An explicit open image theorem for products of elliptic curves

Davide Lombardo [*]

Département de Mathématiques d'Orsay

Abstract

Let K be a number field and $E_1, \ldots, E_n$ be elliptic curves over K, pairwise non-isogenous over $\overline{K}$ and without complex multiplication over $\overline{K}$. We study the image G_∞ of the adelic representation of $\operatorname{Gal}\left(\overline{K}/K\right)$ naturally attached to $E_1 \times \cdots \times E_n$. The main result is an explicit bound for the index of G_∞ in $\left\{(x_1, \ldots, x_n) \in \operatorname{GL}_2(\hat{\mathbb{Z}})^n \bigm| \det x_i = \det x_j \quad \forall i, j\right\}$.

1 Introduction

In this work we prove an explicit, adelic surjectivity result for the Galois representation attached to a product of pairwise non-isogenous, non-CM elliptic curves, extending the result of [2]. Our main theorem is as follows:

Theorem 1.1. *Let $E_1, \ldots, E_n$, $n \geq 2$, be elliptic curves defined over a number field K, pairwise not isogenous over $\overline{K}$. Suppose that $\operatorname{End}_{\overline{K}}(E_i) = \mathbb{Z}$ for $i = 1, \ldots, n$, and denote by G_∞ the image of $\operatorname{Gal}\left(\overline{K}/K\right)$ inside*

$$\prod_{i=1}^{n} \prod_{\ell} \operatorname{Aut}(T_\ell(E_i)) \cong \operatorname{GL}_2(\hat{\mathbb{Z}})^n.$$

Set $\gamma := 10^{13}$, $\delta := \exp\exp\exp(12)$, and let $H = \max\left\{1, \log[K : \mathbb{Q}], \max_i h(E_i)\right\}$, where $h(E_i)$ denotes the stable Faltings height of E_i. The group G_∞ has index at most

$$\delta^{n(n-1)} \cdot \left([K : \mathbb{Q}] \cdot H^2\right)^{\gamma n(n-1)}$$

in

$$\Delta := \left\{(x_1, \ldots, x_n) \in \operatorname{GL}_2(\hat{\mathbb{Z}})^n \bigm| \det x_i = \det x_j \quad \forall i, j\right\}.$$

Remark 1.2. Note that the compatibility of the Weil pairing with the action of Galois forces G_∞ to be contained in Δ. Also note that we shall prove slightly more precise statements (see lemma 7.3 and theorem 7.5 below), which immediately imply theorem 1.1 by proposition 2.7 and elementary estimates.

It should be noted that it has been known since the work of Serre and Masser-Wüstholz (cf. [5], Main Theorem and Proposition 1) that the isogeny theorem (section 2 below) gives an effective bound ℓ_0 on the largest prime ℓ for which the image of the representation

$$\operatorname{Gal}\left(\overline{K}/K\right) \to \operatorname{Aut}(T_\ell(E_1 \times \cdots \times E_n))$$

does not contain $\operatorname{SL}_2(\mathbb{Z}_\ell)^n$. As it was in [2], the main difficulty in proving theorem 1.1 lies in controlling the image of the representation modulo powers of primes smaller than ℓ_0.

[*] davide.lombardo@math.u-psud.fr

The proof of theorem 1.1 is somewhat technical, so before fiddling with the details we describe the main ideas behind it. The general framework is the same as that of the proof of the non-effective open image theorem for such a product (cf. for example [9, Theorem 3.5]), with the added difficulties that naturally arise when trying to actually compute the index. In particular, when writing 'of finite index' or 'open' in the sketch that follows we tacitly imply that the index in question is explicitly computable in terms of the data. Whenever the need arises to actually quantify indices, it will be useful to work with the following 'standard' open subgroups:

Definition 1.3. *For a prime ℓ and a positive integer s we let $\mathcal{B}_\ell(s)$ be the open subgroup of $\operatorname{SL}_2(\mathbb{Z}_\ell)$ given by*

$$\left\{x \in \operatorname{SL}_2(\mathbb{Z}_\ell) \bigm| x \equiv \operatorname{Id} \pmod{\ell^s}\right\}.$$

We also set $\mathcal{B}_\ell(0) = \operatorname{SL}_2(\mathbb{Z}_\ell)$, and for non-negative integers $k_1, \ldots, k_n$ we denote by $\mathcal{B}_\ell(k_1, \ldots, k_n)$ the open subgroup $\prod_{j=1}^n \mathcal{B}_\ell(k_i)$ of $\operatorname{SL}_2(\mathbb{Z}_\ell)^n$.

Let us now describe the proof method proper. It is not hard to see that it is enough to study the intersection $G_\infty \cap \operatorname{SL}_2(\mathbb{Z}_\ell)^n$, because the determinant of elements in G_∞ can be easily understood in terms of the cyclotomic character. A short argument then shows that it suffices to consider products $E_1 \times E_2$ involving only two factors: this is done by proving that a subgroup of $\operatorname{SL}_2(\mathbb{Z}_\ell)^n$ whose projection on any *pair* of factors is of finite index is itself of finite (and explicitly bounded) index. This step will be carried out in section 3 below, and should be thought of as the 'integral' version of [10, Lemma on p. 790].

With this result at hand we are thus reduced to dealing with subgroups G of $\operatorname{SL}_2(\mathbb{Z}_\ell) \times \operatorname{SL}_2(\mathbb{Z}_\ell)$ whose projections on either factor are of finite index in $\operatorname{SL}_2(\mathbb{Z}_\ell)$. Note that the fact that this index is finite is the open image theorem for a single elliptic curve, which was proved by Serre in [12] and made explicit in [2]. We wish to show that G is of (explicitly bounded) finite index in $\operatorname{SL}_2(\mathbb{Z}_\ell)^2$, that is, we want to produce a t such that G contains $\mathcal{B}_\ell(t,t)$: this comes down to proving that the two kernels $K_i = \ker\left(G \xrightarrow{\pi_i} \operatorname{SL}_2(\mathbb{Z}_\ell)\right)$, when identified with subgroups of $\operatorname{SL}_2(\mathbb{Z}_\ell)$, are of (explicitly bounded) finite index. By symmetry, we just need to deal with K_1.

In section 4 we linearize the problem by reducing it to the study of certain $\mathbb{Z}_\ell$-Lie algebras: we give the statements of two technical results whose proof, being rather lengthy, is deferred to the companion paper [3]; while the results themselves are more complicated, the methods used to show them do not differ much from those of [2].

A simple lemma, again given in section 4, further reduces the problem of finding an integer t such that $\mathcal{B}_\ell(t)$ is contained in K_1 to the (easier) question of finding a t such that $K_1(\ell^t)$, the reduction modulo ℓ^t of K_1, is nontrivial. We exploit here the fact that $\pi_2(G)$ (the projection of G on the second factor $\operatorname{SL}_2(\mathbb{Z}_\ell)$) acts by conjugation on K_1, the latter being a normal subgroup of G: we prove that a group whose reduction modulo ℓ^t is nontrivial and that is stable under conjugation by a finite-index subgroup of $\operatorname{SL}_2(\mathbb{Z}_\ell)$ must itself be of finite index in $\operatorname{SL}_2(\mathbb{Z}_\ell)$. This reduction step is made simpler by the fact that we can work with Lie algebras instead of treating the corresponding groups directly (which might be quite complicated).

Next we ask what happens if we suppose that the smallest integer t such that $K_1(\ell^t)$ is nontrivial is in fact very large. The conclusion is that the Lie algebra of G looks 'very much like' the graph of a Lie algebra morphism $\mathfrak{sl}_2(\mathbb{Z}_\ell) \to \mathfrak{sl}_2(\mathbb{Z}_\ell)$, namely it induces an actual Lie algebra morphism when regarded modulo ℓ^N for a very large N (depending on t). Following for example the approach of Ribet (cf. the theorems on p. 795 of [10]), we would like to know that all such morphisms are 'inner', that is, they are given by conjugation by a certain matrix: it turns out that this is also true in our context, even though the result is a little less straightforward to state (cf. section 5).

In section 6 we then deal with the case of two elliptic curves, applying the aforementioned results to deduce an open image theorem for each prime ℓ. It is then an easy matter to deduce, as we do in section 7, the desired adelic result for any finite product.

Acknowledgments. The present work forms part of the author's PhD thesis, and I thank my advisor N. Ratazzi for his constant support during its writing. I would also like to thank the anonymous referee for his helpful comments.

The author gratefully acknowledges financial support from the Fondation Mathématique Jacques Hadamard (grant ANR-10-CAMP-0151-02 in the “Programme des Investissements d’Avenir”).

2 Preliminaries on isogeny bounds

The main tool that makes all the effective estimates possible is the isogeny theorem of Masser and Wüstholz [6] [7], which we employ in the explicit version proved in [1]. We need some notation: we let $\alpha(g) = 2^{10}g^3$ and define, for any abelian variety A/K of dimension g,

$$b(A/K) = b([K:\mathbb{Q}], g, h(A)) = \left((14g)^{64g^2} [K:\mathbb{Q}] \max\left(h(A), \log[K:\mathbb{Q}], 1\right)^2 \right)^{\alpha(g)}.$$

Theorem 2.1. *([1, Théorème 1.4]) Let K be a number field and A, A^* be two abelian K-varieties of dimension g. If A, A^* are isogenous over K, then there exists a K-isogeny $A^* \to A$ whose degree is bounded by $b([K:\mathbb{Q}], \dim(A), h(A))$.*

Remark 2.2. As the notation suggests, the three arguments of b will always be the degree of a number field K, the dimension g of an abelian variety A/K and its stable Faltings height $h(A)$.

We shall need a slight refinement of this bound. Following Masser [4], we introduce the following definition:

Definition 2.3. *Let A/K be an abelian variety. We say that A is a TM-product (“trivial multiplication”) over K if A is isomorphic (over K) to $A_1^{e_1} \times \cdots \times A_n^{e_n}$, where $A_1, \ldots, A_n$ are K-simple abelian varieties, mutually non-isogenous (over K) and with trivial endomorphism ring (over K).*

Adapting arguments given by Masser in [4], it is easy to prove

Theorem 2.4. *([2, Theorem 2.4]) Suppose that A/K is a TM-product over K. Let $b \in \mathbb{R}$ be a constant with the following property: for every K-abelian variety A^* isogenous to A over K there exists an isogeny $\psi : A^* \to A$ with $\deg \psi \leq b$. Then there exists an integer $b_0 \leq b$ with the following property: for every K-abelian variety A^* isogenous to A over K there exists an isogeny $\psi_0 : A^* \to A$ with $\deg \psi_0 \bigm| b_0$.*

Definition 2.5. *We will denote by $b_0(A/K)$ the minimal b_0 with the property of the above theorem; in particular we have $b_0(A/K) \leq b(A/K)$.*

Suppose now that, in addition to A/K being a TM-product over K, its simple factors A_i are *absolutely* simple and pairwise non-isogenous *over* $\overline{K}$. Then for any field extension K' of K the hypotheses of the previous theorem hold for $A_{K'}$, so it makes sense to consider the quantity $b_0(A/K')$ as K' ranges through all the finite extensions of K of degree bounded by d. Since $b_0(A/K') \leq b(d[K:\mathbb{Q}], h(A), \dim(A))$ stays bounded, the number $\operatorname{lcm}_{[K':K]\leq d} b_0(A/K')$ is finite, and we give it a name:

