An explicit open image theorem for products of elliptic curves

Davide Lombardo

Abstract

We bound the index of the adelic representation of $\mathrm{Gal}\left(\overline{K}/K\right)$ associated with a product $E_1 \times \ldots \times E_n$ of pairwise non-isogenous elliptic curves (defined over K, a number field) that do not admit complex multiplication.

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 [Lom14]. 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 $\mathrm{End}_{\overline{K}}(E_i) = \mathbb{Z}$ for $i = 1, \ldots, n$, and denote G_∞ the image of $\mathrm{Gal}\left(\overline{K}/K\right)$ inside*

$$\prod_\ell \mathrm{Aut}(T_\ell(E_1 \times \cdots \times E_n)) \subset \mathrm{GL}_2(\hat{\mathbb{Z}})^n.$$

Set $\gamma := 9 \cdot 10^{11}, \delta := \exp\exp\exp(13)$, and let $H = \max\{1, \log[K:\mathbb{Q}], \max_i h(E_i)\}$, 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

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

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 the statement we actually prove (theorem 7.5 below) is more precise and expressed in terms of the function b_0 of definition 2.4: theorem 1.1 then follows immediately by corollary 2.6 and elementary estimates.

It should be noted that it has been known since the work of Serre and Masser-Wüstholz (cf. [MW93], Main Theorem and Proposition 1) that the isogeny theorem (section 2 below) implies an effective bound ℓ_0 on the largest prime ℓ for which the image of the representation $\mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(T_\ell(E_1 \times \ldots \times E_n))$ does not contain $\mathrm{SL}_2(\mathbb{Z}_\ell)^n$. As it was in [Lom14], the main difficulty here lies in controlling the image of the representation modulo powers of primes smaller than ℓ_0.

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 [Rib75, 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. In those instances when the need will arise 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 $\mathrm{SL}_2(\mathbb{Z}_\ell)$ given by*

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

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

Let us now describe the proof method proper.

As a first step, a short argument shows that it is enough to consider products $E_1 \times E_2$ involving only two factors: this is done by proving that a subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)^n$ 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 [Rib76, Lemma on p. 790].

With this result at hand we are thus reduced to dealing with subgroups G of $\mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{SL}_2(\mathbb{Z}_\ell)$ whose projections on either factor are of finite index in $\mathrm{SL}_2(\mathbb{Z}_\ell)$. Note that this latter fact is the open image theorem for a single elliptic curve, which was proved by Serre in [Ser72] and made explicit in [Lom14]. We wish to show that G is of (explicitly bounded) finite index in $\mathrm{SL}_2(\mathbb{Z}_\ell)^2$, that is, we want to exhibit a t such that G contains $\mathcal{B}_\ell(t,t)$: this clearly comes down to proving that the two kernels $K_i = \ker\left(G \xrightarrow{\pi_i} \mathrm{SL}_2(\mathbb{Z}_\ell)\right)$, when identified with subgroups of $\mathrm{SL}_2(\mathbb{Z}_\ell)$, 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 also give the statements of two technical results whose proof, being rather lengthy, is deferred to the companion paper [Lom15]; while the results themselves are more complicated, the methods used to show them do not differ much from those of [Lom14], where the case of a single elliptic curve is treated.

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 $\mathrm{SL}_2(\mathbb{Z}_\ell)$) 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 $\mathrm{SL}_2(\mathbb{Z}_\ell)$ must itself be of finite index in $\mathrm{SL}_2(\mathbb{Z}_\ell)$. The simplicity of this reduction step is mainly due to the fact that we can consider Lie algebras instead of working directly with the corresponding groups (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 [Rib76]), 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 more complicated 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, in section 7, the desired adelic result for any finite product.

Notation. Throughout the whole paper, the prime 2 plays a rather special role, and special care is needed to treat it. 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

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

We will also consistently use the following notations:

- G_ℓ, to denote the image of $\mathrm{Gal}\left(\overline{K}/K\right)$ in $\mathrm{Aut}(T_\ell(A))$;
- $G(\ell^n)$, where G is a closed subgroup of a certain $\mathrm{GL}_2(\mathbb{Z}_\ell)^k$, to denote the reduction of G modulo ℓ^n, that is to say its image in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})^k$;
- $N(G)$, where G is as above, to denote the largest normal pro-ℓ subgroup of G;
- G', to denote the topological closure of the commutator subgroup.

2 Preliminaries on isogeny bounds

The main tool that makes all the effective estimates possible is a very explicit isogeny-type theorem taken from [GR14]. 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. *([GR14] 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 $h(A)$.

