About the method of Chabauty-Kim, after Dogra-Le Fourn

Elie Studnia, under the supervision of Loic Mérel

July 14, 2020

Contents

1 The original Chabauty method

1.1 General idea

Consider a geometrically connected smooth projective curve X defined over $\operatorname{Spec}\mathbb{Q}$, with genus g, with a rational point. It is well-known that its set of rational points exhibits very different behavior when g varies.

When $g = 0$, X is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ (see for instance [25, Proposition 7.4.1]) and its set of rational points is thus the complete rational line $\mathbb{Q} \cup \{\infty\}$. When X is given explicitly, we can even use rational parametrizations to compute every rational point of X from a given rational point.

When $g = 1$, X is an elliptic curve, and the Mordell-Weil theorem (see [38, Theorem VIII.6.7]) states that, given a fixed rational point, $X(\mathbb{Q})$ has a natural structure of a finitely generated abelian group. However, although there are systematic methods to compute the rank, the torsion group, or generators, $X(\mathbb{Q})$ remains difficult to compute. The computation of the rank, in particular, is especially complicated, as, for example, it is not known whether there are elliptic curves over $\mathbb{Q}$ whose group of rational points has arbitrary rank. The highest unconditional known rank is 20, found in Elkies-Klagsbrun in 2020, according to [15] while, according to [38, Chapter VIII.10] an earlier example found by Elkies has rank at least 28 (and exactly 28 conditionally on analytic number theory conjectures such as Birch and Swinnerton-Dyer or GRH, as shown in [3] or improved more recently in [23]). The torsion subgroups, on the other hand, are better-known, at least over $\mathbb{Q}$: as shown in Mazur's important paper [28, Theorem III-5.1], there are fifteen of them.

The case $g > 1$ is the hardest case. It was Mordell's conjecture that the set $X(\mathbb{Q})$ of rational points was finite, and it was proved by Faltings only in 1984. Faltings' proof provides a bound for that number of rational points, but it is hard to make explicit, and is often far coarser than the actual number. The proof does not give a criterion to generate all rational points, or to determine whether a given list of rational points is complete.

Chabauty's method, dating back from about 1940, is a method to try and make more explicit the set of rational points of a curve in the last case. It relies on the commutative diagram 1, where J is the Jacobian of X and the closed immersion $X \to J$ is given by an Abel-Jacobi map, $P \longmapsto [P] - [O]$ where O is a given rational point on the curve (we also could do with $O \in X(K)$ where K is a number field Galois with degree d and group G over $\mathbb{Q}$ and the map being $P \longmapsto d[P] - \sum_{s\in G}[s \cdot O]$, but we will assume, for the sake of simplicity, that we already know a rational point), given a prime number p.

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) \end{array}$$

Figure 1 – Diagram of Chabauty's original method

To explain the idea behind Chabauty's method, we use a language more appropriate to real differential geometry, which we informally extend to describe p-adic varieties. The actual relevant formalism will be developed in the following subsections. As we see in the diagram, $X(\mathbb{Q})$ is contained in the intersection of two p-adic subvarieties of $J(\mathbb{Q}_p)$, the p-adic closure J' of $J(\mathbb{Q})$ and $X(\mathbb{Q}_p)$. If $J(\mathbb{Q})$ has rank r, then it is natural to assume that J' will have dimension at most r (as a p-adic variety), while $X(\mathbb{Q}_p)$ will only have dimension 1. So, if $r < g$, and if J' and $X(\mathbb{Q}_p)$ intersect transversally, their intersection should be a closed strict subvariety of $X(\mathbb{Q}_p)$, so is a p-adic variety of dimension 0, that is, a finite set.

It remains to make explicit that intersection. Still informally, J', $J(\mathbb{Q}_p)$ are p-adic Lie groups (the former a subgroup of positive codimension of the latter): there should be, therefore, an algebraic function over $J(\mathbb{Q}_p)$ that vanishes over J' but not over $X(\mathbb{Q}_p)$. We can compute the zero set of that function on $X(\mathbb{Q}_p)$, which should already be finite, and extract from it the rational points.

The condition $r < g$ which we used here is not a merely technical assumption: it is necessary for the idea to work in this form, and our informal description of the idea cannot be adapted to the case $r \geq g$, where the global behavior of $J(\mathbb{Q})$ inside $J(\mathbb{Q}_p)$ cannot be so easily predicted. We will come back to this limitation later.

The remaining subsections develop this idea and explain the formalism necessary to its proof. Section 1.2 introduces the notion of Coleman integrals, the appropriate tool we use to describe the algebraic function evoked above. Section 1.3 proves a first very explicit bound by Coleman using Chabauty's method. Our approach for that part is mostly that of [29]. Section 1.4 will briefly explain subsequent improvements on these results: Stoll's "free" slightly better bound, results for number fields or in cases of bad reduction...

1.2 Jacobian and Coleman integrals

First, we define some notations that we keep for the rest of the section. Given a scheme X and a point $x \in X$, unless explicitly indicated otherwise, $\mathcal{O}_X$ is its structural sheaf, $\mathcal{O}_{X,x}$ is the ring of stalks of $\mathcal{O}_X$ at x, $\mathfrak{m}_x$ is its maximal ideal and $\kappa(x)$ (or $\kappa^X(x)$ if necessary) the residual field.

We first consider a prime number p and $Y \to \operatorname{Spec} \mathbb{Z}_p$ a smooth proper scheme with connected generic fiber.

We will first need some prerequisites from algebraic geometry, and we refer to the annex A.1 for the details of the proof:

Lemma 2.1

- *Its generic fiber is a dense open subscheme.*
- *Y is a regular integral scheme.*
- *Every nonempty closed subset of Y meets the closed fiber.*
- *The natural map $Y(\mathbb{Z}_p) \to Y(\mathbb{Q}_p)$ is a bijection.*
- *The map of sets $Y(\mathbb{F}_p) \to \{y \in Y_{\mathbb{F}_p}, \kappa(y) = \mathbb{F}_p\}$ mapping P to the unique point in the set-theoretical image of P is a bijection.*
- *The map of sets $Y(\mathbb{Q}_p) \to \{y \in Y_{\mathbb{Q}_p}, \kappa(y) = \mathbb{Q}_p\}$ mapping P to the unique point in the set-theoretical image of P is a bijection.*
- *If the generic fiber is geometrically connected, so is the special fiber.*

We can now define the reduction mod p of the $\mathbb{Q}_p$-points of C.

Definition Let $P \in Y(\mathbb{Q}_p)$; we know that P extends uniquely to a morphism $P_1 \in Y(\mathbb{Z}_p)$. Now, we have a reduction mod p morphism $\mathbb{Z}_p \to \mathbb{F}_p$ inducing a natural map $r_p : Y(\mathbb{Z}_p) \to Y(\mathbb{F}_p)$. The *reduction mod p* of P is $r_p(P_1) \in Y(\mathbb{F}_p)$.

If $Z \in Y(\mathbb{F}_p)$, the set of points of $Y(\mathbb{Q}_p)$ that reduce mod p to Z is called the residue disk of Z. We denote it as $Y(\mathbb{Q}_p)_Z$. The *completed residue disk* of Z is the scheme $\operatorname{Spec} \mathcal{O}_{Y,Z}$ (where we identified Z to the set-theoretical image of the morphism Z as in the lemma). It is endowed with a canonical morphism $\operatorname{Spec} \mathcal{O}_{Y,Z} \to Y$, which is topologically a homeomorphism onto its image and is an isomorphism on all rings of stalks. The *schematic residue disk* is the open subscheme $\operatorname{Spec} \mathcal{O}_{Y,Z}[p^{-1}]$ (they both are naturally $\mathbb{Z}_p$-schemes). We recall from the annex A.1:

Lemma 2.2 *The schematic residue disk and the completed residue disk have the same $\mathbb{Q}_p$-points, which are canonically identified to the points of $Y(\mathbb{Q}_p)_Z$.*

Now, and from now on, we take $Y = X$ a smooth proper scheme of relative dimension 1 over $\mathbb{Z}_{(}$, C its generic fiber, which we suppose is a geometrically connected (hence integral) curve of genus g over $\mathbb{Q}_p$. We denote as F the special fiber.

Definition Let $z \in X(\mathbb{F}_p) = F(\mathbb{F}_p)$ be a closed point. A *uniformizer* at z is a function $t \in \mathcal{O}_{X,z}$ such that the maximal ideal of this ring is generated by (p, t) (which is then a system of parameters). We easily note that, in the usual sense for curves, t is a uniformizer at z for $X_{\mathbb{F}_p}$.

It is proved in greater generality (any relative dimension) in the annex A.1 that such uniformizers always exist. We admit this fact for now.

The interesting properties of the uniformizers are summarized in the two propositions below, proved in greater generality in the annex A.

Proposition 2.3 *Let t be a uniformizer at a point $z \in X(\mathbb{F}_p)$. Given a point $P \in C(\mathbb{Q}_p)_z$, it corresponds to a morphism $P_1 \in X(\mathbb{Z}_p)$ mapping the closed point to z, and thus induces a morphism of local rings $\mu_P : \mathcal{O}_{X,z} \to \mathbb{Z}_p$. We define $t(P) = \mu_P(t) \in p\mathbb{Z}_p$. Then $P \in C(\mathbb{Q}_p)_z \longmapsto t(P) \in p\mathbb{Z}_p$ is a bijection.*

Proposition 2.4 *Let $z \in X(\mathbb{F}_p)$, let t be a uniformizer at p. Let S and D be the schematic and complete residue disks, respectively, at z. Then the $\mathbb{Q}_p[t]$ (resp. $\mathbb{Z}_p[t]$)-submodule of $\Omega^1_{D/\mathbb{Z}_p}(D)$ (resp. $\Omega^1_{S/\mathbb{Z}_p}(S)$) generated by dt is free and t-adically dense. Furthermore, $\Omega^1_{S/\mathbb{Z}_p}(S) = \Omega^1_{D/\mathbb{Z}_p}(D) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. In particular, every global 1-form on S can be written uniquely as a $p^u R(t)dt$, where $R \in \mathbb{Z}_{(}[[T]]$ not divisible by p and $u \in \mathbb{Z}$ (however, not all such power series define a global 1-form).*

We can now state the following fundamental theorem, which we partially prove in Annex A:

Theorem 2.5 (Coleman '85,[7]) *We keep the notations above. Let, furthermore, J be the Jacobian of C, and $j : C \to J$ be an Abel-Jacobi injection. Then J has a proper Néron model over $\mathbb{Z}_p$, and we have a unique pairing*

$$(P, \omega) \in J(\mathbb{Q}_p) \times H^0(C, \Omega^1) \longmapsto \int_0^P \omega \in \mathbb{Q}_p$$

satisfying the following properties:

1. *For any ω, $P \in J(\mathbb{Q}_p) \longmapsto \int_0^P \omega$ is additive.*
2. *For any $Q \in J(\mathbb{Q}_p)$, $\omega \longmapsto \int_0^Q \omega$ is $\mathbb{Q}_p$-linear.*
3. *If $z \in X(\mathbb{F}_p)$, S is its schematic residue disk, t is a uniformizer at z, $P, Q \in X(\mathbb{Q}_p)_z$, then, for any $\omega \in H^0(C, \Omega^1)$ such that $\omega_{|S} = p^u \sum_{n=0}^{\infty} a_n t^n dt$ (the restriction is a pull-back in formal terms), with $u \in \mathbb{Z}$ and $a_n \in \mathbb{Z}_p$, then*

$$\int_0^{j(Q)} \omega - \int_0^{j(P)} \omega = p^u \sum_{n=0}^{\infty} \frac{a_n}{n+1} \left(t(Q)^{n+1} - t(P)^{n+1} \right).$$

Coleman's definition is actually much more powerful than what is sketched here, but we only take what we need. For instance, it is invariant under any lift of the Frobenius, a very useful property when it comes to actually compute such integrals (indeed, a point is in the same residue disk as its image, so computing the "error terms" is easy, and the transformation of the differential form is effectively computable; for examples, one may consult e.g. [1] and look especially at Algorithms 1.52, 1.53).

Corollary 2.6 *Let us keep the same notations, with g the genus of C and r the rank of $J(\mathbb{Q})$. Assume $r < g$. Then there exists a subvector space (over $\mathbb{Q}_p$) $V \subset H^0(X, \Omega^1)$, with dimension at least $g - r$, such that for any $\omega \in V$, for any $P \in J(\mathbb{Q})$, $\int_0^P \omega = 0$.*

Proof. – Simply consider a system of generators of the free part of $J(\mathbb{Q})$: they define as many equations for V, because if $P \in J(\mathbb{Q})_{\text{tors}}$, $\int_0^P \cdot = 0$. □

1.3 Coleman's bound

Once given the datum of section 1.2, that is, a smooth proper geometrically connected curve C of genus g with a rational point, its Jacobian J and an Abel-Jacobi map j, a smooth proper model $X \to \operatorname{Spec} \mathbb{Z}_p$ of X, it remains to apply the idea explained in section 1.1. It decomposes practically in two steps: we bound the number of rational points on each residue disk, and we assemble the local bounds to get a global one.

The bound we get is the following:

Theorem 3.1 (Coleman '85, [7])

If C_1 is a smooth geometrically connected projective curve over $\mathbb{Q}$ of genus $g > 1$ with good reduction at a prime $p > 2g$ and Jacobian J_1, (which corresponds to the case above, where X is a base change of a smooth proper $X_1 \to \operatorname{Spec} \mathbb{Z}_{(p)}$ of relative dimension 1 with geometrically connected generic fiber). Assume the rank r of $J_1(\mathbb{Q})$ satisfies $r < g$. Then $|C_1(\mathbb{Q})| \leq |X_1(\mathbb{F}_p)| + 2g - 2$.

The proof results from two steps: a step of local analysis, that estimates the number of potential rational points on a residue disk, and a step of global analysis, where the local bounds are mixed. In this situation, the global step is relatively straightforward. For now, we take ω any nonzero differential.

First, we see that $\Omega^1_{X/\mathbb{Z}_p}$ is a locally free $\mathcal{O}_X$-module, in particular p is a regular element. Restricting along affine subsets, we find that $H^0(X,\Omega^1_{X/\mathbb{Z}_p})\otimes_{\mathbb{Z}_p}\mathbb{Q}_p = H^0(C,\Omega^1_{C/\mathbb{Q}_p})$ and $H^0(X,\Omega^1_{X/\mathbb{Z}_p})\otimes_{\mathbb{Z}_p}\mathbb{F}_p$ injects naturally by pullback into $H^0(F,\Omega^1_{F/\mathbb{F}_p})$ where F is the special fiber.

Also, $X\to \operatorname{Spec}\mathbb{Z}_p$ is proper (see e.g. [17]), and by the above, $H^0(X,\Omega^1_{X/\mathbb{Z}_p})$ is a torsion-free finitely generated $\mathbb{Z}_p$-module, so it is a free $\mathbb{Z}_p$-module of finite rank. So, up to multiplication by the right power of p, we can assume $\omega\in H^0(X,\Omega^1_{X/\mathbb{Z}_p})\backslash pH^0(X,\Omega^1_{X/\mathbb{Z}_p})$, so that ω reduces to a nonzero global differential form ω_1 on $X_{\mathbb{F}_p}$.

Note finally that as C is geometrically connected and smooth, by Lemma 2.1, $X_{\mathbb{F}_p}$ is also a smooth proper geometrically connected curve over $\mathbb{F}_p$.

Lemma 3.2 (Local bound)
Let $z\in X(\mathbb{F}_p)$, t a uniformizer at z, S the associated schematic residue disk, write $\omega_{|S}=f(t)dt$, $f\in\mathbb{Z}_p[[T]]\backslash p\mathbb{Z}_p[[T]]$. Let m be the multiplicity of z in $\operatorname{div}\omega_1$. Let $F\in\mathbb{Q}_p[[t]]$ be any antiderivative of f.

1. *The valuation of $f \bmod p$ (i.e. the order of the first nonvanishing coefficient) is m.*
2. *If $m<p-2$, F has at most $m+1$ zeros as an analytic function defined over $p\mathbb{Z}_p$.*
3. *There are at most $m+1$ points $L\in X(\mathbb{Q}_p)_z$ satisfying $\int_0^{j(L)}\omega=0$.*

Proof. – Note that t-adically in $(\Omega^1 X_{\mathbb{F}_p}/\mathbb{F}_p)_z$, ω_1 is $(f \bmod p)(t)dt$. So if $f \bmod p=0$, then ω_1 is zero on a non-empty open subset, so is zero. The formula before also proves the first claim. The third claim follows from properties of Coleman integrals, residue disks, and from the second claim. So the second claim is the most interesting one. We can see it as a p-adic Rolle theorem. First, we notice that if consider a $z\in p\mathbb{Z}_p$, then $F(z)-F(0)\in p\mathbb{Z}_p$. Indeed, write $f(t)=\sum_{n=0}^{\infty}a_nt^n$. Then, the p-adic valuation of $\frac{a_n}{n+1}z^{n+1}$ is at least 1 if $n<m<p-2$ (because of a_n, and $n+1$ is not a multiple of p); the p-adic valuation of the same expression for $m\le n<p-1$ is at least $m+1$; when $n\ge p-1$, the valuation is at least $n+1-v_p(n+1)\ge n-p+2$ (the inequality is proved by induction). So if $F(0)\notin p\mathbb{Z}_p$, the statement holds. Let $z=(z_1,\dots,z_{m+1})\in(p\mathbb{Z}_p)^{m+1}$ be a set of $m+1$ roots of F, pairwise distinct (if we can't find any such list, we are done). Define, for every $k\ge 0$,

$$b_k=\sum_{\ell\in\mathbb{N}^{m+1}} z^\ell\frac{a_{k+|\ell|+m}}{k+|\ell|+m+1}.$$

The series is unconditionally convergent in $\mathbb{Q}_p$, because for any k, for large enough $l\ge 0$, $l-v_p(k+l+m+1)$ (a term not greater than the p-adic valuation of the sum of the terms with $|\ell|=l$) is greater than $l/2$. Furthermore, one can check the following formal identity, in the variables $X_1,\dots,X_{m+1},T$:

$$\sum_{v=0}^{\infty}T^v\sum_{\ell\in\mathbb{N}^{m+1},|l|=v}X^\ell=\prod_{i=1}^{m+1}\sum_{t=0}^{\infty}(X_iT)^t=\prod_{i=1}^{m+1}\frac{1}{1-X_iT}.$$

Arranging the equation so that the right hand side is 1, specializing $X_i=z_i$, and denoting σ_i the i-th degree symmetric polynomial in z, letting $S_w(z)=\sum_{\ell\in\mathbb{N}^{m+1},|\ell|=w}z^\ell$, we get for $w>0$

$$\sum_{i=0,i\le w}^{m+1}(-1)^i\sigma_iS_{w-i}(z)=0.$$

By rearranging sums,

$$G=\sum_{k\ge0}b_kX^k\prod_{k=1}^{m+1}(X-z_k)-F(X)=\sum_{k=0}^{\infty}X^k\sum_{v=0}^{\infty}u_{k+v}\sum_{\substack{t+l=v\\0\le t\le m\\k+t\ge m}}S_l(z)\sigma_t(-1)^t$$

is a polynomial of degree at most m. Now, if the p-adic norm of b_k is $o(p^k)$ as $k \to \infty$, then we can evaluate the equality at each z_i, and it follows $G(z_i) = 0$. As the z_i are distinct, and there are more of then than the degree of G, $G = 0$.

Thus, it remains to prove two things:

- That $|b_k|_p = o(p^k)$.
- That $H(X) = \sum_{k\geq 0} b_k X^k$ has no zeros in $p\mathbb{Z}_p$.

For the first item, simply note that the p-adic valuation of b_k is $v_k = \inf\{l - v_p(k+l+m+1),\, l \geq 0\}$. Thus

$$p^{v_k} \geq \inf\left\{\frac{p^l}{x+k+m+1},\, x \geq 0\right\},$$

and the function is minimal when $x = 0$ or $x + m + 1 = (\ln p)^{-1}$. As $p - 2 > m > 0$, $p \geq 3$, so the latter condition isn't met in $[0, \infty)$. So $p^{v_k} \geq \frac{1}{k+m+1}$ and thus $|b_k|_p$ grows linearly, hence the conclusion.

For the second term, let $y \in p\mathbb{Z}_p$, $\ell \in \mathbb{N}^{m+1}$ and $k \geq 0$ with $k + |\ell| > 0$ and let us show that $t_{k,\ell} = y^k z^\ell \frac{a_{k+|\ell|+m}}{k+|\ell|+m+1}$ has positive valuation. If $s = k + |\ell| + m + 1 < p$, it is clear. Else, $v_p(s) \leq s - (p-1) < s - (m+1) = k + |\ell|$. Adding everything together, it follows that $b_k y^k \in p\mathbb{Z}_p$ for $k \geq 1$ and $b_0 y^0 - \frac{a_m}{m+1} \in p\mathbb{Z}_p$. But as $m + 1 < p$ and $a_m \notin p\mathbb{Z}_p$, $b_0 \notin \mathbb{Z}_p$. So $H(y) \notin p\mathbb{Z}_p$, and we are done. □

Now we can prove Coleman's theorem:

Proof. – We choose $\omega \in V$. Let $z \in X_1(\mathbb{F}_p)$, let m_z be the multiplicity of z in $\operatorname{div}\omega_1$. For each point $q \in C_1(\mathbb{Q}) \cap C(\mathbb{Q}_p)_z$, then if t is a uniformizer at z (in X), $\int_0^{j(q)} \omega = 0$ (where we have a natural embedding $C_1(\mathbb{Q}) \to C(\mathbb{Q}_p)$). So there are at most $1 + m_z$ points in $C_1(\mathbb{Q}) \cap C(\mathbb{Q}_p)_z$. Now, using Riemann-Roch and the fact that both C_1 and X_1 have no nontrivial global function (they are geometrically connected and smooth proper curves over their respective fields), and Euler characteristics invariance,

$$\sum_z 1 + m_z = |X_1(\mathbb{F}_p)| + \sum_z m_z \leq |X_1(\mathbb{F}_p)| + \deg\operatorname{div}\omega_1 = |X_1(\mathbb{F}_p)| + 2g - 2.$$

□

1.4 Further refinements

The results of this section are mostly inspired by David Zureick-Brown's lecture [45] on Abelian Chabauty at the Arizona Winter School 2020.

We first talk about Stoll's improvement of Coleman's bound. This is a case where the bound is improved unconditionally. The idea is simple: the proof of the Coleman theorem only uses the existence of one vanishing differential. Then we locate its zeroes on each residue disk, and the Riemann-Roch theorem lets us bound the total vanishing order of the differential form.

But if the rank of the Jacobian is smaller than the genus of the curve, there can be several independent differentials in V, and perhaps we can pick different ones for each residue disk, the ones best suited to each disk. This is the crux of Stoll's improved bound.

Theorem 4.1 (Stoll, [42]) *Let $C \to \operatorname{Spec}\mathbb{Q}$ be a geometrically connected smooth projective curve with genus $g > 1$ and with good reduction at some prime number $p > 2g$, let $X \to \operatorname{Spec}\mathbb{Z}_{(p)}$ be a smooth proper model of C. Let r be the rank of the finitely generated group of rational points of its Jacobian. If $r < g$, then $|C(\mathbb{Q})| \leq |X(\mathbb{F}_p)| + 2r$.*

Proof. – Let V be the orthogonal of $J(\mathbb{Q})$ in $H^0(C_{\mathbb{Q}_p}, \Omega^1_{C_{\mathbb{Q}_p}/Qp})$, with dimension $g - r$ at least. For every nonzero $\omega \in V$, there exists a unique $u \in \mathbb{Z}$ such that $p^u\omega$ extends to a global differential on $X_{\mathbb{Z}_p}$ with nonzero reduction $\overline{\omega}$ on the special fiber. For each $Q \in X(\mathbb{F}_p)$, let $m_{\omega,Q}$ be the vanishing order at Q of $\overline{\omega}$. Denote by m_Q, for each $Q \in X(\mathbb{F}_p)$, the minimum value over all such ω of $m_{\omega,Q}$.

Then by Lemma 3.2, for each $Q \in X(\mathbb{F}_p)$, $|C(\mathbb{Q})_Q| \leq 1 + m_Q$. Then, $D = \sum_Q m_Q \cdot Q$ is a divisor on the special fiber (which is known to be geometrically connected, smooth of relative dimension 1 and proper) satisfying $|C(\mathbb{Q})| \leq |X(\mathbb{F}_p)| + \deg D$.

Now, D is a *special* (as defined in [17, Example IV.1.3.4]) effective divisor, as any $\overline{\omega}$, for nonzero $\omega \in V$, is a holomorphic differential on $X_{\mathbb{F}_p}$ with $\div\omega \geq D$. Thus, by Clifford's theorem ([17, Theorem IV.5.4]), $2\ell(D) - 2 \leq \deg D$. But by Riemann-Roch (see eg [25, Theorem 7.3.26, Remark 7.3.27]), $\ell(D) = \deg D + 1 - g + \dim\{u \in H^0(X_{\mathbb{F}_p}, \Omega^1_{X_{\mathbb{F}_p}/\mathbb{F}_p}),\ \mathrm{div}\, u - D \geq 0\}$.

Now, the latter dimension is at least the dimension of $\left(V \cap H^0(X_{\mathbb{Z}_p}, \Omega^1_{X_{\mathbb{Z}_p}/\mathbb{Z}_p})\right) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$, which is $\dim V \geq g - r$. So finally $\ell(D) - 1 \geq \deg D + r$. Thus $2\deg D + 2r \leq 2(\ell(D) - 1) \leq \deg D$, hence $\deg D \leq 2r$ and we are done. □

A well-known related question, but broader and somewhat bolder, is the uniformity problem, formulated in [5]. It consists in finding a uniform upper bound on the number of rational points of a curve, depending only on its genus, assumed to be at least 2. Some progress was made in the recent work of [12], which proves a uniform upper bound depending only on r and g.

In view of this question, we notice that the quality of the bound when applying Chabauty's method depends heavily on the prime p of good reduction, which could even be arbitrarily large. That is why the Coleman bound was adapted, using other arguments from p-adic geometry, intersection theory or tropical geometry, to the case of bad reduction:

Theorem 4.2 (Lorenzini, Tucker, [27]) *$|C(\mathbb{Q})| \leq |X^{sm}(\mathbb{F}_p)| + 2g - 2$ if $p > 2g$, $r < g$, where X is a regular proper scheme over $\mathbb{Z}_{(p)}$ with generic fiber $C_{\mathbb{Q}_p}$, and X^{sm} is its smooth locus.*

Theorem 4.3 (Katz, Zureick-Brown, [19]) *With the same notations, if we only require $p > 2r + 2$ and $r < g$, then $|C(\mathbb{Q})| \leq |X^{sm}(\mathbb{F}_p)| + 2r$, where X^{sm} is the smooth locus of a regular model of C over $\mathbb{Z}_{(p)}$.*

The drawback of these bounds is that $X^{sm}(\mathbb{F}_p)$ could be huge: for instance, if C is an elliptic curve with j-invariant in $p^{-n}\mathbb{Z}_p^\times$, it turns out that $X^{sm}_{\mathbb{F}_p}$ is a reunion of n $\mathbb{P}^1_{\mathbb{F}_p}$.

Another aspect of the method of Chabauty-Coleman is the fact that better rank bounds yield better bounds on the number of points. It can be done in an elementary way, with a p-adic valuation analysis not unlike the proof of Lemma 3.2; some corresponding results can be found in [29]. In a more recent article, combining improved rank bounds but using instead a *minimal, non regular* model of the curve, Stoll derived the following *uniform* bound for hyperelliptic curves, regardless of reduction.

Theorem 4.4 (Stoll, [43]) *With the same notations, if $r \leq g - 3$, and if C is hyperelliptic, then $|C(\mathbb{Q})| \leq 8(r + 4)(g - 1) + g\max(1, 4r)$.*

Using more refined non-Archimedean analytic tools, such as Berkovich spaces, and tropical geometry, the statement was then generalized to *all* curves:

Theorem 4.5 (Katz, Rabinoff, Zureick-Brown, [18]) *If $r \leq g - 3$, then $|C(\mathbb{Q})| \leq 84g^2 - 98g + 28$.*

2 Kim's non-abelian generalization and application to modular curves

2.1 Kim's diagram

The method now known as Chabauty-Kim's method relies on a variant of Figure 1, where the Jacobian is replaced by another object constructed using the curve. In loose terms, the Jacobian is an abelian version of a richer invariant, which is in this case a fundamental group.

We consider a smooth projective curve X over a field K with characteristic 0 with a base point $b \in X(K)$. Let $\overline{K}$ be an algebraic closure of K, and G be the absolute Galois group of K, which has a profinite topology. Using Deligne's ideas from [9], a $\mathbb{Q}_p$-*unipotent fundamental group* (which is actually a group scheme) $\pi_1^{(p,u)}(X_{\overline{K}}, b)$ can be defined, as well as, for any $x \in X(\overline{K})$, a right *torsor of paths* $P(X_{\overline{K}}, b, x)$ under $\pi_1^{(p,u)}(X_{\overline{K}}, b)$ can be defined.

If $x \in X(K)$, we have compatible natural actions of G on $\pi_1^{(p,u)}(X_{\overline{K}}, b)$ and $P(X_{\overline{K}}, b, x)$, because b and x are invariant under G. This defines a map $j_K^{\text{full}} : X(K) \to H^1(G, \pi_1^{(p,u)}(X_{\overline{K}}, b))$ (see Annex B).

We actually simplify this map by replacing $\pi_1^{(p,u)}(X_{\overline{K}}, b)$ with a more tractable object: we consider its *lower central series* given by $U^{(1)} = \pi_1^{(p,u)}(X_{\overline{K}}, b)$ and $U^{(n+1)}$ is the closed subgroup generated by the set of commutators of elements of $U^{(1)}$ and $U^{(n)}$. These subgroups are clearly stable under continuous group automorphisms; in particular, they are stable under the action of the Galois group. We define $U_n = U^{(1)}/U^{(n+1)}$ for each $n \geq 1$, they are topological groups with continuous actions of G.

More generally, let us consider a closed subgroup Q of $U^{(1)}$, stable under Galois, and $U = U^{(1)}/Q$, then j_K^{full} becomes, through the Galois-equivariant quotient $\pi_1^{(p,u)}(X_{\overline{K}}, b) \to U$, a map $j : X(K) \to H^1(G, U)$.

Now, we consider changing base fields, we take $K = \mathbb{Q}$ and then $K = \mathbb{Q}_v$ for some prime number v. For U such as defined above, we can have a diagram:

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_v) \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j_v} \\ H^1(G_{\mathbb{Q},T}, U) & \xrightarrow{loc_v} & H^1(G_{\mathbb{Q}_v}, U) \end{array}$$

Figure 2 – Chabauty-Kim diagram, first version

where T is a set of primes containing v and the primes of bad reduction of X, and $G_{\mathbb{Q},T}$ is the Galois group of the maximal algebraic extension of $\mathbb{Q}$ unramified outside T, so that $G_{\mathbb{Q},T}$ acts on $\pi_1^{(p,u)}(X_{\overline{\mathbb{Q}}}, b)$ (as the curve has good reduction outside T), and $G_{\mathbb{Q}_v}$ is, by a given embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_v}$, a subgroup of $G_{\mathbb{Q},T}$.

The two following theorems follow from Kim's work in [20] and are stated in [2].

The first statement is that all our constructions actually work as p-adic varieties:

Theorem 1.1 *There exist group schemes of finite type over $\mathbb{Q}_p$ making each of the formerly defined $U^{(i)}/U^{(k)}$, $i < k$, their sets of $\mathbb{Q}_p$-points, and all the canonical maps between these groups come from morphisms of schemes.*

The second statement is the fact that the cohomology spaces of unipotent group schemes over $\mathbb{Q}_p$ are actually cohomology schemes:

Theorem 1.2 *Let G be a profinite group acting continuously on U_n and U be a quotient of U_n by a subgroup scheme stable under G, so that U is a $\mathbb{Q}_p$-group scheme of finite type. Then the functor $R \longmapsto H^1(G, U(R))$ (from $\mathbb{Q}_p$-algebras to pointed sets) is represented by an affine $\mathbb{Q}_p$-scheme of finite type, which we denote as $H^1(G, U)$ as well.*

Assume we have two quotients V and W of U_n by subgroup schemes stable under G. Let $f : V \to W$ be a morphism of group schemes, G and H be two profinite groups acting respectively on V and W, and $p : H \to G$ be continuous such that for each $x \in U(R)$, $h \in H$, $h(f(x)) = f(p(h)x)$, then the natural morphism of functors $H^1(p, f) : H^1(G, V(R)) \to H^1(H, W(R))$ is a morphism of schemes.

For all groups with this form, and all morphisms of exact sequences with various profinite groups, the diagram from Theorem 0.6 comes from a diagram of schemes.

This already tells us more information about the diagram of Figure 2, namely that the map loc_v is actually a map of p-adic algebraic varieties.

When p is a prime of good reduction of X, the image of the map $X(\mathbb{Q}_p) \to H^1(G_{\mathbb{Q}_p}, U)$ has a further property: the torsors in the image are *crystalline*, a "good-reduction-like" property which we will not detail here. It is stated in [2] that the subspace $H^1_f(G_{\mathbb{Q}_p}, U)$ of $H^1(G_{\mathbb{Q}_p}, U)$ corresponding to crystalline torsors is also the set of $\mathbb{Q}_p$-points of a $\mathbb{Q}_p$-scheme.

From now on, we fix a prime of good reduction p of X. Let U be a quotient of $U^{(1)}$ by a closed subgroup. its abelianization U^{ab} is a quotient of $\pi_1^{(p,u)}(X_{\overline{\mathbb{Q}}}, b)^{\mathrm{ab}}$. But the set of $\mathbb{Q}_p$-points of the latter group, considered as a Galois module, is the $\mathbb{Q}_p$-vector space $V_J = T_p(J) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, where $T_p(J)$ is the Tate module of the Jacobian.

An idea of why this holds true is to look at the Riemann-surface analog: the Jacobian is the quotient of a g-dimensional complex vector space by the lattice generated by the $2g$ generators of the topological fundamental group. The Tate module of the Jacobian is, by definition, the $\mathbb{Z}_p$-module generated by said lattice, thus, the free $\mathbb{Z}_p$-module generated by the loops. On the other side of the identification, when we abelianize the fundamental group and consider its $\mathbb{Q}_p$-completion, all that remains is the free $\mathbb{Q}_p$-vector space generated by the loops.