Definition 2.6. *Let A/K be an abelian variety such that A is a TM-product over K, with simple factors that are absolutely simple and pairwise non-isogenous over $\overline{K}$. We set*

$$b_0(A/K; d) = \operatorname{lcm}_{[K':K]\leq d} b_0(A/K').$$

A slight modification of the arguments of [4, Theorem D], combined with theorem 2.1, gives

Proposition 2.7. *([2, Proposition 2.6]) Let A/K be a g-dimensional abelian variety that is isomorphic over K to a product $A_1^{e_1} \times \cdots \times A_n^{e_n}$, where $A_1, \ldots, A_n$ are simple over $\overline{K}$, mutually non-isogenous over $\overline{K}$, and have trivial endomorphism ring over $\overline{K}$. Then we have*

$$b_0(A/K; d) \leq b(A/K; d) := 4^{\exp(1)\cdot\left(d(1+\log d)^2\right)^{\alpha(g)}} b([K:\mathbb{Q}], \dim(A), h(A))^{1+\alpha(g)\log(d(1+\log d)^2)}.$$

3 An integral Goursat-Ribet lemma for $\mathrm{SL}_2(\mathbb{Z}_\ell)$

As anticipated, a (necessary and) sufficient condition for a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)^n$ to be open is that all its projections on pairs of factors $\mathrm{SL}_2(\mathbb{Z}_\ell)^2$ are themselves open. This is precisely the content of lemma 3.2 below. Before stating it, we remark that – throughout the whole paper – the prime 2 plays a rather special role, and special care is needed to treat it. We then find it useful to introduce the following convention:

Notation 3.1. *In order to give uniform statements that hold for every prime we put $v = 0$ or 1 according to whether the prime ℓ we are working with is odd or equals 2, that is we set*

$$v = v_\ell(2) = \begin{cases} 0, & \text{if } \ell \text{ is odd} \\ 1, & \text{otherwise.} \end{cases}$$

Lemma 3.2. *([3, Lemma 2.9]) Let n be a positive integer, G a closed subgroup of $\prod_{i=1}^n \mathrm{SL}_2(\mathbb{Z}_\ell)$, and π_i the projection from G on the i-th factor. Suppose that, for every $i \neq j$, the group $(\pi_i \times \pi_j)(G)$ contains $\mathcal{B}_\ell(s_{ij}, s_{ij})$ for a certain non-negative integer s_{ij} (with $s_{ij} \geq 2$ if $\ell = 2$ and $s_{ij} \geq 1$ if $\ell = 3$): then G contains $\prod_{i=1}^n \mathcal{B}_\ell\left(\sum_{j\neq i} s_{ij} + (n-2)v\right)$.*

Corollary 3.3. *Let G be a closed subgroup of $\prod_{i=1}^n \mathrm{SL}_2(\hat{\mathbb{Z}})$ with $n \geq 2$. Suppose that for every pair of indices $i \neq j$ there exists a subgroup $S^{(i,j)}$ of $\mathrm{SL}_2(\hat{\mathbb{Z}})^2$ with the following properties:*

- *the projection of G on the direct factor $\mathrm{SL}_2(\hat{\mathbb{Z}}) \times \mathrm{SL}_2(\hat{\mathbb{Z}})$ corresponding to the pair of indices (i,j) contains $S^{(i,j)}$;*
- *$S^{(i,j)}$ decomposes as a direct product $\prod_{\ell \text{ prime}} S_\ell^{(i,j)} \subseteq \prod_\ell \mathrm{SL}_2(\mathbb{Z}_\ell)^2$;*
- *for every prime ℓ the group $S_\ell^{(i,j)}$ is of the form $\mathcal{B}_\ell(f_\ell^{(i,j)}, f_\ell^{(i,j)})$, where $f_\ell^{(i,j)}$ is a non-negative integer, with $f_2^{(i,j)} \geq 2$ if $\ell = 2$ and $f_3^{(i,j)} \geq 1$ if $\ell = 3$.*
- *for almost every ℓ, the group $S_\ell^{(i,j)}$ is all of $\mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{SL}_2(\mathbb{Z}_\ell)$ (so $f_\ell^{(i,j)} = 0$);*

Denote by $c^{(i,j)}$ the index of $S^{(i,j)}$ in $\mathrm{SL}_2(\hat{\mathbb{Z}}) \times \mathrm{SL}_2(\hat{\mathbb{Z}})$ and $c = \max\limits_{i\neq j} c^{(i,j)}$. The index of G in $\prod_{i=1}^n \mathrm{SL}_2(\hat{\mathbb{Z}})$ is strictly less than $2^{3n(n-2)}\zeta(2)^{n(n-1)}c^{n(n-1)/2}$.

Proof. Let $\ell > 3$ be a prime. If $S_\ell^{(i,j)} = \mathrm{SL}_2(\mathbb{Z}_\ell)^2$ for all (i,j), then the previous lemma (with $s_{ij} = 0$ for every pair of indices (i,j)) shows that $\prod_{k=1}^n \mathrm{SL}_2(\mathbb{Z}_\ell)$ is contained in G. Suppose on the other hand that either $\ell \leq 3$ or for at least one pair (i,j) we have $S_\ell^{(i,j)} \neq \mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{SL}_2(\mathbb{Z}_\ell)$. The previous lemma tells us that the projection of G on the direct factor $\prod_{i=1}^n \mathrm{SL}_2(\mathbb{Z}_\ell)$ of $\prod_{i=1}^n \mathrm{SL}_2(\hat{\mathbb{Z}})$ contains

$$B_\ell\left(\sum_{j\neq 1} f_\ell^{(1,j)} + (n-2)v, \; \cdots, \; \sum_{j\neq n} f_\ell^{(n,j)} + (n-2)v\right) = \prod_i \mathcal{B}_\ell\left(\sum_{j\neq i} f_\ell^{(i,j)} + (n-2)v\right).$$

Notice that the index of $\mathcal{B}_\ell(s)$ in $\mathrm{SL}_2(\mathbb{Z}_\ell)$, for $s \geq 1$, is $(\ell^2-1)\ell^{1+3(s-1)} < \ell^{3s}$, so the index of the above product in $\prod_{i=1}^n \mathrm{SL}_2(\mathbb{Z}_\ell)$ is bounded by

$$\prod_{i=1}^n \left(\ell^{3\sum_{j\neq i} f_\ell^{(i,j)} + 3(n-2)v}\right) = 2^{3n(n-2)v} \prod_{i=1}^n \prod_{j\neq i} \ell^{3f_\ell^{(i,j)}}.$$

Let $\mathcal{P} = \{2,3\} \cup \left\{\ell \mid \exists (i,j) : S_\ell^{(i,j)} \neq \mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{SL}_2(\mathbb{Z}_\ell)\right\}$. By what we have just seen,

$$\left[\prod_{k=1}^n \mathrm{SL}_2(\hat{\mathbb{Z}}) : G\right] \leq 2^{3n(n-2)} \prod_{\ell\in\mathcal{P}} \prod_{i=1}^n \prod_{j\neq i} \ell^{3f_\ell^{(i,j)}}.$$

On the other hand, note that the index of $S_\ell^{(i,j)}$ in $\mathrm{SL}_2(\mathbb{Z}_\ell)\times\mathrm{SL}_2(\mathbb{Z}_\ell)$ is at least $\ell^{6f_\ell^{(i,j)}}\cdot\left(\frac{\ell^2-1}{\ell^2}\right)^2$ (with equality if $f_\ell^{(i,j)}\geq 1$), so the above product is bounded by

$$\begin{aligned}
2^{3n(n-2)}\prod_{\ell\in\mathcal{P}}\prod_{i<j}&\left\{\left[\mathrm{SL}_2(\mathbb{Z}_\ell)^2 : S_\ell^{(i,j)}\right]\cdot\left(\frac{\ell^2}{\ell^2-1}\right)^2\right\}\\
&< 2^{3n(n-2)}\prod_{\ell}\left(\frac{\ell^2}{\ell^2-1}\right)^{n(n-1)}\cdot\prod_{i<j}\prod_{\ell\in\mathcal{P}}\left[\mathrm{SL}_2(\mathbb{Z}_\ell)^2 : S_\ell^{(i,j)}\right]\\
&\leq 2^{3n(n-2)}\zeta(2)^{n(n-1)}\prod_{i<j}c^{(i,j)}\\
&\leq 2^{3n(n-2)}\zeta(2)^{n(n-1)}c^{n(n-1)/2}.
\end{aligned}$$

□

4 Lie subalgebras of $\mathfrak{sl}_2(\mathbb{Z}_\ell)^n$ and some Pink-type results

Let us briefly recall the construction (essentially due to Pink) of the $\mathbb{Z}_\ell$-Lie algebra associated with a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)^n$:

Definition 4.1. *(cf. [8]) Let ℓ be a prime. Define maps Θ_n as follows:*

$$\begin{array}{cccc}
\Theta_n : & \mathrm{GL}_2(\mathbb{Z}_\ell)^n & \to & \bigoplus_{i=1}^n \mathfrak{sl}_2(\mathbb{Z}_\ell)\\
& (g_1,\ldots,g_n) & \mapsto & \left(g_1-\frac{1}{2}\operatorname{tr}(g_1),\ldots,g_n-\frac{1}{2}\operatorname{tr}(g_n)\right).
\end{array}$$

*If G is a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)^n$ (resp. of $\mathcal{B}_2(1,\ldots,1)$ in case $\ell=2$), define $L(G)\subseteq\mathfrak{sl}_2(\mathbb{Z}_\ell)^n$ to be the $\mathbb{Z}_\ell$-span of $\Theta_n(G)$. We call $L(G)$ the **Lie algebra** of G.*

The importance of this construction lies in the fact that it allows us to linearize the problem of showing that certain subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)^n$ contain an explicit open neighbourhood of the identity: indeed, we have the following two results, for whose proof we refer the reader to [3].

Theorem 4.2. *([3, Theorem 3.1]) Let $\ell>2$ be a prime number and G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)\times\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let G_1, G_2 be the two projections of G on the two factors $\mathrm{GL}_2(\mathbb{Z}_\ell)$, and let m_1, m_2 be positive integers such that G_i contains $\mathcal{B}_\ell(m_i)$ for $i=1,2$. Suppose furthermore that for every $(g_1,g_2)\in G$ we have $\det(g_1)=\det(g_2)$. At least one of the following holds:*

- *G contains $\mathcal{B}_\ell(20\max\{m_1,m_2\}, 20\max\{m_1,m_2\})$*
- *there exists a subgroup H of G, of index dividing $2^9\cdot 3^2$, with the following properties:*
  1. *if $L(H)$ contains $\ell^k\mathfrak{sl}_2(\mathbb{Z}_\ell)\oplus\ell^k\mathfrak{sl}_2(\mathbb{Z}_\ell)$ for a certain integer k, then T contains $\mathcal{B}_\ell(p,p)$, where*
  $$p=2k+\max\{2k, 8m_1, 8m_2\}.$$
  2. *let (h_1,h_2) be any element of H and let $[h_1],[h_2]$ be the images of h_1,h_2 in $\mathrm{GL}_2(\mathbb{F}_\ell)$. If both $[h_1]$ and $[h_2]$ are multiples of the identity, then they are equal;*
  3. *for any (h_1,h_2) in H, the determinant of h_1 is a square in $\mathbb{Z}_\ell^\times$ (hence the same is true for the determinant of h_2).*

Remark 4.3. The last property of the group H is not stated explicitly in [3], but it is clear from the construction (see [3, Proof of theorem 3.1 assuming theorem 3.2]).

