{-1} S(n, mN^{\phi(d)-1}; d) J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{N}}\right),$$

where δ is the Kronecker symbol, J_1 is the Bessel function of the first kind of order 1, (d,N) is the greatest common divisor of d and N and ϕ is the Euler totient function.

Notice that summing Akbary's formula for $\varepsilon = 1$ and -1 gives Petersson's trace formula. As a normalized eigenform $f \in S_2(\Gamma_0(N))$ contributes for zero in (a_m, L_χ) if $f_{|w_N} = \chi(-N)f$ by (9), $(a_m, L_\chi)_N = (a_m, L_\chi)_N^\varepsilon$ with $\varepsilon = -\chi(-N) = \chi(N)$. For every $f \in S_2(\Gamma_0(N))^\varepsilon$, we have from (8)

$$L_\chi(f) = 4\pi \int_{1/(D\sqrt{N})}^{+\infty} (f \otimes \chi)(iu) du = 2 \sum_{n=1}^{+\infty} \frac{a_n(f)\chi(n)}{n} e^{-\frac{2\pi n}{D\sqrt{N}}} \tag{11}$$

For convenience, we use throughout this section the notation

$$x = \frac{2\pi}{D\sqrt{N}}.$$

From (11), we get $(a_m, L\chi)_N = 2\sum_{n=1}^{+\infty} \frac{\chi(n)}{n} e^{-nx} (a_m, a_n)_N^\varepsilon$ hence by Akbary's formula

$$(a_m, L\chi)_N = 4\pi\chi(m)e^{-mx} - 8\pi^2\sqrt{m}\left(A(m,\chi,N) + \frac{\varepsilon}{\sqrt{N}} B(m,\chi,N)\right) \tag{12}$$

with

$$A(m,\chi,N) := \sum_{n=1}^{+\infty} \frac{\chi(n)}{\sqrt{n}} e^{-nx} \sum_{\substack{c>0 \\ N|c}} c^{-1} S(m,n;c) J_1\left(\frac{4\pi\sqrt{mn}}{c}\right)$$

$$B(m,\chi,N) := \sum_{n=1}^{+\infty} \frac{\chi(n)}{\sqrt{n}} e^{-nx} \sum_{\substack{d>0 \\ (d,N)=1}} d^{-1} S(n, mN^{\phi(d)-1}; d) J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{N}}\right)$$

This is where our approach starts to differ from [8] : this exact formula allows better results in general. It can be readily checked with help of the Weil bounds (Proposition 5.3) and the classical bounds for Bessel functions that these double sums converge absolutely, so we can switch the terms. We obtain

$$A(m,\chi,N) = \sum_{\substack{c>0 \\ N|c}} \frac{\mathcal{S}_A(c)}{c} \quad \text{with} \quad \mathcal{S}_A(c) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{\sqrt{n}} S(m,n;c) J_1\left(\frac{4\pi\sqrt{mn}}{c}\right) e^{-nx}. \tag{13}$$

$$B(m,\chi,N) = \sum_{\substack{d>0 \\ (d,N)=1}} \frac{\mathcal{S}_B(d)}{d} \quad \text{with} \quad \mathcal{S}_B(d) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{\sqrt{n}} S(n, mN^{\phi(d)-1}; d) J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{N}}\right) e^{-nx}. \tag{14}$$

These sums are the ones we are going to bound in two different ways, for every $N|c$ and every d prime to N. Let us recall the Weil bounds on Kloosterman sums.

Proposition 5.3. *For every positive integers m, n, c, we have*

$$|S(m,n;c)| \leq (m,n,c)^{1/2}\tau(c)\sqrt{c}$$

with $\tau(c)$ the number of positive divisors of c. Furthermore, if for an odd prime p, we have $c = p^\alpha c'$ with $(p,c') = 1$ and $\alpha \geq 1$,

$$|S(m,n;c)| \leq 2\tau(c')(m,n,c)^{1/2}\sqrt{c}$$

and the latter bound is replaced by $\tau(c')(m,n,c)^{1/2}\sqrt{c'}$ when p divides m but not n (or the reverse) and $\tau(c/p)(m,n,c)^{1/2}\sqrt{c}$ when p divides m and n.