Thus, using the results from Annex B we have a natural map $\mu : J(\mathbb{Q}) \otimes \mathbb{Q}_p \to H^1(G_{\mathbb{Q},T}, U^{\mathrm{ab}})$ when X (hence J) has good reduction at v.

We actually have significant information about the diagram of Figure 2. The following theorem is stated in [2] from [22]:

Theorem 1.3 *For each prime v of bad reduction, $j_v(X(\mathbb{Q}_v)) \subset H^1(G_{\mathbb{Q}_v}, U(\mathbb{Q}_p))$ is finite.*

Let now T_0 be the set consisting of all the primes of bad reduction of X, then $p \notin T_0$, and we denote from now on $T = T_0 \cup \{x\}$. We have an algebraic map $\mathrm{loc} : H^1(G_{\mathbb{Q},T}, U) \to S_1 := \prod_{v \in T} H^1(G_{\mathbb{Q}_v}, U)$. S_1 is a $\mathbb{Q}_p$-scheme, and has a finite set B of p-adic points corresponding to the image of the product of the images of the $j_v(X(\mathbb{Q}_v))$. We denote $S_2 = \mathrm{loc}^{-1}(B) \times_{H^1(G_{\mathbb{Q}_p},U)} H^1_f(G_{\mathbb{Q}_p}, U) = (H^1(G_{\mathbb{Q},T}, U) \times_{S_1} B) \times_{H^1(G_{\mathbb{Q}_p},U)} H^1_f(G_{\mathbb{Q}_p}, U)$.

We can see $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ as the set of $\mathbb{Q}_p$-points of a finite-dimensional affine space PJ over $\mathbb{Q}_p$, and similarly for U^{ab} and $H^1_f(G_{\mathbb{Q}_p}, U^{\mathrm{ab}})$ (without the finite-dimensional assumption for the latter), so the map $J(\mathbb{Q}) \otimes \mathbb{Q}_p \to H^1_f(G_{\mathbb{Q},T}, U^{\mathrm{ab}})$ comes from a morphism of schemes.

We define the *Selmer scheme* $\mathrm{Sel}(U)$ of U as $S_2 \times_{H^1_f(G_{\mathbb{Q},T}, U^{\mathrm{ab}})} (J(\mathbb{Q}) \otimes \mathbb{Q}_p)$.

In particular, $\mathrm{Sel}(U)(\mathbb{Q}_p)$ corresponds to cohomology classes α of $H^1(G_{\mathbb{Q},T}, U)$ satisfying the following conditions:

1. If v is a prime of bad reduction, $\mathrm{loc}_v(\alpha) \in j_v(X(\mathbb{Q}_v))$.
2. $\mathrm{loc}_p(\alpha) \in H^1_f(G_{\mathbb{Q}_p}, U)$.
3. The image of α in $H^1(G_{\mathbb{Q},T}, U^{\mathrm{ab}})$ is in the image of μ.

At this point, we have the following diagram:

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j_p} \\ \mathrm{Sel}(U)(\mathbb{Q}_p) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_{\mathbb{Q}_p}, U(\mathbb{Q}_p)) \end{array}$$

Figure 3 – Chabauty-Kim diagram, second version

It becomes thus natural to define $X(\mathbb{Q}_p)_U = j_p^{-1}(\mathrm{loc}_p(\mathrm{Sel}(U)(\mathbb{Q}_p)))$. It is a set of particular p-adic points of the curve, containing in particular $X(\mathbb{Q})$. This notation was implicit in Kim's work [21], when U is one of the U_n, and he showed that usual conjectures such as the Bloch-Kato conjecture or the Fontaine-Mazur conjecture implied the finiteness of $X(\mathbb{Q}_p)_{U_n}$ for large n, using the sufficient condition below.

We have the following information on the maps, according to [2] (which ultimately sources [21]):

Theorem 1.4 *j_p is analytic on each residue disk and the image of the residue disk of b is Zariski-dense. loc_p comes from a morphism of $\mathbb{Q}_p$-schemes.*

Corollary 1.5 *If loc_p is not dominant as a map of varieties, then $X(\mathbb{Q}_p)_U = j_p^{-1}(\mathrm{loc}_p(\mathrm{Sel}(U)(\mathbb{Q}_p)))$ is finite (and in particular $X(\mathbb{Q})$ is finite!).*

Proof. – Let Z be the scheme theoretical image of loc_p, which is a closed subscheme (with strictly smaller underlying space) of $H^1_f(G_{\mathbb{Q}_p}, U(\mathbb{Q}_p))$ which is affine from [2]. Thus, there is an nontrivial algebraic morphism of $\mathbb{Q}_p$-schemes $\alpha : H^1_f(G_{\mathbb{Q}_p}, U(\mathbb{Q}_p)) \to \mathbb{A}^1_{\mathbb{Q}_p}$ vanishing on Z, so that $\alpha \circ j_p : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ is locally analytic, nonzero on the residue disk of b, and vanishes on $X(\mathbb{Q}_p)_U$. Thus $X(\mathbb{Q}_p)_U$ has finitely many points on the residue disk of b.

If we change the base point, we have a (non-natural) isomorphism between the two corresponding Chabauty-Kim diagrams due to the existence of a "rational" path linking the two points (see [39, Tag 0BND] and then perform the pro-p-unipotent completion). So the hypothesis is independent of the base point, so that $X(\mathbb{Q}_p)_U$ has finitely many points on each residue disk. □

Computing loc_p precisely, to determine when it is dominant, can be difficult, but there is a simple sufficient condition:

Proposition 1.6 *If $\dim \mathrm{Sel}(U) < \dim H^1_f(G_{\mathbb{Q}_p}, U)$, then $X(\mathbb{Q}_p)_U$ is finite and in particular $X(\mathbb{Q})$ is finite.*

Proof. – Note that the two schemes are affine of finite type over $\mathbb{Q}_p$, so it is enough to show that if A, B are two finitely generated K-algebras such that $A \to B$ has nilpotent kernel (ie $\operatorname{Spec} B \to \operatorname{Spec} A$ is dominant), then $\dim B \geq \dim A$. By Noether normalization, A is finite over a polynomial ring in $\dim A$ variables, so we may assume that $A = K[X_1, \dots, X_d]$ for some $d \geq 0$. Write $C_1, \dots, C_p$ the irreducible components of $\operatorname{Spec} B$, the reunion of the closures of the images of the C_i in $\operatorname{Spec} A$ is the closure of the image of $\operatorname{Spec} B$, so contains the generic point. Therefore, some C_i is dominant over $\operatorname{Spec} A$. As $\dim C_i \leq \dim B$, we can thus assume $\operatorname{Spec} B$ irreducible and even integral. As the morphism is dominant (scheme-theoretically) , it follows that $A \to B$ is injective, and thus we have an injection on the fraction fields. But the transcendance degree of the fraction field of A is d, and for B it is $\dim B$, so $\dim B \geq d$. □

In [13], the dimension estimate used to use the criterion above is the following (it is adapted from [2, Lemma 3.1]):

Theorem 1.7 *Assume, in addition to the original setting, that U is a quotient of U_2, so that its derived subgroup is central. We are in the setting of "Quadratic Chabauty". Let A be an abelian variety over $\mathbb{Q}$, which is a quotient of the Jacobian J of X. Assume that we have an exact sequence (in the sense of $\mathbb{Q}_p$-complete groups with Galois actions) $1 \to \mathbb{Q}_p(1)^n \to U(\mathbb{Q}_p) \to T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to 1$, where the second-to-last map is the abelianization of U. Then:*

1. *$\mathrm{Sel}(U)$ has dimension at most the rank of $A(\mathbb{Q})$.*
2. *$H^1_f(G_{\mathbb{Q}_p}, U)$ has dimension $\dim A + n$.*

Corollary 1.8 *With the notations and assumptions of the theorem, if moreover $\mathrm{rank}\ A(\mathbb{Q}) < \dim A + n$ then $X(\mathbb{Q}_p)_U$ is finite and thus the cardinality of $X(\mathbb{Q})$ can be bounded.*

The strategy of the proof in [13] is now as follows, when X is a modular curve $X_0(N)^+$ or $X_{\mathrm{ns}}(N)^+$ (we will define these curves more precisely):

1. Find through modular form theory a suitable isogeny of abelian varieties $J \to A \times B$ such $\mathrm{Hom}(A, B) = 0$ (and, moreover, $A(\mathbb{Q})$ has rank $\dim A$).

2. Define a partial function $\theta : \mathrm{NS}(A) \to B(\mathbb{Q}) \otimes \mathbb{Q}$ whose kernel K has positive rank r.

3. Show that quadratic Chabauty works in this setting as soon as $\mathrm{rk} A(\mathbb{Q}) < \dim A + r$ (that is, prove Theorem 1.7).

The third point of this program is done in Section 3 of [13]. We will not focus on it, because it uses more involved tools, and instead we will admit Theorem 1.7 and focus on the first two points of the program.

2.2 Correspondences on curves and applications

2.2.1 Correspondences on curves

In the following (at least until we specialize), we consider general curves over fields K of characteristic zero, that is, smooth projective geometrically connected one-dimensional K-schemes with a K-rational point. Our first interest is to show that correspondances, as Cartier divisors of a product of two curves, induce morphisms between the Picard groups and Jacobians.

Proposition 2.1 *Let X_1, X_2 be curves with rational points b_1, b_2. Define $\pi_i : X_1 \times_K X_2 \to X_i$ the projections, and $i_1 : X_1 \to X_1 \times_K X_2$ given by (id, b_2) (and same for i_2). Then we have maps $\pi_i^* : \mathrm{Pic}(X_i) \to \mathrm{Pic}(X \times X)$, and $i_k^* : \mathrm{Pic}(X \times X) \to \mathrm{Pic}(X_k)$, such that, as abelian groups:*

$$\mathrm{Pic}(X_1 \times X_2) = \pi_1^* \mathrm{Pic}(X_1) \oplus \pi_2^* \mathrm{Pic}(X_2) \oplus (\ker i_1^* \cap \ker i_2^*).$$

Proof. – We have a right-to-left natural map, the addition a. Consider, as a map left-to-right, the map $c = (\pi_1^* i_1^*, \pi_2^* i_2^*, \mathrm{id} - \pi_1^* i_1^* - \pi_2^* i_2^*)$. Indeed, since $\pi_k \circ i_k = \mathrm{id}$, $i_k^* \pi_k^* = \mathrm{id}$; if $k \neq l$, $\pi_l \circ i_k$ is constant, so $i_k^* \pi_l^*$ is the trivial map. Thus c is well-defined. Clearly, $a \circ c = \mathrm{id}$. To show that $c \circ a = \mathrm{id}$, it is enough to check it on the three coordinates separately.

If $\mathscr{L} = \pi_k^* \mathscr{M}$, $\pi_k^* i_k^* \mathscr{L} \cong \pi_k^* (i_k^* \pi_k^*) \mathscr{M} \cong \pi_k^* \mathscr{M} \cong \mathscr{L}$; if $l \neq k$, $\pi_l^* i_l^* \mathscr{L} \cong \pi_l^* i_l^* \pi_k^* \mathscr{M} \cong \pi_l^* 0 \cong 0$ where 0 is the trivial line bundle, and the third coordinate is by definition $\mathscr{L} - \mathscr{L} - 0 = 0$ (where the law group on the Picard groups is denoted additively). □

Lemma 2.2 *Let X_1, X_2 be curves over a field K. Let $\mathscr{L}$ be a line bundle over $X_2 \times_K X_1$. Let $X = X_1 \times_K X_1$, p and q be the right projections from X to X_1. Then $\mathscr{M} = (\mathrm{id} \times p)^* \mathscr{L} \otimes (\mathrm{id} \times q)^* \mathscr{L}^{-1}$ is a line bundle on $X_2 \times X$, such that for each $t \in X$, $\mathscr{M}_t$ (which is a line bundle on the curve $(X_2)_{\kappa(t)}$) has degree 0. Moreover, if Δ is the diagonal subscheme of X, $\mathscr{M}_{|X_2 \times \Delta}$ is trivial.*

Proof. – Only the degree 0 part is not an easy verification. Let $\mathscr{L}_p = (\mathrm{id} \times p)^* \mathscr{L}$ and $\mathscr{L}_q = (\mathrm{id} \times q)^* \mathscr{L}$, and $\mathscr{K}$ be any of them. We know $t \in X \longmapsto \chi((\mathrm{id}, t)^* \mathscr{O}_{X_2 \times_K X}) + \chi_{\kappa(t)}(\mathscr{K}_t)$ is locally constant, from the cohomology of schemes (see e.g. [30, Theorem 4.2]). As X_1 is geometrically connected, X is connected, and the map above, which is $t \in X \longmapsto \deg_{(X_2)_{\kappa(t)}} \mathscr{K}_t$, is constant.

Now, take $s \in X_1$ a closed point, and $t = (s, s)$ its image under the diagonal injection. One easily checks that $(\mathscr{L}_p)_t \cong (\mathscr{L}_g)_t$, hence the conclusion follows. □

Corollary 2.3 *With the same notations, there is a unique morphism of abelian varieties $\psi(\mathscr{L}) : J_1 \to J_2$ such that its composition with the difference map $X_1 \times X_1 \to J_1$ corresponds to the class of $\mathscr{M}$ in $J_2(X)$ as described in [31, Theorem 1.1]. $\psi : \mathrm{Pic}(X_2 \times X_1) \to \mathrm{Hom}(J_1, J_2)$ is a map with kernel containing $\pi_1^* \mathrm{Pic}(X_1) + \pi_2^* \mathrm{Pic}(X_2)$.*

Proof. – We use the Albanese property from [31, Proposition 6.4], and the functor description of the Jacobian ([31, Theorem 1.1]): the homomorphisms $J_1 \to J_2$ are in bijection with the morphisms $X_1 \times X_1 \to J_2$ vanishing on the diagonal. Some of these morphisms are represented by the line bundles $\mathscr{P}$ on $X_2 \times (X_1 \times X_1)$ such that for all $t \in X_1 \times X_1$, $\mathscr{P}_t$ has degree 0 as a line bundle on $(X_2)_{\kappa(t)}$, and such that $\mathscr{P}_{|X_2 \times \Delta}$ is the pull-back of a line bundle on X_1 under $X_2 \times \Delta \to \Delta \to X_1$. This describes all the morphisms if $X_2(X_1 \times X_1)$ is not empty. As there are morphisms $X_1 \times X_1 \to X_1$ and $X_1 \to X_1 \times X_1$, $X_2(X_1 \times X_1)$ is not emmpty iff there is a morphism $X_1 \to X_2$.

That, for $i \in \{1, 2\}$, ψ vanishes on $\pi_i^* \mathrm{Pic}(X_i)$ is easy to see: if $\mathscr{L} = \pi_2^* \mathscr{N}$, then $\mathscr{M} = (X_2 \times X \to X_2)^* \mathscr{L} \otimes (X_2 \times X \to X_2)^* \mathscr{L}^{-1}$ is trivial. If $\mathscr{L} = \pi_1^* \mathscr{N}$, then $\mathscr{M} = (X_2 \times X \to X)^* (p^* \mathscr{N} \otimes q^* \mathscr{N}^{-1})$ so

corresponds to the null morphism $J_1 \to J_2$. □

The properties of this map are clearer when X_1 and X_2 have both rational points, thanks to the existence of Abel-Jacobi injections.

Proposition 2.4 *With the same notations, if $b_i \in X_i(K)$, $\psi(\mathscr{L})$ is uniquely defined by the equality $\psi(\mathscr{L}) \circ AJ_{b_1} = \mu$, where $AJ_{b_1} : X_1 \to J_1$ is the Abel-Jacobi injection mapping b_1 to 0, and $\mu : X_1 \to J_2$ is defined by the line bundle $(\mathrm{id}, p, b_1)^*\mathscr{M} = (\mathrm{id}, b_1)^*\mathscr{L}^{-1} \otimes \mathscr{L} \in \mathrm{Pic}(X_2 \times X_1)$. Then the kernel of ψ is exactly $\pi_1^* \mathrm{Pic}(X_1) \oplus \pi_2^* \mathrm{Pic}(X_2)$ and ψ is onto.*

Proof. – Let $\delta : X_1 \times X_1 \to J_1$ be the difference map, then $\delta \circ (\mathrm{id}, b_1) = AJ_{b_1}$, so that $\psi(\mathscr{L}) \circ AJ_{b_1} = \psi(\mathscr{L}) \circ \delta \circ (\mathrm{id}, b_1)$. But $f = \psi(\mathscr{L}) \circ \delta$ is defined by $\mathscr{M}$ in the functor-of-points approach. Thus $\mu := f \circ (\mathrm{id}, b_1)$ is described by the corresponding pullback of $\mathscr{M}$ along $(\pi_2, p, b_1) : X_2 \times X_1 \times X_1 \to X_2 \times X_1 \times \mathrm{Spec}\, K = X_2 \times X_1$.

Let $\mathscr{L}$ be a line bundle on $X_2 \times X_1$ such that for each $t \in X_1$, $(\mathrm{id} \times t)^*\mathscr{L}$ has degree 0. Let $\mathscr{M} = (\mathrm{id}, b_1)^*\mathscr{L}^{-1}$ (where b_1 is the morphism $X_2 \to \mathrm{Spec}\, k = \mathrm{Spec}\, \kappa(b_1) \to X_1$), then $\pi_2^*\mathscr{M} \cong ((\mathrm{id}, b_1) \circ \pi_2)^*\mathscr{L}^{-1} = (\mathrm{id}, b_1)^*\mathscr{L}^{-1}$. Thus $\psi(\mathscr{L})$ is the endomorphism associated to $\mathscr{L}$ by [31, Theorem 1.1]. By the Albanese property, this shows that ψ is surjective.

If $\mathscr{L}$ is a line bundle on X_2, then $(\mathrm{id}, b_1)^*\pi_2^*\mathscr{L} \cong \pi_2^*\mathscr{L}$ (as $\pi_2 \circ (\mathrm{id}, b_1) = \pi_2$, thus $\pi_2^* \mathrm{Pic}(X_2) \subset \ker \psi$.

By the description of the Jacobian as a functor of points, see again [31, Theorem 1.1], $\pi_1^* \mathrm{Pic}(X_1) \subset \ker \psi$.

Let $\mathscr{L} \in \mathrm{Pic}(X_2 \times_K X_1)$ be such that $\psi(\mathscr{L})$ is the zero endomorphism. This implies that for some line bundle $\mathscr{M}$ on X_1, $\mathscr{L} \cong (\mathrm{id}, b_1)^*\mathscr{L} \otimes \pi_1^*\mathscr{M}$. But, as $\pi_2 \circ (\mathrm{id}, b_1) = \pi_2$, it follows that the first term is in $\pi_2^* \mathrm{Pic}(X_2)$. This concludes thanks to the previous proposition. □

Note that this morphism is canonical and stable under base change by any field extension. This has the following application:

Corollary 2.5 *In the general case (ie X_1, X_2 no longer necessarily have rational points), $\pi_1^* \mathrm{Pic}(X_1)$ and $\pi_2^* \mathrm{Pic}(X_2)$ are in direct sum. Moreover, the quotient of $\ker \psi$ by this sum is a torsion group; the cokernel of ψ is as well a torsion group. If there is a Galois field extension L/K such that $X_1(L)$ and $X_2(L)$ are nonempty, then $[L : K]$ vanishes both of these groups.*

Proof. – Let L/K be a finite Galois extension such that both $Y_i = X_i \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L$ have rational points. Algebraic geometry results (something akin to [30, Lemmas 5.4, 6.2]) show that the pull-backs $\mathrm{Pic}(X_i) \to \mathrm{Pic}(Y_i)$ are injections (and similarly for $\mathrm{Pic}(X_1 \times X_2) \to \mathrm{Pic}(Y_1 \times Y_2)$), so this proves the "direct sum" part.

If $\psi(\mathscr{L}) = 0$ (with $\mathscr{L}$ line bundle over $X_1 \times X_2$), let $\mathscr{L}'$ be its pull-back to a line bundle on $Y_1 \times Y_2$. Then $\psi(\mathscr{L}') = 0$ as well, so $\mathscr{L}' = \pi_1^*\mathscr{M}_1' \otimes \pi_2^*\mathscr{M}_2'$ for line bundles $\mathscr{M}_i'$ on Y_i. Let $\mathscr{M}_i$ be the tensor product of all the images of $\mathscr{M}_i'$ under the action of the Galois group of L/K: then $\mathscr{M}_i$ is a Galois-invariant line bundle on $X_i \times_K \mathrm{Spec}\, L$, so is the pull-back of a line bundle $\mathscr{N}_i$ defined on X_i. As $\mathscr{L}'$ is invariant under the action of the Galois group of L/K, $\mathscr{L}'^{[L:K]} = \pi_1^*\mathscr{M}_1 \otimes \pi_2^*\mathscr{M}_2$. By the injectivity in the Picard groups of the pullback of $Y_1 \times_L Y_2 \to X_1 \times X_2$, $\mathscr{L}^{[L:K]} = \pi_1^*\mathscr{N}_1 \otimes \pi_2^*\mathscr{N}_2$.

Let $u : J_1 \to J_2$ be a homomorphism, we know that there is a line bundle $\mathscr{L}$ on $Y_1 \times Y_2$ such that $\psi(\mathscr{L}) = u$. For any σ in the Galois group of L/K, one easily sees that $\psi(\sigma^*\mathscr{L}) = \sigma^* u = u$, since u is defined over K itself. In particular, by the same reasoning as the above, there is a line bundle $\mathscr{M}$ on $X_1 \times X_2$ whose pull-back $\mathscr{N}$ under $Y_1 \times_L Y_2 \to X_1 \times_K X_2$ is the tensor product of all the conjugates of $\mathscr{L}$ under the action of the Galois group. Thus $\psi(\mathscr{N}) = [L : K]u$, and by stability under base change $\psi(\mathscr{M}) = [L : K]u$, which implies the conclusion. □

We now give two more explicit descriptions of the construction, which will be useful when considering the θ morphism later on.

Lemma 2.6 *Let $b, b' \in X_1(K)$ and $\mathscr{L}$ be a line bundle on $X_2 \times_K X_1$. Then the image of $\psi(\mathscr{L})([b - b'])$ is the point of J_2 associated with $\mathscr{L}_{|X_2 \times \{b\}} - \mathscr{L}_{|X_2 \times \{b'\}}$.*

Proof. – It is enough to show it when $b' = b_1$. By the description of the functor of points of the Jacobian from [31], the conclusion follows. □

Lemma 2.7 *Assume K is algebraically closed. With the same notations, if Z is a prime divisor on $X_1 \times X_2$ (i.e. an integral closed subscheme of codimension 1) associated to the line bundle $\mathscr{L}$, then, $\psi(\mathscr{L}) : J_1(K) \to J_2(K)$ is the quotient of the map $\mathrm{Div}(X_1) \to \mathrm{Div}(X_2)$ given by $\mathrm{Div}_{\mathrm{Cartier}}(X_1) \xrightarrow{(\pi_1 : Z \to X_1)^*}$*

$\mathrm{Div}_{\mathrm{Cartier}}(Z) \to \mathrm{Div}_{\mathrm{Weil}}(Z) \overset{(\pi_2:Z\to X_2)_*}{\longrightarrow} \mathrm{Div}_{\mathrm{Weil}}(X_2)$. *That map maps divisors of degree* 0 *to divisors of degree* 0*, and, by construction, divisors of meromorphic functions to divisors of meromorphic functions, so it induces a map* $\mathrm{Pic}(X_1) \to \mathrm{Pic}(X_2)$ *(that is the corresponding Jacobian map on the bundles of degree* 0*).*

Proof. – The second part follows from standard properties of Cartier and Weil divisors, see [25, Definition 7.2.17, Proposition 7.3.8], and from the first part. Let us thus see the first one. As $J_i(K)$ is generated by $X_i(K) - b_i$, it is enough to check the statement for inputs of the form $[P] - [b_1]$ for $P \in X_1(K)$. Given $P \in X_1(K)$, its image under our divisor map is $\sum_{Q\in X_2(K),(Q,P)\in Z} e_{\mathcal{O}_{Z,(Q,P)}/\mathcal{O}_{X_1,P}}[Q]$ (the factor will from now on be denoted as e_Q simply). Let $U_2 \subset X_2, U_1 \subset X_1$ be affine open subsets containing all the Q in the sum above and b_2, and P and b_1 respectively, with coordinate rings A_2 and A_1 (Dedekind rings and finitely generated K-algebras). Let I be the kernel of $A_2 \otimes_K A_2 \to A_2$, $\mathscr{L}_{|U_2\times U_1}$ correspond to a locally principal ideal J of $A_2 \otimes_K A_1$.

We show that, as ideals of A_2 through the canonical identifications $\{P\} \cong \{Q\} \cong \mathrm{Spec}\, K$, $\mathscr{L}_{|U_2\times\{P\}}$ is equal to the product of the $I_{|U_2\times\{Q\}} = I_Q$, each factor being counted e_Q times. Indeed, $\mathscr{L}_{|U_2\times\{P\}}$ is $J/m_P J$, an ideal of $(A_2 \otimes A_1)/(m_P(A_2 \otimes A_1)) = A_2 \otimes (A_1/m_P) = A_2$. By definition, e_Q is the length of the $((A_2)_{m_Q} \otimes (A_1)_{m_P})/(J)$-module $((A_2)_{m_Q} \otimes (A_1)_{m_P})/(J, m_P)$.

For each Q, we have a split exact sequence of K-vector spaces $0 \to I \to A_2 \otimes A_2 \to A_2 \to 0$, the last arrow being given by the multiplication. So its restriction to $U_2 \times \{Q\}$ is $0 \to I_Q \to A_2 \otimes (A_2/m_Q) \to A_2/m_Q \to 0$. Thus, seen as an ideal of A_2, I_Q becomes m_Q. So the goal is to show that if J' is the ideal of A_2 given by reducing mod m_P all the elements of $J \subset A_2 \otimes A_1$, then J' is the product of the $m_Q^{e_Q}$. But by the above, e_Q is the length of $(A_2)_{m_Q}/(J')$.

It follows that, letting U_1 and U_2 run over all possible affine open subsets, $\mathscr{L}_{|X_2\times\{P\}} \cong \bigotimes_Q I_{|X_2\times\{Q\}}^{\otimes e_Q}$. Now, let $\mathscr{M} = (\pi_2, b_1)^*\mathscr{L}^{-1} \otimes \mathscr{L}$, then

$$\mathscr{M}_{|X_2\times\{P\}} = \mathscr{L}_{|X_2\times\{P\}} \otimes \mathscr{L}^{-1}_{|X_2\otimes\{b_1\}} \cong \bigotimes_j I_{|X_2\times\{Q_j\}}^{\otimes m_j},$$

where $\sum_j m_j Q_j$ is the image of $[P]-[b_1]$ under the divisor map. By the interpretations and identifications of the Jacobian in [31], that line bundle is the bundle $\mathscr{U}_{|X_2\times\{[\sum_j m_j Q_j]\}}$, so the image of P under the map $X_1 \to J_2$ constructed while defining $\psi(\mathscr{L})$ is $\sum_j m_j Q_j$. The image of b_1 under this map is zero, which concludes. □

2.2.2 Definition of the θ morphism

Let K be a field of characteristic zero and X be a curve over K. We make the following assumptions:

- X has a rational point b.
- The Jacobian J of X has a map of abelian varieties $(\pi_A, \pi_B) : J \to A \times B$.

We denote AJ (or AJ_b when there is an ambiguity) the immersion $X \to J$ mapping b to 0. Define the map $\tilde{AJ} : \mathrm{Pic}(J) \to \mathrm{Pic}(X)$ as $\mathscr{L} \longmapsto AJ^*\mathscr{L} \otimes (-AJ)^*\mathscr{L}$.

If $\delta : X \times X \to J$ is the difference map, $\Delta = (\mathrm{id}, \mathrm{id}) : X \to X$, $i_1 = (\mathrm{id}, b) : X \to X \times X$, $i_2 = (b, \mathrm{id}) : X \to X \times X$, one easily checks that the following diagram commutes:

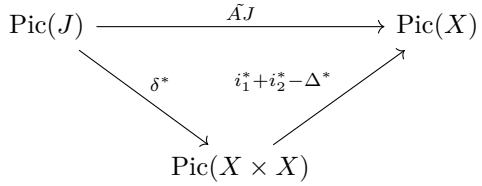

Figure 4 – Factorization of $\tilde{AJ}$

We recall the following definitions from [30]:

Definition Let U be an abelian variety over a field K. Let π_1, π_2 denote the projections $U \times U \to U$, and m denote the multiplication map. We define $\mathrm{Pic}^0(U)$ to be the subgroup of $\mathrm{Pic}(U)$ of equivalence

classes of line bundles $\mathscr{L}$ over U satisfying $m^*\mathscr{L} \cong \pi_1^*\mathscr{L} \otimes \pi_2^*\mathscr{L}$. The *Néron-Severi* group of U is the group $NS(U) = \mathrm{Pic}(U)/\mathrm{Pic}^0(U)$. It is free with finite rank denoted $\rho(U)$.

Lemma 2.8 *In Figure 4, the maps δ^* and $\tilde{AJ}$ vanish at all elements of $\mathrm{Pic}^0(J)$.*

Definition Let $G(A)$ be the inverse image of $\mathrm{Pic}^0(X)$ under $NS(A) \overset{\pi_A^*}{\to} NS(J) \overset{\tilde{AJ}_b}{\to} \mathrm{Pic}(X)$ (we will see below that it does not depend on b, hence justifying the notation). The θ morphism, based at b (depending also of π_A, π_B but we leave the dependency nonexplicit for the sake of easier notation), is the map $\theta_b : G(A) \to \mathrm{Pic}^0(X) = J(K) \overset{\pi_B}{\to} B(K)$.

The previous study gives us an important criterion for the vanishing of θ_b:

Proposition 2.9 *Let $b \in X(K)$ and $\Omega \supset K$ be an algebraically closed field. Let F be a group of Cartier divisors on $X \times X$. Assume that :*

1. *There is a subset $S \subset X(\Omega)$ such that every K-divisor of null degree on X with support in S projects into $B(K)$ as a torsion point.*
2. *For every $k = 1, 2$, $D \in F$, the supports of $(i_k^*(b)D)(\Omega)$, and $\Delta^*D(\Omega)$ are in S.*
3. *$\mathrm{End}(J)/\psi(F)$ is a torsion group.*

Then θ_b maps into $B(K)_{tors}$.

Proof. – Let $\mathscr{L}$ be a line bundle on A reducing to an element of $G(A)$. Let $\mathscr{M} = (\pi_A \circ \delta)^*\mathscr{L}$. We know that there exists an integer $d \geq 1$ such that $\psi(\mathscr{M}^d) = \psi([D])$ for some $D \in F$. Therefore, there are line bundles $\mathscr{N}_1, \mathscr{N}_2$ on X such that $\mathscr{M}^d = \pi_1^*\mathscr{N}_1 + \pi_2^*\mathscr{N}_2 + [D]$. By definition,

$$-d\theta_b(\mathscr{L}) = \pi_B\left(\Delta^*\mathscr{M}^d - i_1(b)^*\mathscr{M}^d - i_2(b)^*\mathscr{M}^d\right).$$

But for each $k \in \{1, 2\}$, $\Delta^*\pi_k^*\mathscr{N}_k - i_k(b)^*\pi_k^*\mathscr{N}_k - i_{3-k}(b)^*\pi_k^*\mathscr{N}_k = \mathscr{N}_k - \mathscr{N}_k - b^*\mathscr{N}_k = 0$ computed in $\mathrm{Pic}(X)$. Thus

$$-d\theta(\mathscr{L}) = \pi_B\left([\Delta^*D - i_1(b)^*D - i_2(b)^*D]\right).$$

Now, $\Delta^*D - i_1(b)^*D - i_2(b)^*D$ is a K-divisor on X with support in S, and with degree 0 by the assumptions on $\mathscr{L}$. So its image under π_B is torsion in $B(K)$, which concludes. □

The homomorphism θ_b can seem a little far-fetched: its interest comes from the following theorem from [13, Section 3], which asserts that it suits the Chabauty-Kim-related part of the program, that is,

Theorem 2.10 *With the above notations, assume that $(\pi_A, \pi_B) : J \to A \times B$ is an isogeny, $K = \mathbb{Q}$ and $\mathrm{Hom}(A, B) = 0$. Let r be the rank of the kernel of $\theta_b \otimes \mathbb{Q} : G(A) \to B(\mathbb{Q}) \otimes \mathbb{Q}$. Assume finally that X has genus at least 2. Then there exists a Galois-stable quotient U of $U_2(b)$ such that its abelianization has $T_p(A) \otimes \mathbb{Q}_p$ as space of $\mathbb{Q}_p$-points and such that the space of $\mathbb{Q}_p$-points of $[U, U]$ is $\mathbb{Q}_p(1)^r$ (all of this being compatible to the Galois actions).*

From the theorems quoted in Section 2.1,

Corollary 2.11 *If $A(\mathbb{Q})$ has rank less than $\dim A + r$, then $X(\mathbb{Q}_p)_U$ is finite and thus so is $X(\mathbb{Q})$.*

2.2.3 A basepoint-free definition under further assumptions

We immediately notice that the θ morphism commutes with base change under a finite field extension, provided the base point is the same. We could stop our study of the construction there, but we would struggle with a major technical difficulty in Section 2.4, due to the fact that points that behave well enough under the Hecke operators, i.e. the cusps, are not rational. To address this issue, we investigate the changes θ morphisms undergo when changing the base point.