Theorem 4.4. *([3, Theorem 4.1]) Let G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)\times\mathrm{GL}_2(\mathbb{Z}_2)$ whose projection modulo 4 is trivial. Denote by G_1, G_2 the two projections of G on the factors $\mathrm{GL}_2(\mathbb{Z}_2)$, and let $n_1\geq 4, n_2\geq 4$ be integers such that G_i contains $\mathcal{B}_2(n_i)$. Suppose furthermore that for* *every* $(g_1, g_2) \in G$ *we have* $\det(g_1) = \det(g_2) \equiv 1 \pmod 8$. *If* $L(G)$ *contains* $2^k\mathfrak{sl}_2(\mathbb{Z}_2) \oplus 2^k\mathfrak{sl}_2(\mathbb{Z}_2)$ *for a certain* $k \geq 2$, *then* G *contains*

$$\mathcal{B}_2(12(k + 11n_2 + 5n_1 + 12) + 1, 12(k + 11n_1 + 5n_2 + 12) + 1).$$

Finally, we shall need the following simple lemma regarding conjugation-stable subalgebras of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$:

Lemma 4.5. *([3, Lemma 2.4]) Let* t *be a non-negative integer. Let* $W \subseteq \mathfrak{sl}_2(\mathbb{Z}_\ell)$ *be a Lie subalgebra that does not reduce to zero modulo* ℓ^{t+1}. *Suppose that* W *is stable under conjugation by* $\mathcal{B}_\ell(s)$ *for some non-negative integer* s, *where* $s \geq 2$ *if* $\ell = 2$ *and* $s \geq 1$ *if* $\ell = 3$ *or* 5. *Then* W *contains the open set* $\ell^{t+4s+4v}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.

5 The automorphisms of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$ are inner

In this section we obtain a description of the automorphisms of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$ which shows that – in a suitable sense – they are all inner. In order to establish the required result we first need a few simple preliminaries, starting with the following well-known version of Hensel's lemma:

Lemma 5.1. *Let* $p(x) \in \mathbb{Z}_\ell[x]$ *be a monic polynomial and let* α *be an element of* $\mathbb{Z}_\ell$. *Suppose that* $v_\ell(p(\alpha)) > 2v_\ell(p'(\alpha))$: *then* $p(x)$ *admits a root* $\bar{\alpha} \in \mathbb{Z}_\ell$ *such that* $v_\ell(\alpha - \bar{\alpha}) \geq v_\ell(p(\alpha)) - v_\ell(p'(\alpha))$.

Here is the main tool we will use to produce approximate roots of polynomials:

Lemma 5.2. *Let* ℓ *be a prime number,* $n \geq 1, m \geq 1$, $g \in \operatorname{End}(\mathbb{Z}_\ell^m)$ *and* $p_g(t)$ *the characteristic polynomial of* g. *Let* $\lambda \in \mathbb{Z}_\ell$ *and* $w \in \mathbb{Z}_\ell^m$ *be such that* $gw \equiv \lambda w \pmod{\ell^n}$. *If* w *is nonzero modulo* $\ell^{\beta+1}$, *then* $p_g(\lambda) \equiv 0 \pmod{\ell^{n-\beta}}$.

Proof. Denote by $(g - \lambda \operatorname{Id})^*$ the adjugate matrix of $(g - \lambda \operatorname{Id})$, that is the operator such that $(g - \lambda \operatorname{Id})^*(g - \lambda \operatorname{Id}) = \det(g - \lambda \operatorname{Id}) \cdot \operatorname{Id}$. Multiplying the congruence $(g - \lambda \operatorname{Id})w \equiv 0 \pmod{\ell^n}$ on the left by $(g - \lambda \operatorname{Id})^*$ we obtain $\det(g - \lambda \operatorname{Id}) \cdot \operatorname{Id} w \equiv 0 \pmod{\ell^n}$, and by considering the coordinate of w of smallest valuation we deduce $p_g(\lambda) = \det(g - \lambda \operatorname{Id}) \equiv 0 \pmod{\ell^{n-\beta}}$ as claimed. □

The properties of the adjoint representation of $\mathfrak{sl}_2$ (or an immediate computation) also show:

Lemma 5.3. *Let* $g \in \mathfrak{sl}_2(\mathbb{Z}_\ell)$. *The linear operator* $\operatorname{ad}_g := [g, \cdot]$ *from* $\mathfrak{sl}_2(\mathbb{Z}_\ell)$ *to itself has eigenvalues* $0, \pm 2\mu$, *where* $\pm\mu$ *are the eigenvalues of* g, *so its characteristic polynomial* $p_{\operatorname{ad}_g}(t)$ *is equal to* $t(t^2 - 4\mu^2)$.

Combining the previous results we obtain the following lemma, which will be very useful for our purposes:

Lemma 5.4. *Let* g *be an element of* $\mathfrak{sl}_2(\mathbb{Z}_\ell)$, w *be a vector in* $\mathbb{Z}_\ell^2$, *and* β *be the minimal valuation of the coefficients of* w. *Suppose* $gw \equiv \lambda w \pmod{\ell^n}$. *Then either* g *has an eigenvalue* ν *such that* $v_\ell(\nu - \lambda) \geq v_\ell(\lambda) + 3$ *or else* β *is at least* $n - 2(2 + v_\ell(\lambda))$.

Proof. Let $\pm\mu$ be the eigenvalues of g. From lemma 5.2 we deduce that $v_\ell(p_g(\lambda)) \geq n - \beta$; notice further that $p_g(t) = t^2 - \mu^2$, so $p_g'(t) = 2t$. Suppose that $\beta < n - 2(2 + v_\ell(\lambda))$: then $n - \beta > 2(2 + v_\ell(\lambda)) > 2v_\ell(p_g'(\lambda))$, and by Hensel's lemma $p_g(t)$ has a root ν such that

$$v_\ell(\nu - \lambda) \geq v_\ell(p_g(\lambda)) - v_\ell(p_g'(\lambda)) \geq n - \beta - v - v_\ell(\lambda) \geq v_\ell(\lambda) + 3.$$

□

We now come to the central result of this section, which as anticipated is essentially a description of the Lie algebra automorphisms of (the finite quotients of) $\mathfrak{sl}_2(\mathbb{Z}_\ell)$.

Proposition 5.5. *Let L_1 be a subalgebra of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$ and $n \geq 1, s \geq 0$ be integers. Suppose that L_1 contains $\ell^s \mathfrak{sl}_2(\mathbb{Z}_\ell)$ and that $\varphi : L_1 \to \mathfrak{sl}_2(\mathbb{Z}_\ell)$ is a linear map such that*

$$[\varphi(a), \varphi(b)] \equiv \varphi([a,b]) \pmod{\ell^n} \quad \forall a, b \in \ell^s \mathfrak{sl}_2(\mathbb{Z}_\ell).$$

Define

$$x = \varphi\left(\ell^s \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right), \ y = \varphi\left(\ell^s \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right), \ h = \varphi\left(\ell^s \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right)$$

and let α be the minimal integer such that x, y are both nonzero modulo $\ell^{\alpha+1}$. Suppose that $n \geq \alpha + 10s + 5v + 6$. There exists a matrix $M \in M_2(\mathbb{Z}_\ell)$, at least one of whose coefficients is nonzero modulo ℓ, such that for every $w \in (\mathbb{Z}_\ell)^2$ and every $g_1 \in L_1$ we have

$$M(g_1 \cdot w) \equiv \varphi(g_1) \cdot M(w) \pmod{\ell^{n-\alpha-6s-4v-6}}.$$

Furthermore, $\det(M)$ *does not vanish modulo ℓ^{4s+v}, and for every g_1 in L_1 we have*

$$\operatorname{tr}\left(\varphi(g_1)^2\right) \equiv \operatorname{tr}\left(g_1^2\right) \pmod{\ell^{n-\alpha-10s-5v-6}}$$

and

$$\varphi(g_1) \equiv M g_1 M^{-1} \pmod{\ell^{n-\alpha-10s-5v-6}}, \quad M^{-1}\varphi(g_1)M \equiv g_1 \pmod{\ell^{n-\alpha-10s-5v-6}}$$

Remark 5.6. A moment's thought (considering the limiting cases when s or α become very large) will reveal that it is indeed necessary for all three parameters n, s, and α to appear in the conclusion of the proposition. The question of whether the *dependence* on these parameters is optimal, on the other hand, is far more complicated, and there is almost certainly room for improvement.

Here again let us say a few words about the method of proof before fiddling with the technical details. To simplify matters, consider the algebra $L = \mathfrak{sl}_2(\mathbb{Q}_\ell)$. Proving that every automorphism of L is inner basically boils down to showing that the only 2-dimensional representation of $\mathfrak{sl}_2(\mathbb{Q}_\ell)$ is the standard one, a result which is usually proved through the 'highest weight vector' machinery: one shows that it is possible to choose an eigenvector v for h that is killed by x, and then describes its full orbit under the action of x, y, h. More precisely, one shows that yv is an eigenvector for h, that xyv is proportional to v, and that $y^2 v = 0$.

The proof that follows mimics this very argument by producing a vector v_+, by definition an eigenvector for h, which plays the role of the highest weight vector, and subsequently finding its orbit under the action of h, x, y. The main difficulty lies in the initial step, where we need to prove that the eigenvalues of h lie in $\mathbb{Z}_\ell$ and are of a certain form. Once this is done, most of the proof looks very much like the one for $\mathfrak{sl}_2(\mathbb{Q}_\ell)$, with the additional complication that we have to keep track of valuations along the way.

Notation. For the remainder of this section, in order to make notation lighter, when a is a positive integer we write $x = y + O(a)$ for $x \equiv y \pmod{\ell^a}$.