Proof. By multiplicativity of Kloosterman sums, this only needs to be checked for $c = p^\alpha$. If $p|nm$, this boils down to Ramanujan sums ([22], (3.2) and (3.3)). If $\alpha \geq 2$, there is an elementary proof ([22], Corollary 11.12), and if $\alpha = 1$ and $(p, mn) = 1$, this is a famous result of Weil ([22], Theorem 11.11). □

Remark 5.3.1. What we gain from the second bound is $2\tau(c')$ instead of $\tau(c)$, which will be an advantage for the case (1) ($m = 1$, $N = p^2$) and the third and fourth bounds will be of use in case (3) ($m = N = p$) for the next proposition.

Proposition 5.4. *For every $N|c$ and every d prime to N,*

$$|\mathcal{S}_A(c)| \leq \frac{2D\sqrt{N}\tau(c/N)}{\sqrt{c}}, \qquad |\mathcal{S}_B(d)| \leq \frac{D\sqrt{m}\tau(d)}{\sqrt{d}}$$

in cases (1), (2) *and* (3). *These bounds will be called "Weil-induced bounds".*

Proof. For every $x \in \mathbb{R}$, we have $|J_1(x)| \leq x/2$. By triangular inequality, this gives

$$|\mathcal{S}_A(c)| \leq \frac{2\pi\sqrt{m}}{c}\sum_{n=1}^{+\infty}|S(m,n;c)|e^{-nx}, \qquad |\mathcal{S}_B(d)| \leq \frac{2\pi\sqrt{m}}{d\sqrt{N}}\sum_{n=1}^{+\infty}|S(n,mN^{\phi(d)-1};d)|e^{-nx}.$$

In cases (1) and (2), $m = 1$ so $|S(m,n;c)| \leq 2\tau(c/N)\sqrt{c}$ and $|S(n,mN^{\phi(d)-1};d)| \leq \tau(d)\sqrt{d}$ by Weil bounds, as $(d,N) = 1$. But

$$\sum_{n=1}^{+\infty}e^{-nx} = \frac{1}{e^x - 1} \leq \frac{1}{x} = \frac{D\sqrt{N}}{2\pi}$$

so we get the upper bounds for $\mathcal{S}_A$ and $\mathcal{S}_B$. In case (3), $\mathcal{S}_B$ gives the upper bound by the same process as $(m,d) = 1$. For $\mathcal{S}_A$, we use the third and fourth bounds of previous proposition and get

$$\begin{aligned}\mathcal{S}_A(c) &\leq \frac{2\pi\sqrt{p}}{c}\sum_{(n,p)=1}\tau\left(\frac{c}{p}\right)\sqrt{\frac{c}{p}}e^{-nx} + \frac{2\pi\sqrt{p}}{c}\sum_{n=1}^{+\infty}\tau\left(\frac{c}{p}\right)\sqrt{pc}\,e^{-pnx} \\ &\leq \frac{2\pi\tau(c/p)}{(e^x-1)\sqrt{c}} + \frac{2\pi p\tau(c/p)}{(e^{px}-1)\sqrt{c}} \leq \frac{2D\sqrt{p}\tau(c/p)}{\sqrt{c}}\end{aligned}$$

with the same estimates. □

We will now obtain other bounds for $|\mathcal{S}_A|$ and $|\mathcal{S}_B|$ which will happen to be really sharper for "small" c and d. They rely on an Abel transform on the sums definining $\mathcal{S}_A$ and $\mathcal{S}_B$. For this, we use the following lemma which are analogues of Gauss sums and Polya-Vinogradov inequality for the twisting terms of (13) and (14).