In [Mas98] (cf. especially lemma 3.4) Masser shows the following:

Theorem 2.3. *(Masser) Suppose that A/K is an Abelian variety that is isomorphic over $\overline{K}$ to a product $A_1^{e_1} \times \ldots \times A_m^{e_m}$, where each A_i is simple and has trivial endomorphism ring over $\overline{K}$. Suppose furthermore that for every A^* isogenous to A over K we can find an isogeny $A^* \to A$ of degree bounded by b for a certain constant b. Then there exists an integer $b_0 \leq b$ such that we can always choose a K-isogeny $A^* \to A$ of degree dividing b_0.*

We will denote $b_0(A/K)$ the minimal b_0 with the property of the above theorem; in particular $b_0(A/K) \leq b(A/K)$. Consider now $b_0(A/K')$ as K' ranges through all the finite extensions of K of degree bounded by d. On one hand, $b_0(A/K)$ divides $b_0(A/K')$ ([Mas98], p.190); on the other $b_0(A/K') \leq b(d[K:\mathbb{Q}], h(A), \dim(A))$ stays bounded, and therefore the number

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

exists and is finite. We give this function a name:

Definition 2.4. *Suppose A/K is a product of simple varieties with absolutely trivial endomorphism ring. Then we define*

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

The function $b_0(A/K; d)$ is studied in [Mas98, Theorem D]. Adapting the argument given by Masser to the form of the function $b(d[K:\mathbb{Q}], h(A), \dim(A))$ at our disposal it is immediate to prove:

Proposition 2.5. *If A/K is as in the previous definition and of dimension g, then*

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

In particular, for $d = 2\cdot 48^2$ and $g = 2$ we have

Corollary 2.6. *If $E_1, E_2/K$ are elliptic curves without potential complex multiplication, we have*

$$b_0\left(E_1 \times E_2/K; 2\cdot 48^2\right) \leq \exp\exp\exp(12.5)\cdot\left([K:\mathbb{Q}]\cdot H^2\right)^{1.5\cdot 10^9},$$

where $H = \max\{1, \log[K:\mathbb{Q}], h(E_1), h(E_2)\}$.

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

As anticipated, we show that a (necessary and) sufficient condition for a 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 will follow rather easily from the following elementary lemma (whose easy verification we omit):

Lemma 3.1. *Let s_1, s_2 be non-negative integers. The commutator group $[\mathcal{B}_\ell(s_1), \mathcal{B}_\ell(s_2)]$ contains $B_\ell(s_1 + s_2 + 2v)$, and the iterated commutator $\underbrace{[\cdots[}_{(n-1)\text{ times}} \mathcal{B}_\ell(s_1), \mathcal{B}_\ell(s_2)\ ], \mathcal{B}_\ell(s_3)], \cdots, \mathcal{B}_\ell(s_n)]$ contains $B_\ell(s_1 + \cdots + s_n + 2(n-1)v)$.*

Lemma 3.2. *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 $\mathrm{SL}_2(\mathbb{Z}_\ell)$. 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 s_{ij}: then G contains*

$$\prod_{i=1}^n \mathcal{B}_\ell\left(\sum_{j\neq i} s_{ij} + (n-2)v\right).$$

Proof. Clearly by the symmetry of the problem it is enough to show that G contains

$$\{\mathrm{Id}\} \times \cdots \times \{\mathrm{Id}\} \times \mathcal{B}_\ell\left(\sum_{j\neq n} s_{nj} + (n-2)v\right).$$

Thanks to the above lemma, for any g in $\mathcal{B}_\ell\left(\sum_{j\neq n} s_{ij} + (n-2)v\right)$ there exist elements y_i in $\mathcal{B}_\ell(s_{in})$ (for $i = 1, \ldots, n-1$) such that g can be written as the iterated commutator $[\cdots[[y_1, y_2], y_3], \cdots, y_{n-1}]$. By hypothesis we can find $x_1, \ldots, x_{n-1} \in G$ such that $\pi_i(x_i) = \mathrm{Id}$ and $\pi_n(x_i) = y_i$ for all i between 1 and $n-1$. Consider now the iterated commutator

$$\tilde{g} = [\cdots[[x_1, x_2], x_3], \cdots, x_{n-1}]:$$

this is a product of elements of G, and therefore it is itself an element of G. For $i \leq n-1$, the i-th component of $\tilde{g}$ is trivial, since

$$\pi_i(\tilde{g}) = [\cdots[\cdots[[\pi_i(x_1), \pi_i(x_2)], \pi_i(x_3)], \cdots, \underbrace{\pi_i(x_i)}_{\mathrm{Id}}], \cdots, \pi_i(x_{n-1})]$$

On the other hand, our choice of $y_1, \ldots, y_{n-1}$ ensures that

$$\pi_n(\tilde{g}) = [\cdots[[y_1, y_2], y_3], \cdots, y_{n-1}] = g.$$

We have thus shown that $(1, 1, \ldots, 1, g) = \tilde{g}$ is an element of G for any choice of g in $\mathcal{B}_\ell\left(\sum_{j\neq n} s_{ij} + (n-2)v\right)$, and repeating the argument for the other projections gives the required result. □

Corollary 3.3. *Let G be a closed subgroup of $\prod_{i=1}^n \mathrm{SL}_2(\hat{\mathbb{Z}})$. Suppose that for every pair of indices $i \neq j$ we can find a group $S^{(i,j)} \subseteq \mathrm{SL}_2(\hat{\mathbb{Z}})^2$ 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 $\prod_\ell S_\ell^{(i,j)}$;*
- *for almost every ℓ, the group $S_\ell^{(i,j)}$ is all of $\mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{SL}_2(\mathbb{Z}_\ell)$;*

- *for every prime ℓ such that $S_\ell^{(i,j)} \neq \mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{SL}_2(\mathbb{Z}_\ell)$ there exists an integer $f_\ell^{(i,j)}$ such that $S_\ell^{(i,j)} = \mathcal{B}_\ell(f_\ell^{(i,j)}, f_\ell^{(i,j)})$.*

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

$$2^{12n(n-2)} \zeta(2)^2 c^{n(n-1)/2}.$$

Proof. Let ℓ be an odd prime. If $S_\ell^{(i,j)} = \mathrm{SL}_2(\mathbb{Z}_\ell)^2$ for all (i,j), then the previous lemma applies with $s = 0$ and shows that $\prod_{k=1}^n \mathrm{SL}_2(\mathbb{Z}_\ell)$ is contained in G.