Proof. Denote by ad_h the linear endomorphism of $\mathfrak{sl}_2(\mathbb{Z}_\ell) \cong \mathbb{Z}_\ell^3$ given by taking the commutator with h. It is clear that

$$\operatorname{ad}_h(x) = [h, x] \equiv \varphi\left[\ell^s \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ell^s \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right] \equiv \varphi\left(2\ell^s \cdot \ell^s \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right) \equiv 2\ell^s x \pmod{\ell^n},$$

so x is an (approximate) eigenvector of ad_h associated with the (approximate) eigenvalue $2\ell^s$. Lemma 5.2 yields

$$p_{\operatorname{ad}_h}(2\ell^s) \equiv 0 \pmod{\ell^{n-\alpha}}.$$

If we let $\pm\mu$ denote the eigenvalues of h, then $p'_{\mathrm{ad}_h}(t) = (t^2-4\mu^2)+2t^2$, and evaluating at $2\ell^s$ we find

$$p'_{\mathrm{ad}_h}(2\ell^s) = 4(\ell^{2s}-\mu^2)+8\ell^{2s} = \frac{p_{\mathrm{ad}_h}(2\ell^s)}{2\ell^s}+8\ell^{2s}.$$

To estimate the ℓ-adic valuation of this last expression observe that

$$v_\ell\left(\frac{p_{\mathrm{ad}_h}(2\ell^s)}{2\ell^s}\right) = v_\ell\left(p_{\mathrm{ad}_h}(2\ell^s)\right) - v_\ell(2) - s \geq n-\alpha-v-s > 3v+2s = v_\ell(8\ell^{2s}),$$

so $v_\ell\left(p'_{\mathrm{ad}_h}(2\ell^s)\right) = v_\ell\left(8\ell^{2s}\right) = 3v+2s$. By Hensel's lemma (lemma 5.1), $p_{\mathrm{ad}_h}(t)$ admits a root $\lambda \in \mathbb{Z}_\ell$ such that

$$v_\ell(\lambda - 2\ell^s) \geq v_\ell(p_{\mathrm{ad}_h}(2\ell^s)) - v_\ell(p'_{\mathrm{ad}_h}(2\ell^s)) \geq n-\alpha-2s-3v > 2s+1.$$

Note that λ cannot be zero, because $v_\ell(0-2\ell^s)=v+s$ is strictly smaller than $v_\ell(\lambda-2\ell^s)$. It follows that λ is one of the other two roots of $p_{\mathrm{ad}_h}(t)$, namely $\pm 2\mu$, and hence

$$\pm\mu = \pm\frac{1}{2}\left(2\ell^s + O(n-\alpha-2s-3v)\right) = \pm\ell^s(1+O(n-\alpha-3s-4v)).$$

To sum up, the two eigenvalues of h belong to $\mathbb{Z}_\ell$ and are of the form $\pm\ell^s+O(n-\alpha-2s-4v)$, and in particular of the form $\pm\ell^s+O(s+4)$. Let μ_+ be the one of the form $\ell^s+O(n-\alpha-2s-4v)$ and $v_+ \in \mathbb{Z}_\ell^2$ be a corresponding eigenvector, normalized in such a way that at least one of the two coordinates is an ℓ-adic unit. Set furthermore $v_- = yv_+$.

As anticipated, our next objective is to describe the action of x, y, h on $v_\pm$. We expect v_+ to be annihilated by x and v_- to be an eigenvector for h that is annihilated by y: of course this is not going to be exactly true at all orders, but only up to a certain error term that depends on n, α and s. Let β be the minimal valuation of the coordinates of xv_+: this is a number we want to show to be large.

The idea is that if xv_+ were not very close to zero, then it would be an eigenvector of h associated with an eigenvalue that h does not possess. Note that

$$h(xv_+) \equiv [h,x]v_+ + xhv_+ \equiv (2\ell^s+\mu_+)xv_+ \pmod{\ell^n},$$

so by lemma 5.4 either h has an eigenvalue ξ such that $v_\ell(\xi-(\mu_++2\ell^s)) \geq 3+v_\ell(\mu_++2\ell^s) \geq s+3$ or $\beta \geq n-2(2+v_\ell(\mu_++2\ell^s))$. Note that we cannot be in the first case: indeed h would have an eigenvalue of the form $3\ell^s+O(s+3)$, but we have already seen that the eigenvalues of h are $\pm\ell^s+O(s+4)$, contradiction. Hence we are in the second situation, and furthermore $v_\ell(\mu_++2\ell^s) \leq s+1$: hence $\beta \geq n-2(2+v_\ell(\mu_++2\ell^s)) \geq n-2s-6$, and by definition of β this means $xv_+ \equiv 0 \pmod{\ell^{n-2(s+3)}}$. Next we compute

$$\begin{aligned} hv_- &= hyv_+ \\ &= [h,y]v_+ + yhv_+ \\ &= -2\ell^s \cdot yv_+ + y(\mu_+v_+) + O(n) \\ &= (\mu_+-2\ell^s)v_- + O(n) \\ &= (-\ell^s+O(n-\alpha-2s-4v))v_- + O(n) \\ &= -\ell^s v_- + O(n-\alpha-2s-4v), \end{aligned} \tag{1}$$

$$\begin{aligned} xv_- &= xyv_+ \\ &= [x,y]v_+ + yxv_+ \\ &= \ell^s hv_+ + O(n-2(s+3)) \\ &= \ell^s\mu_+v_+ + O(n-2(s+3)) \\ &= \ell^s\left(\ell^s+O(n-\alpha-2s-4v)\right)v_+ + O(n-2(s+3)) \\ &= \ell^{2s}v_+ + O(n-\alpha-2(s+3)); \end{aligned} \tag{2}$$

this settles the question of the action of h and x on v_-. We are left with showing that v_- is (approximately) killed by y. Again, we do this by showing that yv_- – unless it is very close to 0 – yields an eigenvector of h associated with an eigenvalue that h does not possess:

$$\begin{aligned} h \cdot yv_- &= [h, y]v_- + yhv_- \\ &= -2\ell^s \cdot yv_- + y\left((-\ell^s) + O(n-\alpha-2s-4v)\right)v_- + O(n) \\ &= -3\ell^s yv_- + O(n-\alpha-2s-4v), \end{aligned}$$

so that yv_- is an (approximate) eigenvector of h, associated with the (approximate) eigenvalue $-3\ell^s$. Let γ be minimal among the valuations of the coefficients of yv_-. Apply lemma 5.4: either $\gamma \geq n-\alpha-2s-4v-2(2+v_\ell(-3\ell^s)) \geq n-\alpha-4s-4v-6$ or h has an eigenvalue ν satisfying $v_\ell(\nu+3\ell^s) \geq v_\ell(-3\ell^s)+3 \geq s+3$. This second possibility contradicts what we have already proven on the eigenvalues of h, hence $\gamma \geq n-\alpha-4s-4v-6$, that is to say $yv_- = O(n-\alpha-4s-4v-6)$.

Putting all together, we have proved that up to an error of order $\ell^{n-\alpha-4s-4v-6}$ we have

$$xv_+ = 0,\ yv_+ = v_-,\ hv_+ = \ell^s v_+,\ xv_- = \ell^{2s} v_+,\ yv_- = 0,\ hv_- = -\ell^s v_-.$$

Write $\overline{x}$ (resp. $\overline{y}, \overline{h}$) for $\ell^s \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ (resp. $\ell^s \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \ell^s \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$) and consider the matrix $\tilde{M}$ whose columns are given by $\ell^s v_+$ and v_-. The above relations may be stated more compactly as

$$\tilde{M}\overline{x} = x\tilde{M},\ \tilde{M}\overline{y} = y\tilde{M},\ \tilde{M}\overline{h} = h\tilde{M} \tag{3}$$

modulo $\ell^{n-\alpha-4s-4v-6}$. Let δ be minimal among the valuations of the coefficients of $\tilde{M}$: by construction, at least one of the coordinates of v_+ is an ℓ-adic unit, so $\delta \leq s$. Set $M = \ell^{-\delta}\tilde{M}$. Dividing equations (3) by ℓ^δ we see that M satisfies analogous equations up to error terms of order $n-\alpha-5s-4v-6$, and by construction at least one of the coefficients of M is an ℓ-adic unit.

Let g be any element of L_1. The matrix $\ell^s g$ belongs to $\ell^s \mathfrak{sl}_2(\mathbb{Z}_\ell)$, so it is a linear combination of $\overline{x}, \overline{y}, \overline{h}$ with coefficients in $\mathbb{Z}_\ell$. Write $\ell^s g = \lambda_1 \overline{x} + \lambda_2 \overline{y} + \lambda_3 \overline{h}$. We have

$$\begin{aligned} \ell^s Mg &= M(\ell^s g) \\ &= M(\lambda_1 \overline{x} + \lambda_2 \overline{y} + \lambda_3 \overline{h}) \\ &= (\lambda_1 x + \lambda_2 y + \lambda_3 h)M + O(n-\alpha-5s-4v-6) \\ &= \varphi(\ell^s g)M + O(n-\alpha-5s-4v-6) \\ &= \ell^s \varphi(g)M + O(n-\alpha-5s-4v-6), \end{aligned}$$

so that dividing by ℓ^s we deduce $Mg = \varphi(g)M + O(n-\alpha-6s-4v-6)$ for every $g \in L_1$, which is the first statement in the proposition.

Let us now turn to the statement concerning the determinant. We can assume that v_+ is normalized so that $v_+ = \begin{pmatrix} 1 \\ c \end{pmatrix}$. We also write $v_- = \begin{pmatrix} b \\ d \end{pmatrix}$. It is clear that $v_\ell(\det M) \leq v_\ell(\det \tilde{M})$, and that $\det \tilde{M} = \ell^s \det \begin{pmatrix} 1 & b \\ c & d \end{pmatrix}$, so let us consider $D := v_\ell\left(\det \begin{pmatrix} 1 & b \\ c & d \end{pmatrix}\right)$. Suppose by contradiction $D > 3s + v$; by definition of the determinant we have $d = bc + O(D)$, which implies

$$v_- = \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} b \\ bc + O(D) \end{pmatrix} = bv_+ + O(D).$$

Applying h to both sides of this equality and using equation (1) we get

$$\mu_- v_- + O(n-\alpha-2s-4v) = hv_- = h(bv_+ + O(D)) = b\mu_+ v_+ + O(D).$$

Comparing the first coordinate of these vectors we deduce

$$b\mu_- = b\mu_+ + O(\min\{D, n-\alpha-2s-4v\}),$$

hence

$$\mu_- = \mu_+ + O(\min\{D - v_\ell(b), n - \alpha - 2s - 4v - v_\ell(b)\}). \tag{4}$$

Note that since $d = bc + O(D)$ we have $v_\ell(d) \geq \min\{v_\ell(b), D\}$. Moreover, we see by equation (2) that $xv_- = \ell^{2s}v_+ + O(n - \alpha - 2(s+3))$, and since the right hand side does not vanish modulo ℓ^{2s+1} (since $n - \alpha - 2(s+3) > 2s+1$ and $\ell^{2s}v_+ = \begin{pmatrix} \ell^{2s} \\ \ell^{2s}c \end{pmatrix}$) we must in particular have $v_- \not\equiv 0 \pmod{\ell^{2s+1}}$. Hence $\min\{v_\ell(b), v_\ell(d)\} \leq 2s$. Let us show that we also have $v_\ell(b) \leq 2s$. Suppose that $v_\ell(b) \geq 2s+1$: then

$$v_\ell(d) \geq \min\{v_\ell(b), D\} \geq \min\{2s+1, 3s+v+1\} \geq 2s+1,$$

which implies $\min\{v_\ell(b), v_\ell(d)\} \geq 2s+1$ and contradicts what we just proved.

Therefore $v_\ell(b) \leq 2s$, hence equation (4) implies $\mu_- = \mu_+ + O\,(D - 2s)$: notice that if the minimum in (4) were attained for $n - \alpha - 2s - 4v - v_\ell(b) \geq 3s+2$ we would have $\ell^s = -\ell^s + O(3s+2)$, a clear contradiction. On the other hand, we know that $\mu_\pm = \pm\ell^s + O(s+4)$, so the above equation implies $2\ell^s + O(s+4) = O(D-2s)$. Hence we have proved $v_\ell(2\ell^s) \geq D - 2s$, i.e. $D \leq 3s + v$, a contradiction. It follows, as claimed, that $v_\ell(\det M) \leq v_\ell(\det \tilde{M}) = s + D \leq 4s + v$.