Lemma 5.5. *Let $c \neq D$ and m be three fixed positive integers and F the least common multiple of c and D. Let χ be a quadratic Dirichlet character of conductor D. Then for every integer α,*

$$\left|\sum_{n=0}^{F-1} \chi(n) S(m,n;c) e^{2i\pi n\alpha/F}\right| \leq c\sqrt{D}$$

and the sum is zero when $(\alpha, F/(c,D)) \neq 1$. With the same notations, we have

$$\sup_{K,K'\in\mathbb{N}} \left|\sum_{n=K}^{K'} \chi(n) S(m,n;c)\right| \leq \frac{4c\sqrt{D}}{\pi^2}(\log(Dc)+1.5).$$

Remark 5.5.1. For $c=1$ (no Kloosterman sum), this is one of the versions of Polya-Vinogradov inequality for Dirichlet characters (weaker than [27]). For $D=1$ (no Dirichlet character), this is an analogous inequality for Kloosterman sums that we could not find in the literature but should exist in sharper versions.

Proof. We define $c' = c/(c,D)$ and $D' = D/(c,D)$. By definition of Kloosterman sums,

$$\sum_{n=0}^{F-1} \chi(n) S(m,n;c) e^{2i\pi n\alpha/F} = \sum_{v\in(\mathbb{Z}/c\mathbb{Z})^*} e^{2i\pi m\overline{v}/c} \sum_{n=0}^{F-1} \chi(n) e^{2i\pi n(v/c+\alpha/F)} \tag{15}$$

$$= \sum_{v\in(\mathbb{Z}/c\mathbb{Z})^*} e^{2i\pi m\overline{v}/c} \left(\sum_{n'=0}^{D-1} \chi(n')\theta^{n'}\right)\left(\sum_{\ell=0}^{c'-1} \theta^{\ell D}\right) \tag{16}$$

with $\theta = \exp(2i\pi(v/c+\alpha/F))$, because χ only depends on $n \mod D$. As θ^D is a c'-th root of unity, the right term of this equality is nonzero if and only if $\theta^D = 1$, that is if and only if

$$F|(D'v+\alpha)D \Longleftrightarrow c'|D'v+\alpha \Longleftrightarrow v = -(D')^{-1}\alpha \mod c'.$$

Let I_α be the set of the invertible $v \in (\mathbb{Z}/c\mathbb{Z})^*$ congruent to $(D')^{-1}\alpha \mod c'$. Notice first that if $(\alpha, c') \neq 1$, $I_\alpha = \emptyset$, hence the whole sum is zero. If $(\alpha, c') = 1$, $I_\alpha \neq \emptyset$ and we have

$$\sum_{n=0}^{F-1} \chi(n) S(m,kn;c) e^{2i\pi n\alpha/F} = c' \sum_{v\in I_\alpha} e^{2i\pi m\overline{v}/c} \sum_{n'=0}^{D-1} \chi(n')\theta^{n'}.$$

The inner sum is a Gauss sum on χ as θ is a D-th root of unit. More precisely, if we define $G(\chi) = \sum_{n=0}^{D-1} \chi(n) e^{2in\pi/D}$, by the usual properties of Gauss sums, $|G(\chi)| = \sqrt{D}$ and

$$\sum_{n=0}^{F-1} \chi(n) S(m,n;c) e^{2i\pi n\alpha/F} = c' \sum_{v\in I_\alpha} e^{2i\pi m\overline{v}/c} \chi\left(\frac{D'v+\alpha}{c'}\right) G(\chi).$$

Now, if $(D',\alpha) \neq 1$, $\chi((D'v+\alpha)/c') = 0$ for all $v \in I_\alpha$ so the sum is zero. In the general case, the cardinality of I_α is at most (c,D), so

$$\left|\sum_{n=0}^{F-1} \chi(n) S(m,n;c) e^{2i\pi n\alpha/F}\right| \leq c'(c,D)\sqrt{D} = c\sqrt{D}.$$

We now prove the second inequality, using Polya-Vinogradov approach. Take K, K' any integers. By discrete Fourier transform, as $\chi(n)S(m,n;c)$ is F-periodic in n, we have

$$\sum_{n=K}^{K'} \chi(n) S(m,n,c) = \frac{1}{F} \cdot \sum_{\gamma=0}^{F-1} \left[\sum_{\beta=0}^{F-1} \chi(\beta) S(m,\beta;c) e^{2i\pi\gamma\beta/F} \sum_{n=K}^{K'} e^{-2i\pi\gamma n/F}\right].$$