Lemma 2.12 *Let $\mathscr{L}$ be a line bundle on $X \times X$ and $b, b' \in X(K)$. We denote $i_1(b) = (\mathrm{id}, b) : X \to X \times X$, $i_1(b') = (\mathrm{id}, b') : X \to X \times X$, and similarly for $i_2(b), i_2(b')$. Then $i_1(b)^*\mathscr{L} + i_2(b)^*\mathscr{L} - i_1(b')^*\mathscr{L} - i_2(b')^*\mathscr{L} = \psi(\mathscr{L})([b - b']) + \psi_{s^*\mathscr{L}}([b - b'])$ as points in $J(K) = \mathrm{Pic}^0(X)$, where $s : X \times X \to X \times X$ exchanges the coordinates. In particular, if $\mathscr{P}$ is a line bundle on J, $\deg \tilde{AJ}_b\mathscr{P} = \deg \tilde{AJ}_{b'}\mathscr{P}$, thus $G_b(A) = G_{b'}(A)$, justifying the notational abuse above.*

Proof. – By Lemma 2.6, $\psi(\mathscr{L})([b-b']) = i_2(b)^*\mathscr{L} - i_2(b')^*\mathscr{L}$, and similarly $\psi(s^*\mathscr{L})([b-b']) = i_1(b)^*\mathscr{L} - i_1(b')\mathscr{L}$. □

Lemma 2.13 *If $b, b' \in X(K)$, $\mathscr{L}$ a line bundle on A, $(\pi_A \circ \delta)^*\mathscr{L} = \mathscr{M}$, as a line bundle, then $\psi(\mathscr{M})([b-b']) = (\pi_A \circ AJ_{b'})^*(t^*_{[b'-b]_A}\mathscr{L} \otimes \mathscr{L}^{-1})$.*

Proof. – Computation. □

Lemma 2.14 *Let $\mathscr{L}$ be a line bundle on A. There is a morphism $r_{b',\mathscr{L}} : A \to J$ corresponding, for every finite field extension L, to the map $P \in A(L) \longmapsto AJ^*_{b'}\pi^*_A(t^*_P(A_L \to A)^*\mathscr{L} \otimes (A_L \to A)^*\mathscr{L}^{-1}) \in \mathrm{Pic}^0(X_L) = J(L)$.*

Proof. – Clearly π^*_A extends to a morphism $A^\vee \to J^\vee$ and $AJ_{b'}$ extends to a map $J^\vee \to J$. The inner map is the morphism $A \to A^\vee$ associated to the line bundle $m^*\mathscr{L} \otimes p^*\mathscr{L}^{-1} \otimes q^*\mathscr{L}^{-1}$, where $m, p, q : A \times A \to A$ are respectively the multiplication, the first and the second projection (see [30, Sections 9,10] for elaborations on this). □

Corollary 2.15 *Let $b, b' \in X(K)$, and $\mathscr{L} \in G(A)$ then $\theta_b(\mathscr{L}) - \theta_{b'}(\mathscr{L}) = \pi_B \circ (r_{b',\mathscr{L}} + r_{b',(-1)^*\mathscr{L}}) \circ \pi_A(AJ_{b'}(b))$.*

Proof. – Follow the computations. □

Proposition 2.16 *Let L/K be finite a Galois extension with group G, b a point of $X_L(L)$, $b' \in X(K)$. We have θ morphisms associated with b' ($G(A) \to B(K)$), and to the $\sigma(b)$, $\sigma \in G$, defined $G(A_L) \to B(L)$. Assume that $\mathrm{Hom}(A, B) = 0$. Then $\sum_{\sigma\in G} \theta_{\sigma(b)}$ restricts to a homomorphism $G(A) \to B(K)$, which is $|G|\theta_{b'}$.*

Proof. – Let $\sigma \in G$. Let $\mathscr{L}$ be a line bundle on A that is in $G(A)$. Then $\theta_{\sigma(b)}(\mathscr{L}) - \theta_{b'}(\mathscr{L}) = \pi_B \circ (r_{b',\mathscr{L}} + r_{b',(-1)^*\mathscr{L}}) \circ \pi_A \circ AJ_{b'}(\sigma(b))$ by following all the calculations in L from the previous lemmas. But the last two morphisms in the composition become a K-homomorphism $A \to B$, so must vanish, and the right hand side vanishes. Then we sum over σ. □

Definition So, given a curve X over K with a rational point b, a Jacobian J, and an isogeny $(\pi_A, \pi_B) : J \to A \times B$ such that $\mathrm{Hom}(A, B)$ is zero, the associated θ morphism is the $\theta_b : G(A) \to B(K)$ as defined above, quotiented by torsion, so that $\theta : G(A) \to B(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. It does not depend on the base point.

Corollary 2.17 *Let $b' \in X(K)$, $b \in X(L)$ for a Galois extension L/K with group G. Let $\Omega \supset L$ be an algebraically closed field. Let F be a group of Cartier divisors on $X \times X$. Assume that :*

1. $\mathrm{Hom}(A, B) = 0$.
2. *There is a subset $S \subset X(\Omega)$ such that every K-divisor of null degree on X with support in S projects into $B(K)$ as a torsion point.*
3. *For every $\sigma \in G$, $k = 1, 2$, $D \in F$, the supports of $[i_k^*(\sigma(b))D](\Omega)$, and $\Delta^*D(\Omega)$ are in S.*
4. $\mathrm{End}(J)/\psi(F)$ *is a torsion group.*

Then θ is the null homomorphism.

Proof. – Let $\mathscr{L}$ be a line bundle on A reducing to an element of $G(A)$. Let $\mathscr{M} = (\pi_A \circ \delta)^*\mathscr{L}$. We know that there exists an integer $d \geq 1$ such that $\psi(\mathscr{M}^d) = \psi([D])$ for some $D \in F$. Therefore, there are line bundles $\mathscr{N}_1, \mathscr{N}_2$ on X such that $\mathscr{M}^d = \pi_1^*\mathscr{N}_1 + \pi_2^*\mathscr{N}_2 + [D]$. By definition,

$$-[L:K]d\theta(\mathscr{L}) = \pi_B\left([L:K]\Delta^*\mathscr{M}^d - \sum_{\sigma\in G, 1\leq k\leq 2} i_k(\sigma(b))^*\mathscr{M}^d\right).$$

But for each $k \in \{1, 2\}$, $\Delta^*\pi_k^*\mathscr{N}_k - i_k(\sigma(b))^*\pi_k^*\mathscr{N}_k - i_{3-k}(\sigma(b))^*\pi_k^*\mathscr{N}_k = \mathscr{N}_k - \mathscr{N}_k - \sigma(b)^*\mathscr{N}_k = 0$ computed in $\mathrm{Pic}(X_L)$. Thus

$$-d[L:K]\theta(\mathscr{L}) = \pi_B\left(\left[[L:K]\Delta^*D - \sum_{\sigma\in G, k\in\{1,2\}} i_k(\sigma(b))^*D\right]\right).$$

Now, if $\sigma \in G$, $D_\sigma = \Delta^*D - i_1(\sigma(b))^*D - i_2(\sigma(b))^*D$ is a divisor on X_L with support in S, and the sum of all the D_σ is a divisor defined over K, with support in S, and with degree 0 by the assumptions on $\mathscr{L}$. So its image under π_B is torsion in $B(K)$, which concludes. □

2.3 The θ morphism for the curves $X_0(N)$ and $X_0^+(N)$

2.3.1 Reminders about modular forms

We start with a few reminders on modular curves – for proofs, examples or details, one may consult for instance [10].

$\mathbb{H} = \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}$ is the upper half-plane. It has a natural action of $GL_2^+(\mathbb{R})$ (invertible 2×2 matrices with real entries and positive determinant) given by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \tau = \frac{a\tau+b}{c\tau+d}$.

$SL_2(\mathbb{Z})$ has the following family of finite-index normal subgroups, called the *congruence subgroups*, the $\Gamma(N) = \ker(SL2(\mathbb{Z}) \to SL_2(\mathbb{Z}/(n)))$, for $N \geq 1$. A *congruence subgroup* of $SL_2(\mathbb{Z})$ is any subgroup containing some $\Gamma(N)$.

Natural examples of congruence subgroups include $\Gamma_0(N)$, the group of $SL_2(\mathbb{Z})$ matrices that are upper triangular mod N, and the group of $\Gamma_1(N)$, its subgroup of matrices that are unipotent mod N.

If Γ is a congruence subgroup, it is possible to endow $Y(\Gamma) = \Gamma\backslash\mathbb{H}$ with the structure of a connected (noncompact) Riemann surface $Y(\Gamma)$. This Riemann surface can be compactified into $X(\Gamma) = \Gamma\backslash(\mathbb{H}^*)$, where $\mathbb{H}^*$ is the completed Poincaré half-plane, corresponding to $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, where the point at infinity corresponds to the limit $\mathrm{Im}(z) \to +\infty$ in $\mathbb{H}$.

We denote $X_0(N), X_1(N)$ (and similarly $Y_0(N), Y_1(N)$ for the noncompact version) the compact connected Riemann surfaces $X(\Gamma)$ for $\Gamma = X_0(N), X_1(N)$. The (finitely many) points in $X_i(N)\backslash Y_i(N)$ are the cuspidal points.

Theorem 3.1 *Let $N \geq 1$. $Y_0(N)$ represents the set $S_0(N)$ of equivalence classes of (E, C), where E is a complex elliptic curve, and C is a cyclic cubgroup of order N in the following sense: the application $\psi : \tau \in \mathbb{H} \longmapsto (\mathbb{C}/(\tau\mathbb{Z} \oplus \mathbb{Z}), \langle[1/N]\rangle)$ satisfies $\psi(\tau) \cong \psi(\tau')$ iff τ and τ' are in the same orbit under the action of $\Gamma_0(N)$, and every pair (E, C) as above is isomorphic to some $\psi(\tau)$. Similarly, the application $\tau \in \mathbb{H} \longmapsto (\mathbb{C}, (\tau\mathbb{Z} \oplus \mathbb{Z}), [1/N])$ realizes a bijection between $Y_1(N)$ and the set $S_1(N)$ of isomorphism classes of (E, Q) where E is a complex elliptic curve and Q is a point of order N.*

For each $k \in \mathbb{Z}$, there is a right action of $GL_2(\mathbb{R})^+$ of weight k on the space of functions and $\mathbb{H} \to \mathbb{C}$, given by $\left(f|_k \begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)(\tau) = \frac{(ad-bc)^{k-1}}{(c\tau+d)^k} f\left(\frac{a\tau+b}{c\tau+d}\right)$. In the rest of the section, we are concerned only with the action of weight 2. When Γ is a congruence subgroup, $\mathcal{S}_2(\Gamma)$ is the space of holomorphic functions $f : \mathbb{H} \to \mathbb{C}$ that are invariant under the weight-2 action of Γ, and such that for each $\alpha \in SL_2(\mathbb{Z})$ $f|_2\alpha(\tau) \to 0$ as $\mathrm{Im}(\tau) \to \infty$.

For each congruence group Γ, $\mathcal{S}_2(\Gamma)$ is a Hermitian space with the Petersson scalar product, defined up to a constant in [10, Chapter 5.4].

Lemma 3.2 *Let Γ be any congruence subgroup.*

- *For any $f \in \mathcal{S}_2(\Gamma)$, $f(\tau)d\tau$ goes to the quotient to a holomorphic differential form on $Y_0(N)$, such that it can be extended into a global holomorphic differential form on $X_0(N)$.*
- *If ω is a holomorphic differential form on $X_0(N)$, its pullback under the natual map $\mathbb{H} \to Y_0(N) \to X_0(N)$ is some $f(\tau)d\tau$ with $f \in \mathcal{S}_2(\Gamma)$.*

Proof. – Let f be a holomorphic function on $\mathbb{H}$ such that it is invariant under the weight-2 action of Γ. Then the 1-form $f(\tau)d\tau$ is invariant under the action of Γ so extends to a differential form u on $Y_0(N)$. It remains to check when u extends to a differential form on $X_0(N)$ as a whole.

Let $s \in \mathbb{Q} \cup \{\infty\}$ be a cusp point, let $\gamma \in SL_2(\mathbb{Z})$ be a matrix mapping s to ∞, with second row (c, d), let $0 < h < \infty$ be the index of $\gamma\Gamma\gamma^{-1}\{\pm I_2\}$ in the stabilizer of ∞ in $SL_2(\mathbb{Z})$. Now, let $M > 10$ and consider the image U' of $U = \gamma^{-1}(\{\tau \in \mathbb{H},\ \mathrm{Im}(\tau) > M\} \cup \{\infty\})$ in $X_0(N)$; we have a map $\tau \in U \longmapsto e^{2i\pi\gamma(\tau)/h}\mathbb{C}$ which factors into an injective holomorphic map $U' \to \mathbb{C}$ mapping s to 0. Now, the push-forward u_s under $U' \to \mathbb{C}$ of u is the push-forward of $f(\tau)d\tau$ under $\tau \in U \longmapsto e^{2i\pi\gamma(\tau)/h} = q_h(\tau) \in \mathbb{C}$, and $dq_h(\tau) = q_h(\tau)\frac{2i\pi}{h}(c\tau + d)^{-2}$, thus the push-forward is $f(\tau)(c\tau + d)^2 \frac{h}{2i\pi}\frac{dq_h(\tau)}{q_h(\tau)}$. One easily checks that $f[\gamma^{-1}]_2(\gamma(\tau)) = f(\tau)(c\tau + d)^2$, thus $u_s = \frac{h}{2i\pi} f[\gamma^{-1}]_2(\gamma q_h^{-1}(z))\frac{dz}{z}$.

u is holomorphic at s if and only if u_s is holomorphic at 0, iff $f[\gamma^{-1}]_2(\gamma q_h^{-1}(z))$ goes, as $z \to 0$, to 0. This occurs iff $f[\gamma^{-1}]_2$ goes to 0 at $i\infty$. Now, the reunion of the $\Gamma\gamma^{-1}$, over all the $\gamma \in SL_2(\mathbb{Z})$ mapping

∞ to some cusp, is exactly $SL_2(\mathbb{Z})$. Thus u extends to a global holomorphic differential iff f is a cusp form. In particular, this implies the first point.

For the second point, note that said pullback $f(\tau)d\tau$ must be holomorphic on the Poincaré half-plane and invariant under Γ, which forces f to be invariant under the weight-2 action of Γ. But now u is the global holomorphic extension of the pushforward of $f(\tau)d\tau$, so by the above f must be a cusp form.□

We denote as $J_0(N), J_1(N)$ the Jacobians of $X_0(N), X_1(N)$ respectively.

A particular family of operators acts on $J_0(N)$ and $J_1(N)$, and especially on their spaces of holomorphic differential forms. They are the *Hecke operators*. All these operators commute, and for each integer $N \geq 1$, there is an orthogonal decomposition into subspaces stable under the Hecke operators $\mathcal{S}_2(\Gamma_0(N)) = \mathcal{S}_2(\Gamma_0(N))^{\text{old}} \oplus \mathcal{S}_2(\Gamma_0(N))^{\text{new}}$ (the "oldspace" and the "newspace"), where $\mathcal{S}_2(\Gamma_0(N))^{\text{old}}$ is generated by the $f|_2\text{diag}(q,1)$ where $f \in \mathcal{S}_2(\Gamma_0(p))$ for all $pq|N$. Moreover, there exists an orthogonal basis of $\mathcal{S}_2(\Gamma_0(N))^{\text{new}}$ made with functions f that are eigenvectors for each Hecke operator and such that $f(\tau) \sim e^{2i\pi\tau}$ as $\text{Im}(\tau) \to \infty$. They are called *newforms* of level N.

If f is a newform of level N, we get a morphism from the level N Hecke algebra $T_{\mathbb{Z},N}$ into $\text{End}(J_0(N))$. We also have a natural morphism $T_{\mathbb{Z},N} \to \mathbb{C}$ given by $T \longmapsto a_1(Tf)$, with kernel I_f. The abelian variety associated with f is $A_f = J_0(N)/I_f J_0(N)$.

There is also in level N, an involution we will call the Atkin-Lehner involution of $\mathcal{S}_2(\Gamma_0(N))$, denoted as $w_N = \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$. We can check it is self-adjoint for the Petersson inner product, and that it preserves the oldspace and newspace. By [10, Theorem 5.5.3, (5.16)], it commutes with the Hecke operators, so that every newform must be an eigenvector of w_N, that is, either $w_N(f) = f$ (f is "positive") or $w_N(f) = -f$ (f is "negative").

If N is prime, there is an isogeny $J_0(N) \to \prod_f A_f$, where f runs over the equivalence classes of newforms of $\mathcal{S}_2(\Gamma_0(N))$ modulo the Galois action. We will divide these A_f in two groups, so that we get two isogeny factors for $J_0(N)$ (and $J_0^+(N)$ as we will see later), according to whether $L'(f,1)$ vanishes.

All the constructions above of holomorphic varieties can actually be realized algebraically as proper algebraic varieties over $\mathbb{Q}$. Let us show a result from [40]; we reproduce the proof because the document is unpublished.

Proposition 3.3 *Let f be a newform for $\Gamma_0(N)$ for some integer $N \geq 1$. Every Hecke operator acts on A_f as an algebraic endomorphism defined over $\mathbb{Q}$. Let T be the subring of $\text{End}_{\mathbb{Q}}(A_f)$ generated by the Hecke operators. Then A_f is simple, the abelian group $\text{End}_{\mathbb{Q}}(A_f)/T$ is finite, and $T \otimes \mathbb{Q}$ is naturally isomorphic to the quotient $T_{\mathbb{Q},N}/I_f$.*

Proof. – By [34, Corollary 4.2], A_f is simple with rational endomorphism algebra E isomorphic to the coefficient field of f, i.e. $\dim E = \dim T_{\mathbb{Q},N}/I_f$. But we have a natural morphism $T_{\mathbb{Q},N}/I_f \to T \otimes \mathbb{Q}$ which is injective, because f is a natural holomorphic differential form on A_f, and a Hecke operator acting trivially on A_f must thus vanish f. This morphism is also surjective, so that $\dim T \otimes \mathbb{Q} = \dim T_{\mathbb{Q},N}/I_f = \dim E$, and thus $E = T \otimes \mathbb{Q}$. This concludes because $\text{End}(A_f)$ is free of finite rank by [30, Theorem 12.5]. □

We want to be able to apply Corollary 2.17 to show that the θ morphism for $X_0^+(N)$ vanishes. To do that, we need a set of geometric points and a group of Cartier divisors with specific properties. They will be the *Heegner points* (and cusps) and *Hecke correspondances*, as detailed in the following subsection, which checks conditions 2 and 3. The two base points are the cusp point at infinity, which is defined over $\mathbb{Q}$.

2.3.2 Heegner points and Hecke correspondances

Let N and m be two integers, we have two maps $i_m^1, i_m^2 : X_0(mN) \to X_0(N)$, which are best expressed in terms of moduli spaces for the complex points (algebraic geometry arguments such as [25, Corollary 4.1.17] ensure that such maps, provided that they are, indeed, algebraic, which we admit here, can be extended to the whole curve). These two maps are given by $(E,C) \longmapsto (E,mC)$ and $(E,C) \longmapsto (E/NC, C/NC)$.

Let C_m be the image of $X_0(mN)$ under (i_m^2, i_m^1), and Δ_m be inverse image under the diagonal morphism: as i_m^1 is different from i_m^2, Δ_m is a divisor on $X_0(N)$.

Definition A *Heegner point* on $Y_0(N)$ corresponds to a pair (E, C) such that E and E/C have isomorphic orders of an imaginary quadratic field K with conductor prime to N as endomorphism rings.

Lemma 3.4 *Assume m is coprime to a prime integer N, and $m < N^2/4$, then the non-cuspidal complex points in the support of Δ_m correspond to Heegner points.*

Proof. – Let R be an order in a quadratic imaginary field. For any $\omega \in R$ such that $(1, \omega)$ generates R, we have a unique degree 2 vanishing polynomial for ω: $P_\omega = X^2 - a_\omega X + b_\omega$. Its negative discriminant $4b_\omega - a_\omega^2$ is positive and does not depend on ω. We call it the discriminant of R.

Let E be a complex elliptic curve with an endomorphism $\nu : E \to E$ with cyclic kernel of cardinality m. Thus ν is no multiple of identity, thus E has complex multiplication. Let $R = \mathbb{Z} \oplus \mathbb{Z}\omega$ be its ring of endomorphisms with discriminant D, with $\omega^2 - A\omega + B = 0$ and $A^2 - 4B < 0$, so that $\hat{\omega} = A - \omega$. Write $\nu = a\omega + b$, then $m = (a\omega + b)(a\hat{\omega} + b) = a^2\omega(A - \omega) + ab(\omega + (A - \omega)) + b^2 = a^2B + abA + b^2$, so that $4m = a^2(4B - A^2) + (b + 2aA)^2$. In particular, there are integers a, b such that $4m = Da^2 + b^2$.

Let P be a noncuspidal point in the support of Δ_m: P is some pair $(E, C) \in S_0(N)$ such that there is a pair $(E_1, C_1) \in S_0(mN)$ satisfying $(E, C) \cong (E_1, mC_1) \cong (E_1/NC_1, C_1/NC_1)$. Now, let $\mu_1 : E_1 \to E_1/NC_1$ be the isomorphism: we have an endomorphism $\nu_1 : E_1 \to E_1/NC_1 \overset{\mu_1^{-1}}{\to} E_1$ with cyclic kernel of order m, NC_1. So if R_1 is the endomorphism ring of E_1, with discriminant D_1, there are integers a_1, b_1 such that $4m = D_1a_1^2 + b_1^2$.

Now, we similarly have an isomorphism $\mu_2 : E_1/mC_1 \to E_1/C_1$, with kernel C_1/mC_1 cyclic of order m, and, as above, if R_2 is the ring of endomorphisms of E_1/mC_1 with discriminant D_2, then we have integers a_2, b_2 such that $4m = D_2a_2^2 + b_2^2$.

To conclude, we apply the next lemma to the elliptic curves E_1 and E_1/mC_1 to show that if $R_1 \neq R_2$, then some D_i is a multiple of N^2, which contradicts $4m < N^2$ (and by construction, R_1 is the ring of endomorphisms of E, R_2 that of E/C).

If the conductor of R_i is not coprime to N, then there is an algebraic integer $x \notin R_i$ such that $Nx \in R_i$. If $(1, u)$ is a basis of R_i, write $Nx = a + bu$ with a, b integers. If b is divisible by N, then, up to adding a multiple of u to x, we may assume $b = 0$. Then x is a rational algebraic integer, thus an integer and $x \in R_i$, a contradiction. Otherwise, let $X^2 - yX + z$ be the minimal polynomial of u, then the minimal polynomial of bu is $X^2 - byX + b^2z$, thus the minimal polynomial of $Nx = a + bu$ must be $X^2 - (by - 2a)X + (a^2 - bya + b^2z) = X^2 + CX + D$. So the minimal polynomial of x (with integral coefficients) must be $X^2 - \frac{by-2a}{N}X + \frac{a^2-bya+b^2z}{N^2}$. From computing the discriminant of this polynomial (which must be an integer), it follows that $N^2 | C^2 - 4D = b^2D_i$, so D_i is divisible by N^2 and we get as above a contradiction. □

Lemma 3.5 *Let E,E' be complex elliptic curves with rings of endomorphisms R and R', both with complex multiplication, and let $\pi : E \to E'$ be an isogeny with cyclic kernel of order a prime number N. Then R and R' are orders of the same quadratic imaginary field, and $\frac{D}{D'} \in N^{2\mathbb{Z}}$. If $D = D'$, then $R = R'$.*

Proof. – We have $\mathbb{Z}$-linear morphisms $\phi : R \to R'$, $\psi : R' \to R$, given respectively by $f \longmapsto \pi \circ f \circ \hat{\pi}$, $f \longmapsto \hat{\pi} \circ f \circ \pi$. It is easy to see that ϕ, ψ are injections, and $\phi \circ \psi = N^2$, $\phi \circ \psi = N^2$. Thus $\phi \otimes \frac{1}{N} : R \otimes \mathbb{Q} \to R' \otimes \mathbb{Q}$, $\psi \otimes \frac{1}{N} : R' \otimes \mathbb{Q} \to R \otimes \frac{1}{N}$ are inverse multiplicative isomorphisms, hence R and R' have the same fraction fields.

We know that $\det\phi \det\psi = N^4$, and $\phi(1) = N$, $\psi(1) = N$, so we may assume that (up to exchanging R and R') $\det\phi \in \{\pm N, \pm N^2\}$. Let $(1, u)$ be a basis of R, it is mapped by ϕ to $(N, u') \in R'^2$. Write $\begin{bmatrix} N \\ u' \end{bmatrix} = \begin{bmatrix} N & 0 \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ v \end{bmatrix}$, where $(1, v)$ is a basis of R'. Since $Nd = \det\phi$, $d \in \{\pm 1, \pm N\}$. Now, write $X^2 - aX + b$ the minimal polynomial of u: then an easy computation yields $u'^2 = \phi(Nu)$, so that $u'^2 = \phi(Nau - Nb) = Nau' - N^2b$, and u' has $N^2a^2 - 4N^2b = N^2D$ as discriminant of its minimal polynomial (we call it the discriminant of u' for short).

But the discriminant of $dv = u' - c$ is easily seen to be the same as that of u', thus the discriminant of v (which is D') is $\frac{N^2D}{d^2}$, which proves the second statement.

It remains to study the case $D = D'$, which implies $d = \pm N$ thus $\det\phi = \det\psi$. With the same notations as above, note that the minimal polynomial of $Nv = \pm(u' - c)$ is $(X + c)^2 - Na(X + c) + N^2b = X^2 - (Na - 2c)X + (c^2 - Nac + N^2b)$. Taking $X = Nv$ and reducing mod N, it follows that $\frac{c^2}{N}$ is an algebraic integer and a rational number, thus $N | c$. It follows that ϕ (and by symmetry, ψ) has exactly NR' (resp. NR') as its image, and thus the morphisms $\frac{\phi}{N} : R \to R'$ and $\frac{\psi}{N} : R' \to R$ are well-defined, additive and multiplicative, and they are inverse one of the other. So R and R' are isomorphic, so (they are orders in an imaginary quadratic number field) they are either equal or Galois conjugates. But in

quadratic number fields, orders are invariant under Galois (the conjugate y of an nonreal element x is uniquely defined by the property that $xy, x+y$ are real numbers, and if $x^2 = ax - b$ is the minimal polynomial, then $y = a - x$ works). □

The intrinsic interest of Heegner points is the following *explicit* Gross-Zagier formula, from [4, Theorem 1.1] that allows us to study their behavior through L-functions:

Theorem 3.6 *Let $f \in \mathcal{S}_2(\Gamma_0(N))$ be a positive newform – meaning that the sign of the functional equation is $\Lambda(f,s) = -\Lambda(f, 2-s)$. Let A_f the abelian variety associated with f that is consequently defined over $\mathbb{Q}$. Let K be a quadratic imaginary field extension of $\mathbb{Q}$, P a Heegner point of $X_0(N)$ with complex multiplication by an order $\mathcal{O}$ of K with ray class field H (see [32, Chapter 16] for elaboration on these properties). Let $P' = \sum_{\sigma \in \mathrm{Gal}(H/K)} [\sigma(P) - \deg_{\mathbb{Q}}([\sigma(P)])\infty] \in J_0(N)(K) \subset J_0(N)(H)$. If $L'(f,1) = 0$, the projection of P' into $A_f(K)$ is a torsion point.*

Proof. – By [4, Theorem 1.1], complex multiplication theory and height theory (for instance, [37, Theorem 4.3]), we know that P' is torsion in $A_f(K)$ as soon as $L'(f, 1_{\mathcal{O}}, 1) = 0$. Now, $L'(f, 1_{\mathcal{O}}, 1)$ is a multiple of $L'(f, 1_K, 1)$, but $L(f, 1_K, s) = L(f,s)L(f \otimes \chi_K, s)$. Because f is positive, $L(f,s)$ vanishes at $s=1$ with order 2, thus so does $L(f, 1_K, s)$. Therefore $L'(f, 1_K, 1) = 0$ and thus $L'(f, 1_{\mathcal{O}}, 1) = 0$, which concludes. □

Corollary 3.7 *Let $f \in \mathcal{S}_2(\Gamma_0(N))$ be a positive newform, let $D \in \mathrm{Div}^0(X_0(N))(\overline{\mathbb{Q}})$ be invariant under the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$ and supported on Heegner points and cusps. Assume $L'(f,1) = 0$. Then the image of D in $A_f(\overline{\mathbb{Q}})$ is actually in $A_f(\mathbb{Q})$ and is torsion.*

Proof. – Write $D = \alpha c_1 + \beta c_2 + \sum_{i=1}^d n_i P_i$ where P_i is a Heegner point of $X_0(N)$ corresponding to complex multiplication by an order $\mathcal{O}_i$ of a quadratic imaginary field extension $K_i/\mathbb{Q}$ with ray class field H_i (and $n_i \in \mathbb{Z}$), and the c_i are the two rational cusp points of $X_0(N)$. Let $L/\mathbb{Q}$ be a finite Galois extension containing all the H_i. Then a simple computation gives

$$S_i = \sum_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} [\sigma(P_i) - \deg_{\mathbb{Q}}(\sigma(P_i))\infty] = [L : H_i](P_i' + \sigma_i(P_i')) \in J_0(N)(\mathbb{Q}),$$

where P_i' is defined as in the previous theorem and σ_i is the unique nontrivial automorphism of K_i. It follows from the previous theorem that the projection of S_i in $A_f(\mathbb{Q})$ is torsion.

Now, $[L:\mathbb{Q}]D = \sum_{s \in \mathrm{Gal}(L/\mathbb{Q})} s(D) = \sum_{i=1}^d n_i S_i + [L:\mathbb{Q}] \sum_{i=1}^d n_i \deg_{\mathbb{Q}}(P_i)[\infty] + [L:\mathbb{Q}]\alpha c_1 + [L:\mathbb{Q}]\beta c_2$. Now $X_0(N)$ has two cusps, 0 and ∞, so they are exchanged by the Atkin-Lehner involution, therefore, in A_f, $[c_1 - c_2] = 0$. As D has degree zero, the second part of the sum projects to $[L:\mathbb{Q}](\alpha[c_1 - \infty] + \beta[c_2 - \infty])$ which is zero by the previous sentence. Thus D projects to a torsion point $\pi(D) \in A_f(\overline{\mathbb{Q}})$. But as D is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so is $\pi(D)$ thus $\pi(D) \in A_f(\mathbb{Q})$. □

2.3.3 Hecke correspondances and Jacobian endomorphisms

This paragraph aims at showing the fourth condition of Corollary 2.17.

Lemma 3.8 *If $m \geq 1$ is an integer and N is prime, with m and N coprime, then the complex divisor map induced by C_m is the coset operator $\Gamma_0(N) \begin{bmatrix} 1 & 0 \\ 0 & m \end{bmatrix} \Gamma_0(N)$.*

Proof. – The non-cuspidal complex points of $X_0(N)$ are the $\tau \bmod \Gamma_0(N)$ for $\tau \in \mathbb{H}$, τ corresponding to the elliptic curve $\mathbb{C}/(\tau\mathbb{Z} \oplus \mathbb{Z})$ with the cyclic subgroup generated by $1/N$. Thus, the set of noncuspidal points of $C_m(\mathbb{C})$ (with a transparent notation) is $\{(\tau \bmod \Gamma_0(N), \tau/m \bmod \Gamma_0(N)), \tau \in \mathbb{H}\}$. Not taking the ramification of the map $\mathbb{H} \to X_0(N)$ into account, the image by the divisor map of some $\Gamma_0(N)\tau$ is the sum of the set of $\Gamma_0(N)\tau'/m = \Gamma_0(N) \begin{bmatrix} 1 & 0 \\ 0 & m \end{bmatrix} \tau'$, where $\tau' \in \Gamma_0(N)\tau$. We get the exact definition of the coset operator. □

Corollary 3.9 *If l and N are coprime, the endomorphism T_l of $J_0(N)$ is a linear combination of the $\psi(C_m)$, for $l \geq m \geq 1$ coprime with N.*

Proof. – See the formulas in [10, Chapter 5.3]. □

Lemma 3.10 *Let A be an abelian variety over a field of characteristic zero, and u be an endomorphism of A such that for all global differentials ω on A, $u^*\omega = 0$. Then $u = 0$.*

Proof. – We can assume that the field is algebraically closed and the variety is simple. Then if u is nonzero, u is an isogeny. By [30, Section 8], there are integers $n > 0$, and an endomorphism v of A such that $n_A = v \circ u$. Thus, if ω is a nonzero global differential on A, $n\omega = n_A^*\omega = u^*(v^*\omega)$ is nonzero, hence a contradiction. □

Corollary 3.11 *If a $\mathbb{Z}$-linear combination of Hecke operators vanishes on $\mathcal{S}_2(\Gamma_0(N))$, it vanishes as a linear combination of endomorphisms of $J_0(N)$.*

Proof. – The space of holomorphic differential forms of $J_0(N)$ is the same as that of $X_0(N)$, and this one is exactly $\mathcal{S}_2(\Gamma_0(N))$ by Lemma 3.2. This space is a supspace of the space of global algebraic differential forms on $J_0(N)_{\mathbb{C}}$ and the action of the Hecke operators is, by construction, equivariant. □

Proposition 3.12 *If N is a prime number, then every element in the Hecke ring over $\mathbb{Z}$ for $\mathcal{S}_2(\Gamma_0(N))$ has a multiple which is a $\mathbb{Z}$-linear combination of the T_k, $1 \leq k \leq (N+1)/6$.*

Proof. – It is the bound from [41, Theorem 9.23], since $\Gamma_0(N)$ has index $N+1$ in $SL_2(\mathbb{Z})$. Indeed, the index of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$ is exactly the index of the subgroup of upper triangular matrices with determinant 1 of $\mathscr{M}_2(\mathbb{Z}/N\mathbb{Z})$ into $SL_2(\mathbb{Z}/N\mathbb{Z})$. The former group has cardinality $(N-1)N$ (the first row determines the matrix, the only constraint being that the first diagonal coefficient is nonzero); the second group has cardinality $(N^2-1)(N^2-N)/(N-1) = N(N^2-1)$. □

Corollary 3.13 *If N is prime, any endomorphism of $J_0(N)$ has a scalar multiple in the abelian group of endomorphisms generated by the Hecke operators T_l, $1 \leq l \leq (N+1)/6$. In particular, if F is the subgroup of Cartier divisors of $X_0(N) \times X_0(N)$ generated by the C_l, for $1 \leq l \leq (N+1)/6$, $\mathrm{End}(J_0(N))/\psi(F)$ is a torsion group.*

Proof. – It is standard (see for instance [33, Corollary 3.3]) that for N prime, the endomorphism algebra of $J_0(N)$ is generated (as a $\mathbb{Q}$-algebra) by the Hecke operators. Then we apply Proposition 3.12 and Corollary 3.11. □

2.3.4 Vanishing of the θ morphism for $X_0^+(N)$.

In this paragraph, we apply the results proved in the previous section to show that with respect to a specific decomposition of the Jacobian of $X_0(N)^+$, the θ morphism vanishes. First, we define this curve and give some of its properties.