Next we prove the statement concerning traces. Let g be any element of L_1. Setting, for the sake of simplicity, $N = n - \alpha - 6s - 4v - 6$, we have $Mg = \varphi(g)M + O(N)$, so (multiplying on the left by the adjugate M^* of M) we deduce $\det(M)g = M^*\varphi(g)M + O(N)$. Didiving through by $\det(M)$ we have $g = M^{-1}\varphi(g)M + O(N - (4s+v))$; note that this equality would a priori only hold in $\mathfrak{sl}_2(\mathbb{Q}_\ell)$, but since both g and the error term are ℓ-integral we necessarily also have $M^{-1}\varphi(g)M \in \mathfrak{sl}_2(\mathbb{Z}_\ell)$. Squaring and taking traces then yields $\operatorname{tr}\left(g^2\right) = \operatorname{tr}\left[\left(M^{-1}\varphi(g)M\right)^2\right] + O(N - (4s+v))$, i.e.

$$\operatorname{tr}\left(g^2\right) = \operatorname{tr}\left(\varphi(g)^2\right) + O(N - (4s+v))$$

as claimed. Finally, essentially the same argument shows the last two statements: we can multiply the congruence $Mg_1 \equiv \varphi(g_1)M \pmod{\ell^N}$ on the right (resp. left) by M^* and divide by $\det M$ to get

$$Mg_1M^{-1} \equiv \varphi(g_1) \pmod{\ell^{N-4s-v}}, \quad g_1 \equiv M^{-1}\varphi(g_1)M \pmod{\ell^{N-4s-v}}.$$

□

6 Products of two curves

6.1 Notation and preliminaries

Let E_1, E_2 be two elliptic curves over K, let ℓ be a prime number, and write G_ℓ for the image of $\operatorname{Gal}\left(\overline{K}/K\right)$ inside $\operatorname{Aut} T_\ell(E_1) \times \operatorname{Aut} T_\ell(E_2) \cong \operatorname{GL}_2(\mathbb{Z}_\ell)^2$. To study the Galois representation attached to $E_1 \times E_2$ we are going to pass to a suitable extension of K over which the study of the Lie algebra of G_ℓ is sufficient to yield information on G_ℓ itself. Before doing this, however, we need to dispense with some necessary preliminaries. Let $G_{\ell,1}, G_{\ell,2}$ be the two projections of G_ℓ onto the two factors $\operatorname{GL}_2(\mathbb{Z}_\ell)$, and m_1, m_2 be integers such that $\mathcal{B}_\ell(m_i)$ is contained in $G_{\ell,i}$ for $i = 1, 2$. We want to apply theorem 4.2, so for the whole section (with the exception of proposition 6.12) we make the following

Assumption 6.1. *If ℓ is odd, G_ℓ does not contain $\mathcal{B}_\ell\left(20\max\{m_1, m_2\}, 20\max\{m_1, m_2\}\right)$.*

Under this assumption, we define K_ℓ to be the extension of K associated with the following closed subgroups of G_ℓ:

$$\begin{cases} \ker\left(G_2 \to \operatorname{GL}_2(\mathbb{Z}/8\mathbb{Z})^2\right), \text{ if } \ell = 2 \\ H_\ell, \text{ if } \ell \neq 2, \end{cases}$$

where H_ℓ is the group given by an application of theorem 4.2 under our assumption. Note that the degree $[K_2 : K]$ is at most $3^2 2^{16}$, that is to say the order of

$$\left\{(x,y) \in \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})^2 \;\middle|\; \det x = \det y\right\},$$

whereas $[K_\ell : K]$ is uniformly bounded by $2^9 \cdot 3^2$ for $\ell \neq 2$. Note that H_ℓ is by construction the image of $\operatorname{Gal}\left(\overline{K_\ell}/K_\ell\right)$ in $\operatorname{Aut} T_\ell(E_1) \times \operatorname{Aut} T_\ell(E_2) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)^2$.

Definition 6.2. *We write $H_{\ell,1}, H_{\ell,2}$ for the projections of H_ℓ on the two factors $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Furthermore, we let n_1, n_2 be integers such that $H_{\ell,1}, H_{\ell,2}$ respectively contain $\mathcal{B}_\ell(n_1), \mathcal{B}_\ell(n_2)$. Notice that if $\ell = 2$ we have $n_1, n_2 \geq 2$; on the other hand, for $\ell = 3$ or 5 we explicitly demand that $n_1, n_2 \geq 1$.*

Remark 6.3. Note that if $m_1, m_2 > 0$ we can take $n_1 = m_1, n_2 = m_2$ unless $\ell \leq 3$: indeed for primes $\ell \geq 5$ the index of H_ℓ in G_ℓ is not divisible by ℓ, so for any positive value of n the (pro-ℓ) group $\mathcal{B}_\ell(n)$ is contained in $H_{\ell,i}$ if and only if it is contained in $G_{\ell,i}$. Furthermore, it is clear by definition that we can always assume without loss of generality $m_1 \leq n_1, m_2 \leq n_2$, because the groups $H_{\ell,i}$ are subgroups the corresponding groups $G_{\ell,i}$.

Definition 6.4. *We let $L \subseteq \mathfrak{sl}_2(\mathbb{Z}_\ell)^{\oplus 2}$ (resp. $L_1, L_2 \subseteq \mathfrak{sl}_2(\mathbb{Z}_\ell)$) be the Lie algebra of H_ℓ (resp. of $H_{\ell,1}$, of $H_{\ell,2}$). We choose a basis of L of the form $(a_1, b_1), (a_2, b_2), (a_3, b_3), (0, y_1), (0, y_2), (0, y_3)$. Such a basis clearly exists.*

By our assumption $H_{\ell,1} \supseteq \mathcal{B}_\ell(n_1)$ we have $L_1 \supseteq \ell^{n_1}\mathfrak{sl}_2(\mathbb{Z}_\ell)$. Notice that $(0, y_1), (0, y_2), (0, y_3)$ span a Lie-subalgebra: indeed $[(0, y_i), (0, y_j)] = (0, [y_i, y_j])$ must be a linear combination with $\mathbb{Z}_\ell$-coefficients of the basis elements; however, since a_1, a_2, a_3 are linearly independent over $\mathbb{Z}_\ell$, we deduce that this commutator is a linear combination of $(0, y_1), (0, y_2), (0, y_3)$, so that these three elements do indeed span a Lie algebra, which we call L_0. Note that L_0 can equivalently be described as the kernel of the projection from $L \subseteq \mathfrak{sl}_2(\mathbb{Z}_\ell) \oplus \mathfrak{sl}_2(\mathbb{Z}_\ell)$ to the first copy of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$. We shall interchangeably consider L_0 as a subalgebra of $\mathfrak{sl}_2(\mathbb{Z}_\ell) \oplus \mathfrak{sl}_2(\mathbb{Z}_\ell)$ or as a subalgebra of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$, identifying L_0 to its projection on the second copy of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$.

Lemma 6.5. *$L_0 \subseteq \mathfrak{sl}_2(\mathbb{Z}_\ell)$ is stable under conjugation by $\mathcal{B}_\ell(n_2)$.*

Proof. For the proof, consider L_0 as a subalgebra of $\mathfrak{sl}_2(\mathbb{Z}_\ell) \oplus \mathfrak{sl}_2(\mathbb{Z}_\ell)$. Take any element $l \in L_0$: it is the limit of a sequence $l_n = \sum_{i=1}^n \lambda_{n,i}\Theta(g_{n,i})$ for certain $g_{n,i} \in H_\ell$ and $\lambda_{n,i} \in \mathbb{Z}_\ell$. For any $g \in B_\ell(n_2)$ there exists $h \in H_{\ell,1}$ such that (h, g) is in H_ℓ. We have

$$\begin{aligned}(h,g)^{-1} l_n (h,g) &= \sum_{i=1}^n \lambda_{n,i}(h,g)^{-1}\Theta(g_{n,i})(h,g) = \sum_{i=1}^n \lambda_{n,i}(h,g)^{-1}\left(g_{n,i} - \frac{\operatorname{tr}(g_{n,i})}{2}\operatorname{Id}\right)(h,g) \\ &= \sum_{i=1}^n \lambda_{n,i}\left((h,g)^{-1}g_{n,i}(h,g) - \frac{\operatorname{tr}((h,g)^{-1}g_{n,i}(h,g))}{2}\operatorname{Id}\right) \\ &= \sum_{i=1}^n \lambda_{n,i}\Theta((h,g)^{-1}g_{n,i}(h,g)) \in \langle\Theta(H_\ell)\rangle,\end{aligned}$$

so the sequence $\left((h,g)^{-1}l_n(h,g)\right)_{n\geq 0}$ is in L, and by continuity of conjugation converges to the element $(h,g)^{-1}l(h,g)$ of L. If we write $l = (l^{(1)}, l^{(2)}) = (0, l^{(2)})$ we have

$$(h,g)^{-1}l(h,g) = (h,g)^{-1}(0, l^{(2)})(h,g) = (0, g^{-1}l^{(2)}g) \in L,$$

and since L_0 is exactly the sub-algebra given by the elements whose first coordinate vanishes the claim is proved. □

Corollary 6.6. *Fix an integer t, and suppose that at least one among y_1, y_2, y_3 is nonzero modulo ℓ^{t+1}: then L_0 contains $\ell^{t+4n_2+4v}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.*

Proof. Apply lemma 4.5 with $s = n_2$ (the hypotheses of this lemma are satisfied thanks to our assumptions on n_1, n_2, cf. definition 6.2). □

Our task is therefore to bound the values of t for which the y_i all vanish modulo ℓ^t; doing this will allow us to prove proposition 6.12 below, which is the crucial ingredient in proving theorem 1.1. The desired bound on t will be established in §6.2; in the present section we content ourselves with showing two basic lemmas in linear algebra (over $\mathbb{Z}_\ell$) which will be useful later. Notice that – since we are only looking for an upper bound on t – there is no loss of generality in assuming that $y_i \equiv 0 \pmod{\ell^{n_2+1}}$ for $i = 1, 2, 3$, for otherwise we are already done. Thus we can assume that we are given an integer $t \geq n_2 + 1$ such that $y_i \equiv 0 \pmod{\ell^t}$ for $i = 1, 2, 3$: we shall endeavour to show an upper bound on the value of t. As a first modest step in this direction we have:

Lemma 6.7. *Suppose y_1, y_2, y_3 all vanish modulo ℓ^t, where $t \geq n_2 + 1$. The $\mathbb{Z}_\ell$-submodule of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$ generated by b_1, b_2, b_3 contains $\ell^{n_2}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.*

It is clear that the previous lemma follows immediately from the following more general statement:

Lemma 6.8. *Let $b_1, \ldots, b_k$ and $y_1, \ldots, y_k$ be elements of $\mathbb{Z}_\ell^k$, and let n be a non-negative integer. Suppose that $y_1, \ldots, y_k$ are all zero modulo ℓ^{n+1}, and that the submodule of $\mathbb{Z}_\ell^k$ generated by $b_1, \ldots, b_k, y_1, \ldots, y_k$ contains $\ell^n\mathbb{Z}_\ell^k$. Then the submodule of $\mathbb{Z}_\ell^k$ generated by $b_1, \ldots, b_k$ contains $\ell^n\mathbb{Z}_\ell^k$. Let furthermore $e_1, \ldots, e_k$ be the standard basis of $\mathbb{Z}_\ell^k$: there exists a $T \in \operatorname{End}_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell^k)$ such that $Tb_i = \ell^n e_i$ for $i = 1, \ldots, k$.*

Proof. Let B, Y be the $k \times k$ matrices that have the b_i (resp. the y_j) as columns. The hypothesis implies that there exist two matrices $\tilde{B}, \tilde{Y}$ such that $\ell^n \operatorname{Id} = B\tilde{B} + Y\tilde{Y}$. Notice that by assumption Y is zero modulo ℓ^{n+1}, so we can rewrite this equation as $\ell^n \left(\operatorname{Id} - \ell \dfrac{Y}{\ell^{n+1}}\tilde{Y}\right) = B\tilde{B}$, where $\dfrac{Y}{\ell^{n+1}}$ has ℓ-integral coefficients. Observe that $\left(\operatorname{Id} - \ell \frac{Y}{\ell^{n+1}}\tilde{Y}\right)$, being congruent to the identity modulo ℓ, is invertible in $\operatorname{End}_{\mathbb{Z}_\ell}\left(\mathbb{Z}_\ell^k\right)$; it follows that $\ell^n \operatorname{Id} = B\tilde{B}\left(\operatorname{Id} - \ell \frac{Y}{\ell^{n+1}}\tilde{Y}\right)^{-1}$, which gives a representation of the vectors $\ell^n e_i$ as $\mathbb{Z}_\ell$-linear combinations of $b_1, \ldots, b_k$. Finally, since left- and right- inverses of matrices agree, we also have $\ell^n \operatorname{Id} = \tilde{B}\left(\operatorname{Id} - \ell \frac{Y}{\ell^{n+1}}\tilde{Y}\right)^{-1} B$, so for the second statement we can take $T := \tilde{B}\left(\operatorname{Id} - \ell \frac{Y}{\ell^{n+1}}\tilde{Y}\right)^{-1}$. □

We shall also need the following consequence of lemmas 6.7 and 6.8.