The interest of the previous step of the lemma is now clear : we have a geometric sum on n that is easy to bound on the right. Notice that the sum on β at $\gamma = 0$ is zero from the previous results because $(0, c'D') \neq 1$. We obtain

$$\left|\sum_{n=K}^{K'} \chi(n)S(m,n,c)\right| \leq \frac{1}{F} \cdot \sum_{\gamma=1}^{F-1} c\sqrt{D} \left|\frac{1-e^{-2i\pi\gamma(K'-K+1)/F}}{1-e^{-2i\pi\gamma/F}}\right| \leq \frac{c\sqrt{D}}{F} \cdot \sum_{\gamma=1}^{F-1} \frac{|\sin(\pi\gamma(K'-K+1)/F)|}{\sin(\pi\gamma/F)}.$$

Hence, it only remains to prove that for every integers $F \geq 1$ and K,

$$S_{K,F} := \sum_{\gamma=1}^{F-1} \frac{|\sin(\pi\gamma K/F)|}{\sin(\pi\gamma/F)} \leq \frac{4F}{\pi^2} \cdot (\log(F) + 1.5) \tag{17}$$

From Lemma 2 and proof of Lemma 3 of [27], we know that for every $n \in \mathbb{N}$ and every $x \in \mathbb{R}$,

$$\sum_{j=1}^{n} \frac{\cos(jx)}{j} > -\log(2) - \frac{2}{n}, \tag{18}$$

$$A_{K,F} := \sum_{\gamma=1}^{F-1} \frac{1}{\sin(\pi\gamma/F)} \leq \frac{2F}{\pi} (\log(F) + 0.13). \tag{19}$$

Using the Fourier series expansion of $|\sin\theta|$, we have

$$S_{K,F} = \frac{2}{\pi} \sum_{\gamma=1}^{F-1} \frac{1}{\sin(\pi\gamma/F)} - \frac{4}{\pi} \sum_{m=1}^{+\infty} \frac{1}{4m^2-1} \left(\sum_{\gamma=1}^{F-1} \frac{\cos(2\pi mK\gamma/F)}{\sin(\pi\gamma/F)} \right)$$

$$S_{K,F} = \frac{2}{\pi} A_{K,F} - \frac{4}{\pi} \sum_{m=1}^{+\infty} \frac{B_{m,K,F}}{4m^2-1}. \tag{20}$$

The bound for $A_{K,F}$ is given by (19), to there is only $B_{m,K,F}$ left to study. Suppose F is odd. For every $x \in [0, \pi/2]$, $\sin(x) = x - \varepsilon_x x^3/6 \geq 0$ with $\varepsilon_x \in [0,1]$, so we have

$$\left|\frac{1}{\sin(x)} - \frac{1}{x}\right| \leq \frac{x}{6-x^2}.$$

From this, we get

$$\begin{aligned} B_{m,K,F} &= 2 \sum_{\gamma=1}^{(F-1)/2} \frac{\cos(2\pi mK\gamma/F)}{\sin(\pi\gamma/F)} \\ &\geq 2 \sum_{\gamma=1}^{(F-1)/2} \frac{\cos(2\pi mK\gamma/F)}{\pi\gamma/F} - 2 \sum_{\gamma=1}^{(F-1)/2} \frac{\pi\gamma/F}{6-(\pi\gamma/F)^2} \\ &\geq -\frac{2F}{\pi}(\log(2) + 4/(F-1)) - \frac{2F}{\pi} \int_0^{\pi/2} \frac{udu}{6-u^2} \\ &\geq -\frac{2F}{\pi}(0.96 + 4/(F-1)). \end{aligned}$$

Here, we use (18) for the first sum and a careful sum-integral comparison for the second. Finally, as $\sum_{m=1}^{+\infty} 1/(4m^2-1) = 1/2$, we obtain from (19) and (20) the inequality

$$S_{K,F} \leq \frac{4F}{\pi^2}(\log(F) + 1.09 + 4/(F-1)),$$

which gives the result when $F \geq 11$, and we complete the proof by computation for $F \leq 10$. The proof works the same way for F even, except we have to take aside the term $\gamma = F/2$. □

These bounds on partial sums will give us new bounds on $|\mathcal{S}_A|$ and $|\mathcal{S}_B|$ that we write in the next proposition.