Suppose on the other hand that either $\ell = 2$ or for at least one pair (i,j) we have $S_\ell^{(i,j)} \neq \mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{SL}_2(\mathbb{Z}_\ell)$, and set $f_\ell = \max_{i \neq j} f_\ell^{(i,j)}$. 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

$$B_\ell \left(\sum_{j \neq 1} f_\ell^{(j,1)} + 2(n-2)v, \ldots, \sum_{j \neq n} f_\ell^{(j,n)} + 2(n-2)v \right).$$

Note that the index of this group in $\prod_{i=1}^n \mathrm{SL}_2(\mathbb{Z}_\ell)$ is at most

$$\prod_{j=1}^n \left(\ell^{3 \sum_{j \neq i} f_\ell^{(j,i)} + 12(n-2)v} \right) = 2^{12(n-2)v} \prod_{j=1}^n \prod_{i \neq j} \ell^{3 f_\ell^{(j,i)}}.$$

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

$$\left[\prod_{k=1}^n \mathrm{SL}_2(\hat{\mathbb{Z}}) : G \right] \leq 2^{12n(n-2)} \prod_{\ell \in \mathcal{P}} \prod_{j=1}^n \prod_{i \neq j} \ell^{3 f_\ell^{(j,i)}}.$$

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 $\ell^{6 f_\ell^{(i,j)}} \cdot \left(\frac{\ell^2 - 1}{\ell^2} \right)^2$ (and this is true even if $f_\ell^{(i,j)} = 0$), so the above product is bounded by

$$\begin{aligned}
2^{12n(n-2)} \prod_{\ell \in \mathcal{P}} \prod_{i<j} \left\{ \left[\mathrm{SL}_2(\mathbb{Z}_\ell)^2 : S_\ell^{(i,j)} \right] \cdot \left(\frac{\ell^2}{\ell^2 - 1} \right)^2 \right\} & \\
&\leq 2^{12n(n-2)} \prod_{\ell} \left(\frac{\ell^2}{\ell^2 - 1} \right)^2 \cdot \prod_{i<j} \prod_{\ell \in \mathcal{P}} \left[\mathrm{SL}_2(\mathbb{Z}_\ell)^2 : S_\ell^{(i,j)} \right] \\
&\leq 2^{12n(n-2)} \zeta(2)^2 \prod_{i<j} c^{(i,j)} \\
&\leq 2^{12n(n-2)} \zeta(2)^2 c^{n(n-1)/2}.
\end{aligned}$$

□

4 Lie subalgebras of $\mathrm{sl}_2(\mathbb{Z}_\ell)^n$ 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. [Pin93]) Let ℓ be a prime. Define maps Θ_n as follows:*

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

If G is a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)^n$ (resp. of $B_2(2, \ldots, 2)$ in case $\ell = 2$), define $L(G) \subseteq \mathfrak{sl}_2(\mathbb{Z}_\ell)^n$ as the $\mathbb{Z}_\ell$-span of $\Theta_n(G)$. We call $L(G)$ the Lie algebra of G.

The crucial importance of this construction lies in the fact that it allows us to linearize the problem of showing that a certain subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)^n$ contains an open neighbourhood of the identity. Indeed, we have the following two results, for whose proof we refer the reader to [Lom15].

Theorem 4.2. *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 n_1, n_2 be integers such that G_i contains $\mathcal{B}_\ell(n_i)$ 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 $\mathcal{B}_\ell(4n_1 + 16n_2, 8n_2)$*
- *there exists a subgroup T of G, of index dividing $2 \cdot 48^2$, with the following properties:*
  - *if $L(T)$ 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*
  $$p = 2k + \max\{2k, 8n_1, 8n_2\}.$$
  We call this property $(*)$.
  - *for any (t_1, t_2) in T, if both $[t_1]$ and $[t_2]$ are diagonal, then they are equal.*

Theorem 4.3. *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 G_1, G_2 the two projections of G on the factors $\mathrm{GL}_2(\mathbb{Z}_2)$, and let n_1, n_2 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 $\det(g_1) = \det(g_2)$.*

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

$$\mathcal{B}_2(12(k + 13n_2 + 5n_1 + 6), 12(k + 13n_1 + 5n_2 + 6)).$$

Finally, the following easy lemma characterizes conjugation-stable subalgebras of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$:

Lemma 4.4. *([Lom15, Lemma 2.1]) Let ℓ be a prime number, t a non-negative integer, and $W \subseteq \mathfrak{sl}_2(\mathbb{Z}_\ell)$ a Lie subalgebra that does not reduce to zero modulo ℓ^t and that is stable under conjugation by $\mathcal{B}_\ell(s)$, where $s \geq 0$ is at least 2 if $\ell = 2$ and at least 1 if $\ell = 3$ or 5 (no conditions are necessary if $\ell \geq 7$). The open set $\ell^{t+4s+4v} \mathfrak{sl}_2(\mathbb{Z}_\ell)$ is contained in W.*

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

We will obtain in this section a description of the automorphisms of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$ showing that they are all inner, in a suitable sense. 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 $p(x) \in \mathbb{Z}_\ell[x]$ and $\alpha \in \mathbb{Z}_\ell$. Suppose that $v_\ell(p(\alpha)) > 2v_\ell(p'(\alpha))$: then $p(x)$ admits a root $\bar{\alpha}$ such that $v_\ell(\alpha - \bar{\alpha}) \geq v_\ell(p(\alpha)) - v_\ell(p'(\alpha))$.*

The main tool we will use to produce approximate solutions to polynomials is the following simple lemma:

Lemma 5.2. *Let ℓ be a prime number, $n \geq 1, m \geq 1$, $g \in \mathrm{End}(\mathbb{Z}_\ell^m)$ and $p_g(t)$ the characteristic polynomial of g. Let furthermore $\lambda \in \mathbb{Z}/\ell^n\mathbb{Z}, w \in (\mathbb{Z}/\ell^n\mathbb{Z})^m$ be such that $gw \equiv \lambda w \pmod{\ell^n}$. Suppose that at least one of the coordinates of w has valuation at most α: then $p_g(\lambda) \equiv 0 \pmod{\ell^{n-\alpha}}$.*

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

An immediate computation also shows:

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

Let us also recast Hensel's lemma into a form that is very useful for our purposes:

Lemma 5.4. *Let g be an element of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$, w a vector in $\mathbb{Z}_\ell^2$ and let β be the minimal valuation of the coefficients of w. Let furthermore $\pm\mu$ be the eigenvalues of g, and 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. 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 $v_\ell(\nu - \lambda) \geq n - \beta - v - v_\ell(\lambda) \geq v_\ell(\lambda) + 3$. □

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) $\mathfrak{sl}_2(\mathbb{Z}_\ell)$.

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 $x \equiv y \pmod{\ell^a}$.

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*

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

Denote

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

and let α be the minimal integer such that x, y are both nonzero modulo $\ell^{\alpha+1}$.

There exists a matrix $M \in M_2(\mathbb{Z}_\ell)$ at least one of whose coefficients is nonzero modulo ℓ and such that for every $w \in (\mathbb{Z}_\ell)^2$ and every $g_1 \in L_1$ we have

$$M(g_1 \cdot w) \equiv \varphi(g_1) \cdot M(w) \pmod{\ell^{n-\alpha-6s-4v-6}}. \tag{1}$$

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

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

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. The reader might wonder whether it is really necessary for all the three parameters n, α and s to appear in equation (1). The answer is yes. This is apparent for n, if the result is to say something nontrivial about φ. Consider next the limiting case where $\varphi \equiv 0$ (i.e. α goes to ∞): this map satisfies the hypotheses in the proposition for every n, but it is easy to realize that (independently of n) the equality

$$M(g_1 \cdot w) \equiv \varphi(g_1) \cdot M(w) = 0 \pmod{\ell^N}$$

can only hold for bounded N; of course a similar conclusion holds if α stays finite, but is very large. Finally, choose an n and any linear map φ and suppose s is sent to infinity. For s large enough, the condition in the proposition will become void, since both sides of the equality will automatically be 0 modulo ℓ^n: but then we cannot hope to deduce anything meaningful about φ, so that s, too, has to appear in the conclusion.

The question of whether the *dependence* on the 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 starting 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 $y^2 h = 0$.

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 complication lies probably in the initial step, where we need to prove that the eigenvalues of h lie in $\mathbb{Z}_\ell$ and are of a certain shape. Once this is done, most of the proof looks very much like the one for $\mathfrak{sl}_2(\mathbb{Q}_\ell)$, with the only added complication that we have to keep track of valuations along the way.

Proof. Denote $\mathcal{C}_h$ the linear operator given by taking the commutator with h. It is clear that

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

so x is an (approximate) eigenvector of $\mathcal{C}_h$ associated with the (approximate) eigenvalue $2\ell^s$. Lemma 5.2 yields

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

If we let $\{0, \pm\mu\}$ denote the eigenvalues of h, then $p'_{\mathcal{C}_h}(t) = (t^2 - 4\mu^2) + 2t^2$, and evaluating at $2\ell^s$ we find

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

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

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

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

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

Note that λ cannot be zero, because clearly $v_\ell(0 - 2\ell^s) = v + s$ is strictly smaller than $v_\ell(\lambda - 2\ell^s)$. It follows that λ is one of the other two roots of $p_{\mathcal{C}_h}(t)$, namely $\pm 2\mu$, and hence $\lambda^2 = 4\mu^2$. This gives us a way to estimate μ^2: indeed we have $4\mu^2 = \lambda^2 = (2\ell^s + O(n - \alpha - 2s - 3v))^2$, whence

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

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 $v_+ \in \mathbb{Z}_\ell^2$ 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 now 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

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

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

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:

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

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 it 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 $\tilde{M} = \left(\ell^s v_+ \mid v_-\right)$. The above relations may be stated more compactly as

$$\tilde{M}\overline{x} = x\tilde{M},\ \tilde{M}\overline{y} = y\tilde{M},\ \tilde{M}\overline{h} = h\tilde{M} \tag{4}$$

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 (4) by ℓ^δ we see that M satisfies analogous equations up to error terms of order $n-\alpha-5s-4v-6$. By construction, at least one of the coefficients of M is an ℓ-adic unit.