Lemma 6.9. *Let $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}_\ell$ and let n be a non-negative integer. Suppose that*

$$\lambda_1 b_1 + \lambda_2 b_2 + \lambda_3 b_3 \equiv 0 \pmod{\ell^{n_2+n}} : \tag{5}$$

then $\lambda_1, \lambda_2, \lambda_3$ are all zero modulo ℓ^n.

Proof. Let $e_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $e_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. By the previous lemma, there is a $T \in \operatorname{End}_{\mathbb{Z}_\ell}(\mathfrak{sl}_2(\mathbb{Z}_\ell))$ such that $Tb_i = \ell^{n_2} e_i$ for $i = 1, 2, 3$. Applying T to both sides of (5) we find $\ell^{n_2}\left(\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3\right) \equiv 0 \pmod{\ell^{n_2+n}}$: this implies that $\lambda_1, \lambda_2, \lambda_3$ are all zero modulo ℓ^n. □

6.2 An explicit open image theorem for G_ℓ

Let us now return to our elliptic curves E_1, E_2. We continue with the notation from the previous section. Notice that a_1, a_2, a_3 are $\mathbb{Z}_\ell$-linearly independent, hence there exists a unique $\mathbb{Z}_\ell$-linear map $\varphi : L_1 \to L_2$ such that $\varphi(a_i) = b_i$ for $i = 1, 2, 3$.

For two indices j,k write $[a_j,a_k]=\sum_{i=1}^3 \mu_i^{(j,k)} a_i$ for certain structure constants $\mu_i^{(j,k)} \in \mathbb{Z}_\ell$. Recall furthermore that t is a positive integer no less than n_2+1 and such that y_1, y_2, y_3 are all zero modulo ℓ^t. Since L is a Lie algebra, there exist scalars $\nu_i^{(j,k)}$ such that

$$[(a_j,b_j),(a_k,b_k)] = \sum_{i=1}^3 \mu_i^{(j,k)}(a_i,b_i) + \sum_{i=1}^3 \nu_i^{(j,k)}(0,y_i),$$

and reducing the second coordinate of this equation modulo ℓ^t gives

$$\begin{aligned}[][\varphi(a_j),\varphi(a_k)] = [b_j,b_k] &\equiv \sum_{i=1}^3 \mu_i^{(j,k)} b_i \equiv \sum_{i=1}^3 \mu_i^{(j,k)}\varphi(a_i) \\ &\equiv \varphi\left(\sum_{i=1}^3 \mu_i^{(j,k)} a_i\right) \equiv \varphi\left([a_j,a_k]\right) \pmod{\ell^t}.\end{aligned}$$

We want to apply proposition 5.5 to φ. We claim that, in the notation of that proposition, we can take $\alpha \leq n_2+n_1$. By lemma 6.9, a linear combination $\lambda_1 b_1+\lambda_2 b_2+\lambda_3 b_3$ can vanish modulo $\ell^{n_1+n_2+1}$ only if $\lambda_1,\lambda_2,\lambda_3$ all vanish modulo ℓ^{n_1+1}.

Since the $\mathbb{Z}_\ell$-module generated by a_1,a_2,a_3 contains $\ell^{n_1}\mathfrak{sl}_2(\mathbb{Z}_\ell)$ we can choose scalars $\lambda_1,\lambda_2,\lambda_3 \in \mathbb{Z}_\ell$ such that $\ell^{n_1}\begin{pmatrix}0&1\\0&0\end{pmatrix} = \lambda_1 a_1+\lambda_2 a_2+\lambda_3 a_3$, and at least one among λ_1, λ_2, λ_3 is nonzero modulo ℓ^{n_1+1}. It follows by lemma 6.9 that

$$\varphi\left(\ell^{n_1}\begin{pmatrix}0&1\\0&0\end{pmatrix}\right) = \varphi\left(\lambda_1 a_1+\lambda_2 a_2+\lambda_3 a_3\right) = \sum_{i=1}^3 \lambda_i b_i$$

is nonzero modulo $\ell^{n_1+n_2+1}$ as claimed, and a perfectly analogous argument applies to the image of $\ell^{n_1}\begin{pmatrix}0&0\\1&0\end{pmatrix}$. We also claim that by construction of φ and by our assumption on t we have

$$(l_1,l_2)\in L(H_\ell) \Rightarrow l_2 \equiv \varphi(l_1) \pmod{\ell^t}.$$

To see this, recall first that every element $(l_1,l_2)\in L(H_\ell)$ is a linear combination of the (a_i,b_i) (for $i=1,2,3$) and of the $(0,y_j)$ (for $j=1,2,3$). Writing $(l_1,l_2)=\sum_{i=1}^3 \sigma_i(a_i,b_i)+\sum_{j=1}^3 \tau_j(0,y_j)$ for some scalars $\sigma_i,\tau_j\in\mathbb{Z}_\ell$, and using the fact that $y_j\equiv 0 \pmod{\ell^t}$ for $j=1,2,3$, we find $l_1=\sum_{i=1}^3 \sigma_i a_i$ and

$$l_2 = \sum_{i=1}^3 \sigma_i b_i + \sum_{j=1}^3 \tau_j y_j \equiv \sum_{i=1}^3 \sigma_i \varphi(a_i) \equiv \varphi\left(\sum_{i=1}^3 \sigma_i a_i\right) \equiv \varphi(l_1) \pmod{\ell^t}.$$

Set $T=t-11n_1-n_2-5v-6$. By proposition 5.5, there is a matrix $M\in M_2(\mathbb{Z}_\ell)$ such that:

1. for all $(l_1,l_2)\in L(H_\ell)$ we have $l_2\equiv M\cdot l_1\cdot M^{-1} \pmod{\ell^T}$ and $M^{-1}\cdot l_2\cdot M\equiv l_1 \pmod{\ell^T}$;
2. at least one of the coefficients of M is an ℓ-adic unit;

furthermore, the map φ satisfies

3. $\operatorname{tr}({l_1}^2)\equiv\operatorname{tr}(\varphi(l_1)^2)\equiv\operatorname{tr}({l_2}^2) \pmod{\ell^T} \quad \forall (l_1,l_2)\in L(H_\ell)$.

Take any element $(g_1,g_2)\in H_\ell$. We know that the determinant of g_1 (which is equal to the determinant of g_2) is a square in $\mathbb{Z}_\ell^\times$: for $\ell\neq 2$ this is property (3) in theorem 4.2, while for $\ell=2$ it follows from the fact that elements congruent to 1 (mod 8) admit a square root in $\mathbb{Z}_2^\times$. We can therefore choose a square root of $\det g_1$ in $\mathbb{Z}_\ell^\times$ and write

$$(g_1,g_2)=\sqrt{\det g_1}(g_1',g_2') \tag{6}$$

for a certain $(g_1', g_2') \in \mathrm{SL}_2(\mathbb{Z}_\ell)$. Set $(l_1, l_2) = \Theta_2(g_1', g_2')$, and notice that (l_1, l_2) differs from $\Theta_2(g_1, g_2)$ by an invertible scalar factor, so it lies again in $L(H_\ell)$. By definition of Θ_2, there exists a pair $(\lambda_1, \lambda_2) \in \mathbb{Z}_\ell^2$ such that

$$(g_1', g_2') = (\lambda_1, \lambda_2) \cdot \mathrm{Id} + (l_1, l_2)\,, \tag{7}$$

and we wish to show that λ_1 is congruent to λ_2 modulo a large power of ℓ:

Proposition 6.10. *We have* $\lambda_1 \equiv \lambda_2 \pmod{\ell^{T-2v}}$ *and* $g_2 \equiv M g_1 M^{-1} \pmod{\ell^{T-2v}}$.

Proof. Notice first that the second statement follows immediately from the first, combined with equations (6) and (7) and the fact that for all $(l_1, l_2) \in L(H_\ell)$ we have $l_2 \equiv M l_1 M^{-1} \pmod{\ell^T}$ by the properties of M. Hence we just need to prove the first congruence.

We begin by discussing the case of odd ℓ. Squaring equation (7) we obtain

$$\left((g_1')^2, (g_2')^2\right) = ({\lambda_1}^2 \cdot \mathrm{Id} + {l_1}^2 + 2\lambda_1 l_1, {\lambda_2}^2 \cdot \mathrm{Id} + {l_2}^2 + 2\lambda_2 l_2).$$

The left hand side is simply $\dfrac{1}{\det g_1}\left({g_1}^2, {g_2}^2\right)$, an element of H_ℓ up to scalar factors. The image of this matrix through Θ_2 is then an element of $L(H_\ell)$, so applying Θ_2 to the right hand side of the previous equation we get

$$\left(\Theta_1({l_1}^2) + 2\lambda_1 l_1, \Theta_1({l_2}^2) + 2\lambda_2 l_2\right) \in L(H_\ell), \tag{8}$$

which by the properties of M implies $\Theta_1({l_2}^2) + 2\lambda_2 l_2 \equiv M\left(\Theta_1({l_1}^2) + 2\lambda_1 l_1\right) M^{-1} \pmod{\ell^T}$, or equivalently

$${l_2}^2 - \frac{\operatorname{tr}\left({l_2}^2\right)}{2} \mathrm{Id} + 2\lambda_2 l_2 \equiv M \left({l_1}^2 - \frac{\operatorname{tr}\left({l_1}^2\right)}{2} \mathrm{Id} + 2\lambda_1 l_1\right) M^{-1} \pmod{\ell^T}. \tag{9}$$