Proposition 5.6. *For every integers $N|c$ and $(d,N)=1$ different from D, we have*

$$|\mathcal{S}_A(c)| \leq 6\sqrt{Dm}(\log(Dc)+1.5) \qquad |\mathcal{S}_B(d)| \leq \frac{6\sqrt{Dm}(\log(Dd)+1.5)}{\sqrt{N}}.$$

Proof. For every integer $n \geq 0$, define

$$A_n := \sum_{k=1}^{n} \chi(k) S(m,k;c), \qquad B_n := \sum_{k=1}^{n} \chi(k) S(k, mN^{\phi(d)-1}; d).$$

so that

$$\mathcal{S}_A(c) = \sum_{n=1}^{+\infty} (A_n - A_{n-1}) \frac{4\pi\sqrt{m} f_A(n)}{c}, \qquad \mathcal{S}_B(d) = \sum_{n=1}^{+\infty} (B_n - B_{n-1}) \frac{4\pi\sqrt{m} f_B(n)}{d\sqrt{N}}$$

with

$$f_A(y) = \frac{cJ_1\left(\frac{4\pi\sqrt{my}}{c}\right)}{4\pi\sqrt{my}} e^{-yx}, \qquad f_B(y) = \frac{d\sqrt{N}J_1\left(\frac{4\pi\sqrt{my}}{d\sqrt{N}}\right)}{4\pi\sqrt{my}} e^{-yx}.$$

Therefore, with the Abel transform, we have

$$|\mathcal{S}_A(c)| \leq \frac{4\pi\sqrt{m}}{c} \cdot \sum_{n=1}^{+\infty} |A_n| \cdot |f_A(n) - f_A(n+1)| \qquad |\mathcal{S}_B(d)| \leq \frac{4\pi\sqrt{m}}{d\sqrt{N}} \cdot \sum_{n=1}^{+\infty} |B_n| \cdot |f_B(n) - f_B(n+1)|$$

$$|\mathcal{S}_A(c)| \leq \frac{16\sqrt{Dm}}{\pi} \operatorname{Totvar}(f_A)(\log(Dc)+1.5) \qquad |\mathcal{S}_B(d)| \leq \frac{16\sqrt{Dm}}{\pi\sqrt{N}} \operatorname{Totvar}(f_B)(\log(Dd)+1.5)$$

from Proposition 5.5, with $\operatorname{Totvar}(f_A)$ and $\operatorname{Totvar}(f_B)$ the total variations of f_A and f_B on $[0,+\infty[$. It is clear from their expression that these two total variations are both bounded by the total variation of $J_1(x)/x$ on $[0,+\infty[$, which is equal to

$$\int_0^{+\infty} \left|\frac{J_2(x)}{x}\right| dx \leq 1.1$$

Rounding up $16/\pi \cdot 1.1$ to 6, we obtain the desired bounds. □

For the next estimates, we recall some standard bounds in the following lemma.

Lemma 5.7. *For every integer $\lambda \geq 1$, we have*

$$\sum_{n=1}^{\lambda} \frac{1}{n} \leq \log(\lambda)+1, \qquad \sum_{n=1}^{\lambda} \frac{\log(n)}{n} \leq \frac{\log(\lambda)^2+1}{2}, \qquad \sum_{n\geq\lambda} \frac{\tau(n)}{n^{3/2}} \leq \frac{2\log(\lambda)+8}{\sqrt{\lambda}}.$$

with $\tau(n)$ the number of positive divisors of n.