Let now 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 both sides we deduce $Mg = \varphi(g)M + O(n-\alpha-6s-4v-6)$ for every $g \in L_1$. This proves the first statement in the proposition.

Let us now turn to the statement about 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 work with this last matrix. Write D for $v_\ell\left(\det \begin{pmatrix}1 & b\\ c & d\end{pmatrix}\right)$, and suppose by contradiction $D > 3s+v$. By definition of the determinant we have $d = bc + O(D)$. This 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 (3) 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

$$\mu_- = \mu_+ + O(\min\{D - v_\ell(b), n-\alpha-2s-4v-v_\ell(b)\}). \tag{5}$$

Note now that since $d = bc + O(D)$ we have $v_\ell(d) \geq \min\{v_\ell(b), D\}$. Moreover, we see by equation (3) 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 deduce that $\min\{v_\ell(b), v_\ell(d)\} \leq 2s$. Let us show that we also have $v_\ell(b) \leq 2s$. Suppose that $v_\ell(b) \geq 2s+1$: then

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

which implies $\min\{v_\ell(b), v_\ell(d)\} \geq 2s+1$ and contradicts what we just proved. Therefore $v_\ell(b) \leq 2s$ and $\mu_- = \mu_+ + O(D-2s)$ by equation (5). 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 about 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 adjoint 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

Let E_1, E_2 be two elliptic curves over K and ℓ a rational prime. 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 $\mathrm{GL}_2(\mathbb{Z}_\ell)$, and m_1, m_2 be integers such that $\mathcal{B}_\ell(m_i)$ is contained in $G_{\ell,1}$.

Suppose for the moment that ℓ is odd. We want to apply theorem 4.2, so for the whole section (up until the very last proposition) we make the following

Assumption. If ℓ is odd, G_ℓ does not contain $\mathcal{B}_\ell\left(4m_1 + 16m_2, 8m_2\right)$.

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

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

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 $3^2 2^{14}$, 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 $2 \cdot 48^2$ for $\ell \neq 2$. Note that H_ℓ is by construction the image of $\mathrm{Gal}\left(\overline{K_\ell}/K_\ell\right)$ in $\mathrm{Aut}\, T_\ell(E_1 \times E_2)$; we write $H_{\ell,1}, H_{\ell,2}$ for its two projections 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 $\mathcal{B}_\ell(n_1), \mathcal{B}_\ell(n_2)$.

Remark 6.1. Note that if $m_1, m_2 > 0$ we can in fact 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_ℓ if and only if it is contained in G_ℓ.

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. $H_{\ell,1}, H_{\ell,2}$). 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. Since by our assumption $H_{\ell,1} \supseteq \mathcal{B}_\ell(n_1)$ we have $L_1 \supseteq \ell^{n_1}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.

Also note 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_3. Note that L_3 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 $\mathfrak{sl}_2(\mathbb{Z}_\ell)$.

Lemma 6.2. *L_3 is stable under conjugation by $B_\ell(n_2)$.*

Proof. Take any element $l \in L_3$: it is the limit of a certain sequence $l_n = \sum_{i=1}^k \lambda_{n,i}\Theta(g_{n,i})$ for certain $g_{n,i} \in H_\ell$. For any $g \in B_\ell(n_2)$ there exists a certain $h \in H_{\ell,1}$ such that (h, g) is in H_ℓ. We have

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

so the sequence $\left((h,g)^{-1}l_n(h,g)\right)_{n\geq 0}$ is in L, and by continuity of conjugation tends to the element $(h,g)^{-1}l(h,g)$ of L. Now 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_3 is exactly the sub-algebra given by the elements whose first coordinate vanishes the claim is proved. □

Lemma 6.3. *Fix an integer t, and suppose that at least one among y_1,y_2,y_3 is not zero modulo ℓ^t: then L_3 contains $\ell^{t+4n_2+4v}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.*

Proof. Apply lemma 4.4 with $s=n_2$. □

Our task is therefore to bound the values of t for which the y_i's all vanish modulo ℓ^t. If this is the case, then none of b_1,b_2,b_3 can be zero modulo ℓ^t, for otherwise L_2 could not contain $\ell^{n_2}\mathfrak{sl}_2(\mathbb{Z}_\ell)$. Even more, the b_i's must generate $\ell^{n_2}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.