Since we also have $\frac{1}{2}\operatorname{tr}\left({l_1}^2\right) \equiv \frac{1}{2}\operatorname{tr}\left({l_2}^2\right) \pmod{\ell^T}$ (recall that ℓ is odd, so we can safely divide by 2) and ${l_2}^2 \equiv M {l_1}^2 M^{-1} \pmod{\ell^T}$ we see that (9) implies

$$2\lambda_1 l_2 \equiv M\left(2\lambda_1 l_1\right) M^{-1} \equiv 2\lambda_2 l_2 \pmod{\ell^T}.$$

If l_2 has at least one coordinate not divisible by ℓ, this last equation implies $\lambda_1 \equiv \lambda_2 \pmod{\ell^T}$. If not, then g_2' reduces modulo ℓ to a multiple of the identity (cf. equation (7)). Moreover, as $\det(g_2') = 1$, we have in particular

$$1 = \det(\lambda_2 \mathrm{Id} + l_2) = {\lambda_2}^2 - \frac{\operatorname{tr}\left({l_2}^2\right)}{2},$$

from which we find

$$\lambda_2 = \pm\sqrt{1 + \frac{\operatorname{tr}({l_2}^2)}{2}}, \tag{10}$$

where the square root can be computed via the usual series expansion $\sqrt{1+t} = \sum_{j \geq 0} \binom{1/2}{j} t^j$, which converges because l_2 is trivial modulo ℓ (hence the same is true for $\frac{1}{2}\operatorname{tr}\left({l_2}^2\right)$; recall that we have assumed ℓ to be odd). Symmetrically we prove that either the congruence $\lambda_1 \equiv \lambda_2 \pmod{\ell^T}$ holds or else l_1 is trivial modulo ℓ and

$$\lambda_1 = \pm\sqrt{1 + \frac{\operatorname{tr}({l_1}^2)}{2}}. \tag{11}$$

Suppose then l_1, l_2 to both be trivial modulo ℓ: then $\operatorname{tr}({l_1}^2)$ and $\operatorname{tr}({l_2}^2)$ are divisible by ℓ, hence the square roots appearing in equations (10) and (11) can both be computed by the series expansion recalled above. Using the congruence $\frac{\operatorname{tr}({l_1}^2)}{2} \equiv \frac{\operatorname{tr}({l_2}^2)}{2} \pmod{\ell^T}$ we obtain $\sqrt{1+\frac{\operatorname{tr}({l_1}^2)}{2}} \equiv \sqrt{1+\frac{\operatorname{tr}({l_2}^2)}{2}} \pmod{\ell^T}$, hence to prove our claim $\lambda_1 \equiv \lambda_2 \pmod{\ell^T}$ it suffices to show that the signs in equations (10) and (11) are the same.

Since $\sqrt{1+\frac{\operatorname{tr}({l_1}^2)}{2}} \equiv \sqrt{1+\frac{\operatorname{tr}({l_2}^2)}{2}} \equiv 1 \pmod{\ell}$, in order to prove this it is enough to show that $\lambda_1 \equiv \lambda_2 \pmod{\ell}$. Observe that g_1', g_2' reduce to diagonal matrices $\operatorname{diag}(\lambda_i, \lambda_i)$ in $\operatorname{SL}_2(\mathbb{F}_\ell)$, so we have $\lambda_1 \equiv \lambda_2 \pmod{\ell}$ if and only if g_1', g_2' (or equivalently g_1, g_2) have the same reduction modulo ℓ, and this is exactly property (2) of H_ℓ given in theorem 4.2. This establishes the claim when ℓ is odd.

Consider now the case $\ell = 2$. Then l_1, l_2 vanish modulo 4 by definition of H_2, and the same argument as above shows that

$$\lambda_i = \pm\sqrt{1+\frac{\operatorname{tr}({l_i}^2)}{2}},\ i = 1, 2. \tag{12}$$

Given that $2\lambda_i \equiv \operatorname{tr}(g_i') \equiv 2 \pmod{8}$ by our construction of H_2, we have $\lambda_1 \equiv \lambda_2 \equiv 1 \pmod{4}$, so the sign in equation (12) must be a plus both for $i = 1$ and $i = 2$. From the congruence $\frac{\operatorname{tr}\left({l_1}^2\right)}{2} \equiv \frac{\operatorname{tr}\left({l_2}^2\right)}{2} \pmod{2^{T-1}}$ we then deduce

$$\lambda_1 \equiv \sqrt{1+\frac{\operatorname{tr}({l_1}^2)}{2}} \equiv \sqrt{1+\frac{\operatorname{tr}({l_2}^2)}{2}} \equiv \lambda_2 \pmod{2^{T-2}}$$

as claimed. □

Let us take a moment to summarize what we have proved so far. We have set L_0 to be the kernel of the natural projection from $L(H_\ell)$, the Lie algebra of H_ℓ, to L_1, the Lie algebra of $L(H_{\ell,1})$. We know that L_0 is generated by three elements $(0, y_1), (0, y_2), (0, y_3)$, and we have just proved that if y_1, y_2, y_3 are all zero modulo ℓ^t for a certain positive integer $t \geq n_2 + 1$, then there exists a matrix $M \in M_2(\mathbb{Z}_\ell)$ with the following properties:

- at least one of the coefficients of M is an ℓ-adic unit;
- for every $(g_1, g_2) \in H_\ell$ we have $g_2 \equiv M g_1 M^{-1} \pmod{\ell^{T-2v}}$.

These facts can be combined to give an upper bound on the values of t for which we can have $y_1 \equiv y_2 \equiv y_3 \equiv 0 \pmod{\ell^t}$:

Proposition 6.11. *Set* $t_{\max} := \left\lfloor \frac{v_\ell(b_0(E_1 \times E_2/K_\ell))}{2} \right\rfloor + 11n_1 + n_2 + 7v + 7$. *At least one of* y_1, y_2, y_3 *does not vanish modulo* $\ell^{t_{\max}}$.

Proof. If one of y_1, y_2, y_3 is nonzero modulo ℓ^{n_2} we are done, so suppose once more that $t \geq n_2 + 1$ is an integer such that $y_1 \equiv y_2 \equiv y_3 \equiv 0 \pmod{\ell^t}$. We keep using the symbols M, T from above, and set $H := T - 2v$. We shall prove that $t \leq t_{\max} - 1$.

By definition, for every $w \in E_1[\ell^H]$ we have $\ell^H w = 0$, so for every $(g_1, g_2) \in H_\ell$ we have

$$M g_1 w = M g_1 M^{-1} M w = (g_2 M + O(\ell^H))w = g_2 M w.$$

It follows that the subgroup $\Gamma = \left\{(w, Mw) \mid w \in E_1[\ell^H]\right\}$ of $E_1 \times E_2$ is defined over K_ℓ: indeed for any $(g_1, g_2) \in H_\ell$ and $(w, Mw) \in \Gamma$ we have

$$(g_1, g_2) \cdot (w, Mw) = (g_1 w, g_2 M w) = (g_1 w, M g_1 w) \in \Gamma.$$

Thus the abelian variety $A^* = (E_1 \times E_2)/\Gamma$ is defined over K_ℓ, and the canonical projection $E_1 \times E_2 \to A^*$ is an isogeny of degree $|E_1[\ell^H]| = \ell^{2H}$; on the other hand, since we are in the situation of theorem 2.4, we also have an isogeny $A^* \to E_1 \times E_2$ of degree b dividing $b_0(E_1 \times E_2/K_\ell)$ (recall that the function b_0 has been introduced in definition 2.5). The composition of these two isogenies is an endomorphism φ of $E_1 \times E_2$ that kills Γ. Since E_1, E_2 are not isogenous over $\overline{K}$, such an endomorphism corresponds to a pair (φ_1, φ_2) where φ_i is an endomorphism of E_i, and the assumption $\operatorname{End}_{\overline{K}}(E_i) = \mathbb{Z}$ implies that each φ_i is multiplication by an integer. Moreover, since at least one of the coefficients of M is an ℓ-adic unit, we deduce that the projection of Γ on E_2 contains at least one point of exact order ℓ^H, so φ, which kills Γ, must be of the form $\begin{pmatrix} \ell^H e_1 & 0 \\ 0 & \ell^H e_2 \end{pmatrix}$ for some $e_1, e_2 \in \mathbb{Z}$. It follows that ${e_1}^2 {e_2}^2 \ell^{4H} = \deg(\varphi) = \ell^{2H} b$, hence we have $2H \leq v_\ell(b) \leq v_\ell(b_0(E_1 \times E_2/K_\ell))$ and $2t \leq v_\ell(b_0(E_1 \times E_2/K_\ell)) + 2(11n_1 + n_2 + 7v + 6)$. This inequality is not satisfied for any $t \geq t_{\max}$. □

Combined with corollary 6.6, the last proposition shows that L_0 contains $\ell^{f_1}\mathfrak{sl}_2(\mathbb{Z}_\ell)$, where

$$f_1 = \left\lfloor \frac{v_\ell(b_0(E_1 \times E_2/K_\ell))}{2} \right\rfloor + 11n_1 + 5n_2 + 11v + 7,$$

and therefore $L(H_\ell)$ contains $0 \oplus \ell^{f_1}\mathfrak{sl}_2(\mathbb{Z}_\ell)$. Exchanging the roles of E_1 and E_2 and repeating the whole argument, we deduce that $L(H)$ contains $\ell^f\mathfrak{sl}_2(\mathbb{Z}_\ell) \oplus \ell^f\mathfrak{sl}_2(\mathbb{Z}_\ell)$, where now

$$f = \left\lfloor \frac{v_\ell(b_0(E_1 \times E_2/K_\ell))}{2} \right\rfloor + 16 \max\{n_1, n_2\} + 11v + 7. \tag{13}$$

We have all we need to prove the following proposition:

Proposition 6.12. *Let E_1, E_2 be elliptic curves over K that are not isogenous over $\overline{K}$ and do not admit complex multiplication over $\overline{K}$. Let ℓ be a prime number.*

Suppose the image of $\operatorname{Gal}(\overline{K_\ell}/K_\ell) \to \operatorname{Aut}(T_\ell(E_i))$ *contains $\mathcal{B}_\ell(n_i)$ for $i = 1, 2$ (where $n_i \geq 2$ for $\ell = 2$ and $n_i \geq 1$ for $\ell = 3$ or 5). Let f be given by formula (13). If ℓ is odd, the image G_ℓ of* $\operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}(T_\ell(E_1)) \times \operatorname{Aut}(T_\ell(E_2))$ *contains $\mathcal{B}_\ell(4f, 4f)$; if $\ell = 2$, the image G_2 of* $\operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}(T_2(E_1)) \times \operatorname{Aut}(T_2(E_2))$ *contains*

$$\mathcal{B}_2(12(f + 17\max\{n_1, n_2\} + 13) + 1, 12(f + 17\max\{n_1, n_2\} + 13) + 1).$$

Proof. For $\ell = 2$ the result follows at once from theorem 4.4. For odd ℓ, and under assumption 6.1, the result similarly follows from property (1) of H_ℓ given in theorem 4.2 and the fact that $2f > 8\max\{n_1, n_2\}$. On the other hand, if assumption 6.1 does *not* hold, then G_ℓ contains $\mathcal{B}_\ell(20\max\{n_1, n_2\}, 20\max\{n_1, n_2\})$ (note that we can assume $m_1 \leq n_1, m_2 \leq n_2$ without loss of generality, cf. remark 6.3), which is stronger than what we are claiming. □

7 Conclusion

Consider again the case of two elliptic curves E_1, E_2 defined over K, non-isogenous over $\overline{K}$ and such that $\operatorname{End}_{\overline{K}}(E_i) = \mathbb{Z}$. Let $\mathcal{P}$ be the set of primes ℓ for which G_ℓ does not contain $\operatorname{SL}_2(\mathbb{Z}_\ell)^2$.