Lemma 3.14 *We recall that the Atkin-Lehner involution on $X_0(N)$ is the extension of the quotient of the $\Gamma_0(N)$-equivariant map $\tau \longmapsto \frac{-1}{N\tau}$ from $Y_0(N)$ to itself. In terms of moduli spaces, it corresponds to the map $(E, C) \longmapsto (E/C, E[N]/C)$. It is an involution defined over $\mathbb{Q}$. The quotient of $X_0(N)$ under this involution is denoted as $X_0^+(N)$.*

Proof. – From [10, Chapter 7.7], the function field of $X_0(N)$ over $\mathbb{Q}$ is $\mathbb{Q}(j, j_N)$ where $j_N(\tau) = j(N\tau)$ and j is the usual modular invariant. It is easy to see that $\tau \longmapsto \frac{-1}{N\tau}$ exchanges j and j_N, so that application is defined over $\mathbb{Q}$. □

Lemma 3.15 *The Atkin-Lehner involution exchanges the two cusps of $X_0(N)$, which are rational, so that $X_0^+(N)$ has a single cusp, defined over $\mathbb{Q}$.*

Proof. – First recall from e.g. [10, Chapter 3.8] that $X_0(N)$ has two cusps defined over $\mathbb{C}$, the point at ∞ and the point at 0. Let us now show that the Atkin-Lehner involution, as a complex-analytic function, exchanges the two cusps. Let $\tau \in \mathbb{H}$ have imaginary part $t \geq 2$. Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$ be any matrix, so that $d \neq 0$: then $M \cdot \frac{1}{-N\tau} = \frac{a - bN\tau}{c - dN\tau}$ has imaginary part $\frac{Nt}{|c-dN\tau|^2} \leq \frac{Nt}{N^2t^2} = \frac{1}{Nt} < 2$. Thus the image of $\frac{-1}{N\tau}$ in $X_0(N)$ remains away from infinity. Thus the cusp at infinity is not a fixed point of the Atkin-Lehner involution. As this map preserves $Y_0(N)$, the image of infinity must be the other cusp.

Now we show that the cusps must be defined over $\mathbb{Q}$. Consider the rational function $k = j_N/j^N$ defined on $X_0(N)$ over $\mathbb{Q}$. As τ goes to infinity, $k(\tau) \sim e^{-2i\pi N\tau}(e^{2i\pi\tau})^N = 1$ using the usual q-expansion of j. However, as τ goes to infinity, $k(-1/\tau) = j(\tau/N)/j(\tau)^N \sim e^{-2i\pi\tau/N}(e^{2i\pi\tau})^N \to 0$. So scheme-theoretically, the rational cusps (we call i the cusp at infinity and c the other one) are distinct closed points of the rational curve $X_0(N)$. No point in $i(\mathbb{C})$ or $c(\mathbb{C})$ can be in $Y_0(N)$, because the rational function $1/j$ would be vanishing at these points and it doesn't vanish on $Y_0(N)$. As $i(\mathbb{C})$ and $c(\mathbb{C})$ are

$$\begin{array}{ccc} \mathrm{Pic}(J_0(N)) & \xrightarrow{\tilde{A}J_{b_0}} & \mathrm{Pic}(X_0(N)) \\ {\scriptstyle (q_J)^*}\uparrow & & \uparrow{\scriptstyle q^*} \\ \mathrm{Pic}(J_0(N)^+) & \xrightarrow{\tilde{A}J_b} & \mathrm{Pic}(X_0(N)^+) \end{array}$$

(a) Twisted Abel-Jacobi maps and the Atkin-Lehner involution

$$\begin{array}{ccc} G(J_0(N)) & \xrightarrow{\tilde{A}J_{b_0}} & J_0(N)(\mathbb{Q}) \\ {\scriptstyle (q_J)^*}\uparrow & & \uparrow{\scriptstyle q^*} \\ G(J_0(N)^+) & \xrightarrow{\tilde{A}J_b} & J_0(N)^+(\mathbb{Q}) \end{array}$$

(b) Partial θ morphism and the Atkin-Lehner involution

clearly nonempty, disjoint, and contained in $X_0(N)(\mathbb{C})\backslash Y_0(N)(\mathbb{C})$ which has two elements, it follows that $i(\mathbb{C})$ and $c(\mathbb{C})$ have one element.

If K is a number field, $(\mathrm{Spec}\, K)(\mathbb{C})$ is the set of morphisms $K \to \mathbb{C}$ and always has dimension $[K : \mathbb{Q}]$. So the residue fields of c and i have dimension 1 over $\mathbb{Q}$, i.e. i and c are rational. □

Lemma 3.16 *Take b the cusp at infinity of $X_0(N)$. Let f be a positive newform of weight 2 and level N such that $L'(f,1) = 0$. Then the morphism $\theta_b \otimes \mathbb{Q}$ associated to the map $J_0(N) \to J_0(N) \times A_f$ is zero.*

Proof. – Apply the first vanishing criterion, i.e. Proposition 2.9, with S being the set of Heegner points and cusps, F being the subgroup generated by the Hecke correspondances. The conditions of the criterion are satisfied according to Corollary 3.7, Lemma 3.4, and Corollary 3.13. (and notice that the Hecke correspondances always associate only cusps to cusps). □

Proposition 3.17 *Let b be the cusp of $X_0(N)^+$ and f be a positive newform of weight 2 and level N such that $L'(f,1) = 0$. Then the morphism $\theta_b \otimes \mathbb{Q}$ associated to the map $J_0(N)^+ \to J_0(N)^+ \times A_f$ is zero, where $J_0(N)^+$ is the Jacobian of $J_0(N)$.*

Proof. – Let $q : X_0(N) \to X_0(N)^+$ be the quotient map, $q_J : J_0(N) \to J_0(N)^+$ the associated morphism of Jacobians, and $b_0 \in X_0(N)(\mathbb{Q})$ be the cusp at infinity. The diagram of Figure 5a commutes, thus so does the diagram from Figure 5b (where the notation G is defined in Section 2.2).

However, as f is positive, the projection $J_0(N) \to A_f$ factors through $q_J : J_0(N) \to J_0^+(N)$ (as f is invariant under the Atkin-Lehner involution, so is A_f, and $q_J : J_0(N) \to J_0^+(N)$ is the quotient under said involution), and the map $J_0(N)^+ \to A_f$ used above is the map involved in the construction of the θ morphism above. If $\mathscr{L} \in G(J_0(N)^+$, then $2\tilde{A}J_b(\mathscr{L}) = q_J q^* \tilde{A}J_b(\mathscr{L}) = q_J(\tilde{A}J_{b_0}((q_J)^*\mathscr{L}))$. Thus $2\theta_b(\mathscr{L}) = \theta_{b_0}((q_J)^*\mathscr{L})$. By the above lemma, $\theta_b \otimes \mathbb{Q} = 0$. □

We have essentially proven the third bullet of the following statement, which is essentially the first case of [13, Proposition 1.8], one of the main ingredients of the proof. Let us note that, according to the authors of [13], the first two bullets follow from standard theory about simple abelian varieties and modular forms (for instance, the first point is mostly done in [10, Chapter 6.6]).

Theorem 3.18 *Let $X = X_0^+(N)$ and b be the image of the point at infinity. Let J be the Jacobian of the curve, let A, B be the product of the abelian varieties A_f over the Galois conjugation classes of the positive newforms f of $S_2(\Gamma_0(N))$ such that $L'(f,1) \neq 0$ and $L'(f,1) = 0$ respectively. Then:*

1. *$(\pi_A, \pi_B) : J \to A \times B$ is an isogeny.*
2. *$Hom(A, B) = 0$*
3. *The θ morphism defined above is zero.*

Proof. – The first two points follow (at least in part) from [10, Chapter 6.6], standard theory about simple abelian varieties, and the fact that the A_f are simple and pairwise non-isogenous. The third point comes from the proposition above (θ is the "product" of the $\theta_b \otimes \mathbb{Q}$ morphism for all the A_f appearing in B, composed with $G(A) \to G(J)$). □

2.4 Case of the non-split Cartan modular curve

Here, we reproduce the reasoning of Sections 2.3 and 2.2 to prove the equivalent of Theorem 3.18 another modular curve, the nonsplit Cartan curve, which we now define. The process is similar: we define

Hecke correspondances and Heegner points, show that (up to a scalar multiple torsion) enough Hecke correspondances generate the endomorphism ring of the Jacobian, that these are supported on Heegner points, and that such Heegner points are torsion in a suitable isogeny factor of the Jacobian.

Here, N is a prime number, and $\epsilon \in \mathbb{Z}$ is a non-square mod N.

2.4.1 Definitions

Definition The non-split Cartan group of level N is the group $\Gamma_{ns}(N) = \{A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}),\ a = d \bmod N,\ c = b\epsilon \bmod N\}$.

The normalized non-split Cartan group of level N is the group $\Gamma^+_{ns}(N) = \{A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}),\ \exists s \in \{\pm 1\}, a = ds \bmod N,\ c = b\epsilon s \bmod N\}$.

Both of these groups are congruence subgroups; the former is normal in the latter. The quotients of the extended Poincaré plane under these groups are the modular curves $X_{ns}(N)$ and $X^+_{ns}(N)$. The set of non-cuspidal points of these curves are denoted $Y_{ns}(N)$ and $Y^+_{ns}(N)$.

Both of these curves can be realized algebraically as smooth projective curves over $\mathbb{Q}$.

Proof. – Just note that $\Gamma(N) \subset \Gamma_{ns}(N) \subset \Gamma^+_{ns}(N) \subset SL_2(\mathbb{Z})$. For the normality, it is enough to note that in the notations, the application mapping a matrix of $\Gamma^+_{ns}(N)$ to the corresponding s is a group homomorphism with kernel $\Gamma_{ns}(N)$. Thus $\Gamma_{ns}(N)$ is a subgroup of $\Gamma^+_{ns}(N)$ with index 2, hence normal. □

Again, we have a moduli space interpretation of $Y_{ns}(N)$.

Lemma 4.1 *Consider a morphism $\tau \longmapsto \mu(\tau) = (E_\tau, \phi_{\epsilon,\tau})$, where $\tau \in \mathbb{H}$, $E_\tau = \mathbb{C}/\Lambda_\tau$, $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$), and $\phi_{\epsilon,\tau}$ is the endomorphism of $(\Lambda_\tau/N)/\Lambda_\tau = E_\tau[N]$ with square ϵ mapping τ/N to $1/N$ and $1/N$ to $\epsilon\tau/N$.*

Then, for $\tau, \tau' \in \mathbb{H}$, there is an isomorphism $\psi : E_\tau \to E_{\tau'}$ mapping $\phi_{\epsilon,\tau}$ to $\phi_{\epsilon,\tau'}$ iff $\tau' \in \Gamma_{ns}(N)\tau$. If these conditions do not hold, $\tau' \in \Gamma_{ns}(N)\tau$ iff there is an isomorphism $E_\tau \to E_{\tau'}$ mapping $\phi_{\epsilon,\tau}$ to $-\phi_{\epsilon,\tau'}$.

If E is a complex elliptic curve with a morphism $\phi : E[N] \to E[N]$ with square ϵ, there exists a $\tau \in \mathbb{H}$ and an isomorphism $(E, \phi) \to (E_\tau, \phi_{\epsilon,\tau})$.

In particular, $Y_{ns}(N)$ represents the isomorphism classes of pairs (E, u), where E is a complex elliptic curve and u is an endomorphism of $E[N]$ with square ϵ (and u need not come from an endomorphism of E).

Proof. – Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ be a matrix such that $\tau' = M \cdot \tau$. Then $\Lambda_\tau = (c\tau + d)\Lambda_{\tau'}$, so division by $c\tau + d$ is an isomorphism $\psi : E_\tau \to E_{\tau'}$. Moreover, ψ maps $1/N$ to $1/(N(c\tau+d)) = (a - c\tau')/N$ and τ/N to $(d\tau' - b)/N$. So the image ϕ' of $\phi_{\epsilon,\tau}$ as an endomorphism of $E_{\tau'}[N]$ maps $(a - c\tau')/N$ to $\epsilon(d\tau' - b)/N$ and $(d\tau' - b)/N$ to $(a - c\tau')/N$. Thus, this endomorphism maps $[1/N] = d[(a - c\tau')/N] + c[(d\tau' - b)/N]$ to $d\epsilon[(d\tau' - b)/N] + c[(a - c\tau')/N] = (-db\epsilon + ac)[1/N] + (d^2\epsilon - c^2)[\tau'/N]$, and $[\tau'/N] = a[(d\tau' - b)/N] + b[(a - c\tau')/N]$ to $(a^2 - b^2\epsilon)[1/N] + (bd\epsilon - ac)[\tau'/N]$.

So $\phi' = \phi_{\epsilon,\tau}$ iff $a^2 - b^2\epsilon = 1 \bmod N$, $bd\epsilon = ac \bmod N$, $d^2\epsilon - c^2 = \epsilon \bmod N$. Write $c' = c\epsilon_1$ where ϵ_1 is the multiplicative inverse of ϵ mod N, so that the condition is equivalent to $a^2 - b^2\epsilon = d^2 - c'^2\epsilon = ad - \epsilon bc' \bmod N = 1$ and $ac' = bd \bmod N$. Let F be the field $\mathbb{F}_N[\sqrt{\epsilon}]$, let $u_\pm = a - b\sqrt{\epsilon}$, $v_\pm = d - c\sqrt{\epsilon}$, then the condition is equivalent to $u_-u_+ = v_-v_+ = u_-v_+$, which is equivalent to $u_- = v_-$ and thus to $M \in \Gamma_{ns}(N)$.

Similarly, $\phi' = -\phi_{\epsilon,\tau}$ iff $M \in \Gamma^+_{ns}(N) \backslash \Gamma_{ns}(N)$.

Finally, we show that for any E_τ and any endomorphism u of $E_\tau[N]$ with square ϵ, there exists an isomorphism $E_\tau \cong E_{\tau'}$ mapping u to $\phi_{\epsilon,\tau}$ such that $u = \phi_{\epsilon,\tau'}$. To do that, we first show that there exists $x_0 \in E_\tau[N]$ such that $Q(x_0) = \det(x_0, u(x_0)) = 1$ (in the basis $[1/N], [\tau/N]$). Indeed, given any nonzero x, $\det(x, u(x)) \in \mathbb{F}_N^\times$; if it is a square, a scalar multiple of x works. If not, let $\alpha \in \mathbb{F}_N$, then $Q(\alpha x + u(x)) = (\alpha^2 - \epsilon)Q(x)$. If neither x nor any $\alpha x + u(x)$ work, then $Q(x)$ is not a square and neither are all the $\alpha^2 - \epsilon$. Thus, if β is a square, so is $\beta - \epsilon$, and we get a contradiction.

So take $x_0 = a[1/N] + b[\tau/N]$ such that $u(x_0) = c[1/N] + d[\tau/N]$ and $Q(x_0) = ad - bc = 1 \bmod N$. We can choose the integers a, b, c, d such that $ad - bc = 1$. Consider now $\tau' = \frac{a\tau + b}{c\tau + d}$, and the isomorphism $E_{\tau'} \to E_\tau$ given by multiplication by $c\tau + d$. □

2.4.2 Hecke correspondances and Heegner points

Now, we define Hecke correspondances on the curves $X_{ns}(N)$: by Section 2.2 they define endomorphisms of the Jacobians.

Definition Let m be an integer coprime with N, let $X_{ns}(N,m) = X_{ns}(N) \times_{X(1)} X_0(m)$ (it is a disjoint reunion of finitely many Riemann surfaces, and is a compactified moduli space for the triples (E,u,C), (E,u) corresponding to the classes of $Y_{ns}(N)$, and C is a cyclic subgroup of E of order m). We define two maps $i_1^m, i_2^m : X_{ns}(N,m) \to X_{ns}(N)$, the first one being the projection, and the second one is (as a moduli space problem) $(E,u,C) \longmapsto (E/C, \pi_C \circ u \circ \pi_C^{-1})$, where $\pi_C : E \to E/C$ is the projection, and is an isomorphism on the N-torsion points.

The Hecke correspondance C_m is the image of the map (i_m^1, i_m^2).

Proposition 4.2 *The curves $X_{ns}(N)$ and $X_{ns}^+(N)$ can be defined over $\mathbb{Q}$. The Hecke correspondances from above arise from algebraic, rational correspondances.*

The following Chen-Edixhoven theorem (from [6, 8]) gives us information on the Jacobian of these nonsplit Cartan curves, linking them to the corresponding $X_0(N^2)$ curves.

Theorem 4.3 *The new part of the Jacobian of $X_0(N^2)$ (resp. of $X_0^+(N^2)$) is isogenous to the Jacobian of $X_{ns}(N)$ (resp. of $X_{ns}^+(N)$), and the isogenies are Hecke equivariant.*

In particular, we have isomorphisms of Hecke modules $\mathcal{S}_2(\Gamma_{ns}(N)) \cong \mathcal{S}_2(\Gamma_0(N^2))^{\text{new}}$ and $\mathcal{S}_2(\Gamma_{ns}(N)^+) \cong \mathcal{S}_2(\Gamma_0(N^2))^{+,\text{new}}$.

Now, as in Section 2.3, we introduce a class of geometric points on $X_{ns}(N)$ that (as we will see later) behave well with respect to the Hecke correspondances.

Definition A (Kohen-Pacetti) Heegner point on $Y_{ns}(N)$ is a pair (E,u) such that E has complex multiplication by an order $\mathcal{O}_c$ of a quadratic imaginary extension K of $\mathbb{Q}$, with $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ and u comes from an endomorphism of E, where K is inert at N and c and N are coprime.

Lemma 4.4 *If $m \leq N^2/4$ is coprime with N, the complex points of $\Delta^{-1}(C_m)$ (a Cartier divisor of $X_{ns}(N)$) are Heegner points or cusps.*

Proof. – A complex non-cusp point of $\Delta^{-1}(C_m)$ is a pair (E,u) such that E has a cyclic subgroup C of order m, such that (E,u) and $(E/C, \pi_C \circ u\pi_C^{-1})$ are isomorphic: let ψ be this isomorphism. Let thus $\alpha = \psi^{-1} \circ \pi_C$: α is an endomorphism of E with cyclic kernel C, so E has complex multiplication, and α commutes with u. Let β be an endomorphism of E such that (id, β) is a basis of the ring of endomorphisms of E. Up to substracting a multiple of id to β, we may assume that $\beta + \beta^* in \{0, \mathrm{id}\}$.

Assume $\alpha = k + Nr\beta$, with k, r integers. Then the norm of α is $m = k^2 + kNr(\beta+\beta^*) + N^2r^2 \deg\beta$. Now, $k^2 + kNr(\beta+\beta^*) + (Nr)^2/4 \geq 0$, so $N^2 \geq 4m \geq N^2r^2(4\deg\beta - 1)$, which implies $r = 0$ and α scalar, a contradiction.

Assume that α acts as a scalar on $E[N]$. We want to show that α is of the form above. We may assume that α is zero on $E[N]$ and we want to show that α is N times an endomorphism of E. Write $E = \mathbb{C}/\Lambda$, then α is the multiplication by a scalar λ that preserves Λ, and $\lambda\Lambda/N \subset \Lambda$, thus λ/N preserves Λ so defines a complex endomorphism of E, and we are done.

As α commutes with u on $E[N]$ and that none are scalars, and since $u^2 = \epsilon$, then $u = a + b\alpha$ for some integers a, b with b and N coprime, so that u comes from an endomorphism of E.

If the order $\mathcal{O}_c$ satisfies $N|c$, then as α is not a scalar, we can write $\alpha = k + Na$, where k, a are algebraic integers, such that $r = a + \overline{a}$ is either 0 or 1. Taking norms, it follows $N^2 \geq 4m \geq (4k^2 + 4rNk + N^2) + 3N^2$ and we get a contradiction as $|r| \leq 1$. □

Now, we show that the Hecke correspondances we consider are enough to generate enough of the ring of endomorphisms of $J_{ns}(N)^+$ to be able to use Corollary 2.17.

Lemma 4.5 *Let $f \in \mathcal{S}_2(\Gamma_0(p^2))$, then $T_p(f)$ is invariant under $\Gamma_0(p)$, where p is a prime number.*

Proof. – Let $M = \begin{bmatrix} a & b \\ pc & d \end{bmatrix} \in \Gamma_0(p^2)$. For each $i \in \mathbb{Z}$, we denote $j_i = bd + id^2$, so that $i \longmapsto j_i$ is a bijection from $\mathbb{Z}/p\mathbb{Z}$ to itself. Let j_i' be the remainder of j_i mod p, and $j_i = q_j p + j_i'$. Thus, we have a bijection $i \in [\![0; p-1]\!] \longmapsto j_i' \in [\![0; p-1]\!]$. The conclusion then follows from the identity

$$\begin{bmatrix} 1 & i \\ 0 & p \end{bmatrix} M = \begin{bmatrix} a + ipc & -bc(b+id) - ij_ic \\ p^2c & d - pcj_i \end{bmatrix} \begin{bmatrix} 1 & j_i \\ 0 & p \end{bmatrix},$$

as the right hand side is in $\Gamma_0(p^2)\begin{bmatrix}1 & q_j\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & j_i'\\ 0 & p\end{bmatrix} = \Gamma_0(p^2)\begin{bmatrix}1 & j_i'\\ 0 & p\end{bmatrix}$. □

Lemma 4.6 *Let N be an odd prime number. Then the Hecke algebra over $\mathbb{Z}$ acting on $J_0(N^2)^{new}$ is generated as an abelian group by the Hecke operators T_l, for $1 \leq l \leq N^2/4$ with l and N coprime.*

Proof. – Note that the complex-analytic global differentials on $J_0(N^2)^{\text{new}}$ are naturally identified to $\mathcal{S}_2(\Gamma_0(N^2))^{\text{new}}$. Arguing as in the proof of Corollary 3.11, we first show the claim for operators acting on $\mathcal{S}_2(\Gamma_0(N^2))$, without requiring the condition l coprime with N.

We can apply the Sturm bound from [41, Theorem 9.23], as the index of $\Gamma_0(N^2)$ in $SL_2(\mathbb{Z})$ is $\frac{[SL_2(\mathbb{Z}):\Gamma(N^2)]}{[\Gamma_0(N^2):\Gamma(N^2)]} = \frac{|SL_2(\mathbb{Z}/N^2\mathbb{Z})|}{N^2\varphi(N^2)}$. Now, given $a, b \in \mathbb{Z}/N^2\mathbb{Z}$, there exists $c, d \in \mathbb{Z}/N^2\mathbb{Z}$ with $ad - bc = 1$ iff N does not divide both a and b, a situation that happens for all but N^2 pairs, i.e. for $N^4 - N^2$ pairs. For each couple (a, b) such that N does not divide both a and b, $(c, d) \longmapsto ad - bc$ is an onto group homomorphism $(\mathbb{Z}/N^2\mathbb{Z})^2 \to \mathbb{Z}/N^2\mathbb{Z}$ so the inverse image of 1 has cardinality N^2. Thus $|SL_2(\mathbb{Z}/N^2\mathbb{Z})| = N^2(N^4 - N^2) = N^4(N-1)(N+1)$, so that $[SL_2(\mathbb{Z}) : \Gamma_0(N^2)] = N(N+1)$, and the Sturm bound is thus $\frac{N(N+1)}{6} \leq \frac{N^2}{4}$.

To conclude, we show that if $1 \leq l \leq N^2/4$ is not coprime with N, then T_l vanishes on $\mathcal{S}_2(\Gamma_0(N^2))^{\text{new}}$. Indeed, we can write $T_l = AT_N$ for some operator A, so it is enough to show it in the case $l = N$. If f is a newform, $T_N f$ is a multiple of f in $\mathcal{S}_2(\Gamma_0(N))$, so f and $T_N f = a_N(f)f$ are orthogonal, thus $T_N f = 0$. □

Lemma 4.7 *The quotient of* $\text{End}(J_0(N^2)^{new})$ *by the Hecke algebra is a torsion abelian group.*

Proof. – $J_0(N^2)^{\text{new}}$ is isogeneous to a product of A_f (which are simple and pairwise non-homogenous) over the Galois equivalence classes of newforms for $\Gamma_0(N^2)$. The endomorphism algebra of A_f is the quotient of the Hecke algebra $T_{\mathbb{Q}}$ by I_f, the ideal of operators T that vanish at f (by Proposition 3.3). It follows from usual facts about abelian varieties that $\text{End}(J_0(N^2)^{\text{new}}) \otimes \mathbb{Q} = \prod_f T_{\mathbb{Q}}/I_f$. To conclude, we need to show that $T_{\mathbb{Q}} \to \prod_f T_{\mathbb{Q}}/I_f$ is onto. To do that, it is enough to show that the I_f are pairwise distinct maximal ideals of $T_{\mathbb{Q}}$. Indeed, let f be a newform for $\Gamma_0(N^2)$. Then I_f is the kernel of the ring surjective homomorphism $T \in T_{\mathbb{Q}} \longmapsto a_1(Tf) = \frac{Tf}{f} \in K_f$ (we follow the notations of [10, Chapter 6.5]) where K_f is the number field generated by the coefficients of f. So each I_f is a maximal ideal.

Let f be a newform. We have a surjective morphism $e_{f,\mathbb{Q}} : T \in T_{\mathbb{Q}} \longmapsto Tf/f = A_1(Tf) \in K_f$, with kernel I_f.Thus if f and g are newforms with $I_f = I_g$, then $K_f = K_g$ and therefore $e_{g,\mathbb{Q}} \circ e_{f,\mathbb{Q}}^{-1}$ is a $\mathbb{Q}$-automorphism of K_f and is thus a σ in the absolute Galois group of $\mathbb{Q}$. Thus $\sigma(a_n(f)) = \sigma(a_1(Tf)) = \sigma(e_{f,\mathbb{Q}}(T_n)) = e_{g,\mathbb{Q}}(T_n) = a_n(g)$ so f and g are Galois conjugates. □

Corollary 4.8 *The quotient of* $\text{End}(J_0(N^2)^{+,new})$ *by the subgroup generated by the Hecke operators T_l, for $1 \leq l \leq N^2/4$ with l and N coprime, is a torsion abelian group.*

Proof. – It follows from the two previous lemmas, the fact that the Atkin-Lehner involution (defined in Section 2.3 commutes with the Hecke operators. □

Corollary 4.9 *If F is the subgroup of Cartier divisors on $X_{ns}(N)^+ \times X_{ns}(N)^+$ generated by the Hecke correspondances C_m for $1 \leq m \leq N^2/4$ and m and N coprime,* $\text{J}_{\text{ns}}(\text{N})^+/\psi(F)$ *is a torsion group.*

Proof. – It follows from the previous result and the Hecke-equivariant isogeny $i : J_0(N^2)^{+,\text{new}} \to J_{ns}(N)^+$ (so there is a $j : J_{ns}(N)^+ \to J_0(N^2)^{+,\text{new}}$ with $j \circ i = (\deg i)_{J_0(N^2)^{+,\text{new}}}$, $i \circ j = \deg i_{J_{ns}(N)^+}$). Indeed, the Hecke correspondance C_m induces, on almost every complex point (minus cusps, ramification, and possible identity of the different terms) the "geometric" Hecke operator $\mathscr{T}_m^\epsilon$ from [24, Section 1.3], so they are equal over $\mathbb{C}$ thus over $\mathbb{Q}$, and the corresponding operator on the other side is T_m (where $1 \leq m \leq N^2/4$ and m and N are coprime).

So, let u be an endomorphism of $J_{ns}(N)^+$. Then $v = j \circ u \circ i$ is an endomorphism of $J_0(N^2)^{+,\text{new}}$ so for some $d \geq 1$, dv is a $\mathbb{Z}$-linear combination of the T_m, $1 \leq m \leq N^2/4$ with m and N coprime. But $i \circ dv \circ j = (d(\deg i)^2)_{J_{ns}(N)^+} \circ u$, and, for each m coprime with N, $i \circ T_m \circ j$ is $\mathscr{T}_m^\epsilon \circ i \circ j$ so is a multiple of the corresponding Hecke operator on $J_{ns}(N)^+$. As a consequence, a scalar multiple of u is a $\mathbb{Z}$-linear combination of Hecke operators with subscripts $1 \leq m \leq N^2/4$ such that m and N are coprime. □

2.4.3 Gross-Zagier theorem for $X_{ns}^+(N)$

To be able to show that the θ morphism vanishes for $X_{ns}(N)^+$, we want to apply the criterion from Corollary 2.17 with the Heegner points and cusps as set of geometric points and Hecke correspondances as the set of good Cartier divisors. To apply the criterion, we need to prove that rational divisors with

null degree and geometric support on cusps and Heegner points project to torsion points in the second isogeny factor of the Jacobian. As in Section 2.3, we use a formula akin to Gross-Zagier, shown by Zhang in [44] to show that components of such divisors have null height. The added difficulty is that the formalism the formula is proved in differs from ours.

Until explicitly said otherwise, $f \in \mathcal{S}_2(\Gamma_0(N^2))^+$ is a newform with $L'(f,1) = 0$ with N an odd prime number. We choose a positive integer c coprime to N and a quadratic imaginary extension K of $\mathbb{Q}$ inert at N, a basis $(1,\omega)$ of $\mathcal{O}_K$ such that ω has positive imaginary part, and we define $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$. We write $\omega^2 = r\omega - \nu$ for integers r, ν with $r \in \{0,1\}$. $\mathbb{A}_f$ is the ring of adeles of $\mathbb{Q}$ for the finite places of $\mathbb{Q}$ (ie the ring of families $(x_p)_{p\in\mathbb{P}}$ where $x_p \in \mathbb{Q}_p$ for each p and $x_p \in \mathbb{Z}_p$ for every prime p but finitely many).

The choice of the basis $(1,\omega)$ defines an embedding $K \to \mathscr{M}_2(\mathbb{Q})$ and, hence, a subring $R_c = \mathcal{O}_c + N\mathscr{M}_2(\mathbb{Z}) \subset \mathscr{M}_2(\mathbb{Z})$.

Definition The subgroup $U_c \subset GL_2(\mathbb{A}_f)$ is the set of families of $(M_p)_{p\in\mathbb{P}}$ such that if $p \neq N$, $M_p \in GL_2(\mathbb{Z}_p)$, and $M_N \in GL_2(\mathbb{Z}_N) \cap (R_c \otimes \mathbb{Z}_N)$. The corresponding complex Shimura variety is $M_{U_c}(\mathbb{C}) = GL_2(\mathbb{Q})^+ \backslash (\mathbb{H} \times GL_2(\mathbb{A}_f))/U_c$, where U_c acts on the right component only by right multiplication, and $GL_2(\mathbb{Q})^+$ acts on both components by left multiplication.

Lemma 4.10

1. *$GL_2(\mathbb{Q})^+ \cdot U_c = GL_2(\mathbb{A}_f)$.*
2. *There are $a, b \in \mathbb{Z}$ with $b \in \mathbb{Z}_N^\times$ such that $(a+b\omega)^2 = \epsilon \bmod N$.*
3. *Write $T = a + b\omega \in \mathbb{M}_2(\mathbb{Z})$: there is $P_\omega \in SL_2(\mathbb{Z})$ such that $P_\omega T P_\omega^{-1} = \begin{bmatrix} 0 & 1 \\ \epsilon & 0 \end{bmatrix} \bmod N := T_0$.*
4. *If P' is another matrix satisfying the conditions of the claim above (for the role of P_ω), then $P' = N_1 P_\omega$ with $N_1 \in \Gamma_{ns}(N)$, and $P_\omega = P' N_2$ with $N_2 \bmod N$ being in the image mod N of the embedding of $\mathcal{O}_c$. The converse statements also hold.*
5. *$GL_2(\mathbb{Q})^+ \cap U_c \supset \Gamma(N)$ and the quotient is $SL_2(\mathbb{Z}/N\mathbb{Z}) \cap P_\omega^{-1} C P_\omega$, where $C = \{M \in \mathscr{M}_2(\mathbb{Z}/N\mathbb{Z}),\ M_{1,1} = M_{2,2}, M_{2,1} = \epsilon M_{1,2}\}$.*
6. *The map $[(\tau, I_2)] \longmapsto [P_\omega(\tau)]$ defines an isomorphism $M_{U_c}(\mathbb{C}) \to Y_{ns}(N)$, not depending on the choice of P_ω.*
7. *Through this isomorphism, the coset of a pair $[(\tau, I_2)]$ represents the pair $(\mathbb{C}/(\mathbb{Z}\tau \oplus \mathbb{Z}), u)$ from the moduli problem of Lemma 4.1, where u is the endomorphism of $E_\tau[N]$ given in the basis $(1/N, \tau/N)$ by the matrix $T = \begin{bmatrix} a & -b\nu \\ b & a + br \end{bmatrix}$.*

Proof. –

1. Clearly the left hand side is a subset of the right hand side. For the reverse inclusion, we first replace U_c with the product of the $GL_2(\mathbb{Z}_v)$. Clearly, using diagonal matrices, it is enough to consider the case when all the entries are (p-adic) integers. As all but finitely many of the matrices are in $GL_2(\mathbb{Z}_v)$ for the relevant v, by iterating, it is enough to show the following: given a prime number p, a p-adic 2×2 matrix M with nonzero, noninvertible determinant, there exists a rational matrix N with entries in $\mathbb{Z}[p^{-1}]$ and determinant p^{-1} such that NM still has p-adic integral entries.

   Indeed, we can write, as $\mathbb{Z}_p$ is a PID, $M = M_l D M_r$ with $M_l, M_r \in GL_2(\mathbb{Z}_p)$, D diagonal, $D_{1,1} | D_{2,2}$ and $\det M_l = 1$. Take then $N = \mathrm{diag}(1, p^{-1}) N_l$ where N_l is a matrix with integral coefficients and determinant 1 congruent to $M_l^{-1} \bmod p$.

   To conclude, we want to show that any matrix $M \in GL_2(\mathbb{Z}_N)$ can be written as QS, where $Q \in SL_2(\mathbb{Z})$ and S being congruent mod N to a matrix of $\mathscr{O}_c$. It is elementary to show that there is a matrix $S_1 \in \mathcal{O}_c$ such that $\det S_1 = (\det M) \bmod N$, so that $S_1 \in GL_2(\mathbb{Z}_N)$; indeed, for $S_1 \in \mathcal{O}_c$, $(\det S_1) \bmod N$ is the norm of $[S_1] \in \mathcal{O}_c/(N) = \mathcal{O}_K/(N) = \mathbb{F}_{N^2}$ over $\mathbb{F}_N$, which is surjective (indeed, it is $s \longmapsto s^{N+1}$ which is onto as $\mathbb{F}_{N^2}^\times$ is cyclic and $|\mathbb{F}_N^\times| = \frac{|\mathbb{F}_{N^2}^\times|}{N+1}$). Then we take $Q \in SL_2(\mathbb{Z})$ congruent mod N to MS_1^{-1}, and then $S = Q^{-1}M$.