Denote $\varphi:L_1\to L_2$ the only $\mathbb{Z}_\ell$-linear map sending a_i to b_i for $i=1,2,3$. For two indices j,k write $[a_j,a_k]=\sum_{i=1}^3\mu_i^{(j,k)}a_i$. 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

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

We want to apply proposition 5.5 to φ. I claim that, in the notation of that proposition, we can take $\alpha\leq n_2+n_1$. Notice that up to a change of basis we can assume a_3 to be of the form $\begin{pmatrix}0&\ell^u\\0&0\end{pmatrix}$ with $u\leq n_1$ (this follows from the description of triangular basis for free modules). In this case, $\varphi(\ell^{n_1}\begin{pmatrix}0&1\\0&0\end{pmatrix})=\ell^{n_1-u}\varphi(a_3)=\ell^{n_1-u}b_3$, and since b_3 does not vanish modulo ℓ^{n_2} we see that $\varphi\left(\begin{pmatrix}0&\ell^{n_1}\\0&0\end{pmatrix}\right)$ does not vanish modulo $\ell^{n_1+n_2}$. As the property of not vanishing modulo $\ell^{n_1+n_2}$ is invariant under change of basis, this does not depend on our initial choice of basis. The same argument applies to the image of $\ell^{n_1}\begin{pmatrix}0&0\\1&0\end{pmatrix}$. Also note that by construction of φ and by our assumption on t we have

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

Set $T=t-11n_1-n_2-5v-6$. We obtain from proposition 5.5 a matrix $M\in M_2(\mathbb{Z}_\ell)$ with the following properties:

- $\operatorname{tr}l_1^2\equiv\operatorname{tr}(\varphi(l_1)^2)\equiv\operatorname{tr}l_2^2\pmod{\ell^T}\quad\forall(l_1,l_2)\in L(H_\ell)$;
- $l_2\equiv M\cdot l_1\cdot M^{-1}\pmod{\ell^T}\quad\forall(l_1,l_2)\in L(H_\ell)$;

- $\Theta_1(l_2) \equiv M\Theta_1(l_1)M^{-1} \pmod{\ell^T} \quad \forall (l_1, l_2) \in L(H_\ell)$.

Take any element $(g_1, g_2) \in H_\ell$. By our choice of K_ℓ, we know that the determinant of g_1 is a square in $\mathbb{Z}_\ell$, so we can choose a square root of $\det g_1$ and write

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

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

$$(g_1', g_2') = (\lambda_1, \lambda_2) \cdot \mathrm{Id} + (l_1, l_2)\,, \tag{6}$$

and we wish to show that λ_1 is congruent to λ_2 modulo a large power of ℓ. We begin by discussing the case of odd ℓ. Squaring equation (6) we obtain

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

Now 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 multiples. 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

$$\left(\Theta_1(l_1^2) + 2\lambda_1 l_1, \Theta_1(l_2^2) + 2\lambda_2 l_2\right) \in L(H_\ell), \tag{7}$$

which implies

$$\Theta_1(l_2^2) + 2\lambda_2 l_2 = M\left(\Theta_1(l_1^2) + 2\lambda_1 l_1\right) M^{-1}$$

and, by difference,

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

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 diagonal matrix (cf. equation (6)). Moreover, as $\det(g_2') = 1$, we have in particular

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

from which we find

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

where the series converges since l_2 is trivial modulo ℓ. Simmetrically we prove that either the congruence $\lambda_1 \equiv \lambda_2 \pmod{\ell^T}$ holds or else l_1 is trivial modulo ℓ and

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

Suppose then l_1, l_2 to be both trivial modulo ℓ. As $\mathrm{tr}\left(l_1^2\right) \equiv \mathrm{tr}\left(l_2^2\right) \pmod{\ell^T}$, it follows that λ_1 and λ_2 are congruent modulo ℓ^T as soon as λ_1 and λ_2 have the same reduction modulo ℓ. But g_1', g_2' reduce to diagonal matrices $\mathrm{diag}\,(\lambda_i, \lambda_i)$ in $\mathrm{SL}_2(\mathbb{F}_\ell)$, so $\lambda_1 \equiv \lambda_2 \pmod{\ell^T}$ if and only if g_1', g_2' have the same reduction, and this is exactly one of the properties of T_ℓ given by theorem 4.2.

If, on the other hand, $\ell = 2$, then l_1, l_2 vanish modulo 8 by construction and the same argument as above shows that

$$\lambda_i = \pm\sqrt{1 + \frac{\mathrm{tr}(l_i^2)}{2}},\ i = 1, 2. \tag{8}$$

Given that $2\lambda_i = \mathrm{tr}\,(g_i') \equiv 2 \pmod 8$ (by our construction of K_ℓ and consequently of H_ℓ), it follows that $\lambda_{1,2} \equiv 1 \pmod 4$, so the sign in equation (8) must be a plus and $\lambda_1 \equiv \lambda_2 \pmod{2^{T-1}}$.