Proof. The first two bounds are given by sum-integral comparison. For the third one, we have

$$\begin{aligned}\sum_{n\geq\lambda} \frac{\tau(n)}{n^{3/2}} &= \sum_{k,\ell=1}^{+\infty} \frac{\mathbf{1}_{k\ell\geq\lambda}}{(k\ell)^{3/2}} \\ &= \sum_{k=1}^{\lceil\lambda/2\rceil-1} \sum_{\ell=\lceil\lambda/k\rceil}^{+\infty} \frac{1}{(k\ell)^{3/2}} + \sum_{k=\lceil\lambda/2\rceil}^{\lambda-1} \sum_{\ell=2}^{+\infty} \frac{1}{(k\ell)^{3/2}} + \sum_{k=\lambda+1}^{+\infty} \sum_{\ell=1}^{+\infty} \frac{1}{(m\ell)^{3/2}}\end{aligned}$$

and from this cutting-up, we get the wanted bound after a careful computation (leaving small λ aside, but we can check the bound for them afterwards). □

Remark 5.7.1. The bound given here is the sharpest with integral coefficients : for $\lambda = 1$, the sum is about 6.8, which is an explanation for the fact that we need to be very careful throughout the computation to obtain the coefficient 8 above.

We can finally make the estimates for $A(m, \chi, N)$ and $B(m, \chi, N)$.

Proposition 5.8. *With the same notations as before, we have*

$$|A(m,\chi,N)| \leq \min\left(\frac{14D}{N}, \frac{\sqrt{Dm}}{N}\left(9\log^2(D) + 6\log(D)\log(N)\right)\right)$$
$$|B(m,\chi,N)| \leq \min\left(7D\sqrt{m}, \frac{\sqrt{Dm}}{\sqrt{N}}\left(9\log^2(D) + 12\log(D)\log(N) + 6\log^2(N)\right) + \frac{\tau(D)\sqrt{m}}{\sqrt{D}}\right)$$

Now, we finish the proof of Proposition 5.1.

Proof. Let $\lambda \geq 1$ be a parameter. To bound $\mathcal{S}_A(Nc)$, we will choose the "Abel-transform bound" for $c < \lambda$ and the Weil-induced bound for $c > \lambda$. This gives us

$$\begin{aligned}|A(m,\chi,N)| = \left|\sum_{c>0}\frac{\mathcal{S}_A(Nc)}{Nc}\right| &\leq 6\sqrt{Dm}\left(\sum_{c=1}^{\lfloor\lambda\rfloor}\frac{\log(DNc)+1.5}{Nc}\right) + 2D\sqrt{N}\left(\sum_{c>\lceil\lambda\rceil}\frac{\tau(c)}{(Nc)^{3/2}}\right)\\ &\leq \frac{6\sqrt{Dm}}{N}\left((\log(DN)+1.5)(1+\log(\lambda)) + \frac{\log(\lambda)^2+1}{2}\right) + \frac{2D}{N}\left(\frac{2\log(\lambda)+8}{\sqrt{\lambda}}\right)\end{aligned}$$

Notice first that if we choose $\lambda < 1$, this reduces to using only the Weil bound an therefore we get

$$|A(m,\chi,N)| \leq \frac{2D}{N}\sum_{c=1}^{+\infty}\frac{\tau(c)}{c^{3/2}} \leq \frac{14D}{N}$$

We choose $\lambda = D/e^{7/2}$ and develop $\log(\lambda)$ in the expression above. We obtain the bound

$$|A(m,\chi,N)| \leq \frac{\sqrt{Dm}}{N}(9\log(D)^2 + 6\log(D)\log(N)).$$

Actually, these are the dominant terms of the expression for chosen λ, and it is not hard to check that the remainder is negative. If $D < e^4$, the bound also holds. Notice it improves the Weil bound only when D is large enough ($D > 1000$ is a good order of magnitude). We obtain the Weil bound similarly for $B(m, \chi, N)$ and for $\lambda > D$, we have

$$|B(m,\chi,N)| \leq \frac{6\sqrt{Dm}}{\sqrt{N}}\left((\log(D)+1.5)(1+\log(\lambda)) + \frac{\log(\lambda)^2+1}{2}\right) + D\sqrt{m}\cdot\frac{2\log(\lambda)+8}{\sqrt{\lambda}} + \frac{\tau(D)\sqrt{m}}{\sqrt{D}}.$$

The last term in the sum comes from the fact we only have a Weil bound for $d = D$. Similarly, calculating the Weil-only bound and then choosing $\lambda = DN/e^4$, we obtain the desired result. □

Adding these bounds together, we have the following proposition.