2. It is a simple reformulation of the fact that $\mathcal{O}_K/(N)$ is $\mathbb{F}_{N^2}$ and $\mathcal{O}_K = \mathbb{Z} \oplus \omega\mathbb{Z}$, and that ϵ is a nonsquare in $\mathbb{F}_N$.

3. We claim that if $M \in \mathscr{M}_2(\mathbb{Z}/N\mathbb{Z})$ has square ϵI_2, then M is similar to T_0, and we can choose the similarity matrix to have determinant 1. For the first part, we simply consider the matrix of the endomorphism M of $\mathbb{F}_N^2$ in the basis (Mx, x) for any nonzero vector x. Let us deal with the second part: clearly $\mathbb{F}_N[M]$ is isomorphic as a ring to $\mathbb{F}_{N^2}$, and clearly this isomorphism maps det : $\mathbb{F}_N[M] \to F_N$ to the norm, so if PMP^{-1} has the desired form with P invertible, there is a matrix M' commuting with M and determinant equal to the determinant of P. Then $PMP^{-1} = (PM'^{-1})M(PM'^{-1})^{-1}$ and we are done.

4. Write $P' = N_1 P_\omega$, so that N_2 commutes with T_0 mod N. A straightforward calculation shows that N_2 must be a polynomial in T_0 mod N, so that $N_1 \in \Gamma_{ns}(N)$. For N_2, then $P_\omega N_2 T N_2^{-1} P_\omega^{-1} = P_\omega T P_\omega^{-1} = T_0 \bmod N$, hence $N_2 T N_2^{-1} = T \bmod N$ so that N_2 commutes with T mod N. Thus $P_\omega N_2 P_\omega^{-1}$ commutes with T_0 mod N, so is a polynomial in T_0 mod N, so $N_2 = P_\omega^{-1}(P_\omega N_2 P_\omega^{-1})P_\omega$ is a polynomial in T mod N, which is what we wanted to prove.

5. If a rational matrix M with positive determinant is in U_c, then its entries are in every $\mathbb{Z}_N$ and its determinant is in every $\mathbb{Z}_N^\times$, so it must be in $SL_2(\mathbb{Z})$. Conversely, a matrix $M \in SL_2(\mathbb{Z})$ is in U_c iff it is congruent mod N to a matrix given by a element of $\mathcal{O}_c$. As c and N are coprime, it is equivalent to require that M be congruent mod N to a matrix of $\mathcal{O}_K$. Since $(1, a + b\omega)$ is a basis of $\mathcal{O}_K/(N)$ over $\mathbb{F}_N$, it is equivalent to require that $P_\omega M P_\omega^{-1}$ be congruent mod N to a linear combination of I_2 and T_0, which is exactly the description written.

6. Follows from the claims one, four and five.

7. Follows from the above.

□

Next, we show that Heegner points on $Y_{ns}(N)$ correspond to CM points on the Shimura curve.

Lemma 4.11 *Let $\tau \in \mathbb{H}$ be a point such that $E_\tau = \mathbb{C}/(\mathbb{Z}\tau \oplus \mathbb{Z})$ has complex multiplication by $\mathcal{O}_c$. Let $\rho = -\overline{\omega} = \omega - r$. There exist coprime integers u, v, w such that $\tau = \frac{v}{c\rho+u}$, and $u^2 - ruc + \nu c^2 = vw$.*

Proof. – Write $\tau' = v\rho + u = \frac{-1}{\tau}$, $\alpha = b\rho + a \in \mathcal{O}_K$. Then $\alpha \in \mathbb{Z}\tau' \oplus \mathbb{Z}$ iff $\frac{b}{v}, a - \frac{ub}{v} \in \mathbb{Z}$. Since $\alpha\tau' = (au - vb\nu) + \rho(av + bu - bvr)$, α is an endomorphism of $E_{\tau'}$ iff $\frac{b}{v}, a - \frac{ub}{v}, \frac{av+bu-bvr}{v}, au - vb\nu - \frac{u}{v}av + bu - bvr \in \mathbb{Z}$. As E_τ and $E_{\tau'}$ are isomorphic, α is an isomophism of $E_{\tau'}$ iff α isomorphism of E_τ iff $c|b$. But the other condition is equivalent to $\frac{b}{v}, \frac{ub}{v}, vb\nu + \frac{bu^2}{v} - bru \in \mathbb{Z}$. It follows that for any integer b, $c|b$ is equivalent to $\frac{b}{v}, \frac{ub}{v}, vb\nu - bru + \frac{bu^2}{v} \in \mathbb{Z}$. Therefore, the subgroup of $\mathbb{Q}$ generated by $1/v, u/v, v\nu - ru + u^2/v$ is $c^{-1}\mathbb{Z}$. In particular, we can write $v = \frac{c}{v_1}$,$u = \frac{u_1}{v_1}$ for some integers u_1, v_1, and the final condition can be rewritten as $v_1, u_1, w_1 = \frac{c^2\nu - ru_1c + u_1^2}{v_1}$ generating $\mathbb{Z}$, which shows that $u_1, -v_1, -w_1$ work. □

Lemma 4.12 *With the notations above, let p be any prime number, $R = \begin{bmatrix} 0 & v \\ c & u \end{bmatrix}$. For any $a, b \in \mathbb{Q}_p$, $R \begin{bmatrix} a & -b\nu \\ b & a + br \end{bmatrix} R^{-1}$ has entries in $\mathbb{Z}_p$ iff $a, \frac{b}{c} \in \mathbb{Z}_p$.*

Proof. – With $a = 0, b = c$,

$$M \begin{bmatrix} 0 & -c\nu \\ c & cr \end{bmatrix} M^{-1} = \frac{-1}{v} \begin{bmatrix} 0 & v \\ c & u \end{bmatrix} \begin{bmatrix} 0 & -\nu \\ 1 & r \end{bmatrix} \begin{bmatrix} u & -v \\ -c & 0 \end{bmatrix}$$
$$= \frac{-1}{v} \begin{bmatrix} v & vr \\ u & c\nu + ur \end{bmatrix} \begin{bmatrix} u & -v \\ -c & 0 \end{bmatrix} \quad = \frac{-1}{v} \begin{bmatrix} v(u - rc) & -v^2 \\ u^2 - ruc + \nu c^2 & -uv \end{bmatrix} = \begin{bmatrix} rc - u & v \\ -w & u \end{bmatrix},$$

so that shows the "if" part.

For the "only if" part, it is enough to show that if $\alpha, \beta \in \mathbb{Q}_p$ are such that $\alpha + \beta(rc - u), \beta u + \alpha, \beta v, \beta w \in \mathbb{Z}_p$ (we say that the pair (α, β) is nice), then $\alpha, \beta \in \mathbb{Z}_p$. If (α, β) is nice, and $\alpha \in \mathbb{Z}_p$, then $\beta u, \beta v, \beta w \in \mathbb{Z}_p$ so $\beta \in \mathbb{Z}_p$. Similarly, if $\beta u \in \mathbb{Z}_p$ for a nice pair (α, β), then $\alpha, \beta \in \mathbb{Z}_p$.

So let us assume (α, β) is a nice pair such that "$\alpha, \beta \in \mathbb{Z}_p$" is false. Then $p|w$ and $p|v$. As u, v, w are coprime, p and u are coprime, and $p^2|vw = u^2 - c(ru - \nu c)$, so that p and c are coprime as well. As

$\alpha, \beta \notin \mathbb{Z}_p$ by the above, and $\alpha+\beta(rc-u)$, $\alpha+\beta u \in \mathbb{Z}_p$, it follows that the quotient $s = \alpha/\beta$ is congruent to $-u$ and $rc-u$ mod p, so that $p|2u-rc$.

Let I be the ideal $(c\rho+u, p)$: then I is an ideal of $\mathcal{O}_K$ that divides (p), and as cu and p are coprime, $I \neq (p)$. If $I = \mathcal{O}_K$, then $(c\overline{\rho}+u, p) = \mathcal{O}_K$, thus $(|c\rho+u|^2, p) = \mathcal{O}_K$, which contradicts $|c\rho+u|^2 = \nu c^2 - ruc + u^2 = vw$. As $\mathcal{O}_K$ is a Dedekind domain, this forces p to not be inert. If p splits, then $p = \mathfrak{q}_1\mathfrak{q}_2$ for some prime ideals $\mathfrak{q}_i$, and $\mathfrak{q}_1 = \overline{\mathfrak{q}_2}$ (because $K/\mathbb{Q}$ is Galois with only nontrivial automorphism the conjugation, and the Galois group must act transitively on the places above p). As $\overline{I} = I$ ($\overline{\rho} = -r-\rho$, so $\overline{c\rho+u} = u-rc-c\rho = (2u-rc)-(c\rho+u)$ with $p|2u-rc$), I has the same valuation for both $\mathfrak{q}_i$, which entails $(p) = \mathfrak{q}_1\mathfrak{q}_2|I$, another contradiction. So p is ramified, and $I^2 = (p)$. It follows that $((c\rho+u)p, (c\overline{\rho}+u)p, p^2) = (p)$, thus there are $s, t \in \mathcal{O}_K$ such that $\alpha(c\rho+u)+\beta(c\overline{\rho}+u)$ is an integer congruent to 1 mod p. So $1 \in (c\rho+u, c\overline{\rho}+u, p) = I$, a contradiction. □

Proposition 4.13 *Let $P = [(\tau, I_2)] \in M_{U_c}(\mathbb{C})$ correspond to a Heegner point in $Y_{ns}(N)$ with complex multiplication by $\mathcal{O}_c$. Then $P = [(\rho, R^{-1})]$ for some matrix R as above; moreover, under this expression, P is a CM point in the sense of [44, Section 6].*

Proof. – The existence of R is ensured by Lemma 4.11, and Lemma 4.12 ensures that $\mathscr{M}_2(\mathbb{Z}_p) \cap R\{K_{a,b} := \begin{bmatrix} a & -b\nu \\ b & a+br \end{bmatrix}, a, b \in \mathbb{Q}_p\}R^{-1} \cap R\{K_{a,b}, a \in \mathbb{Z}_p, b \in c\mathbb{Z}_p\}R^{-1}$ as rings, so that by taking invertible elements, in the notation of [44] $R^{-1}GL_2(\mathbb{Z}_p)R \cap \{K_{a,b}, a, b \in \mathbb{Q}_p\} = \{K_{a,b}, a \in \mathbb{Z}_p, b \in c\mathbb{Z}_p\}^\times$, for any prime number p. Next, we show that ρ is stable under all the $K_{a,b}$ for $a, b \in \mathbb{Q}$ not both zero: indeed, if $a, b \in \mathbb{Q}$ are both nonzero, $K_{a,b}\rho = \frac{a\rho-b\nu}{b\rho+(a+br)} = \frac{a\rho+b\rho^2+rb\rho}{b\rho+(a+br)} = \rho$. To conclude, it is enough to show that if $a \in \mathbb{Z}_N, b \in c\mathbb{Z}_N$, $RK_{a,b}R^{-1} = \begin{bmatrix} a+b(rc-u) & bv \\ -bw & a+bu \end{bmatrix}$ is congruent mod N, as a $\mathbb{Z}_N$ matrix, to a matrix of $\mathcal{O}_c$. In other words, we want to show $bv = (-\nu)(-bw) \bmod N$ and $a+bu = a+b(rc-u)+r(-bw) \bmod N$. In other words, we need to show that $N|v-\nu w$ and $N|2u+rw-rc$.

There is one hypothesis which we did not use: the fact that the endomorphism of $E_\tau[N]$ came from an endomorphism of E_τ. That endomorphism has, in the basis $(1/N, \tau/N)$, the matrix $\begin{bmatrix} a & -b\nu \\ b & a+br \end{bmatrix}$ with the notation of Lemma 4.10, with N not dividing b. By taking an appropriate multiple of this endomorphism, it follows that there is an $\alpha \in \mathcal{O}_c$ such that its matrix in the basis $(1, \tau)$ is integral and congruent mod N to $\begin{bmatrix} 0 & -\nu \\ 1 & r \end{bmatrix}$. In other words, there are integers a, b, d, e such that $\alpha = Na + (1+Nb)\tau$ and $\alpha\tau = (-\nu+Nd)+(r+Ne)\tau$. The second equation can be rewritten as $\alpha = (-\nu+Nd)\frac{c\rho+u}{v} + r + Ne$. But

$$\tau = \frac{v}{c\rho+u} = \frac{v(c\overline{\rho}+u)}{|c\rho+u|^2} = \frac{v(-c\rho-cr+u)}{vw} = \frac{c\rho+(cr-u)}{-w},$$

so that $c\rho = -w\tau + u - cr$, and $\alpha = r + Ne + (-\nu+Nd)\frac{2u-cr}{v} + \frac{-w(-\nu+Nd)}{v}\tau$.

Identifying the two equalities (everything being rational and $(1, \tau)$ being $\mathbb{Q}$-free) yields $vNa = rv + Nev + (-\nu+Nd)(2u-cr)$ and $v+Nbv = -w(-\nu+Nd)$. The second identity implies $N|v-w\nu$, and the first one implies $N|rv-2u\nu+cr\nu$. Thus, using the congruence just before, $N|\nu(rw-2u+cr)$. Thus, to conclude, it is enough to show that N and ν are coprime. As $\nu = \omega\overline{\omega}$ and N is prime and inert in K, it is enough to show that N does not divide ω. But $(1, \omega)$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$, so N cannot divide ω. □

Given this correspondance of definitions of CM points, we can apply Zhang's Gross-Zagier formula, taking the following technical facts for granted:

1. The Shimura curve can be canonically compactified into a Riemann surface which has a smooth projective model X_{U_c} over $\mathbb{Q}$ and an action by Hecke operators – it is this model which is implicitly used in [44].

2. The isomorphism defined above $M_{U_c}(\mathbb{C}) \to Y_{ns}(N)$ comes from an algebraic isomorphism over $\mathbb{Q}$: $X_{U_c} \to X_{ns}(N)$ which preserves Hodge classes and Hecke operators.

3. If f is a positive newform of level 2, weight N^2 and nebentypus 1 such that $L'(f, s) = 0$, which becomes under the Chen isogenies an eigenvector f_{ns} for the Hecke ring of $\mathcal{S}_2(\Gamma_{ns}(N)^+)$, and an automorphic representation with trivial character ϕ_{ns} for X_{U_c}, then $L(\phi_{ns}, s)$ (in the notation of [44, Section 5], which is shifted with respect to the usual notations from e.g. [10]) vanishes with order 2 at $s = 1/2$.

4. The above isogeny between $Jac(X_{U_c})$ and $J_{ns}(N)$ maps the ϕ_{ns}-isotypical component to the f_{ns}-isotypical component.

Theorem 4.14 *Let P be a Heegner point with complex multiplication by $\mathcal{O}_c$ on $X_{ns}(N)$, it is defined on a Galois extension H_c of K. Let ξ be the Hodge class (which is a rational Cartier divisor supported on cusps). Then the f_{ns}-isotypical component of $\sum_{\sigma\in \mathrm{Gal}(H_c/K)} [\sigma(P) - \xi] \in J_{ns}(N)$ is torsion.*

Proof. – The corresponding ϕ_{ns}-isotypical point has null height by Zhang's Gross-Zagier formula ([44, Theorem 6.1]) so is torsion. □

Corollary 4.15 *The f_{ns}-isotypical decomposition of any rational divisor on $X_{ns}(N)$ with zero degree supported on cusps and Heegner points is torsion.*

Proof. – Using the previous theorem, we argue as in the proof of Corollary 3.7. □

We have now all the ingredients to use the criterion of Corollary 2.17 for the vanishing of the θ morphism for $J_{ns}(N)^+$. Define indeed A to be the product of the A_f, f running through the orbits under the Galois action of the newforms of $\mathcal{S}_2(\Gamma_0(N^2))^+$ such that $L'(f,1) \neq 0$, and B the product of the A_f where $L'(f,1) = 0$.

Proposition 4.16 *If $X_{ns}(N)^+$ has a rational point, then we can apply the critetion of Corollary 2.17 to show that in this situation, the θ morphism vanishes.*

Proof. – Using the Chen isogeny we have an isogeny $J_{ns}(N)^+ \to A \times B$ with $\mathrm{Hom}(A,B) = 0$ (because again, the A_f are $\mathbb{Q}$-simple and pairwise non-isogenous). By Corollary 4.9, the Hecke correspondances generate enough of the endomorphisms of $J_{ns}(N)^+$ to satisfy the fourth condition. By Corollary 4.15, and the Manin-Drinfeld theorem, the second condition is met. As for the third condition, it follows from the fact that the Hecke correspondances map cusps to cusps (and conversely do not map non-cusps to cusps), so it is satisfied using Lemma 4.4, Q.E.D. □

2.5 Rank estimates for the Heegner quotient

2.5.1 Motivation

In the Sections 2.3 and 2.4, when $X = X_0(N)^+$ or $X = X_{ns}(N)^+$ is a modular curve of genus at least 2 with a rational point, we have constructed an isogeny $J \to A \times B$ of rational abelian varieties such that its θ morphism is zero (so that its kernel has rank at least $\rho(A) - 1$) and $\mathrm{Hom}(A,B) = 0$. To show that the Chabauty-Kim method applies, the rank of $A(\mathbb{Q})$ must be lower than $\dim A + \rho(A) - 1$. First, we will partially show that $\rho(A) = \dim A$ is the rank of $A(\mathbb{Q})$; so the final step in the proof is to show that (at least for large enough N) this rank is at least 2, so that the inequality is satisfied.

Lemma 5.1 *Let U, V be two rational abelian varieties such that $\mathrm{Hom}(U,V) = 0$. Then $\rho(U \times V) = \rho(U) + \rho(V)$, $\dim(U \times V) = \dim U + \dim V$ and the rank of $(U \times V)(\mathbb{Q})$ is the sum of the ranks of $U(\mathbb{Q})$ and $V(\mathbb{Q})$.*

Proof. – Only the first claim isn't obvious. Define the natural maps $i_1 : U \to U \times V$, $i_2 : V \to U \times V$, then by definition $\mathrm{Hom}(U, V^\vee) = \ker i_1^* \oplus i_2^* \subset \mathrm{Pic}(U \times V)$. There exists a rational isogeny $V^\vee \to V$, which entails that the left hand side is zero. Thus, arguing as in the proof of Proposition 2.1, it follows $\mathrm{Pic}(U \times V) = \pi_1^* \mathrm{Pic}(U) \oplus \pi_2^* \mathrm{Pic}(V)$, where $\pi_1 : U \times V \to U$, $\pi_2 : U \times V \to V$ are the projections, and the k-th coordinate is given by applying $\pi_k^* i_k^*$ to the line bundle. Given the operations, it follows that this decomposition entails another one $\mathrm{Pic}^0(U \times V) = \pi_1^* \mathrm{Pic}^0(U) \oplus \pi_2^* \mathrm{Pic}^0(V)$, so that $NS(U \times V) = \pi_1^* NS(U) \oplus \pi_2^* NS(V)$. To conclude, it is enough to show that $\pi_1^* : NS(U) \to \pi_1^* NS(U)$ is injective (and the same will hold for V). Indeed, let $\mathscr{L}$ be a line bundle on U such that $\pi_1^* \mathscr{L} \in \mathrm{Pic}^0(U \times V)$. Then $\mathscr{L} = i_1^* \pi_1^* \mathrm{Pic}^0(U)$, and we are done. □

Proposition 5.2 *Let $M \in \{N, N^2\}$ where N is an odd prime number, $f \in \mathcal{S}_2(\Gamma_0(M))$ be a positive newform such that $L'(f,1) \neq 0$. Then $A_f(\mathbb{Q})$ has rank $\dim A_f = \rho(A_f)$.*

Proof. – It is the "rank 1 BSD for modular abelian variety", i.e. [13, Proposition 7.1]. It only remains to show that $\rho(A_f) = \dim A_f$. Now, by the proof of Proposition 3.3, the endomorphism ring of A_f has dimension $\dim A_f$ and is generated (up to a finite cokernel) by the Hecke operators. In other words, its endomorphism algebra E^0 is the quotient of the Hecke ring over $\mathbb{Q}$ by the ideal made up with the operators T with $Tf = 0$, that is, $E^0 = K_f$ and is commutative. It is known (used in the same proof in [13]) that the endomorphisms of A_f are symmetric with respect to any polarization. It follows that for any polarization, the Rosati involution is trivial and by the Galois-equivariant version of [30, Proposition

17.2], it follows that $\rho(A_f)$ is the dimension of the self-dual endomorphism algebra over $\mathbb{Q}$, so is $\dim A_f$. □

Corollary 5.3 *In the cases of Sections 2.3, 2.4, $A(\mathbb{Q})$ has rank $\dim A = \rho(A)$, which is the number of newforms f for $\Gamma_0(N), \Gamma_0(N^2)$ respectively, such that $L'(f,1) \neq 0$.*

Proof. – We use the fact that if f and g are newforms, A_f and A_g are isogenous over $\mathbb{Q}$ only if f and g are Galois conjugates, and they are simple over $\mathbb{Q}$. For the final equality, we use the fact that for any newform f, $\dim A_f$ is the number of forms conjugate to f under the Galois action, and that for any newform f and Galois automorphism σ, $L'(f,1) = 0$ iff $L'(f^\sigma, 1) = 0$. The second fact (which we have used implicitly in the Sections 2.3, 2.4) is from the Gross-Zagier paper, [16, Corollary V.1.3].

The first fact is because $\dim A_f$ is the dimension of the holomorphic complex abelian variety $A_f(\mathbb{C})$ as well as the dimension of the algebra (over $\mathbb{Q}$) of Hecke operators (by the above proposition) acting on $A_f(\mathbb{C})$, which is the dimension of the quotient of the $\mathbb{Q}$-space generated by the Hecke operators by the subspace of such operators T with $Tf = 0$. But this quotient is isomorphic to the number field generated by the coefficients of f, which concludes. □

We have thus proved the following:

Proposition 5.4 *Let $M = N$ (resp. $M = N^2$) where N is a prime number. If there are two distinct positive newforms in $\mathcal{S}_2(\Gamma_0(M))$ the L-function of which has a simple zero at 1, then the quadratic Chabauty-Kim method applies to $X_0(N)^+$ (resp. $X_{ns}(N)^+$).*

In the rest of the section, we show that for large enough M, the condition above is satisfied.

2.5.2 Trace formulae

From now on, we take some notations: N is an odd prime number, M is N or N^2. If $f, g \in \mathcal{S}_2(\Gamma_0(M))$, $\langle f,\, g\rangle_M$ is the Petersson inner product of f and g, that is,

$$\langle f,\, g\rangle_M = \int_{\mathcal{D}_M} f(\tau)\overline{g}(\tau)|\mathrm{Im}(\tau)|^2 \frac{dxdy}{y^2} = \int_{\mathcal{D}_M} f(x+iy)\overline{g}(x+iy)\, dxdy,$$

where $\mathcal{D}_M$ is a fundamental domain in $\mathbb{H}$ for $\Gamma_0(M)$. The associated Euclidean norm is denoted as $\|\cdot\|_M$.

If E is a Hermitian space, and A, B are linear forms on E, the E-product of A and B is $\sum_f \frac{\overline{A(f)}B(f)}{\|f\|_E^2}$, where the sum runs over any orthogonal basis of E. In the following, E will always be a subspace of $\mathcal{S}_2(\Gamma_0(M))$ with the Petersson inner product, corresponding to the eigenspaces of the self-adjoint symmetry $w_M : f \longmapsto f|_2 \begin{bmatrix} 0 & -1 \\ M & 0 \end{bmatrix}$, or spaces of newforms or oldforms. This will be explained by using superscripts and subscripts: for instance, $\langle A,\, B\rangle_M^{-,\mathrm{new}}$ is the E-product of A and B, where $E \subset \mathcal{S}_2(\Gamma_0(M)$ is the space of f orthogonal to the old space and such that $w_M f = -f$.

$L' : \mathcal{S}_2(\Gamma_0(M)) \to \mathbb{C}$ denotes $f \longmapsto L'(f,1)$ (which is well-defined using standard computations, see e.g. [10, Chapter 5.10]). If $m \geq 1$ is an integer, a_m is $f \in \mathcal{S}_2(\Gamma_0(M)) \longmapsto a_m(f)$, the m-th coefficient of the q-expansion of f.

We will estimate $\langle a_m,\, L'\rangle^{+,\mathrm{new}}$ for $m = 1, 2$, in view of the following sufficient condition (it is practically quite *ad hoc*, and much better asymptotic estimates are known at least when $N = M$; however, it is far more explicit).

Lemma 5.5 *If $\langle a_1,\, L'\rangle_M^{+,new}$ is nonzero and $0 < \langle a_2,\, L'\rangle_M^{+,new} < \langle a_1,\, L'\rangle_M^{+,new}$, then $\dim A \geq 2$ (for $X_0(N)^+$ if $M = N$, for $X_{ns}(N)^+$ if $M = N^2$).*

Proof. – If $\dim A = 0$, then for any positive newform f of level M, $L'(f,1) = 0$, so that $\langle a_1,\, L'\rangle_M^{+,\mathrm{new}} = 0$. If $\dim A = 1$, then there is exactly one positive newform f of level M with $L'(f,1) \neq 0$. For any embedding $\sigma : K_f \to \mathbb{C}$, f^σ is also a positive newform of level M such that $L'(f^\sigma, 1) \neq 0$, so that $f^\sigma = f$. It follows that f has rational q-expansion. Then for any $m \geq 1$, $\langle a_m,\, L'\rangle_M^{+,\mathrm{new}} = \frac{L'(f,1)}{\|f\|_M^2} a_m(f)$, so that the quotient is $a_2(f)$, hence a rational algebraic integer, thus in $\mathbb{Z}$, so not in $(0,1)$. We have thus proved the contraposition of the stated result, which concludes. □

Definition We define now the basic special functions we need in our estimates.

1. E_1 is the exponential integral function, defined by $E_1(x) = \int_x^\infty e^{-t}\frac{dt}{t}$ defined for $x > 0$. One has, for every $\epsilon > 0$,

$$e^{-x} = \int_x^\infty e^{-t}dt \geq xE_1(x) \geq \frac{1}{1+\epsilon}\int_x^{(1+\epsilon)x} e^{-t}dt = e^{-x}\frac{1-e^{-\epsilon x}}{1+\epsilon},$$

thus $E_1(x) \underset{x\to\infty}{\sim} \frac{e^{-x}}{x}$.

2. For the sake of symmetry, as seen in lemma Lemma 5.6, we define $E_{-1}(x) = e^{-x}$ for $x \geq 0$.

3. J_1 is the first Bessel function, given by $J_1(x) = \pi^{-1}\int_0^\pi \cos(x\sin\theta - \theta)\,d\theta$.

4. The Kloosterman sums are defined, for integers $m, n, c \geq 1$, by

$$S(m,n;c) = \sum_{k\in(\mathbb{Z}/c\mathbb{Z})^\times} \exp\left(\frac{2i\pi}{c}(mk + nk^{-1})\right)$$

if $c > 1$, where k^{-1} is the multiplicative inverse of k mod c, and $S(m,n;1) = 1$ (note that it only depends on $m \bmod c, n \bmod c$).

Using the integral exponential function, we can express L and L' as functions of the a_m for certain modular forms. L' is the one we are ultimately interested in, but it turns out that we will need estimates for L as well:

Lemma 5.6 *Let $M \geq 1$ be an integer.*

1. *If $f \in \mathcal{S}_2(\Gamma_0(M))$, $|a_n(f)| \leq 2\pi n e\|f(x+iy)y\|_{L^\infty(\mathbb{H})} < \infty$.*
2. *If $f \in \mathcal{S}_2(\Gamma_0(M))^+$, then $L'(f,1) = 2\sum_{n\geq 1}\frac{a_n(f)}{n}E_1\left(\frac{2\pi n}{\sqrt{M}}\right)$.*
3. *If $f \in \mathcal{S}_2(\Gamma_0(M))^-$, then $L(f,1) = 2\sum_{n\geq 1}\frac{a_n(f)}{n}e^{-2\pi n/\sqrt{M}}$.*

Proof. – The first point is classical, see e.g. [10, Proposition 5.9.1]. For the second part, classical calculations, e.g. [10, Section 5.10], show that for any complex number s with large enough real part,

$$M^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s) = \int_1^\infty \frac{dt}{t}\left(f\left(\frac{it}{\sqrt{M}}\right)t^s - w_M(f)\left(\frac{it}{\sqrt{M}}\right)t^{2-s}\right) = 2\int_1^\infty f\left(\frac{it}{\sqrt{M}}\right)(t^s - t^{2-s})\frac{dt}{t}.$$

In the right-hand side, no factor but $L(f,s)$ may vanish at $s = 1$, and the right hand side vanishes at $s = 1$, so $L(f,1) = 0$ and, taking derivatives and evaluating at $s = 1$, it follows $L'(f,1) = 2\frac{2\pi}{M}\int_1^\infty f\left(\frac{it}{\sqrt{M}}\right)\ln t\,dt$. Let us note that

$$\begin{aligned}\sum_{n\geq 1}\int_1^\infty |a_n(f)e^{-2\pi nt/\sqrt{M}}\ln t|dt &\leq C\sum_{n\geq 1} ne^{-2\pi n/\sqrt{M}}\int_0^\infty te^{-2\pi nt/\sqrt{M}}dt \\ &\leq C\sum_{n\geq 1} ne^{-2\pi n/\sqrt{M}}\frac{M}{(2\pi n)^2} < \infty,\end{aligned}$$

so that $L'(f,1) = 2\frac{2\pi}{M}\sum_{n\geq 1}a_n(f)\int_1^\infty e^{-2\pi nt/\sqrt{M}}\ln t\,dt$. Now, let $s > 0$:

$$\int_1^\infty e^{-st}\ln t\,dt = -s^{-1}\left[e^{-st}\ln t\right]_1^\infty + s^{-1}\int_1^\infty \frac{e^{-st}}{t}\,dt = s^{-1}E_1(s).$$

The argument is the same for the third claim, but the computation is simpler as it involves evaluating directly the value of the integral instead of differentiating the integrand. □

The authors of [13] recall a trace formula, along with the classical bounds showing it is well defined:

Proposition 5.7

1. *If $x \in \mathbb{R}$, $|2J_1(x)| \leq \min(|x|, 4/\pi)$.*

2. *If m, n, c are integers with gcd d (resp. m, n, c integers with gcd $d/4$, and M is a prime power dividing c), if c (resp. c/M) has t divisors, then $|S(m,n;c)| \leq t\sqrt{dc}$. In particular, when m or n is fixed, as c grows, $S(m,n;c) = O(c^{1/2+r})$ for any $r > 0$.*

3. *If $m, n, M \geq 1$ are integers and $\epsilon = \pm 1$ is a sign, then*

$$\frac{1}{2\pi\sqrt{mn}}\langle a_m,\, a_n\rangle_M^\epsilon = \delta_{mn} - 2\pi \sum_{c=c'M>0} \frac{S(m,n;c)}{c} J_1\left(\frac{4\pi\sqrt{mn}}{c}\right) - 2\pi\epsilon \sum_{\substack{d>0\\(d,M)=1\\n_d=n/M\in\mathbb{Z}/d\mathbb{Z}}} \frac{S(m,n_d;d)}{d\sqrt{M}} J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{M}}\right),$$

and both sums are absolutely convergent.

Proof. – To show the first part, we expand:

$$\pi J_1(x) = \int_0^\pi \cos(x\sin\theta - \theta)\, d\theta = \int_0^\pi \cos(x\sin\theta)\cos\theta d\theta + \int_0^\pi \sin(x\sin\theta)\sin\theta d\theta.$$

The integrand in the first term is antisymmetric with respect to the transformation $x \longmapsto \pi - x$ so the integral is zero. The second integral is bounded in absolute value by $\int_0^\pi x|\sin\theta|^2 d\theta = \pi|x|/2$. But it is also bounded by $\int_0^\pi \sin\theta\, d\theta = 2$.

The second part is the Weil bounds.

For the third part, we show only the absolute convergence of the sums: the fractions with the Kloosterman terms are $O(c^{-1/3})$ and $O(d^{-1/3})$ respectively thanks to the second point (all the rest are fixed parameters), and the Bessel factor is by the first point $O(c^{-1})$ (resp. $O(d^{-1})$), which concludes. □

We can finally compute $\langle L',\, a_m\rangle_M^+$ in our situation:

Proposition 5.8 *Let $m, M \geq 1$ be integers with $M \geq 2$, let $\epsilon = \pm 1$. Let us denote*

$$\mathscr{S}^\epsilon(n,c) = \frac{1}{cn^{1/2}} S(m,n;c) J_1\left(\frac{4\pi\sqrt{mn}}{c}\right) E_\epsilon\left(\frac{2\pi n}{\sqrt{M}}\right),$$

and, if d is an integer coprime to M,

$$\mathscr{T}^\epsilon(n,d) = \frac{S(m,nM^{-1};d)}{d\sqrt{Mn}} J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{M}}\right) E_\epsilon\left(\frac{2\pi n}{\sqrt{M}}\right).$$

1. *The families $(\mathscr{S}^\epsilon(n,c))_{n\geq 1, M|c}$ and $(\mathscr{T}^\epsilon(n,d))_{n\geq 1,(d,M)=1}$ are summable with sums denoted s^ϵ and t^ϵ.*

2. *The following identity holds:*

$$(4\pi)^{-1}\langle a_m,\, L_\epsilon\rangle_M^\epsilon = E_1\left(\frac{2\pi m}{\sqrt{M}}\right) - 2\pi\sqrt{m}(s^\epsilon + \epsilon t^\epsilon),$$

where $L_{+1} = L'$, $L_{-1} = L$.