Using this information in equation (6) we have thus proved

Lemma 6.4. *There exists a matrix $M \in M_2(\mathbb{Z}_\ell)$ such that, for every element $(g_1, g_2) \in H_\ell$, the congruence $g_2 \equiv M g_1 M^{-1} \pmod{\ell^{T-v}}$ holds.*

Set now $H := T - v$ and choose any $w \in E_1[\ell^H]$: as $\ell^H w = 0$, for every $(g_1, g_2) \in H_\ell$ we have

$$Mg_1 w = Mg_1 M^{-1} Mw = (g_2 M + O(\ell^H))w = g_2 Mw,$$

so the subgroup

$$\Gamma = \left\{(w, Mw) \in E_1[\ell^H] \times E_2[\ell^H] | w \in E_1[\ell^H]\right\}$$

is defined over K_ℓ: indeed for any $(g_1, g_2) \in H_\ell$ we have

$$(g_1, g_2) \cdot (w, Mw) = (g_1 w, g_2 Mw) = (g_1 w, Mg_1 w).$$

Thus the abelian variety $A^* = E_1 \times E_2/\Gamma$ is defined over K_ℓ, and we have an isogeny $A \to A^*$ of degree $|E_1[\ell^H]| = \ell^{2H}$; on the other hand, we also have an isogeny $A^* \to A$ of degree b dividing $b_0(E_1 \times E_2, K_\ell)$, and the composition of the two is an endomorphism of $E_1 \times E_2$ that kills Γ. Here we use the crucial fact that at least one of the coefficients of M is an ℓ-adic unit to deduce that the projection of Γ on E_2 contains at least one point of exact order ℓ^H, so the endomorphism of $E_1 \times E_2$ killing Γ must be of the form $\begin{pmatrix} \ell^H e_1 & 0 \\ 0 & \ell^H e_2 \end{pmatrix}$, of degree $e_1^2 e_2^2 \ell^{4H}$. It follows that $e_1^2 e_2^2 \ell^{4H} = \ell^{2H} b$, hence $2H \leq v_\ell(b_0(E_1 \times E_2, K_\ell))$ and $2t \leq v_\ell(b_0(E_1 \times E_2, K_\ell)) + 2(11n_1 + n_2 + 6v + 6)$. This inequality is certainly not satisfied if we take $t = \left\lfloor \frac{v_\ell(b_0(E_1 \times E_2, K_\ell))}{2} \right\rfloor + 11n_1 + n_2 + 6v + 7$, so for this value of t the Lie algebra L_3 does not vanish modulo ℓ^t. Lemma 6.3 then shows that L_3 contains $\ell^{f_1} \mathfrak{sl}_2(\mathbb{Z}_\ell)$, where $f_1 = \left\lfloor \frac{v_\ell(b_0(E_1 \times E_2, K_\ell))}{2} \right\rfloor + 11n_1 + 5n_2 + 10v + 7$, and therefore $L(H_\ell)$ contains $0 \oplus \ell^{f_1} \mathfrak{sl}_2(\mathbb{Z}_\ell)$. Swapping the roles of E_1 and E_2 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

$$f = \left\lfloor \frac{v_\ell(b_0(E_1 \times E_2/K_2))}{2} \right\rfloor + 16 \max\{n_1, n_2\} + 10v + 7.$$

Proposition 6.5. *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 rational prime. Suppose the image of $\mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(T_\ell(E_i))$ contains $\mathcal{B}_\ell(n_i)$ for $i = 1, 2$. Let f be given by the formula above.*

If ℓ is odd, the image G_ℓ of $\mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(T_\ell(E_1) \times T_\ell(E_2))$ contains $\mathcal{B}_\ell(4f) \times \mathcal{B}_\ell(4f)$; if $\ell = 2$, the image G_2 of $\mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(T_2(E_1) \times T_2(E_2))$ contains $\mathcal{B}_2(12(f + 13n_2 + 5n_1 + 6), 12(f + 13n_2 + 5n_1 + 6))$.

Proof. For $\ell = 2$ the result follows at once from theorem 4.3. For odd ℓ, and under the assumption we made at the beginning of this section, the result similarly follows from property $(*)$ of T_ℓ given in theorem 4.2 and the fact that clearly $2f > 8 \max\{n_1, n_2\}$. On the other hand, if our assumption is *false*, then G_ℓ contains $\mathcal{B}_\ell(4n_1 + 16n_2, 8n_2)$ (note that we can assume $m_1 \leq n_1, m_2 \leq n_2$ without loss of generality), 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 (and non-isogenous over $\overline{K}$). Let $\mathcal{P}$ be the set of primes ℓ for which G_ℓ does not contain $\mathrm{SL}_2(\mathbb{Z}_\ell)^2$. Rewriting Proposition 1 of [MW93] in terms of the function b_0 of definition 2.4 we get:

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

$$6 b_0(E_1/K; 60) b_0\left(E_1^2/K; 2\right) b_0(E_2/K; 60) b_0\left(E_2^2/K; 2\right) b_0(E_1 \times E_2/K; 2),$$

then ℓ is not in $\mathcal{P}$.

Proof. Lemma 8.2 of [Lom14] implies that for a prime ℓ that does not divide

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

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 [MW93, Proposition 1] shows that $G_\ell(\ell)$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)^2$ unless $\ell^2|b_0(E_1\times E_2/K;2)$. Finally, 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 $\mathrm{SL}_2(\mathbb{Z}_\ell)^2$, at least for $\ell\geq 5$ (this is well-known; see for example [Rib97, Proposition 4.2]). □

Corollary 7.2. *The inequality*

$$\prod_{\ell\in\mathcal{P}}\ell < 6b_0(E_1/K;60)b_0\left(E_1^2/K;2\right)b_0(E_2/K;60)b_0\left(E_2^2/K;2\right)b_0(E_1\times E_2/K;2)$$

holds.