Proposition 5.9. *Let K be the imaginary quadratic field of discriminant $-D$ and Dirichlet character χ. For every prime number $p > 50D^{1/4}\log(D)$ not dividing D, $(a_1, L_\chi)_{p^2}^{+,new} \neq 0$.*

Proof. Thanks to formulas (10) and (12), we have

$$\begin{aligned}\frac{|(a_1,L_\chi)_{p^2}^{+,new}|}{4\pi} \geq (e^{-2\pi/(Dp)} - \tfrac{p}{p^2-1} - \tfrac{1}{p^2-1}) \; &-2\pi\left(|A(1,\chi,p^2| + \tfrac{p|A(1,\chi,p)|}{p^2-1} + \tfrac{|A(p,\chi,p)|}{p^2-1}\right)\\ &-2\pi\left(\tfrac{|B(1,\chi,p^2|}{p} + \tfrac{\sqrt{p}|B(1,\chi,p)|}{p^2-1} + \tfrac{|B(p,\chi,p)|}{p^2-1}\right)\end{aligned}$$

The first term is larger than 19/20 because $D \geq 3$ and $p \geq 50 \cdot 3^{1/4}\log(3) \geq 72$. Now, putting together the Abel-transform bounds from Proposition 5.8, we obtain

$$\frac{|(a_1, L_\chi)_{p^2}^{+,new}|}{4\pi} \geq \frac{19}{20} - \frac{\sqrt{D}}{p^2}\left(294\log^2(D) + 416\log(D)\log(p) + 227\log^2(p)\right) - \frac{2\pi\tau(D)}{\sqrt{D}}\left(\frac{1}{p} + \frac{1}{p-1}\right)$$

and after computation, we find that for $D \geq 15$, $p \geq 50D^{1/4}\log(D)$, $(a_1, L_\chi)_{p^2}^{+,new} \neq 0$. For $D < 15$, we have to recover this results with some more computation : when $D = 7, 8$ or 11, this is possible by using Weil bounds for all six terms except for $|B(1, \chi, p^2)|$. When $D = 3$ or 4, we can obtain it back from computations we can find in [1]. More precisely, we mention this article provides sharp estimates for small discriminants ($p \geq 61$ for $D = 4$ and $p \geq 97$ for $D = 8$ in Lemma 14), hence we suggest using it in these cases rather than our own bound. □

An equivalent of Akbary's trace formula for $(a_m, a_n)_N^{w_M}$ with M any divisor of N such that $(M, N/M) = 1$ (Akbary deals with $M = N$) could allow us to give estimates of $(a_1, L)_{dp^2}^{w_p, p-new}$ with prime p and $d > 1$ by the same methods, and thus prove that the jacobian of $X_0(d) \times X_{nonsplit}(p)$ (described in [19]) has a rank zero quotient when p is large enough . This would extend a result of [6] (where the case $g(X_0(d)) = 0$ is considered) to some more cases.