Proof. – Clearly only the summability is to show, as the remaining steps follow from Lemma 5.6 and Proposition 5.7. Now, because of the Weil bounds and upper bounds on J_1 and E_1, if τ is the divisor-counting function,

$$|\mathscr{S}^+(n,c)| \leq \frac{\sqrt{m}\tau(c)}{\sqrt{cn}} \frac{2\pi\sqrt{mn}}{c} \frac{\sqrt{M}}{2\pi n} e^{-2\pi n/\sqrt{M}} = m\sqrt{M}\frac{\tau(c)}{c^{3/2}} \frac{e^{-2\pi n/\sqrt{M}}}{n},$$

and the conclusion follows for $\mathscr{S}^+$. The same estimates work as well for $\mathscr{T}^+$. When $\epsilon = -1$, we have instead $|\mathscr{S}^-(n,c)| \leq 2\pi m \frac{\tau(c)}{c^{3/2}} e^{-2\pi n/\sqrt{M}}$ and thus summability still works, as above. □

The formula above does not distinguish between the old and the new part in the inner product; however, when $M = N^2$, we are interested in the new part only. The following proposition enables us to control the old part in the product. It is [13, Lemma 5.5]:

Proposition 5.9 *If N is prime and $m \geq 1$ is not divisible by N,*

$$\langle a_m,\, L'\rangle_{N^2}^{+,old} = \frac{1}{N-1}\left(\langle a_m,\, L'\rangle_N^+ + \frac{\ln N}{2}\langle a_m,\, L\rangle^-\right).$$

Proof. – One easily sees that if $J_N = \mathrm{diag}(N, 1)$, then $J_N w_{N^2} w_N^{-1}/N \in \Gamma_0(N)$, so $w_N w_{N^2} \in \mathbb{Q}^*\Gamma_0(N)J_N$, thus if $f \in \mathcal{S}_2(\Gamma_0(N))$, $f|_2 w_{N^2} = w_N(f)|_2 J_N$ is in the old space. So the Fricke involution w_{N^2} preserves the oldspace. Moreover, these computations show that $w_N(f) = \epsilon f$, then $f|_2 w_{N^2} = \epsilon f|_2 J_N$ and $w_{N^2}(f|_2 J_N) = w_N(f) = \epsilon f$.

By [10, Chapter 5.8], the f and $f|_2 J_N$ form a basis of the old space, if f goes through the eigenforms of $\mathcal{S}_2(\Gamma_0(N))$. If, for an eigenform f, we write $\epsilon_f = w_N(f)/f$ (all the good Hecke operators are self-adjoint and every eigenform at level N is new, so w_N commutes with all the Hecke operators and thus is diagonalized at the eigenforms, by multiplicity one), then by the above, $f \pm \epsilon_f f|_2 J_N$ is an eigenvector of w_{N^2} for ± 1. But all of these forms (when ϵ varies and f runs through the normalized eigenforms of level N) make a basis of the old space, so that a basis of $\mathcal{S}_2(\Gamma_0(N^2))^{+,\mathrm{old}}$ is given by the $f + \epsilon_f f|_2 J_N$.

Now, let f, g be normalized eigenforms at level N. Then $N a_N(f)\langle f,\, g\rangle_N = \langle T_N f,\, g\rangle_{N^2} = \langle f,\, T_N^* g\rangle_{N^2} = \langle f, w_{N^2}(T_N w_{N^2} g)\rangle_{N^2} = \epsilon_g \langle w_{N^2} f,\, T_N(g|_2 J_N)\rangle_{N^2}$. But one easily notices $T_N(g|_2 J_N) = Ng$, so that $N a_N(f)\langle f,\, g\rangle_N = \epsilon_g \epsilon_f N \langle f|_2 J_N,\, g\rangle_{N^2}$. In particular the RHS is zero if $f \neq g$, which shows that the $f + \epsilon_f f|_2 J_N$ are pairwise orthogonal, and, if f is a normalized eigenform of level N, $a_N(f)\|f\|_N^2 = \langle f|_2 J_N,\, f\rangle_{N^2}$.

Now, one can see that $\Gamma_0(N)$ acts by left multiplication on the set D_N of 2×2 matrices with integer coefficients, determinant N, and a second row divisible by N, and that representatives of the cosets are given by the matrices $\beta_k = \begin{bmatrix} 1 & k \\ 0 & N \end{bmatrix}$, $0 \leq k < N$, and $\beta_\infty \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$. It follows, as D_N is stable unde right multiplication by $SL_2(\mathbb{Z})$, that the collection of the cosets $\Gamma_0(N)\beta_k$, $k \in \mathbb{P}^1(\mathbb{F}_N)$, is invariant under right multiplication by $SL_2(\mathbb{Z})$. Thus, the image of $T_N + w_N$ is a subset of $\mathcal{S}_2(\Gamma_0(1)) = \{0\}$, so that $T_N = -w_N$, and $\langle w_{N^2} f,\, f\rangle_{N^2} = -\|f\|_N^2$. Therefore, $\|f + w_{N2}(f)\|_{N^2}^2 = 2(N-1)f$.

As, for every eigenform f of level N, $a_m(f|_2 J_N) = 0$,

$$2(N-1)\langle a_m,\, L'\rangle_{N^2}^{old,+} = \sum_f \overline{a_m(f)} L'(f + w_{N^2}(f), 1),$$

where the sum runs through the newforms of level N. We have a functional equation in level N^2 linking f and $w_{N^2}(f)$: if $\Lambda(g, s) = \frac{N^s}{(2\pi)^s}\Gamma(s)L(g, s)$, then Λ is defined at $\mathrm{Re}(s) > 2$ but actually extends to an entire function satisfying $\Lambda(g, s) = -\Lambda(w_{N^2}(g), 2 - s)$ (see e.g. [10, Chapter 5.10] at level N^2), so that, if f is a normalized eigenform of level N, $\Lambda'(f, 1) = \Lambda'(w_{N^2}(f), 1)$.

Note that $\frac{2\pi}{N}\Lambda'(g, 1) = L'(g, 1) + L(g, 1)\left(\ln\frac{N}{2\pi} + \gamma\right)$ for any $g \in \mathcal{S}_2(\Gamma_0(N^2))$, and $L(w_{N^2}(f), 1) = -L(f, 1)$ by the functional equation. Summing the formulas for $g = f$ and $g = w_{N^2}(f)$ yields $c(f) := L'(f + w_{N^2}(f), 1) = \frac{4\pi}{N}\Lambda'(f, 1) = 2\left(L'(f, 1) + \left(\ln\frac{N}{2\pi} + \gamma\right)L(f, 1)\right)$.

But, if $\Lambda_N(f, s) = N^{-s/2}\Lambda(f, s)$, we also have a functional equation (from the same properties of modular forms, but at level N) $\Lambda_N(f, s) = -\epsilon_f \Lambda(f, 2 - s)$. So if $\epsilon_f = 1$, $\Lambda_N(f, 1) = 0$ so $L(f, 1) = 0$ and $c(f) = 2L'(f, 1)$; if $\epsilon_f = -1$, $\Lambda_N'(f, 1) = 0$, which is rewritten as $L'(f, 1) + \left(\ln\frac{\sqrt{N}}{2\pi} + \gamma\right)L(f, 1) = 0$ so that $c(f) = 2\ln\sqrt{N}L(f, 1)$, which concludes. □

2.5.3 First estimates

We want to show that for $m = 1, 2$ and large enough $M \in \{N, N^2\}$ (with N odd prime), the term $E_\epsilon(2\pi m/\sqrt{M})$ is the dominant one. Note that even with the crude estimates above, we still find (because we sum over $M|c$) a $O(1/\sqrt{M})$ error term, which yields the result for large enough M. But we wish for more explicit estimates, which require more careful computations.

Let, for each $c \geq 1$, $\epsilon = \pm 1$, $\mathscr{S}^\epsilon(c) = \sum_{n=1}^\infty \mathscr{S}^\epsilon(n, cM)$. The following result is mostly [13, Lemma 5.6].

Lemma 5.10 *If $m \leq 2$, and $\epsilon = \pm 1$, then $|\mathscr{S}^\epsilon(c)| \leq s(m, c)\sqrt{m}\frac{\tau(c/d)}{c^{3/2}M}$, with $s(m, c) = 2$ if c odd or $m = 1$, $s(m, c) = 1 + \sqrt{2}$ else if c is not divisible by 4, and $s(m, c) = \sqrt{2}$ otherwise, and $d = 2$ if $4|c$ and $d = 1$ else.*

Proof. – If $m = 1$, or $m = 2$ and c is odd, we apply the Weil bound $|S(m,n;cM)| \leq 2\tau(c)\sqrt{cM}$, the Bessel function bound $2|J_1(x)| \leq |x|$, and a sum-integral comparison to show that $\sum_{n\geq 1} E_1(\alpha u) \leq \int_0^\infty E_1(\alpha u)\, du = \alpha^{-1}$.

When $m = 2$ and c is even and not divisible by 4, we split the sum to cover the cases n odd and n even, so that it becomes, after the Bessel function bound and the Weil bound,

$$\frac{4\pi\tau(c)\sqrt{m}}{(cM)^{3/2}} \sum_{n\geq 1, n \text{ odd}} E_1\left(\frac{2\pi n}{\sqrt{M}}\right) + \frac{4\pi\tau(c)\sqrt{2m}}{(cM)^{3/2}} \sum_{n=1}^{\infty} E_\epsilon\left(\frac{4\pi n}{\sqrt{M}}\right).$$

The same sum-integral comparison shows that the second term is bounded by $\frac{\sqrt{2m}\tau(c)}{Mc^{3/2}}$. For the first term, let $f(x) = E_\epsilon(\frac{2\pi n}{\sqrt{M}})$. f is non-negative, decreasing, convex, so that for every odd integer n, $f(n) \leq \frac{1}{2}\int_{n-1}^{n+1} f(u)du$. Summing over all odd integers n, it follows that $\sum_{n\geq 1, n \text{ odd}} f(n) \leq \frac{1}{2}\int_0^\infty f = \frac{\sqrt{M}}{4\pi}$, so that the first term is bounded by $\frac{\sqrt{m}\tau(c)}{Mc^{3/2}}$.

If c is divisible by 4 (and $m = 2$), we claim that $S(2,n;cM) = 2S(1,n/2;cM/2)$ if n is even and 0 is n is odd. Indeed, an element $k \in \mathbb{Z}/cM\mathbb{Z}$ is invertible iff $k + cM/2$ is invertible, as $(cM/2)^2 = 0$, and in this case $(k + n/2)^{-1} = (k^{-1} - k^{-2}(cM/2)) = k^{-1} + cM/2$. Thus,

$$S(2,n;cM) = \sum_{\substack{1\leq k<cM/2 \\ k\in(\mathbb{Z}/cM\mathbb{Z})^\times}} \exp\left(\frac{2i\pi}{cM}(2k + nk^{-1})\right) + \exp\left(\frac{2i\pi}{cM}(2k + 2(cM/2) + nk^{-1} + n(cM/2))\right),$$

and if n is odd, the two terms in the sum cancel out; if n is even, they are equal and we can simplify the argument in the exponential.

Thus, the sum $\mathscr{S}^+(c)$ only needs to be on the even n and the Weil bound then reads $|S(2,n;Mc)| = 2|S(1,n/2;Mc/2)| \leq 4\tau(c/2)\sqrt{Mc/2} = 2\sqrt{2}\tau(c/2)\sqrt{Mc}$. The entire sum is thus bounded by

$$\frac{2\pi\sqrt{m}\tau(c/2)\sqrt{Mc}2\sqrt{2}}{(Mc)^2} \sum_{n=1}^{\infty} E_\epsilon\left(\frac{4\pi n}{\sqrt{M}}\right) \leq \frac{\sqrt{2m}\tau(c/2)}{Mc^{3/2}}.$$

□

Corollary 5.11 *If $m = 1$, $M|s^\epsilon| \leq 2\zeta(3/2)^2 \leq 13.65$.*

If $m = 2$, $M|s^\epsilon|/\sqrt{2} \leq \left(3 + 1/\sqrt{2}\right)\zeta(3/2)^2\left(1 - \frac{1}{2\sqrt{2}}\right)^2 + \frac{\sqrt{2}}{4}\zeta(3/2)^2 \leq 12.986$.

Proof. – If $m = 1$, we simply take the sum over the bound and use the fact that $\zeta^2(s) = \sum_n \tau(n)n^{-s}$ if $s > 1$. If $m = 2$, we split the bound according to the cases c odd (then by the Euler product the corresponding sum of $\tau(c)/c^{3/2}$) is $\zeta(3/2)^2(1 - 2^{-3/2})^2)$, c divisible by 2 but not by 4 (then $\tau(c) = 2\tau(c/2)$ but $c^{-3/2} = 2^{-3/2}(c/2)^{-3/2}$ and $c/2$ is odd, so we come back to the previous sum but multiplied by $\frac{2(1+\sqrt{2})}{2^{3/2}} = 1 + 1/\sqrt{2}$), and c divisible by 4 (so that $\tau(c/2)/c^{3/2} \leq 1/4\tau(c/4)/(c/4)^{3/2}$ and the total sum is thus at most $\sqrt{2}/4\zeta(3/2)^2$). □

Next, we do a similar estimate for $\mathscr{T}^\epsilon(d) = \sum_{n\geq 1} \mathscr{T}^\epsilon(n,d)$:

Lemma 5.12 *If $d \geq 2$ is coprime to M, and $m \leq 2$, then $|\mathscr{T}^\epsilon(d)| \leq t(m,d)\sqrt{m}\frac{\tau(d)}{d^{3/2}\sqrt{M}}$ where $t(m,d) = 1$ if $m = 1$ or d is odd, $t(m,d) = (1+\sqrt{2})/2$ if $d = 2 \bmod 4$, $t(m,d) = 1/\sqrt{2}$ if $4|d$.*

Proof. – If $m = 1$, or $m = 2$ and d is odd, the Weil bound yields $|S(m,nM^{-1};d)| \leq \tau(d)\sqrt{d}$. Using the linear bound for J_1, it follows $|\mathscr{T}^\epsilon(d)| \leq \frac{2\pi\tau(d)\sqrt{m}}{d^{3/2}M}\sum_{n\geq 1} E_\epsilon\left(\frac{2\pi n}{\sqrt{M}}\right) \leq \frac{\tau(d)\sqrt{m}}{d^{3/2}\sqrt{M}}$. Again, if d is even not divisible by 4 and $m = 2$, we split between odd and even n, and use convexity to improve the sum-integral comparison for the odd n. Finally, if d is divisible by 4, only the even n contribute, and we reason as in the previous estimate. □

Putting these estimates together, along with the sum-integral inequality $|\mathscr{T}^\epsilon(1)| \leq \sqrt{m}$, we obtain our first bounds:

Corollary 5.13 *The following bounds hold, where $\zeta_{odd}(3/2)^2 = \sum_{d\geq 1,\, d \text{ odd}} \frac{\tau(d)}{d^{3/2}} = \zeta(3/2)^2(1 - 1/2^{3/2})^2$:*

1. *If $m = 1$, $|t^\epsilon - \mathscr{T}^+(1)| \leq M^{-1/2}(\zeta(3/2)^2 - 1)$.*

2. *If* $m = 2$, $|t^\epsilon - \mathscr{T}^+(1)| \leq M^{-1/2}\sqrt{2}\left(\frac{\zeta(3/2)^2-1}{\sqrt{2}} + (1-1/\sqrt{2})(\zeta_{odd}(3/2)^2 - 1) + \zeta_{odd}(3/2)^2/2^{3/2}\right)$.

3. *If* $m = 1$,
$$\left|\frac{\langle a_m, L_\epsilon\rangle_M^\epsilon}{4\pi} - E_\epsilon\left(\frac{2\pi}{\sqrt{M}}\right) + 2\pi\epsilon\mathscr{T}^\epsilon(1)\right| \leq \frac{36.6}{\sqrt{M}} + \frac{85.8}{M}.$$

4. *If* $m = 2$,
$$\left|\frac{\langle a_m, L_\epsilon\rangle_M^\epsilon}{4\pi} - E_\epsilon\left(\frac{4\pi}{\sqrt{M}}\right) + 2\pi\sqrt{2}\epsilon\mathscr{T}^\epsilon(1)\right| \leq \frac{71.25}{\sqrt{M}} + \frac{93.4}{M}.$$

Proof. – The first two items come from the bounds just above by summing over d, recalling that the original estimates only hold for $d \geq 2$. For $m = 2$, we deal with the different constants for different d by summing $\tau(d)/d^{3/2}\sqrt{2}$ for every $d \geq 2$, then $(1-1/\sqrt{2})\tau(d)/d^{3/2}$ for odd $d > 1$, and summing $0.5(\tau(d)/d^{3/2}) = 2^{-3/2}\tau(d/2)/(d/2)^{3/2}$ for all $d \geq 2$ even and not divisible by 4, so that $d/2$ runs through all odd integers.

The last two items follow from the first two, Corollary 5.11, and Proposition 5.8. □

Proposition 5.14 *For* $M > 1207$, *then* $\langle a_1, L'\rangle_M^+ > 0$. *If moreover* $M \geq 26611$, *then* $0 < \langle a_2, L'\rangle_M^+ < \langle a_1, L'\rangle_M^+$.

Proof. – We prove only the second part, the first one can be proven in a similar but simpler way by numerically checking the estimate at every integer between 1207 and 22611.

The second inequality holds as soon as the following inequality holds (using the previous estimates above): $\frac{107.85}{\sqrt{M}} + \frac{179.2}{M} < 2\pi(\sqrt{2}\mathscr{T}^+_{m=2}(1) - \mathscr{T}^+_{m=1}(1)) + \int_1^2 \frac{e^{-2\pi u/\sqrt{M}}}{u}du$. When $M > 22500 = 150^2$, the left hand side is smaller than $M^{-1/2}(107.85 + 179.2/150) \leq \frac{109.05}{M^{1/2}}$. Now, by sum-integral comparison and the linear bound on J_1, $M^{1/2}|\mathscr{T}^+_{m=1}| \leq 1$. Moreover, when $n \leq \frac{\sqrt{M}}{\pi}$, then $\frac{4\pi\sqrt{2n}}{\sqrt{M}} \leq \frac{4\sqrt{2\pi}}{M^{1/4}} \leq 0.819$, so that, as $x \longmapsto \frac{2J_1(x)}{x}$ decreases on $[0, 3.5]$ (see the next subsection for the argument), $\frac{1}{\sqrt{n}}J_1\left(\frac{4\pi\sqrt{2n}}{\sqrt{M}}\right) \geq \frac{2\pi\sqrt{2}}{\sqrt{M}}\frac{2J_1(0.819)}{0.819} \geq 0.91\frac{2\pi\sqrt{2}}{\sqrt{M}}$. Omitting the positive term corresponding to $\sqrt{M}/\pi < n \leq \sqrt{M}/\pi + 1$, it follows that that

$$\begin{aligned}
\sqrt{M}\mathscr{T}^+_{m=2}(1) &\geq 0.91\frac{2\pi\sqrt{2}}{\sqrt{M}}\sum_{1\leq n\leq\sqrt{M}/\pi} E_1\left(\frac{2\pi n}{\sqrt{M}}\right) - \frac{2\pi\sqrt{2}}{\sqrt{M}}\sum_{n>\sqrt{M}/\pi+1} E_1\left(\frac{2\pi n}{\sqrt{M}}\right)\\
&\geq 0.91\frac{2\pi\sqrt{2}}{\sqrt{M}}\int_1^{\sqrt{M}/\pi} E_1\left(\frac{2\pi u}{\sqrt{M}}\right)du - \frac{2\pi\sqrt{2}}{\sqrt{M}}\int_{\sqrt{M}/\pi}^\infty E_1\left(\frac{2\pi u}{\sqrt{M}}u^{-1/2}\,du\right)\\
&\geq 0.91\sqrt{2}\int_{2\pi/\sqrt{M}}^2 E_1 - \sqrt{2}\int_2^\infty E_1\\
&\geq \sqrt{2}(0.91\times 0.8 - 0.04) \geq 0.68\sqrt{2}.
\end{aligned}$$

Finally, $2\pi\sqrt{M}(\sqrt{2}\mathscr{T}^+_{m=2}(1) - \mathscr{T}^+_{m=1}(1)) \geq 0.72\pi$.

Therefore, the right-hand side is greater (using $e^{-u} \geq 1-u$) $\ln 2 - 1.28\pi/\sqrt{M}$. So if $\sqrt{M} \geq \frac{109.05+1.28\pi}{\ln 2}$, we are done. But $\left(\frac{109.05+1.28\pi}{\ln 2}\right)^2 < 26611$.

As for the other inequality, we need to show that if $M \geq 26611$, $\frac{71.25}{\sqrt{M}} + \frac{93.4}{M} + 2\pi\sqrt{2}\mathscr{T}^+_{m=2}(1) < E_1\left(4\pi/\sqrt{M}\right)$. By a sum-integral comparison, it follows that $2\pi\sqrt{2}\mathscr{T}^+_{m=2}(1) \leq \frac{4\pi}{\sqrt{M}}$, so that we only need to show $\frac{83.82}{\sqrt{M}} + \frac{93.4}{M} < E_1\left(\frac{4\pi}{\sqrt{M}}\right)$. The right-hand side is an increasing function of M, while the left hand side is a decreasing function of M, so we only need to show the result for $M = 26611$, i.e. $\frac{83.82}{\sqrt{26611}} + \frac{93.4}{26611} < E_1\left(\frac{4\pi}{\sqrt{26611}}\right)$. The LHS is bounded above by 0.518, and, as $26611 > 160^2$, the RHS is bounded below by $E_1(4\pi/160) = E_1(\pi/40) \geq E_1(0.1) \geq \frac{1}{e}\int_{0.1}^1 t^{-1}dt = \frac{\ln 10}{e} \geq 0.8$. □

We are interested in the case of newforms as well:

Corollary 5.15 *The following bounds hold, where $M = N^2 > 1600$:*

$$\left|\frac{\langle a_1,\, L'\rangle_M^{+,new}}{4\pi} - E_1\left(\frac{2\pi}{N}\right) + 2\pi\mathscr{T}^+_{N^2,m=1}(1) + \frac{1}{N-1}E_1\left(\frac{2\pi}{\sqrt{N}}\right) + \frac{e^{-2\pi/\sqrt{N}}\ln N}{2(N-1)}\right|$$
$$\leq \frac{36.6}{N} + \frac{22.3\ln N + 44}{N^{3/2}} + \frac{44.7\ln N + 172.2}{N^2}$$
$$\left|\frac{\langle a_2,\, L'\rangle_M^{+,new}}{4\pi} - E_1\left(\frac{4\pi}{N}\right) + 2\pi\sqrt{2}\mathscr{T}^+_{N^2,m=2}(1) + \frac{1}{N-1}E_1\left(\frac{4\pi}{\sqrt{N}}\right) + \frac{e^{-4\pi/\sqrt{N}}\ln N}{2(N-1)}\right|$$
$$\leq \frac{71.25}{N} + \frac{42.96\ln N + 85.92}{N^{3/2}} + \frac{47.9\ln N + 189.2}{N^2}$$

Proof. – We use the formula on the old product and the estimates on the inner products for $\epsilon = \pm 1$ at level N and $\epsilon = 1$ at level N^2, along with the estimate $2\pi\sqrt{mN}|\mathscr{T}^+_{m,N}| \leq 2\pi m$. □

We thus get the fully explicit inequality:

Proposition 5.16 *If $N \geq 47$ is prime, then $\langle a_1,\, L'\rangle_{N^2}^{+,new} > 0$. If, in addition, $N \geq 89$, $\langle a_2,\, L'\rangle_{N^2}^{+,new} > 0$. If moreover $N > 220$, then $0 < \langle a_2,\, L'\rangle_{N^2}^{+,new} < \langle a_1,\, L'\rangle_{N^2}^{+,new}$.*

Proof. – Again, we only show the last two inequalities. Using the estimates from Corollary 5.15 and the method of the proof of Proposition 5.14, we reduce the second inequality in the last claim to proving that for $N > 220$,

$$\ln 2 \geq \frac{107.85 + 1.025\ln 2 + 1.28\pi}{N} + \frac{(65.2 + 1.025/\pi)\ln N + 129.92}{N^{3/2}} + \frac{92.6\ln N + 361.4}{N^2},$$

and this inequality does hold for $N > 220$.

For the first inequality of the final claim, we actually show the second claim. As in the proof of Proposition 5.14, and using $E_{-1} \leq -1$, we only need to show that

$$\frac{71.25 + 4\pi}{N} + \frac{42.96\ln N + 85.92}{N^{3/2}} + \frac{47.9\ln N + 189.2}{N^2} + \frac{\ln N}{2(N-1)} + \frac{1}{N-1}E_1\left(\frac{4\pi}{\sqrt{N}}\right) \leq E_1\left(\frac{4\pi}{N}\right).$$

All the terms in the LHS are easy functions of N, except maybe for the last one, can be shown to be lower than 0.0015. So the LHS is smaller than

$$LHS' = 0.0015 + \frac{71.25 + 4\pi}{N} + \frac{42.96\ln N + 85.92}{N^{3/2}} + \frac{47.9\ln N + 189.2}{N^2} + \frac{\ln N}{N-1},$$

which is a decreasing function of $N \geq 89$. For $N = 89$, $LHS' \leq 1.378$, while $E_1(4\pi/89) \geq E_1(\pi/22) \geq E_1(1/7)$ can be shown to exceed 1.5, which concludes. □

2.5.4 Refining the estimates into computable range

We see that the highest contribution to the error is from the constant in the $O(M^{1/2})$, so we try to lower this constant it in another way. To this end, the authors of [13] use the following average estimate on Kloosterman sums to perform an Abel transform:

Lemma 5.17 *Let $d > 1$, k be invertible mod d, $m, a, b \geq 1$ be integers. Then*

$$\left|\sum_{n=a}^{b} S(m, nk; d)\right| \leq \frac{4d}{\pi^2}(\log d + 1.5).$$

Corollary 5.18 *Let $d \geq 2$ be coprime to M and $m \leq 2$. Assume $\alpha > 1$ satisfies $\alpha < \left(\frac{12.25}{32\pi^2} - \frac{1}{d^4 M}\right) d^2\sqrt{M}$. Then*

$$|\mathscr{T}^+(d)| \leq \frac{4}{\pi^4 M^{3/4}\alpha^{3/2}}\frac{(1.5 + \log d)e^{-2\pi d^2\alpha}}{d^3} + \frac{8\sqrt{m}}{\pi M}\frac{1.5 + \log d}{d}E_1\left(\frac{2\pi}{\sqrt{M}}\right)$$
$$+ \frac{\tau(d)\sqrt{m}}{2\pi\alpha d^{7/2}\sqrt{M}}(e^{-2\pi d^2\alpha}),$$

and

$$|\mathscr{T}^-(d)| \leq \frac{8}{\pi^3 M^{3/4}\alpha^{1/2}}\frac{(1.5+\log d)e^{-2\pi d^2\alpha}}{d} + \frac{8\sqrt{m}}{\pi M}\frac{1.5+\log d}{d}E_{-1}\left(\frac{2\pi}{\sqrt{M}}\right) + \frac{\tau(d)\sqrt{m}}{d^{3/2}\sqrt{M}}(e^{-2\pi d^2\alpha})$$

Proof. – By the Weil bound and the Bessel uniform bound, for $\epsilon = +1$ (the case $\epsilon = -1$ is similar but results in a denominator of $\mathrm{d}^{3/2}\sqrt{M}$):

$$\begin{aligned}\frac{1}{d\sqrt{M}} &\sum_{n>d^2\alpha\sqrt{M}+1} |S(m,nM^{-1};d)|n^{-1/2}\left|J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{M}}\right)\right| E_1\left(\frac{2\pi n}{\sqrt{M}}\right)\\ &\leq \frac{2\pi\tau(d)}{d^{3/2}M}\sum_{n>d^2\alpha\sqrt{M}+1} E_1\left(\frac{2\pi n}{\sqrt{M}}\right)\\ &\leq \frac{\tau(d)\sqrt{m}}{d^{3/2}\sqrt{M}}\int_{2\pi d^2\alpha}^{\infty} E_1\\ &\leq \frac{\tau(d)\sqrt{m}}{2\pi\alpha d^{7/2}\sqrt{M}}e^{-2\pi d^2\alpha}\end{aligned}$$

Moreover, we can see that if $n \leq \alpha d^2\sqrt{M}+1$, then $\frac{4\pi\sqrt{mn}}{d\sqrt{M}} \leq 3.5$. But one easily computes that $J_1'' \leq 0$ and $J_1 \geq 0$ on $[0,3.5]$, so that, as $J_1(0)=0$, $x \longmapsto \frac{J_1(x)}{x}$ is nonnegative decreasing on this interval.

Therefore, for $1 \leq n \leq \alpha d^2\sqrt{M}+1$, the sequence $J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{M}}\right)n^{-1/2}$ is positive decreasing, so that its product with $E_\epsilon\left(\frac{2\pi n}{\sqrt{M}}\right)$ is also nonnegative decreasing.

Thus, an Abel summation, along with the estimate from the previous lemma, yields (the $2/\pi$ comes from the uniform bound on J_1):

$$\left|\frac{1}{d\sqrt{M}}\sum_{1\leq n\leq d^2\alpha M+1}\mathscr{T}^\epsilon(d,n)\right| \leq \frac{4(\log d+1.5)}{\pi^2\sqrt{M}}\left(\frac{2}{\pi d\alpha^{1/2}M^{1/4}}E_\epsilon(2\pi d^2\alpha) + J_1\left(\frac{4\pi\sqrt{m}}{d\sqrt{M}}\right)E_\epsilon\left(\frac{2\pi}{\sqrt{M}}\right)\right),$$

and the conclusion follows (using $E_1(x) \leq e^{-x}/x$). □

For small d, this bound, obtained through Abel summation, is better than the other one, as is has a better decay with respect to M. However, it is unfortunately not summable as d goes to infinity, so that we will need a trade-off between our two bounds. Let us make the cut at $F \geq 5$. Then

$$2\pi\sqrt{m}\left|\sum_{d=2}^{F}\mathscr{T}^+(n,d)\right| \leq 0.51\frac{8\sqrt{m}e^{-8\pi\alpha}}{\pi^3M^{3/4}\alpha^{3/2}} + \frac{m(\zeta(7/2)^2-1)e^{-8\pi\alpha}}{\alpha\sqrt{M}} + \frac{16m}{M}E_1\left(\frac{2\pi}{\sqrt{M}}\right)\sum_{d=2}^{F}\frac{1.5+\ln d}{d}.$$

Now, $\ln^2$ is concave on (e,∞), so $(\ln d+1)^2-(\ln d)^2 \geq \frac{2\ln(d+1)}{d+1}$ if $d \geq 3$. $x \longmapsto 1/x$ is convex, so $1/s \leq \int_{s-1/2}^{s+1/2}\frac{du}{u}$. As $(\ln 3)/3+(\ln 2)/2-(\ln 3)^2/2-1.5*\ln 1.5+1.5*0.5/5 < -0.3$, and ln is concave, it follows

$$2\pi\sqrt{m}\left|\sum_{d=2}^{F}\mathscr{T}^+(n,d)\right| \leq \frac{8m}{M}E_1\left(\frac{2\pi}{\sqrt{M}}\right)\left((\ln F)^2+3\ln F-0.6\right).$$

To estimate the remainder of the $\mathscr{T}^+$ series (i.e. for $d > F$), we need an estimate on the remainder of the L-series of the divisor-counting function.

Lemma 5.19 *If $\ell \geq 5$ is an integer, then $\sum_{d>\ell}\frac{\tau(d)}{d^{3/2}} \leq \frac{2\ln\ell+6.87}{\sqrt{\ell}}$.*

Similarly, if $\ell \geq 12$, $\sum_{d>\ell,d\ odd}\frac{\tau(d)}{d^{3/2}} \leq \frac{\ln\ell+3.487}{\sqrt{\ell}}$.

Proof. – For the first estimate, the sum is over k,t with $kt > \ell$ of the $k^{-3/2}t^{-3/2}$. The cases with $k=1$ or $t=1$ contribute $4/\sqrt{l}$ by sum-integral comparison on the remainder of ζ. The terms $t \geq 2$, $k > \ell/2$ contribute $2(\zeta(3/2)-1)/\sqrt{\ell}$. When $2 \leq k \leq \ell/2$, the contribution is $k^{-3/2}\sum_{t>\ell/k}l^{-3/2}$ and the series

is not greater than $(k/\ell)^{3/2} + 2\sqrt{\ell/k}$ (again, by sum-integral comparison), and the convexity inequality $\frac{1}{x} \le \ln \frac{x+0.5}{x-0.5}$ enables us to treat the second term, as the first term contributes $0.5/\sqrt{\ell}$, and we finally use the numerical computation $2\sqrt{2}(\zeta(3/2)-1) + 4.5 - 2\ln 3 < 6.87$.

For the second sum, it is over the odd k, t with $kt > \ell$. The $k = 1$ or $t = 1$ contribute $2\sum_{t>\ell, t \text{ odd}} t^{-3/2} \le 2\ell^{-1/2}$, because $p^{-3/2} \le \frac{1}{2}\int_{p-1}^{p+1} u^{-3/2} du$. The $t \ge 3$, $k > \ell/3$ contribute $(\zeta_{odd}(3/2)-1)\left((\ell/3)^{-3/2} + \sqrt{3/\ell}\right)$, and $3/\ell \le 1/4$. To deal with the $3 \le k \le \ell/3$, $t > \ell/k$, with again a sum-integral comparison (as usual, each term is bounded by half an integral over an interval of size 2 due to convexity, and given that the first term is at most $(k/\ell)^{3/2}$), we obtain $\frac{1}{3\sqrt{\ell}} + (4\ell)^{-1/2}\sum_{k=3, k \text{ odd}}^{\ell/3} k^{-1}$, and, after another sum-integral comparison, the sum is at most $\ln \frac{\ell/3+1}{2} = \ln(\ell+3) - \ln 6 \le \ln \ell - \ln 6 + \frac{3}{\ell}$ and the conclusion follows by adding all the factors before $\ell^{-1/2}$. □

We assume $F \ge 24$ is even.

If $m = 1$, $2\pi\sqrt{m}\left|\sum_{d>F} \mathscr{T}^+(d)\right| \le \frac{2\pi}{\sqrt{M}} \sum_{d>F} \frac{\tau(d)}{d^{3/2}} \le \frac{4\pi}{\sqrt{MF}}(\ln F + 3.44)$.