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

$$D_j(\infty)=b_0(E_j/K;120)^5b_0(E_j^2/K;2).$$

As ℓ is odd, by [Lom14, Corollary 7.6] we see that $G_{\ell,j}$ contains

$$\mathcal{B}_\ell\left(24(v_\ell(D_j(\infty))+1\right),$$

hence the same is true for $H_{\ell,j}$, cf. remark 6.1. Therefore - in the notation of the previous section - we can take $n_j=n_j(\ell)=24(v_\ell(D_j(\infty))+1$. On the other hand, for $\ell=3$ we apply [Lom14, Theorem 7.5] directly to E_j/K_3 (notice that our present K_3 satisfies the same hypotheses as the field noted K_3 in [Lom14]) and see that we can take

$$n_j(3)=24v_3\left(b_0(E/K_3)^5b_0(E^2/K_3)\right)+24\leq 24(v_3(D_j(\infty))+1);$$

similarly, for $\ell=2$ we can take $n_j(2)=72v_2\left(b_0(E_j/K_2)^5b_0(E_j^2/K_2)\right)+74$.

Applying proposition 6.5 with these values of n_j we get:

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

$$f(\ell)=2v_\ell(b_0(E_1\times E_2/K;2\cdot 48^2))+1536\max\left\{v_\ell(D_1(\infty)),v_\ell(D_2(\infty))\right\}+1564$$

for odd ℓ and

$$f(2)=6v_2(b_0(E_1\times E_2/K_2))+30000\max_j\left\{v_2\left(b_0(E_j/K_2)^5b_0(E_j^2/K_2)\right)\right\}+30500$$

for $\ell=2$.

Using the very same argument as [Lom14], Theorem 9.1 and Proposition 9.2 and some very crude estimates, we deduce

Proposition 7.4. *There exists a subgroup S of G_∞ of the form $\prod_\ell S_\ell$, 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 $b_0(E_1\times E_2/K;2\cdot 48^2)^{1200}$.*

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

Theorem 7.5. *Let $E_1,\dots,E_n$, $n\geq 2$, be elliptic curves defined over K, pairwise non-isogenous over $\overline{K}$. Suppose that $\mathrm{End}_{\overline{K}}(E_i)=\mathbb{Z}$ for $i=1,\dots,n$. Then G_∞ has index at most*

$$2^{12n(n-2)}\zeta(2)^2\cdot[K:\mathbb{Q}]\cdot\max_{i\neq j}b_0\left(E_i\times E_j/K;2\cdot 48^2\right)^{600n(n-1)}$$

in

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

Proof. The exact sequence

$$1 \to G_\infty \cap \mathrm{SL}_2(\hat{\mathbb{Z}})^n \to G_\infty \xrightarrow{\det} \hat{\mathbb{Z}}^\times \to \frac{\hat{\mathbb{Z}}^\times}{\det \circ \rho_\infty \operatorname{Gal}\left(\overline{K}/K\right)} \to 1$$

and the fact that $\left|\dfrac{\hat{\mathbb{Z}}^\times}{\det \circ \rho_\infty \operatorname{Gal}\left(\overline{K}/K\right)}\right| \leq [K : \mathbb{Q}]$ (cf. [Lom14, Proposition 8.1]) show that 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

$$2^{12n(n-2)}\zeta(2)^2 \cdot \max_{i \neq j} b_0(E_i \times E_j/K; 2 \cdot 48^2)^{600n(n-1)}.$$

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 $\mathrm{SL}_2(\hat{\mathbb{Z}})^2$ that satisfies all the requirements of corollary 3.3, and the theorem follows from this corollary upon noticing that the index of $S^{(i,j)}$ in $\mathrm{SL}_2(\hat{\mathbb{Z}})^2$ is bounded by

$$b_0(E_i \times E_j/K; 2 \cdot 48^2)^{1200}.$$

□

References

[GR14] Éric Gaudron and Gaël Rémond. Polarisations et isogénies. *Duke Math. J.*, 163(11):2057–2108, 2014.

[Lom14] D. Lombardo. Bounds for Serre's open image theorem for elliptic curves over number fields. *ArXiv e-prints*, March 2014. Available at `http://arxiv.org/abs/1403.3813`.

[Lom15] D. Lombardo. Pink-type results for general subgroups of $\mathrm{SL}_2(\mathbb{Z}_\ell)^n$. *Preprint*, January 2015. Available from `http://www.math.u-psud.fr/~lombardo/`.

[Mas98] D. W. Masser. Multiplicative isogeny estimates. *J. Austral. Math. Soc. Ser. A*, 64(2):178–194, 1998.

[MW93] D. W. Masser and G. Wüstholz. Galois properties of division fields of elliptic curves. *Bull. London Math. Soc.*, 25(3):247–254, 1993.

[Pin93] 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.

[Rib75] Kenneth A. Ribet. On l-adic representations attached to modular forms. *Invent. Math.*, 28:245–275, 1975.

[Rib76] K. A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[Rib97] K. A. Ribet. Images of semistable Galois representations. *Pacific J. Math.*, Special Issue:277–297, 1997. Olga Taussky-Todd: in memoriam.

[Ser72] J-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.