Lemma 7.1. *Let ℓ be a prime. If ℓ does not divide the product*

$$30 b_0(E_1/K; 60) b_0\left(E_1^2/K; 2\right) b_0(E_2/K; 60) b_0\left(E_2^2/K; 2\right) b_0(E_1 \times E_2/K; 2),$$

then ℓ is not in $\mathcal{P}$.

Proof. Denote by $G_\ell(\ell)$ the modulo-ℓ reduction of G_ℓ, that is, its image in $\operatorname{GL}_2(\mathbb{F}_\ell)^2$. By [2, Lemma 8.2] we know that if a prime ℓ does not divide

$$b_0(E_1/K; 60) b_0\left(E_1^2/K; 2\right) b_0(E_2/K; 60) b_0\left(E_2^2/K; 2\right)$$

then both projections of $G_\ell(\ell)$ on the two factors $\mathrm{GL}_2(\mathbb{F}_\ell)$ contain $\mathrm{SL}_2(\mathbb{F}_\ell)$. Under this hypothesis, the proof of [5, Proposition 1] shows that $G_\ell(\ell)$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)^2$ unless $\ell^2 \bigm| b_0(E_1 \times E_2/K;2)$. Finally, when $\ell \geq 5$ (as is the case here, thanks to the factor 30 appearing in the product) a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)^2$ whose projection modulo ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell)^2$ contains all of $\mathrm{SL}_2(\mathbb{Z}_\ell)^2$ (this is well-known; see for example [11, Proposition 4.2]). □

Corollary 7.2. *We have*

$$\prod_{\ell \in \mathcal{P}} \ell \leq 30 b_0(E_1/K;60) b_0\left(E_1^2/K;2\right) b_0(E_2/K;60) b_0\left(E_2^2/K;2\right) b_0(E_1 \times E_2/K;2).$$

Let ℓ be a prime different from 2 and 3, and for $j=1,2$ set

$$D_j(\infty) = b_0(E_j/K;24)^5 b_0(E_j^2/K;24).$$

Since $\ell^{v_\ell(D_j(\infty))+1}$ does not divide $D_j(\infty)$, we see from [2, Theorem 7.5] that $G_{\ell,j}$ contains $\mathcal{B}_\ell\left(16 v_\ell(D_j(\infty))+12\right)$, hence the same is true for $H_{\ell,j}$, cf. remark 6.3. Therefore – in the notation of the previous section – we can take $n_j = n_j(\ell) = 16 v_\ell(D_j(\infty)) + 12$ (this obviously satisfies the condition $n_1, n_2 \geq 1$ for $\ell = 5$ – cf. definition 6.2). For $\ell = 3$, using the fact that our group $H_{3,j}$ is the group H_3 of [2] we see (again by [2, Theorem 7.5]) that we can take

$$n_j(3) = 16 v_3\left(b_0(E/K_3)^5 b_0(E^2/K_3)\right) + 12 \leq 16 v_3(D_j(\infty)) + 12;$$

similarly, for $\ell = 2$ we can take $n_j(2) = 48 v_2\left(b_0(E_j/K_2)^5 b_0(E_j^2/K_2)\right) + 38$. Applying proposition 6.12 with these values of $n_j(\ell)$ we get:

Lemma 7.3. *Let ℓ be a prime. The group G_ℓ contains $\mathcal{B}_\ell(f(\ell), f(\ell))$, where $f(\ell)$ is given by*

$$f(\ell) = 2 v_\ell(b_0(E_1 \times E_2/K; 2^9 \cdot 3^2)) + 2^{10} \max\left\{v_\ell(D_1(\infty)), v_\ell(D_2(\infty))\right\} + 800$$

for odd ℓ and

$$f(2) = 6 v_2(b_0(E_1 \times E_2/K_2)) + 19008 \max_j \left\{ v_2\left(b_0(E_j/K_2)^5 b_0(E_j^2/K_2)\right)\right\} + 15421$$

for $\ell = 2$.

Using the very same argument as in [2, §9], and some very crude estimates, we deduce

Proposition 7.4. *Denote by G_∞ the image of $\mathrm{Gal}\left(\overline{K}/K\right)$ inside*

$$\prod_\ell \left(\operatorname{Aut} T_\ell(E_1) \times \operatorname{Aut} T_\ell(E_2)\right) \subset \mathrm{GL}_2(\hat{\mathbb{Z}})^2.$$

G_∞ contains a subgroup S of the form $S = \prod_\ell S_\ell$, where each S_ℓ coincides with $\mathrm{SL}_2(\mathbb{Z}_\ell)^2$ except for the finitely many primes that are in $\mathcal{P}$, for which $S_\ell = \mathcal{B}_\ell(f(\ell), f(\ell))$. The index of S in $\mathrm{SL}_2(\hat{\mathbb{Z}})$ is bounded by $b(E_1 \times E_2/K; 2^9 \cdot 3^2)^{10^4}$.

We finally come to the adelic estimate for an arbitrary number of curves:

Theorem 7.5. *Let $E_1, \ldots, E_n$, $n \geq 2$, be elliptic curves defined over K, pairwise non-isogenous over $\overline{K}$. Suppose that $\operatorname{End}_{\overline{K}}(E_i) = \mathbb{Z}$ for $i = 1, \ldots, n$ and let G_∞ be the image of the natural representation*

$$\rho_\infty : \mathrm{Gal}\left(\overline{K}/K\right) \to \prod_{i=1}^n \prod_\ell \operatorname{Aut} T_\ell(E_i) \cong \mathrm{GL}_2(\hat{\mathbb{Z}})^n.$$

Then G_∞ has index at most

$$8^{n(n-2)} \zeta(2)^{n(n-1)} \cdot [K:\mathbb{Q}] \cdot \max_{i \neq j} b\left(E_i \times E_j/K; 2^9 \cdot 3^2\right)^{5000 n(n-1)}$$

in

$$\Delta = \left\{ (x_1, \ldots, x_n) \in \mathrm{GL}_2(\hat{\mathbb{Z}})^n \bigm| \det x_i = \det x_j \quad \forall i,j \right\}.$$

Proof. The Galois-equivariance of the Weil pairing implies that for every index $i = 1, \ldots, n$ an element $g \in \operatorname{Gal}\left(\overline{K}/K\right)$ acts on $T_\ell(E_i)$ through an automorphism of determinant $\chi_\ell(g)$. This immediately implies that $G_\infty \subseteq \Delta$. With a slight abuse of language, we write det for the map $\Delta \to \hat{\mathbb{Z}}$ sending $(x_1, \ldots, x_n)$ to $\det x_1$. The exact sequence

$$1 \to G_\infty \cap \mathrm{SL}_2(\hat{\mathbb{Z}})^n \to G_\infty \xrightarrow{\det} \hat{\mathbb{Z}}^\times \to \frac{\hat{\mathbb{Z}}^\times}{\det(G_\infty)} \to 1$$

and the inequality $\left| \dfrac{\hat{\mathbb{Z}}^\times}{\det(G_\infty)} \right| \leq [K : \mathbb{Q}]$ (cf. [2, Proposition 8.1]) show that in order to establish the theorem it is enough to prove that the index of $G_\infty \cap \mathrm{SL}_2(\hat{\mathbb{Z}})^n$ inside $\mathrm{SL}_2(\hat{\mathbb{Z}})^n$ is bounded by

$$8^{n(n-2)}\zeta(2)^{n(n-1)} \cdot \max_{i \neq j} b(E_i \times E_j/K; 2^9 \cdot 3^2)^{5000n(n-1)}.$$

Set $G = G_\infty \cap \mathrm{SL}_2(\hat{\mathbb{Z}})$. For every pair E_i, E_j of curves, we get from proposition 7.4 a subgroup $S^{(i,j)}$ of

$$\mathrm{SL}_2(\hat{\mathbb{Z}})^2 \subseteq \prod_\ell \operatorname{Aut}\left(T_\ell(E_i)\right) \times \prod_\ell \operatorname{Aut}\left(T_\ell(E_j)\right)$$

that satisfies all the requirements of corollary 3.3, and the theorem follows from this corollary upon recalling that the index of $S^{(i,j)}$ in $\mathrm{SL}_2(\hat{\mathbb{Z}})^2$ is bounded by $b(E_i \times E_j/K; 2^9 \cdot 3^2)^{10000}$. □

The deduction of theorem 1.1 is then immediate:

Proof. The definition of the function $b(A/K; d)$ (cf. proposition 2.7) shows that $b(E_i \times E_j/K; 2^9 \cdot 3^2)$ is a polynomial in $[K : \mathbb{Q}]$ and in the quantity $\max\{1, \log[K : \mathbb{Q}], h(E_i \times E_j)\}$. As the stable Faltings height is additive on products we find that $h(E_i \times E_j) = h(E_i) + h(E_j)$ does not exceed $2\max\{h(E_i), h(E_j)\}$, and it follows that there exists a polynomial $q(d, H) \in \mathbb{R}[d, H]$ such that $\max_{i \neq j} b(E_i \times E_j; 2^9 \cdot 3^2)$ is bounded by $q([K : \mathbb{Q}], H)$, where $H = \max\{1, \log[K : \mathbb{Q}], h(E_1), \ldots, h(E_n)\}$. The previous theorem then yields the inequality

$$[\Delta : G_\infty] \leq C^{n(n-1)} \cdot [K : \mathbb{Q}] \cdot q([K : \mathbb{Q}], H)^{5000n(n-1)},$$

where $C = 8\zeta(2)$, which has the required functional form. The explicit polynomial function given in the statement can now be determined by a straightforward direct computation. □

References

[1] É. Gaudron and G. Rémond. Polarisations et isogénies. *Duke Math. J.*, 163(11):2057–2108, 2014.

[2] D. Lombardo. Bounds for Serre's open image theorem for elliptic curves over number fields. *Algebra and Number Theory.* To appear.

[3] D. Lombardo. Pink-type results for general subgroups of $\mathrm{SL}_2(\mathbb{Z}_\ell)^n$. *ArXiv e-Prints.* Available at http://arxiv.org/abs/1501.03938. Submitted (January 2015).

[4] D. W. Masser. Multiplicative isogeny estimates. *J. Austral. Math. Soc. Ser. A*, 64(2):178–194, 1998.

[5] D. W. Masser and G. Wüstholz. Galois properties of division fields of elliptic curves. *Bull. London Math. Soc.*, 25(3):247–254, 1993.

[6] D. W. Masser and G. Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.

[7] D. W. Masser and G. Wüstholz. Periods and minimal abelian subvarieties. *Ann. of Math. (2)*, 137(2):407–458, 1993.

[8] R. Pink. Classification of pro-p subgroups of SL_2 over a p-adic ring, where p is an odd prime. *Compositio Math.*, 88(3):251–264, 1993.

[9] K. A. Ribet. On ℓ-adic representations attached to modular forms. *Invent. Math.*, 28:245–275, 1975.

[10] K. A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[11] K. A. Ribet. Images of semistable Galois representations. *Pacific J. Math.*, Special Issue:277–297, 1997. Olga Taussky-Todd: in memoriam.

[12] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.