If $m = 2$, as for the naive bound, we sum $1/\sqrt{2}$ times over all $d > F$, $1 - 1/\sqrt{2}$ times over all the odd $d > F$, and $1/2$ times over the odd $d > F/2$, and it follows

$$\begin{aligned} 2\pi\sqrt{m}\left|\sum_{d>F} \mathscr{T}^+(d)\right| &\le \frac{4\pi}{\sqrt{M}}\left(\frac{2\ln F + 6.87}{\sqrt{2F}} + (1-1/\sqrt{2})\frac{\ln F + 3.487}{\sqrt{F}}\right. \\ &\quad \left. + 0.5\frac{\ln F - \ln 2 + 3.487}{\sqrt{F}}\right) \\ &\le \frac{4\pi}{\sqrt{MF}}(2.208\ln F + 4.811) \end{aligned}$$

Using a Python script, we can ensure that for any $8000 \le M \le 50000$ (we choose $\alpha = 3$, and recall that $50000 > 220^2$):

- For $m = 1$, $2\pi\sqrt{m}\left|\sum_{d\ge 2} \mathscr{T}^+(d)\right| \le \frac{16.159}{\sqrt{M}} + \frac{8e^{-24\pi}0.502}{\pi^3 M^{3/4} 3^{3/2}} + \frac{e^{-24\pi}(\zeta(7/2)^2-1)}{3\sqrt{M}} \le \frac{16.16}{\sqrt{M}}$.
- For $m = 2$, $2\pi\sqrt{m}\left|\sum_{d\ge 2} \mathscr{T}^+(d)\right| \le \frac{31.557}{\sqrt{M}} + \frac{8\sqrt{2}e^{-24\pi}0.502}{\pi^3 M^{3/4} 3.5^{3/2}} + \frac{e^{-24\pi}2(\zeta(7/2)^2-1)}{3\sqrt{M}} \le \frac{31.56}{\sqrt{M}}$.

So, for $M \ge 9000$, splitting the sum for $\mathscr{T}^+_{m=2}(1)$ at $n \ge \sqrt{M}/\pi$, using a lower linear bound for lw now n and an upper uniform bound for high n and controlling each term with a sum-integral then, we find $\sqrt{2M}\mathscr{T}^+_{m=2} \ge 1.28$, thus

$$\begin{aligned} \frac{1}{4\pi}\left(\langle a_1, L'\rangle^+_M - \langle a_2, L'\rangle^+_M\right) &\ge \int_{2\pi/M^{1/2}}^{4\pi/M^{1/2}} \frac{e^{-u}}{u}\, du + \frac{2\pi}{\sqrt{M}}\left(\sqrt{2}\mathscr{T}^+_{m=2}(1) - \mathscr{T}^+_{m=1}(1)\right) - \frac{47.72}{\sqrt{M}} - \frac{179.2}{M} \\ &\ge \int_1^2 \frac{e^{-2\pi u/\sqrt{M}}}{u}\, du + \frac{0.56\pi}{\sqrt{M}} - \frac{49.73}{\sqrt{M}} \\ &\ge \ln 2 - \frac{2\pi}{\sqrt{M}} + \frac{0.56\pi}{\sqrt{M}} - \frac{49.73}{\sqrt{M}} \ge \ln 2 - \frac{54.26}{\sqrt{M}} > 0. \end{aligned}$$

Moreover, still for $M \ge 8000$,

$$\begin{aligned} \frac{\langle a_1, L'\rangle^+_M - \langle a_2, L'\rangle^+_M}{4\pi} &\ge E_1\left(\frac{4\pi}{\sqrt{M}}\right) - \frac{93.4}{M} - \frac{2\pi\sqrt{2} + 31.56}{\sqrt{M}} \\ &\ge E_1\left(\frac{4\pi}{\sqrt{M}}\right) - \frac{41.5}{\sqrt{M}} \\ &\ge E_1\left(\frac{4\pi}{\sqrt{8000}}\right) - \frac{41.5}{\sqrt{8000}} \\ &\ge E_1(\pi/22) - 0.464 \ge e^{-1}\ln 22/\pi - 0.464 > 0. \end{aligned}$$

From this calculation, and others similar to this one and to those of the proofs of Corollary 5.15 and Proposition 5.16, we infer that:

Proposition 5.20 *If $M = N \geq 8000$ is prime, then for $X = X_0^+(N)$, A has rank at least 2. If $N \geq 137$ is prime, then for $X_{ns}^+(N)$, A has rank at least 2.*

Now, it remains to see what happens for primes in the ranges not covered by the above.

Querying information from the LMFDB [26], we find that if $N < 8000$ is an odd prime and A has rank at most 1, then $N \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 71, 79, 83, 89, 101, 131\}$, all of which have less than two positive newforms, so that $X_0(N)^+$ has genus at most 1. Similarly, if $N < 100$ is an odd prime and (for $X_{ns}(N)^+$) A has rank at most 1, then $N \in \{3, 5, 7, 11\}$ and there is at most one positive newform of level N^2, so that $X_{ns}^+(N)$ has genus at most 1.

For $101 \leq N \leq 137$ and $X_{ns}(N)^+$, we know that $\langle a_1,\, L' \rangle_{N^2}^{+,\mathrm{new}} > 0$ so that A has rank at least 1. If this rank is 1, then there exists exactly one positive newform f of level N^2, with integer coefficients, and $A = A_f$ is an elliptic curve of conductor N^2 and rank 1. According to the LMFDB [26] (querying elliptic curves of analytic rank 1 and conductor N^2), it is possible only if $N \in \{101, 109, 113, 119\}$. In these cases, we find that there exists only one such elliptic curve, which must thus be A_f. Thus, we must have $a_2(f) = \frac{\langle a_2,\, L' \rangle_{N^2}^{+,\mathrm{new}}}{\langle a_1,\, L' \rangle_{N^2}^{+,\mathrm{new}}} > 0$ by Proposition 5.16. But each of these times, $a_2(f) \leq 0$.

Thus, we have proved that

Proposition 5.21 ([13], Theorem 1.3) *If N is an odd prime number such that the genus of $X_0(N)^+$ (resp. $X_{ns}(N)^+$) is at least 2, then in the isogeny $J_0(N)^+ \to A \times B$ constructed in Section 2.3 (resp. $J_{ns}(N)^+ \to A \times B$ constructed in Section 2.4), A has dimension, rational rank, and Néron-Severi rank all equal and at least 2.*

A Construction of Coleman integrals

A.1 Structure of smooth $\mathbb{Z}_p$-schemes

In this part, we consider a smooth proper $\mathbb{Z}_p$-scheme Y of relative dimension d with connected generic fiber, where p is a prime number, and prove some of its properties. We use the notations and definitions of section 1.2.

Proposition 1.1

- *The generic fiber of Y is a dense open subscheme.*
- *Y is a regular integral scheme.*
- *Every nonempty closed subset of Y meets the closed fiber.*
- *The natural map $Y(\mathbb{Z}_p) \to Y(\mathbb{Q}_p)$ is a bijection.*
- *The map of sets $Y(\mathbb{F}_p) \to \{y \in Y_{\mathbb{F}_p}, \kappa(y) = \mathbb{F}_p\}$ mapping P to the unique point in the set-theoretical image of P is a bijection.*
- *The map of sets $Y(\mathbb{Q}_p) \to \{y \in Y_{\mathbb{Q}_p}, \kappa(y) = \mathbb{Q}_p\}$ mapping P to the unique point in the set-theoretical image of P is a bijection.*
- *If the generic fiber is geometrically connected, so is the special fiber.*

Proof. – Let $V \subset Y$ be a nonempty open subset. Let $s : Y \to \operatorname{Spec} \mathbb{Z}_p$ be the structural morphism. We want to show that $s(V)$ contains the generic point. But s is a smooth morphism of locally Noetherian schemes so is open, thus $s(V)$ is a nonempty open subset of $\operatorname{Spec} \mathbb{Z}_p$ and we are done.

To show that Y is regular integral, it is enough to show that it is regular at every point and irreducible. But its generic fiber is smooth over a field and connected, so is integral thus irreducible. Since that generic fiber is dense, Y is irreducible. Also, Y is smooth over a field at each point of its generic fiber, thus regular; let us check regularity for the points on the special fiber F. Let $x \in F$ be a closed point and A the ring of stalks of Y at p. Then the ring $A/pA = \mathcal{O}_{F,x}$ is local regular because F is smooth over $\mathbb{F}_p$. To show A is regular, it is thus enough to show that $\dim A/pA < \dim A$, because then the difference in dimensions is one (see [25, Theorem 2.5.15]). From the same source, we only need to show that p is a regular element of A. As Y is flat over $\mathbb{Z}_p$, A is flat over $\mathbb{Z}_p$, thus is torsion-free ($p\,\mathrm{id} : \mathbb{Z}_p \to \mathbb{Z}_p$ is injective, so it must remain so when tensoring with A) and we are done.

The third point is an immediate consequence of the fact that $Y \to \operatorname{Spec} \mathbb{Z}_p$ is a closed map. The fourth point is the valuative criterion of properness, see for instance [25, Theorem 3.3.25].

We prove the fifth point only, the sixth is proved in the same way. Let $y \in Y_{\mathbb{F}_p}$ be such that $\kappa(y) = \mathbb{F}_p$. We have a morphism of local rings $\mathcal{O}_{Y,y} \to \kappa(y)$, which we denote $P \in Y(\mathbb{F}_p)$. One easily checks that $y \longmapsto P$ is the inverse to the map in the statement of the theorem.

For the last point, we use Zariski's connectedness principle, see [25, Theorem 5.3.15, Remarks 5.3.3, 5.3.20]. We only need to prove that if G is the generic fiber of Y, then $\mathcal{O}_Y(G) = \mathbb{Q}_p$ and $\mathcal{O}_Y(Y) = \mathbb{Z}_p$. As Y is flat proper over $\mathbb{Z}_p$, $\mathcal{O}_Y(Y)$ is finitely generated (see [11, Théorème III.3.2.1]) and torsion-free over $\mathbb{Z}_p$, thus free of finite rank. As $G = Y \times_{\mathbb{Z}_p}^{\mathbb{Q}_p}$, and Y is Noetherian, [25, Proposition 3.1.24] ensures $\mathcal{O}_Y(Y) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathcal{O}_G(G) = \mathcal{O}_Y(G)$, so it is enough to prove the statement for $\mathcal{O}_G(G)$. But $G \to \operatorname{Spec} \mathbb{Q}_p$ is proper and integral, thus by [25, Proposition 3.3.18], $\mathcal{O}_G(G)$ is an integral $\mathbb{Q}_p$-algebra, the elements of which are algebraic over $\mathbb{Q}_p$, so is an algebraic field extension of $\mathbb{Q}_p$. By [25, Corollary 3.2.14], as G is smooth geometrically connected, it is geometrically integral, so $K(G) \supset \mathcal{O}_G(G)$ cannot contain nontrivial algebraic elements over $\mathbb{Q}_p$. □

Now, we formalize the definitions for the second part of the section, about uniformizers and their generalizations.

Definition Let $z \in Y(\mathbb{F}_p)$. As seen in the earlier proof, $p \in \mathfrak{m}_z$, which is generated by $d + 1 = \dim \mathcal{O}_{Y,z}$ elements. A system of uniformizers is a tuple $(t_1, \ldots, t_d) \in\in \mathfrak{m}_z^d$ such that $(p, t_1, \ldots, t_d)$ generate $\mathfrak{m}_z$.

Lemma 1.2 *With the above notations, there always exists a system of uniformizers.*

Proof. – We know that $\mathcal{O}_{Y_{\mathbb{F}_p},z} = \mathcal{O}_{Y,z}/(p)$ is a regular Noetherian local ring of dimension d. Thus it follows that $p \in \mathfrak{m}_z/\mathfrak{m}_z^2$ is nonzero. So we can complete this one-element family into a $\mathbb{F}_p$-basis of $\mathfrak{m}_z/\mathfrak{m}_z^2$, and the conclusion follows. □

As seen in Section 1.2, there are two important properties we want to associate to uniformizers. We recall the definitions of *reduction mod p*, and the various residue disks.

Definition Given $P \in Y(\mathbb{Q}_p)$, we know from the above lemma that it comes from a $P_1 \in Y(\mathbb{Z}_p)$. The *reduction mod p* of P is the morphism $P_1 \circ q \in Y(\mathbb{F}_p)$, where $q : \operatorname{Spec} \mathbb{F}_p \to \operatorname{Spec} \mathbb{Z}_p$ is the natural closed immersion.

Definition Given a point $z \in Y(\mathbb{F}_p)$, its *residue disk* is the set $Y(\mathbb{Q}_p)_z$ of all points reducing mod p to z. The *completed residue disk* is the scheme $\operatorname{Spec} \mathcal{O}_{Y,z}$, and the *schematic residue disk* is the scheme $\operatorname{Spec} \mathcal{O}_{Y,z}[p^{-1}]$.

This preliminary lemma ensures that the schematic and complete residue disks are scheme-theoretical versions of the point-set residue disk.

Lemma 1.3 *The schematic residue disk and the completed residue disk have the same Q_p-points, which are canonically identified to the points of $Y(\mathbb{Q}_p)_z$.*

Proof. – Let S denote the schematic residue disk and C denote the completed residue disk. We have a natural injection $S(\mathbb{Q}_p) \to C(\mathbb{Q}_p)$. To show it is an isomorphism, it is enough to prove $S = C \times_{\operatorname{Spec} \mathbb{Z}_p} \operatorname{Spec} \mathbb{Q}_p$. But it is clear from the description of S and C as affine $\mathbb{Z}_p$-schemes. Now, if $P \in Y(\mathbb{Q}_p)_z$, it extends to a morphism $P_1 : \operatorname{Spec} \mathbb{Z}_p \to Y$ with set-theoretical image $\{P, z\}$ (for the generic point and closed point s, respectively). So P_1 induces a morphism of local $\mathbb{Z}_p$-algebras $\mu : \mathcal{O}_{Y,z} \to (\mathbb{Z}_p)_s = \mathbb{Z}_p$. So μ induces a morphism $\mathcal{O}_{Y,z}[p^{-1}] \to \mathbb{Q}_p$ thus an element of $S(\mathbb{Q}_p)$. Conversely, we have a natural morphism of $\mathbb{Z}_p$-schemes $S \to C \to Y$ mapping a point in $P \in S(\mathbb{Q}_p)$ to $P_1 \in C(\mathbb{Q}_p)$, and $P_2 \in Y(\mathbb{Q}_p)$, and we thus get a morphism $\nu : \mathcal{O}_{Y,z} \to \mathbb{Q}_p$. If ν has an image into $\mathbb{Z}_p$, we are done: indeed, this proves that P_1 comes from a $P_1' \in C(\mathbb{Z}_p)$, with the closed point of $\mathbb{Z}_p$ to that of C, so P_2 comes from a $P_2' \in Y(\mathbb{Z}_p)$ where the closed point of $\mathbb{Z}_p$ is mapped to the image by $C \to Y$ of the closed point, ie z; in other words, $P_2 \in Y(\mathbb{Q}_p)_z$. We then check that these operations are inverse one of the other. Now, $\mathcal{O}_{Y,z}$ contains $\mathbb{Z}_p$. Thus, if the image of ν is not contained in $\mathbb{Z}_p$, ν is onto, so the kernel of ν is a maximal ideal of $\mathcal{O}_{Y,z}$. Hence, the residual field of $\mathcal{O}_{Y,z}$ would be $\mathbb{Q}_p$. But we know that field is actually $\mathbb{F}_p$, a contradiction. Thus the image of ν is contained in $\mathbb{Z}_p$. □

Now we can prove the structure theorem for residue disks:

Proposition 1.4 *If $t \in \mathcal{O}_{Y,z}[p^{-1}]$, $P \in Y(\mathbb{Q}_p)_z$, then P induces a morphism of local rings $\mathcal{O}_{Y,z} \to \mathbb{Z}_p$, localizing to $\mu_P : \mathcal{O}_{Y,z}[p^{-1}] \to \mathbb{Q}_p$, and we write $t(P) := \mu_P(t)$. In particular, if $t \in \mathfrak{m}_{Y,z}$, $t(P) \in p\mathbb{Z}_p$.*

Let $(t_1, \dots, t_d)$ be a system of uniformizers for z. Then $P \in Y(\mathbb{Q}_p)_z \longmapsto (t_i(P))_{1 \leq i \leq d} \in (p\mathbb{Z}_p)^d$ is a bijection. Moreover, the $\mathfrak{m}_{Y,z}$-adic completion of $\mathcal{O}_{Y,z}$ is isomorphic to $\mathbb{Z}_p[[t_1, \dots, t_d]]$.

Proof. – Recall that every $P \in Y(\mathbb{Q}_p)_z$ induces (by valuative criterion of properness) a morphism of local rings $\mathcal{O}_{Y,z} \to \mathbb{Z}_p$. Conversely, a morphism of local rings $\mathcal{O}_{Y,z} \to \mathbb{Z}_p$ induces a morphism $f : \operatorname{Spec} \mathbb{Z}_p \to C$ where C is the completed residue disk. But we have canonical morphisms $\operatorname{Spec} \mathbb{Q}_p \to \operatorname{Spec} \mathbb{Z}_p$, $C \to Y$ so f induces a morphism $P \in Y(\mathbb{Q}_p)$ by compositions. Following the links, we see that $P \in C(\mathbb{Q}_p)$ thus $P \in Y(\mathbb{Q}_p)_z$. We easily see that these constructions are each other's inverses.

Thus, let $A = \mathcal{O}_{Y,z}$, A is a local Noetherian regular $\mathbb{Z}_p$-algebra, has dimension $d+1$ and $p \notin A^\times$. We know that $(p, t_1, \dots, t_d)$ is a system of parameters of A (in the usual sense for regular rings), and we want to show that $f \in \operatorname{Hom}_{\mathbb{Z}_p,\text{local}}(A, \mathbb{Z}_p) \longmapsto (f(t_i))_{1 \leq i \leq d} \in p\mathbb{Z}_p$ is an isomorphism. Let A' denote the completion of A with respect to its maximal ideal. Then we have a canonical isomorphism $\operatorname{Hom}_{\mathbb{Z}_p,\text{local}}(A, \mathbb{Z}_p) \to \operatorname{Hom}_{\mathbb{Z}_p,\text{local}}(A', \mathbb{Z}_p)$ given by morphism completion (and the inverse is the restriction of the morphism from A' to A).

To conclude, we want to prove that $A' \cong \mathbb{Z}_p[[t_1, \dots, t_d]]$. We first note that we have a natural morphism of local rings $\mathbb{Z}_p[[T_1, \dots, T_d]] \to A'$ given by $T_i \longmapsto t_i$. This morphism can easily be checked to be surjective, so A' is a quotient of the Noetherian local integral domain $\mathbb{Z}_p[[t_1, \dots, t_d]]$ of dimension $d+1 = \dim A = \dim A'$ (see for instance [25, Lemma 4.2.26]), so the morphism must also be injective, and we are done. □

Second, we can prove a structure theorem for differential forms on scheme-theoretic residue disks.

Proposition 1.5 *Let $z \in Y(\mathbb{F}_p)$, S and C the respectively schematic and complete residue disks (both of them affine schemes) at z, $(t_1, \dots, t_d)$ a system of uniformizers at z. We denote as $\mathfrak{m}_C$ and $\mathfrak{m}_S$ the ideals of $\mathcal{O}_C(C)$ and $\mathcal{O}_S(S)$ that they generate.*

$\Omega^1_{C/\mathbb{Z}_p}(C)$ and $\Omega^1_{S/\mathbb{Q}_p}(S)$ are free $\mathcal{O}_C(C)$ and $\mathcal{O}_S(S)$-modules, respectively, with basis $dt_1, \dots, dt_d$.

Let $\omega \in \Omega^1_{C/\mathbb{Z}_p}(C)$. There is a unique d-uple of formal power series $(f_i)_{1\leq i\leq d} \in \mathbb{Z}_p[[T_1,\dots,T_d]]^d$ such that

$$\omega = \sum_{i=1}^{d} f_i(t_1,\dots,t_d)dt_i,$$

where the equality occurs $\mathfrak{m}_C$-adically.

Let $\omega \in \Omega^1_{S/\mathbb{Q}_p}(S)$. There is $l \in \mathbb{Z}$ such that $p^l\omega \in \Omega^1_{C/\mathbb{Z}_p}(C)$. There is a unique d-uple of formal power series $(f_i)_{1\leq i\leq d} \in \mathbb{Q}_p[[T_1,\dots,T_d]]^d$ such that $\mathfrak{m}_S$-adically,

$$\omega = \sum_{i=1}^{d} f_i(t_1,\dots,t_d)dt_i,$$

and each $p^l f_i$ has coefficients in $\mathbb{Z}_p$.

Proof. – We know that $\Omega^1_{S/\mathbb{Q}_p}(S) = \Omega^1_{C/\mathbb{Z}_p}(C)[p^{-1}]$ and $\Omega^1_{C/\mathbb{Z}_p}(C) = \Omega^1_{Y/\mathbb{Z}_p,z}$ is free of rank d because Y is smooth of relative dimension d over $\mathbb{Z}_p$ at z. Now, one easily checks that $\Omega^1_{C/\mathbb{Z}_p}$ is generated by the dt_i, modulo the maximal ideal of $\mathcal{O}_C(C) = \mathcal{O}_{Y,z}$. By Nakayama, the dt_i generate $\Omega^1_{C/\mathbb{Z}_p}$. But there are d of them, the rank of $\Omega^1_{C/\mathbb{Z}_p}$. Thus, the dt_i are a basis of this module. The rest follows by localizing to make p invertible, and using the fact that $\mathcal{O}_C(C)$ is a local ring with $\mathfrak{m}_C$-adic completion $\mathbb{Z}_p[[t_1,\dots,t_d]]$. □

A.2 Differential forms on abelian varieties

This part aims at giving proofs as elementary as possible of the results on abelian varieties we will need to construct Coleman integrals. The properties of abelian varieties can be consulted, for instance, in [30].

Theorem 2.1 *Let $G \to \operatorname{Spec} k$ be a smooth connected group scheme (hence integral). Then $\Omega^1_{G/k}$ is a trivial vector bundle. Moreover, if G is proper over k, then, if $c \in G(k)$, the reduction $H^0(G,\Omega^1_{G/k}) \to \left(\Omega^1_{G/k}\right)_c \otimes_{\mathcal{O}_{G,c}} \kappa(c) = T^*_{G,c}$ is an isomorphism.*

Proof. – Consider the group scheme $G \times_k G$, the left and right projections p_1 and p_2, the multiplication $m : G \times_k G \to G$. The following diagrams are easily seen to be Cartesian:

$$\begin{array}{ccc} G \times_k G & \xrightarrow{p_2} & G \\ \downarrow{\scriptstyle p_1} & & \downarrow \\ G & \longrightarrow & \operatorname{Spec} k \end{array} \qquad \begin{array}{ccc} G \times_k G & \xrightarrow{m} & G \\ \downarrow{\scriptstyle p_1} & & \downarrow \\ G & \longrightarrow & \operatorname{Spec} k \end{array}$$

We deduce the following isomorphisms of vector bundles:

$$p_1^*\Omega^1_{G/k} \oplus p_2^*\Omega^1_{G/k} \cong \Omega^1_{G\times_k G/k}$$
$$p_1^*\Omega^1_{G/k} \oplus m^*\Omega^1_{G/k} \cong \Omega^1_{G\times_k G/k}$$

where the map $f^*\Omega^1_{G/k} \to \Omega^1_{G\times_k G/k}$ is the canonical map for $f : G \to G \times_k G$ being p_i or m. It follows that $p_2^*\Omega^1_{G/k}$ and $m^*\Omega^1_{G/k}$ are two vector subbundles of $\Omega^1_{G\times_k G/k}$ that have a common supplementary subsheaf, so they are isomorphic. Pulling back by the map $(\mathrm{id}, 0) : G \to G \times_k G$, we get an isomorphism $\Omega^1_{G/k} = \mathrm{id}^*\,\Omega^1_{G/k} \cong 0^*\Omega^1_{G/k}$. The right-hand side is the pull-back by the structural morphism of $e^*\Omega^1_{G/k}$, which is a coherent sheaf on $\operatorname{Spec} k$, so is free. Thus so is $\Omega^1_{G/k}$.

If G is proper over k, G is smooth so locally integral, G is connected so G is integral. By [25, Proposition 3.3.18], $\mathcal{O}_G(G)$ is an integral algebra over k made with only algebraic elements, so is an algebraic field extension of k. But, we have a reduction morphism $\mathcal{O}_G(G) \to \kappa(e)$, which must thus be injective. So $\mathcal{O}_G(G) = k$ and the conclusion follows. □

Lemma 2.2 *Let $G \to \operatorname{Spec} k$ be a smooth group scheme with unit section e and multiplication $m : G \times_k G \to G$. Define $i_1 = (\mathrm{id}, e) : G \to G \times_k G$, $i_2 = (e, \mathrm{id}) : G \to G \times_k G$.*

- *The tangent maps to i_1 and i_2 are injections giving an isomorphism of k-vector spaces $T_{G,e} \oplus T_{G,e} \to T_{G\times_k G,(e,e)}$, the coordinate projections being given by the tangent maps of the projections.*
- *In this decomposition, the tangent map to m at (e,e) maps the pair $(x,y) \in T_{G,e} \oplus T_{G,e}$ to $x+y \in T_{G,e}$.*

Proof. – The first part is a general fact from algebraic geometry: it works with two k-schemes of finite type with rational points. It is enough to work in the affine case, that is, A, B are finite type k-algebras with maximal ideals $\mathfrak{m}_A$ and $\mathfrak{m}_B$ such that the quotients are k, then, in $A \otimes_k B$, $\mathfrak{m}_A$ and $\mathfrak{m}_B$ generate a maximal ideal μ with residual field k. If we denote i_A, i_B the projections $A \to k$, $B \to k$, p_A, p_B the injections $A \to A \otimes_k B$, $B \otimes_k B$ (the letters are consistent with the scheme-theoretical interpretation instead of the ring-theoretical ones), then we want to show (before taking duals) that $i.$ induce a map $\mu/\mu^2 \to \mathfrak{m}_\cdot/\mathfrak{m}_\cdot^2$, of which a section is $p. : \mathfrak{m}_\cdot/\mathfrak{m}_\cdot^2 \to \mu/\mu^2$, such that μ/μ^2 becomes by (i_A, i_B) the product of both $\mathfrak{m}_\cdot/\mathfrak{m}_\cdot^2$. Note that if $x \in \mathfrak{m}_A$, $y \in \mathfrak{m}_B$, $x \otimes 1 + 1 \otimes y \in \mu$ has image (x,y); if $z \in \mu/\mu^2$ has image 0, we can write it, up to μ^2 elements, as some $x \otimes 1 + 1 \otimes y$. So its image is (x,y), thus x must be in $\mathfrak{m}_A^2$, y must be in $\mathfrak{m}_B^2$ and $z = 0 \bmod \mu^2$.

For the second part, as the tangent map must be k-linear, there are endomorphisms u, v of $T_{G,e}$ such that the tangent map of m is written, in the decomposition, $x \oplus y \longmapsto u(x) + v(y)$. But, since $m \circ i_1 = \mathrm{id}$, it follows that u is the tangent map at e of id_G, so $u = \mathrm{id}$. Similarly, $v = \mathrm{id}$ and we are done. □

Theorem 2.3 *Let $G \to \operatorname{Spec} k$ a smooth proper geometrically connected group scheme. Let $p_1, p_2, m : G \times_k G \to G$ be the left and right projections, and the multiplication, respectively. Then, if ω is a global 1-form on G, the following equality holds in $H^0(G \times_k G, \Omega^1_{G\times_k G/k})$: $m^*\omega = p_1^*\omega + p_2^*\omega$.*

Proof. – $G \to \operatorname{Spec} k$ is smooth proper geometrically connected, so $G \times_k G \to \operatorname{Spec} k$ is smooth proper connected. So the vector bundle of its 1-forms is trivial, and the equality above holds if it holds at the unit point (e,e). But at the unit point, this version is exactly the dual of the lemma above. □

Corollary 2.4 *If $A \to \operatorname{Spec} k$ is an abelian variety, the global 1-forms on A are translation-invariant.*

Proof. – Let ω be a global 1-form on A, let $c_1 \in A(k)$, let c denote the morphism $A \to \operatorname{Spec} k \xrightarrow{c_1} A$. We know that in $A \times_k A$, $m^*\omega = p_1^*\omega + p_2^*\omega$. So, in the vector bundle $(\mathrm{id}, c)^*\Omega^1_{A\times A/k}$, we have $(\mathrm{id}, c)^*(m^*\omega) = (\mathrm{id}, c)^*(p_1^*\omega) + (\mathrm{id}, c)^*(p_2^*\omega)$. Applying the canonical map $(\mathrm{id}, c)^*\Omega^1_{A\times A/k} \to \Omega^1_{A/k}$, it follows $t_c^*\omega = \omega + c^*\omega$, where $c^*\omega$ is given by the canonical map for the constant morphism $c : A \to A$:

$$c^*\Omega^1_{A/k} \xrightarrow{\mathrm{can}} \Omega^1_{A/k} \xrightarrow{\alpha} \Omega^1_c \to 0.$$

Now, as c is the composition of the structural morphism f and a closed immersion $c_1 : \operatorname{Spec} k \to A$, we also have a canonical exact sequence $f^*\Omega^1 c_1 \to \Omega^1_c \to \Omega^1_{A/k} \to 0$. The first term is zero as c_1 is a closed immersion, so Ω^1_c is isomorphic to $\Omega^1_{A/k}$ so is a free vector bundle of same rank. Therefore, the map α is a surjection between isomorphic free $\mathcal{O}_A$-modules, so is an isomorphism. Thus the map can is zero and the result follows. □

Theorem 2.5 *Let $A \to \operatorname{Spec} k$ be an abelian variety in characteristics not 2. Then global 1-forms on A are closed.*

Proof. – Consider the map $[2] : A \to A$. It acts on the tangent space of the unit element as multiplication by 2. As $\Omega^1_{A/k}$ is free, so is $\Omega^2_{A/k}$; the map $[2]^*$ acts on the vector spaces of these sheaves at the unit point as 2 and 4 respectively, because of the construction of Ω^2. Therefore, the same holds for global sections of these sheaves. So if ω is a global 1-form, $4d\omega = [2]^*d\omega = d([2]^*\omega) = d(2\omega) = 2d\omega$ so $d\omega = 0$. □

A.3 Proof of Coleman's theorem

In this section, we provide a proof of the Coleman theorem, admitting only the following fact: if a smooth projective geometrically connected curve over $\mathbb{Q}_p$ has a smooth proper model over $\mathbb{Z}_p$ (we say it has *good reduction mod p*), then its Jacobian (over $\mathbb{Q}_p$) has good reduction mod p. We actually construct integrals with the desired properties over all abelian varieties over $\mathbb{Q}_p$ with good reduction at p. The Coleman theorem (at least, the version we are using here) follows from the properties of the Jacobian and in

particular the isomorphism $j^* : H^0(J, \Omega^1) \to H^0(X, \Omega^1)$ for a smooth projective geometrically connected curve X over any field, its Jacobian J and an Abel-Jacobi map $j : X \to J$.

We consider V an abelian variety over $\mathbb{Q}_p$ and A its Néron model over $\mathbb{Z}_p$, smooth of relative dimension d.

Definition V has good reduction mod p if V has a smooth proper model over $\mathbb{Z}_p$.

Lemma 3.1 *V has good reduction if and only if A is proper over $\mathbb{Z}_p$.*

Proof. – The "if" part is easy. We prove the "only if": let Z be a smooth proper model of V over $\mathbb{Z}_p$. By the universal property of Neron models, the identity on the generic fiber induces a $\mathbb{Z}_p$-morphism $f : Z \to A$. Now, f is the composition of the closed immersion $Z \times_A A \to Z \times_{\mathbb{Z}_p}$ and the proper morphism $Z \times_{\mathbb{Z}_p} A \to A$, so f is closed. Thus the complement C of the set-theoretical image of f is an open subset of A completely contained in its closed fiber: as $A \to \operatorname{Spec} \mathbb{Z}_p$ is smooth between Noetherian schemes, the image of C in $\operatorname{Spec} \mathbb{Z}_p$ is open and contained in the closed point. So it must be empty and f is surjective. Now, $A \to \operatorname{Spec} \mathbb{Z}_p$ is of finite type, separated, so consider a morphism $B \to \operatorname{Spec} \mathbb{Z}_p$. Then we know that the closed map $c_B : Z \to_{\mathbb{Z}_p} B \to B$ decomposes into $f_B : Z \times_{\mathbb{Z}_p} B \to A \times_{\mathbb{Z}_p} B$ and $p_B : A \times_{\mathbb{Z}_p} B \to B$. As f is onto, f_B is onto as well. So if $T \subset A \times_{\mathbb{Z}_p} B$ is a closed subset, then $p_B(S) = c_B(f_B^{-1}(S))$ is closed.□

In the rest of the subsection, we assume V has good reduction mod p.

Lemma 3.2 *The reduction mod p map $V(\mathbb{Q}_p) \to A(\mathbb{F}_p)$ is a group homomorphism.*

Proof. – The applications $p : A(\mathbb{Z}_p) \to A(\mathbb{F}_p)$ and $g : A(\mathbb{Z}_p) \to A(\mathbb{Q}_p)$ are group homomorphisms, the latter is a bijection thus a group isomorphism, and the reduction mod p is $p \circ g^{-1}$. □

Proposition 3.3 *Let $z \in A(\mathbb{F}_p)$, consider a system of uniformizers $t_1, \dots, t_d$ at z. Let ω be a global differential on V. The pull-back u of ω to the schematic residue disk S of z can be written as $\sum_{i=1}^{d} F_i(t_1, \dots, t_d)dt_i$, where the F_i are formal power series in d variables and coefficients in $\mathbb{Q}_p$ with bounded absolute value, and the equality holds $(t_i)_{1 \leq i \leq d}$-adically in $\mathcal{O}_S(S)$. Moreover, there exists (up to an additive constant) a unique formal power series F in d variables with coefficients in $\mathbb{Q}_p$ such that for every $1 \leq i \leq d$, $F_i = \frac{\partial F}{\partial T_i}$. Finally, a coefficient of degree d in F has p-adic absolute value at most polynomial in d.*

Proof. – The first part stems from the facts of section A.1. For the second part, we use the fact from A.2 that ω is closed, so $du = 0$. As $\Omega^1_S(S)$ has basis the dt_i, it follows that (t_i)-adically in $\mathcal{O}_S(S)$, the series $\frac{\partial F_i}{\partial T_j}(t_1, \dots, t_d)$ converge, their sums are the $s_{i,j}$ and satisfy $s_{i,j} = s_{j,i}$. Multiplying by a large power of p, we may assume that all the coefficients of the power series are in $\mathbb{Z}_p$. Thus the identity holds in $\mathcal{O}_{A,z}$ and in particular in its completion $\mathbb{Z}_p[[t_1, \dots, t_d]]$. Thus $\frac{\partial F_i}{\partial T_j} = \frac{\partial F_j}{\partial T_i}$. The rest is simply algebraic manipulation of formal power series, and the identity $|n|_p^{-1} \leq |n|_{\text{arch}}$ for integers n. □

Definition Let us keep the same notations. Let $P, Q \in V(\mathbb{Q}_p)_z$. We define the *tiny integral* from P to Q of ω as the quantity $\int_P^Q \omega = F(t_1(Q), \dots, t_d(Q)) - F(t_1(P), \dots, t_d(P)) \in \mathbb{Q}_p$.