References

1. Bennett, M., Ellenberg, J., Ng, N.: The diophantine equation $A^4 + 2^\delta B^2 = C^n$. Int. J. Number theory **6**, 311–338 (2010)
2. Bertolini, M., Darmon, H.: A Rigid Analytic Gross-Zagier Formula and Arithmetic Applications. Ann. of Math. **146**(1), 111–147 (1997)
3. Bilu, Y., Parent, P.: Runge's method and modular curves. Int. Math. Res. Not. (9), 1997–2027 (2011)
4. Bilu, Y., Parent, P.: Serre's Uniformity Problem in the Split Cartan case. Ann. of Math. (2) **173**, 569–584 (2011)
5. Cojocaru, A.C.: On the Surjectivity of the Galois Representations Associated to Non-CM Elliptic Curves. Canad. Math. Bull. **48**, 16–31 (2005)
6. Darmon, H., Merel, L.: Winding quotients and some variants of Fermat's Last Theorem. J. Reine Angew. Math. **490**, 81–100 (1997)
7. Ellenberg, J.: Galois Representations Attached to $\mathbb{Q}$-Curves and the Generalized Fermat Equation $A^4 + B^2 = C^p$. Amer. J. Math. pp. 763–787 (2004)
8. Ellenberg, J.: On the error term in Duke's estimate for the average special values of L-functions. Canad. Math. Bull. **48**, 533–546 (2005)
9. Gaudron, E., Rémond, G.: Théorème des périodes et degrés minimaux d'isogénies. Comment. Math. Helv. (2014)
10. Hasegawa, Y.: $\mathbb{Q}$-curves over quadratic fields. Manuscripta mathematica **94**, 347–364 (1997)
11. Masser, D., Wüstholz, G.: Galois properties of division fields of elliptic curves. Bull. London Math. Soc. **25**, 247–254 (1993)
12. Masser, D., Wüstholz, G.: Isogeny Estimates for Abelian Varieties and Finiteness Theorems. Ann. of Math., Second series **137**(3), 459–472 (1993)
13. Mazur, B.: Modular curves and the Eisenstein ideal. Publications mathématiques de l'IHES **47**, 33–186 (1977)
14. Mazur, B.: Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math. **44**(2), 129–162 (1978)
15. Momose, F.: Rational points on the modular curves $X_{\text{split}}(p)$. Compositio Math. **52**(1), 115–137 (1984)
16. Pellarin, F.: Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques. Acta Arithmetica **100**, 203–243 (2001)
17. Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$. Bull. soc. Math. Fr. **102**, 241–280 (1974)
18. Serre, J.P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**(4), 259–331 (1972)
19. de Smit, B., Edixhoven, B.: Sur un résultat d'Imin Chen. Mat. Res. Lett. **7**, 147–153 (2000)
20. Bosch, S., Lütkebohmert, W., Raynaud, M.: Néron models, *Ergebnisse der Mathematik und ihrer Grenzegebiete*, vol. 21. Springer-Verlag (1990)
21. Bump, D.: Automorphic forms and representations. Cambridge Studies in Mathematics (1996)
22. Iwaniec, H., Kowalski, E.: Analytic number theory. Colloquium Publications of the AMS. AMS (2004)
23. Kubert, D., Lang, S.: Modular units. Grundlehren der mathematischen Wissenschaften. Springer-Verlag (1981)
24. Lang, S.: Algebra. Graduate Texts in Mathematics Series. Springer-Verlag (2002)
25. Silverman, J.: The Arithmetic of Elliptic Curves, vol. 106. Springer-Verlag (2009)
26. Elkies, N.: On Elliptic K-curves. In: Modular Curves and Abelian Varieties, *Prog. Math.*, vol. 224, pp. 81–91. Birkhäuser Basel (2004)

27. Pomerance, C.: Remarks on the Pólya-Vinogradov inequality. In: Integers, vol. 11, pp. 531–542 (2011)
28. Ribet, K.: Abelian Varieties over $\mathbb{Q}$ and Modular Forms. In: Modular Curves and Abelian Varieties, *Progr. Math.*, vol. 224, pp. 241–261. Birkhäuser Basel (2004)
29. Akbary, A.: Non-vanishing of modular L-functions with large level. Ph.D. thesis, University of Toronto (1997). URL http://www.cs.uleth.ca/∼akbary/publications.html
30. Dieulefait, L., Freitas, N.: The Fermat-type equations $x^5 + y^5 = 2z^p$ or $3z^p$ solved through $\mathbb{Q}$-curves. ArXiv:1103.5388