Theorem 3.4 *$\int_P^Q \omega$ is well-defined does not depend on a choice of uniformizers.*

Proof. – The definition (dependent on a choice of uniformizers) of the integral works because $F((t_i(Q))_{1 \leq i \leq d})$ is the sum of a series in $\mathbb{Q}_p$ such that a term of degree d has p-adic norm at most p^{-d} (contribution of $t_i(Q)$) times a polynomial in d (the coefficient of F), so the series is normally convergent.

Changing the system of uniformizers in full generality corresponds to applying an invertible (because it must be invertible in the local ring, as we are changing $\mathbb{F}_p$-bases in $\mathfrak{m}_{A,z}/\mathfrak{m}_A, z^2$) $(n+1) \times (n+1)$ square matrix with first unit first row to the (vertical) vector $(p, t_1, \dots, t_d)$. Such a matrix can be decomposed in a product of elementary operations, corresponding to elementary uniformizer changes: permutations, t_i replaced by $t_i - ut_j$ or $t_i - up$, $u \in \mathcal{O}_{A,z}$ or t_i replaced by $u't_i$, $u' \in \mathcal{O}_{A,z}^\times$.

Permutations are the easy case. All three other are treated the same way: we write explicitly how the basis of differential forms changes, how the F_i transform, and thus how F must transform. We treat the case of t_i becoming $t_i - ut_j$, which seems the most difficult case. We use superscript o for the original power series, and n for the new ones. The new system of uniformizers is denoted $s_1, \dots, s_d$ to avoid confusion, even though only s_i differs from t_i: $s_i = t_i - ut_j$.

We can write $du = \sum_{k=1}^{d} u_k dt_k$, where $u_k = \frac{\partial U}{\partial T_k}(t_1, \ldots, t_d)$ and $u = U(t_1, \ldots, t_d)$ in $\mathfrak{m}_{A,z}$-adic topology, so that

$$ds_i = (1 - t_j u_i)\, dt_i - (u + u_j t_j)\, dt_j - \sum_{k \notin \{i,j\}} t_j u_k dt_k.$$

Thus, if $k \neq i, j$, $F_k^n(s_1, \ldots, s_d) = F_k^o(t_1, \ldots, t_d) + \frac{t_j u_k}{1 - t_j u_i} F_i^o(t_1, \ldots, t_d)$. Moreover, $F_j^n(s_1, \ldots, s_d) = F_j^o(t_1, \ldots, t_d) + \frac{t_j u_j + u}{1 - t_j u_i} F_i^o(t_1, \ldots, t_d)$ and $F_i^n(s_1, \ldots, s_d) = \frac{1}{1 - t_j u_i} F_i^o(t_1, \ldots, t_d)$. It follows that formally,

$$\begin{aligned}
F_n^k(T_1, \ldots, T_i - T_j U, \ldots, T_d) &= F_k^o(T_1, \ldots, T_d) + \frac{T_j U_k}{1 - T_j U_i} F_i^o(T_1, \ldots, T_d), \quad k \neq i, j \\
F_j^n(T_1, \ldots, T_i - T_j U, \ldots, T_d) &= F_j^o(T_1, \ldots, T_d) + \frac{T_j U_j + V}{1 - T_j U_i} F_i^o(T_1, \ldots, T_d)) \\
F_i^n(T_1, \ldots, T_i - T_j U, \ldots, T_d) &= \frac{1}{1 - T_j U_i} F_i^o(T_1, \ldots, T_d).
\end{aligned}$$

Now, let $F^m = F^n(T_1, \ldots, T_i - T_j U, \ldots, T_d)$. One easily checks that $\frac{\partial F^m}{\partial T_k} = F_k^o$, so that F^m is F^o up to an additive constant, and the conclusion follows. □

Theorem 3.5 *With the same notations, take $R \in V(\mathbb{Q}_p)$. Then $\int_P^Q \omega = \int_{P+R}^{Q+R} \omega$, both members being tiny integrals.*

Proof. – By the universal property of Néron models the translation by R in V induces a $\mathbb{Z}_p$-morphism t_R from A to itself. Using the explicit inverse and the uniqueness in the universal property, we get that $R \to t_R \in \mathrm{Aut}_{\mathbb{Z}_p}(A)$ is a group homomorphism, and each t_R preserves residue disks.

Let $z' \in A(\mathbb{F}_p)$ be the point to which $P + R$ and $Q + R$ reduce and let S' its schematic residue disk. We have an isomorphism $(t_R)^\# : \mathcal{O}_{A,z'} \to \mathcal{O}_{A,z}$. Let $s_1, \ldots, s_d$ be uniformizers at z', write $\omega_{|S'} = \sum_{i=1}^{d} F_i(s_1, \ldots, s_d) ds_i$. Let F be as in the integral construction, a formal power series the formal gradient of which is (F_i). Let S be the schematic residue disk at z; let the $u_i = (t_R)^\#(s_i)$ be our system of uniformizers at z. Then $s_i(P + R) = u_i(P)$, and similarly for Q. By A.2,

$$\omega_{|S} = (t_R^* \omega)_{|S} = ((t_R)^\#)_* \omega_{|S'} = \sum_{i=1}^{d} F_i(u_1, \ldots, u_d) du_i,$$

thus

$$\int_P^Q \omega = F(u.(Q)) - F(u.(P)) = F(s.(Q + R)) - F(s.(P + R)) = \int_{P+R}^{Q+R} \omega.$$

□

Corollary 3.6 *In particular, if $z = 0_{A(\mathbb{F}_p)}$, $O = 0_{A(\mathbb{Q}_p)}$, then $P \in V(\mathbb{Q}_p)_z \longmapsto \int_O^P \omega$ is a group homomorphism.*

Proof. –

$$\int_O^{P+Q} \omega = \int_O^P \omega + \int_P^{P+Q} \omega = \int_O^P \omega + \int_O^Q \omega,$$

where the first equality stems directly from the definition and the second one follows from the theorem. □

Definition With the same notations, $A(\mathbb{F}_p)$ is finite nonempty; let c denote its cardinality. For any two points $P, Q \in V(\mathbb{Q}_p)$, cP and cQ are in the residue disk of $0_{A(\mathbb{F}_p)}$, and we define the integral of ω from P to Q to be $\int_P^Q \omega = \frac{1}{c} \int_{cP}^{cQ} \omega$, where the right-hand side is a tiny integral.

Now, we are equipped to prove Coleman's theorem.

Proof. – Since we admitted the curve-specific part, it remains to check that the pairing is bi-additive and can be computed with power series on residue disks.

We first notice that from the properties of tiny integrals, the integral we defined matches the tiny integral on the residue disk of $0_{A(\mathbb{F}_p)}$. We also notice that this definition of integral is translation-invariant. It follows that the two bounds of the integral are in the same residue disk, the integral is the same as the tiny integral. After these, the bi-additivity is obvious. □

B Non-abelian continuous group cohomology

In this section, we recall the bases of non-abelian group cohomology.

Definition Let G, U be two topological groups, and consider an continuous action $G \times U \to U$. A continuous map $f : G \to U$ is a cocycle if for each $g, h \in G$, $f(gh) = f(g)(g \cdot f(h))$. The set of such cocycles is denoted as $Z^1(G, U)$.

In the rest of the section, we keep the notations of this definition.

Lemma 0.1 *There is a natural action of R to $Z^1(G, U)$, given by, for $z \in R, f \in Z^1(G, R)$,*

$$(z \cdot f) : h \in G \longmapsto zf(g)(g \cdot z^{-1}).$$

Proof. – First, we need to check that $z \cdot f$ is a cocycle. Indeed, for $g, h \in G$,

$$\begin{aligned}(z \cdot f)(gh) &= zf(gh)((gh) \cdot z^{-1}) = zf(g)(g \cdot f(h))(g \cdot (h \cdot z^{-1})) = zf(g)(g \cdot z^{-1})(g \cdot (zf(h)(h \cdot z^{-1})))\\ &= (z \cdot f)(g)(g \cdot (z \cdot f)(h)).\end{aligned}$$

Clearly, the neutral element of G leaves every cocycle unchanged. Now, let $z, y \in U$, $f \in Z^1(G, U)$, $g \in G$. Then

$$((zy) \cdot f)(g) = zyf(g)(g \cdot (y^{-1}z^{-1})) = z(yf(g)(g \cdot y^{-1}))(g \cdot z^{-1}) = [z \cdot (y \cdot f)](g).$$

□

Definition The quotient set $U \backslash Z^1(G, U)$ is denoted as $H^1(G, U)$. We always consider it as an object of the category **PtSet** of pointed sets, because of the trivial cocycle given by the constant function equal to the neutral element.

Remark If U is a commutative group, then $Z^1(G, U)$ is naturally a subgroup of the abelian group of functions $G \to U$. Moreover, $H^1(G, U)$ is a quotient of $Z^1(G, U)$ by the subgroup generated by the $f^{-1}(z \cdot f)$, $f \in Z^1(G, U), z \in U$. In the former sentence, f^{-1} is the function $g \longmapsto f(g)^{-1}$ and the operation between f^{-1} and $z \cdot f$ is the group multiplication in $Z^1(G, U)$, that is, the pointwise multiplication.

Searching for natural examples of cocycles yields the following construction:

Definition A principal U-bundle over G is a topological space P endowed with continuous actions from G and U, such that

- G has a left action and U has a right action.
- U acts freely and transitively and if $p \in P$, the continuous bijection $u \in U \longmapsto p \cdot u \in P$ is a homeomorphism. (in other words, when forgetting about the actions of G, the choice of any base-point identifies P to U)
- The actions are compatible, that is, for any $p \in P, z \in U, g \in G$, $g \cdot_{G,P} (p \cdot_{P,U} z) = (g \cdot_{G,P} p) \cdot_{P,U} (g \cdot_{G,U} z)$.

We adopt the following notations in the next steps for the sake of simplicity: $\cdot$ is the action of G on R, $g(p)$ denotes the action of G on P and $p.u$ is the action of U on P.

Proposition 0.2 *Let P be a principal U-bundle over G. For any $p \in P$, the function $f_p : g \in G \longmapsto f_p(g) \in U$ such that $p.f_p(g) = g(p)$ is a cocycle. Furthermore, if $z \in U$, $f_{p.z} = (z^{-1} \cdot f_p)$.*

Proof. – Let $g, h \in G$, then

$$p.(f_p(g)(g \cdot f_p(h))) = p.f_p(g).(g \cdot f_p(h)) = g(p).(g \cdot f_p(h)) = g(p.f_p(h)) = g(h(p)) = ((gh)(p),$$

thus f_p is a cocycle. If $z \in U$, $g \in G$,

$$(p.z).(z^{-1} \cdot f_p)(g) = (p.z).(z^{-1} f_p(g)(g \cdot z)) = (p.f_p(g)).(g \cdot z) = g(p).(g \cdot z) = g(p.z),$$

which ends the proof. □

Definition Let P be a principal U-bundle over G. The element of $H^1(G,U)$ defined by f_p ($p \in P$) does not depend of p, and is denoted as $[f_P]$.

Actually, this construction can be seen as an alternative definition of $H^1(G,U)$.

Proposition 0.3 *Let $\alpha \in H^1(G,U)$. There exists a principal U-bundle P over G with $\alpha = [f_P]$.*

If P, Q are two principal U-bundles over G such that $[f_P] = [f_Q]$, then there is a bijection $P \to Q$ that is equivariant for the actions of both G and U.

In other words, through $P \to [f_P]$, $H^1(G,U)$ is the space of isomorphism classes of principal U-bundles over G.

Proof. – Let $f \in Z^1(G,U)$ be a cocycle represented by α. Let P be the set U, where U acts by right multiplication, and G acts by $g(p) = f(g)(g \cdot p)$, $p \in P$. Note that $f(e_G) = f(e_G e_G) = f(e_G)(e_G \cdot f(e_G)) = f(e_G)^2$ so $f(e_G) = e_U$. Thus $e_G(p) = p$ for all $p \in P$. Futhermore, for $g, h \in G$, $p \in P$, $g(h(p)) = f(g)(g \cdot h(p)) = f(g)(g \cdot h(p)) = f(g)(g \cdot (f(h)(h \cdot p)) = f(g)(g \cdot f(h))(gh \cdot p) = f(gh)(gh \cdot p) = (gh)(p)$, so we have defined a left action of G on P. Finally, $g(p.z) = f(g)(g \cdot (pz)) = f(g)(g \cdot p)(g \cdot z) = g(p)(g \cdot z)$, for $g \in G, p \in P, z \in U$, so the actions of G and U on P are compatible. Therefore P is a principal U-bundle over G.

Let $p \in P$, $q \in Q$, we know that for some $z \in R$, $f_q = z \cdot f_p$. Thus, with $p' = p.z^{-1}$, $f_{p'} = f_q$. We define an application $L : P \to Q$ such that for any $r \in U$, $L(p'.r) = q.r$. Clearly L is bijective and equivariant for the action of U; as $f_{p'} = f_q$, we also have, for $g \in G$, $L(g(p')) = g(q)$. Now, let $s \in P$, write $s = p'.z$, $z \in U$. For $g \in G$, $L(g(s)) = L(g(p').(g \cdot z)) = L(g(p')).(g \cdot z) = g(q).(g \cdot z) = g(q.z) = g(L(s))$, so L is the claimed bijection. □

This cohomology space satisfies some functoriality properties with respect to a suitable notion of morphism. We consider the category $\mathscr{C}$ of pairs (G,U) of topological groups endowed with a continuous left action of G over U. A morphism of $\mathscr{C}$ from (G,U) to (H,V) is a pair (p,q) of continuous maps, $p : H \to G$ and $q : U \to V$ satisfying, for all $y \in U$, $h \in H$, $q(p(h)y) = hq(y)$. Two pairs $(p,q) : (G,U) \to (H,V)$ and $(p',q') : (H,V) \to (K,W)$ of morphisms compose to $(p' \circ p, q' \circ q) : (G,U) \to (K,W)$ (which is, indeed,a morphism).

Proposition 0.4 *Let $(G,U), (H,V)$ be two objects of $\mathscr{C}$ and let $(p,q) : (G,U) \to (H,V)$. Then $f \in Z^1(G,U) \longmapsto q \circ f \circ p \in Z^1(H,V)$ is well-defined and descends to H^1 on both sides. Thus we have a functor $F : \mathscr{C} \to$ PtSet mapping a pair (G,U) to its cohomology space $H^1(G,U)$.*

Proof. – The statement relies on similar computations. □

Remark $H^1(G,1)$ being trivial, if we have a trivial morphism $(\mathrm{id}, f) : (G,A) \to (G,B)$, $H^1(\mathrm{id}, f)$ is the trivial map.

To justify this functorial (if low-degree only) cohomological notation theory, we construct some exact sequences:

Theorem 0.5 *Let G be a topological group, and consider $(G,A), (G,B), (G,C)$ three objects of $\mathscr{C}$, with morphisms $(\mathrm{id}, u) : (G,A) \to (G,B)$ and $(\mathrm{id}, v) : (G,B) \to (G,C)$. Assume that $1 \to A \xrightarrow{u} B \xrightarrow{v} C \to 1$ is an exact sequence of groups, with u a homeomorphism onto its image, and v be a topological quotient map. Let $\delta : C^G \to H^1(G,A)$ be given the reduction of, for a given $c = v(b) \in C^G$, $g \longmapsto u^{-1}(b^{-1}(g \cdot b))$. Then δ is well-defined (i.e. doesn't depend on the choice of b) and the following sequence is exact (the first three arrows as morphisms of groups, the three last ones as morphisms of pointed sets):*

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G,A) \xrightarrow{H^1(\mathrm{id},u)} H^1(G,B) \xrightarrow{H^1(\mathrm{id},v)} H^1(G,C).$$

Proof. – First, we check the good definition of δ. For a given $c = v(b) \in C^G$, $b \in B$, if $g \in G$, $v(b^{-1}(g \cdot b)) = v(b)^{-1}(g \cdot v(b)) = c^{-1}(g \cdot c) = e_C$ thus $b^{-1}(g \cdot b) \in u(A)$. If now we consider $g, h \in G$, $b^{-1}(gh \cdot b) = b^{-1}(g \cdot b)(g \cdot b^{-1})(g \cdot (h \cdot b)) = b^{-1}(g \cdot b)(g \cdot (b^{-1}(h \cdot b)))$, thus $c_b : g \longmapsto u^{-1}(b^{-1}(g \cdot b))$ is a cocycle. Now, we need to study what happens when we change our b, that is, b is replaced with some $b' = u(a)b$ for some $a, a' \in A$. Then, $b'^{-1}(g \cdot b') = u(a)^{-1}b^{-1}(g \cdot b)(g \cdot u(a)) = u(a^{-1}c_b(g)g \cdot a)$ and therefore $c_{b'} = (a^{-1} \cdot c_b)$, which finally shows δ to be well-defined.

For the exactness, only the exactness from C^G on needs to be checked. For $c \in C^G$, by the above computation, $\delta(c)$ is trivial iff we can write $c = v(b)$ with $b \in B$, c_b trivial, iff we can write $c = v(b)$ with $b \in B$, $b^{-1}(g \cdot b) = e_B$ for all $g \in G$, iff we can write $c \in v(B^G)$.

For the exactness in $H^1(G, A)$, note that a cocycle $f \in Z^1(G, A)$ has trivial image in $H^1(G, B)$ iff there is some $b \in B$ such that for all $g \in G$, $u(f(g)) = b^{-1}(g \cdot b)$. But for such a b, $b^{-1}(g \cdot b) \in u(A) = \ker v$, thus $v(b) \in C^G$. Therefore, f has trivial image in $H^1(G, B)$ iff $f = c_b$, for some $b \in v^{-1}(C^G)$, so iff $[f] \in \delta(C^G)$.

For the exactness in $H^1(G, B)$, we already know that the composition of the two arrows is trivial. Now, let $f \in Z^1(G, B)$, f has a trivial image in $H^1(G, C)$ iff for some $c \in C$, for all $g \in G$, $v(f(g)) = c^{-1}(g \cdot c)$. As $v : B \to C$ is onto, f is trivial in $H^1(G, C)$ iff for some $b \in B$, for all $g \in G$, $v(f(g)) = v(b^{-1}(g \cdot b))$, that is, $v \circ (b \cdot f)$ is trivial. Now, there is a $b \in B$ such that $v \circ (b \cdot f)$ is trivial iff $b \cdot f$ has values in A, ie iff $b \cdot f$ is $u(A)$-valued, ie iff $b \cdot f = u \circ f_1$ for some $f_1 \in Z^1(G, A)$. Therefore f has a trivial image in $H^1(G, C)$ iff $[f] \in H^1(G, B)$ is in the image of $H^1(G, A)$. □

The construction of this exact sequence gives us an even better statement:

Theorem 0.6 *Let G, H be topological groups, consider $(G, A), (G, B), (G, C), (H, A'), (H, B'), (H, C')$ six objects of $\mathscr{C}$. Assume that we have a map of exact sequences of groups with the topological conditions detailed in the previous theorem: Assume furthermore that we have a map $p : H \to G$ such that*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{u} & B & \xrightarrow{v} & C & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\ 1 & \longrightarrow & A' & \xrightarrow{u'} & B' & \xrightarrow{v'} & C' & \longrightarrow & 1 \end{array}$$

$(p, a), (p, b), (p, c)$, $(\mathrm{id}_G, u), (\mathrm{id}_G, v)$, $(\mathrm{id}_H, u'), (\mathrm{id}_H, v')$ are all morphisms of $\mathscr{C}$. Then we have a morphism between the exact constructed by the previous theorem:

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & A^G & \longrightarrow & B & \longrightarrow & C & \longrightarrow & H^1(G, A) & \longrightarrow & H^1(G, B) & \longrightarrow & H^1(G, C) \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle H^1(p,a)} & & \downarrow{\scriptstyle H^1(p,b)} & & \downarrow{\scriptstyle H^1(p,c)} \\ 1 & \longrightarrow & (A')^H & \longrightarrow & (B')^H & \longrightarrow & (C')^H & \longrightarrow & H^1(H, A') & \longrightarrow & H^1(H, B') & \longrightarrow & H^1(H, C') \end{array}$$

In the rest of this annex, we define the construction of the Kummer $A(\mathbb{Q}) \otimes \mathbb{Q}_p \to H^1(G_T, V(A))$ which is used in Section 2.1 to define Selmer schemes, where A is an abelian variety over $\mathbb{Q}$, G_T is a Galois group unramified outside p and the primes of bad reduction, and $V(A) = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, where $T_p(A)$ is the Tate module of A (endowed with a Galois action).

Lemma 0.7 *Let (G, U) be objects of $\mathscr{C}$ and R be a topological ring. Assume that U is a topological R-module and that G acts R-linearly. Then $Z^1(G, U)$ is a submodule of the R-module of continuous functions $G \to U$, and $H^1(G, U)$ is the quotient of $Z^1(G, U)$ by the submodule generated by the $(z \cdot f) - f$, for $z \in U$, $f \in Z^1(G, U)$, where U is noted additively.*

Proof. – It is clear given the definitions and constructions. □

Lemma 0.8 *Let us keep the above notations, with $R = \mathbb{Z}_p$ and U free finitely generated (so as to keep topological concerns away). Then there are natural compatible isomorphisms $Z^1(G, U) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to Z^1(G, U \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ and $H^1(G, U) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to H^1(G, U \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$.*

Lemma 0.9 *Let G be a profinite group, and $((G,U_i))_{i\geq 1}$ be a projective system in $\mathscr{C}$ with each U_i finite, and the morphisms being $(\mathrm{id}, f_{j,i}) : (G,U_j) \to (G,U_i)$ for $j > i$. Let U be the projective limit of the U_i (as a topological space) and the $f_{j,i}$. Then the following statements are true:*

- *(G,U) is an object of $\mathscr{C}$, and for each i we have a morphism of $\mathscr{C}$ $(\mathrm{id}, p_i) : (G,U) \to (G,U_i)$. In other words, there exists a continuous action of G on U such that the projections $U \to U_i$ are G-equivariant.*
- *We have a projective system $H^1(G,U_i), i \geq 1$, with maps $H^1(\mathrm{id}, f_{j,i})$ for $j > i$, and we denote as P the set-theoretical projective limit.*
- *The $(\mathrm{id}, p_i) : (G,U) \to (G,U_i)$ induce maps $H^1(G,U) \to H^1(G,U_i)$ making $H^1(G,U)$ the projective limit of the system above.*
- *If the U_i are topological modules over a ring R and $f_{j,i}$ are R-linear, all the constructions, maps, and limits are defined as R-modules.*

Proof. – A formal check using the definition shows that $Z^1(G,U)$ is the projective limit of the $Z^1(G,U_i)$ under the natural morphisms $f_{j,i}$, $j > i$, and the generators of the sub-modules match. □

The following lemma is well-known, being closely related to the Ogg-Shafarevich criterion (see [36]), but we include nonetheless a brief proof for the sake of completeness.

Lemma 0.10 *Let A be an abelian variety over $\mathbb{Q}$ with good reduction at a prime number p. Let $\ell \neq p$ ne a different prime, and $x \in A$ be a closed point with residue field F unramified at ℓ. Then every closed point $y \in A$ with $p \cdot y = x$ has residue field unramified at ℓ. Moreover, such y always exist.*

Proof. – By [30, Proposition 8.1, Theorem 8.2], multiplication by p is a finite étale surjective map $A \to A$, moreover by e.g. [25, Proposition 2.5.10], the pre-image of a closed point is a closed point, which settles the second part.

For the first statement, let V be the Néron model over $\mathbb{Z}_{(\ell)}$ of A. By [30, Proposition 20.7], the multiplication by p from V to itself is finite étale (between proper $\mathbb{Z}_{(\ell)}$-schemes, hence surjective). Let v be any place of F unramified above ℓ: by the valuative criterion of properness, x extends to a morphism $\overline{x} : \operatorname{Spec} \mathcal{O}_v \to V$, and let $x_r \in V$ be the image of the closed point. Let $y \in A$ be a closed point with $p \cdot y = x$, with residual field $L \supset F$. Let w be any place above L, similarly y extends to $\overline{y} : \operatorname{Spec} \mathcal{O}_w \to V$, and denote by y_r the image of the closed point.

It follows that in V, $p \cdot y_r = x_r$ (indeed, $p \circ \overline{y}$ and $\overline{x} \circ (\operatorname{Spec} \mathcal{O}_w \to \operatorname{Spec} \mathcal{O}_v)$ are two morphisms $\operatorname{Spec} \mathcal{O}_w \to V$ extending $x \circ (\operatorname{Spec} L \to \operatorname{Spec} F) : \operatorname{Spec} L \to A$). Thus, as the multiplication by p is unramified in V, $\mathcal{O}_{V,x_r} \to \mathcal{O}_{V,y_r}$ is an unramified morphism of local rings.

But the following diagram commutes, with all morphisms being maps of local rings, the horizontal arrows being onto:

$$\begin{array}{ccc} \mathcal{O}_{V,x_r} & \xrightarrow{\overline{x}} & \mathcal{O}_v \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle inc} \\ \mathcal{O}_{V,y_r} & \xrightarrow{\overline{y}} & \mathcal{O}_w \end{array}$$

It follows that $\mathcal{O}_v \to \mathcal{O}_w$ is unramified, so that $\mathbb{Z}_{(\ell)} \to \mathcal{O}_w$ is unramified and thus $L/\mathbb{Q}$ is unramified at ℓ. □

Proposition 0.11 *Let A be an abelian variety over $\mathbb{Q}$ with good reduction at a prime number p, and let G be a quotient of the absolute Galois group of $\mathbb{Q}$ that corresponds to the maximal extension $K/\mathbb{Q}$ unramified outside p and the primes of bad reduction of A. For each $n \geq 1$, we have an exact sequence*

$$1 \to A[p^n](\mathbb{Q}) \to A(\mathbb{Q}) \xrightarrow{p^n} A(\mathbb{Q}) \xrightarrow{\delta_n} H^1(G, A[p^n](K))$$

that yields the following commutative diagram of $\mathbb{Z}_p$-modules, for each $n \geq 1$:

Proof. – Consider the following morphism of exact sequences (Lemma 0.10 shows that $pA(K) = A(K)$) of discrete groups with continuous actions of G: □

$$\begin{array}{ccc} A(\mathbb{Q})/p^{n+1}A(\mathbb{Q}) & \xrightarrow{\delta_{n+1}} & H^1(G, A[p^{n+1}](K)) \\ \downarrow & & \downarrow p \\ A(\mathbb{Q})/p^{n}A(\mathbb{Q}) & \xrightarrow{\delta_{n}} & H^1(G, A[p^{n}](K)) \end{array}$$

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A[p^{n+1}](K) & \longrightarrow & A(K) & \xrightarrow{p^{n+1}} & A(K) & \longrightarrow & 1 \\ & & \downarrow p & & \downarrow p & & \downarrow \mathrm{id} & & \\ 1 & \longrightarrow & A[p^{n}](K) & \longrightarrow & A(K) & \xrightarrow{p^{n}} & A(K) & \longrightarrow & 1 \end{array}$$

Corollary 0.12 *If A is an abelian variety over $\mathbb{Q}$ with good reduction at a prime number p, with the notations above, then these maps above combine into a natural $\mathbb{Z}_p$-linear homomorphism from the p-adic completion of $A(\mathbb{Q})$ into $H^1(G, T_p(A))$. It induces a natural $\mathbb{Q}_p$-linear map $A(\mathbb{Q})\otimes\mathbb{Q}_p \to H^1(G, T_p(A)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p)$.*

Proof. – The only nontrivial part of the proof is the fact that the projective limit of the $A[p^n](K)$ is the Tate module of A, ie that any p^n-torsion point has a residue field unramified at any prime number $\ell \neq p$ of good reduction. But this is exactly Lemma 0.10. □

References

[1] Jennifer Balakrishnan and Jan Steffen Müller, *Computational tools for Quadratic Chabauty*, http://math.bu.edu/people/jbala/2020BalakrishnanMuellerNotes.pdf, March 2020, Lecture notes at the Arizona Winter School 2020. Online; accessed on 10 June 2020.

[2] Jennifer S. Balakrishnan and Netan Dogra, *Quadratic Chabauty and rational points, I: p -adic heights*, Duke Math. J. **167** (2018), no. 11, 1981–2038.

[3] Jonathan W Bober, *Conditionally bounding analytic ranks of elliptic curves*, ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, The open book series, vol. 1, Mathematical Sciences Publishers, 2013, pp. 135–144.

[4] Li Cai, Jie Shu, and Ye Tian, *Explicit Gross-Zagier and Waldspurger formulae*, Algebra & Number Theory **8** (2014), no. 10, 2523–2572.

[5] Lucia Caporaso, Joe Harris, and Barry Mazur, *Uniformity of rational points*, J. Am. Math. Soc. **10** (1997), no. 1, 1–35.

[6] Imin Chen, *On Relations between Jacobians of Certain Modular Curves*, Journal of Algebra **231** (2000), no. 1, 414 – 448.

[7] Robert Coleman, *Torsion points on curves and p-adic abelian integrals*, Annals of Math. **121** (1985), 111–168.

[8] Bart de Smit and Bas Edixhoven, *Sur un résultat d'Imin Chen*, Mat. Res. Let. **7** (2000), no. 2, 147–153.

[9] Pierre Deligne, *Le groupe fondamental de la droite projective moins trois points*, Galois groups over $\overline{\mathbb{Q}}$ (Berkeley, CA, 1987) (Yasutaka Ihara, Kenneth Ribet, and Jean-Pierre Serre, eds.), Springer-Verlag, 1989, pp. 79–298.

[10] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, Springer, 2005.

[11] Jean Dieudonné and Alexander Grothendieck, *Éléments de géométrie algébrique*, Inst. Hautes Études Sci. Publ. Math. **4, 8, 11, 17, 20, 24, 28, 32** (1960–1967).

[12] Vesselin Dimitrov, Ziyang Gao, and Philipp Habegger, *Uniform bound for the number of rational points on a pencil of curves*, 2019.

[13] Netan Dogra and Samuel Le Fourn, *Quadratic Chabauty for modular curves and modular forms of rank one*, 2019.

[14] Bas Edixhoven, Gerard van der Geer, and Ben Moonen, *Abelian Varieties*, URL: https://gerard.vdgeer.net/AV.pdf, Online; Retrieved on March 23rd 2020.

[15] Noam D. Elkies and Zev Klagsbrun, *New rank records for elliptic curves having rational torsion*, 2020.

[16] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[17] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, Springer, 1977.

[18] Eric Katz, Joseph Rabinoff, and David Zureick-Brown, *Uniform bounds for the number of rational points on curves of small Mordell-Weil rank*, Duke Math. J. **165** (2016), no. 16, 3189–3240.

[19] Eric Katz and David Zureick-Brown, *The Chabauty-Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions*, Compos. Math. **149** (2013), no. 11, 1818–1838.

[20] Minhyong Kim, *The motivic fundamental group of $\mathbb{P}^1\backslash\{0,1,\infty\}$ and the theorem of Siegel.*, Invent. math. **161** (2005), 629–656.

[21] ———, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), 89–133.

[22] Minhyong Kim and Akio Tamagawa, *The l-component of the unipotent albanese map*, Math. Ann. **340** (2008), 223 – 235.

[23] Zev Klagsbrun, Travis Sherman, and James Weigandt, *The Elkies Curve has rank 28 subject only to GRH*, Math. Comp. **88** (2019), 837–846.

[24] Daniel Kohen and Ariel Pacetti, *Heegner points on Cartan non-split curves*, Canadian Journal of Mathematics **68** (2016), no. 2, 422–444.

[25] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, Oxford University Press, 2002.

[26] The LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org, 2020, Online; accessed 4 June 2020.

[27] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math **148** (2002), no. 1, 47–77.

[28] Barry Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques de l'IHÉS **47** (1977), 33–186 (en).

[29] William McCallum and Bjorn Poonen, *The Method of Chabauty and Coleman*, Explicit methods in number theory, Panoramas et Synthèses, vol. 36, Soc. Math. France, 2012, pp. 99–117.

[30] James Milne, *Abelian varieties*, Arithmetic Geometry (Gary Cornell and Joseph H. Silverman, eds.), Springer-Verlag, 1985, pp. 103–150.

[31] ———, *Jacobian varieties*, Arithmetic Geometry (Gary Cornell and Joseph H. Silverman, eds.), Springer-Verlag, 1985, pp. 167–212.

[32] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999.

[33] Kenneth A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. Math. **101** (1975), no. 3, 555–562.

[34] ———, *Twists of Modular Forms and Endomorphisms of Abelian Varieties*, Math. Ann **253** (1980), 43–62.

[35] Jean-Pierre Serre, *Cohomologie galoisienne*, Lecture Notes in Mathematics, Springer, 1997.

[36] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. Math. (2) **88** (1968), 492–517.

[37] Joseph H. Silverman, *The theory of height functions*, Arithmetic Geometry (Gary Cornell and Joseph H. Silverman, eds.), Springer-Verlag, 1985, pp. 151–166.

[38] ———, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer-Verlag, 1986.

[39] The Stacks Project Authors, *Stacks Project*, https://stacks.math.columbia.edu, 2020.

[40] William Stein, *Explicitly Computing the Endomorphism Rings of Abelian Modular Varieties*, https://share.cocalc.com/share/5d54f9d642cd3ef1affd88397ab0db616c17e5e0/www/papers/endo_alg/endring.pdf, 2004, Online; accessed 4 June 2020; unpublished.

[41] William A. Stein, *Modular forms: A computational approach*, URL : https://wstein.org/books/modform/stein-modform.pdf, Available online. Last visited on April 28th 2020.

[42] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214.

[43] ———, *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 3, 923–956.

[44] Shou-Wu Zhang, *Gross-Zagier formula for GL(2). II.*, Heegner points and Rankin L-series (Henri Darmon and Shou-Wu Zhang, eds.), Math. Sci. Res. Inst. Publ., vol. 49, Cambridge University Press, 2004, pp. 191–214.

[45] David Zureick-Brown, *Abelian Chabauty*, Online: http://www.math.emory.edu/~dzb/AWS2020/2020ZureickBrownNotes.pdf, March 2020, Lecture notes at the Arizona Winter School 2020. Last visited on 14 April 2020.