TWO NATURAL VARIANTS OF THE LANG-TROTTER CONJECTURE ON PRIMITIVE POINTS FOR ELLIPTIC CURVES

ALEXANDRE BENOIST AND ANTONELLA PERUCCA

ABSTRACT. The Lang-Trotter Conjecture on primitive points is the analogue for elliptic curves of Artin's conjecture on primitive roots. Indeed, if we have an elliptic curve E over $\mathbb{Q}$ with a rational point P of infinite order, we may count the primes p of good reduction for which $(P \bmod p)$ generates $E(\mathbb{F}_p)$. In this work, we formulate and investigate two natural variants of the Lang-Trotter Conjecture. One of them is the following: we require that the order of the point $(P \bmod p)$ equals the exponent of the group $E(\mathbb{F}_p)$: this means that the subgroup generated by the point is as large as possible, and the condition is meaningful also for non-cyclic groups.

1. INTRODUCTION

In 1976, Lang and Trotter [LT77] formulated a conjecture which is the analogue for elliptic curves of Artin's conjecture on primitive roots (for concreteness, they state it for elliptic curves defined over the rationals rather than over a general number field). Artin's conjecture predicts the density of primes for which a given integer is a primitive root. The Lang-Trotter conjecture similarly requires that a given point is *primitive*. Namely, let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})$ be a point of infinite order. If p is a prime of good reduction for E, then we say that P is primitive modulo p if the reduced point $(P \bmod p)$ generates the group $E(\mathbb{F}_p)$. In particular, it is necessary that the group $E(\mathbb{F}_p)$ is cyclic.

In this paper we investigate two natural variants of the Lang-Trotter conjecture. Firstly, we require the cyclic group generated by $(P \bmod p)$ to be as large as possible, namely that the order of $(P \bmod p)$ equals the exponent of $E(\mathbb{F}_p)$. Secondly, we require the possibly weaker condition that the point $(P \bmod p)$ is *indivisible*, meaning that it is not an ℓ-multiple in $E(\mathbb{F}_p)$ for the prime numbers ℓ that divide $\#E(\mathbb{F}_p)$. Both of the conditions are equivalent to the one of Lang-Trotter if $E(\mathbb{F}_p)$ is cyclic.

Let A be an abelian variety of dimension g defined over a number field K, and let S_A be the set of primes of K of good reduction for A. Suppose that there is some point $P \in A(K)$ of infinite order. For $\mathfrak{p} \in S_A$ we denote by $k_\mathfrak{p}$ the residue field at $\mathfrak{p}$ and consider the reduction $(P \bmod \mathfrak{p})$ and the order of this point in $A(k_\mathfrak{p})$.

We consider the following indivisibility condition, where ℓ is a prime number:

$$\ell \mid \#A(k_\mathfrak{p}) \quad \Rightarrow \quad (P \bmod \mathfrak{p}) \notin [\ell]A(k_\mathfrak{p}) \tag{1}$$

The set of primes $\mathfrak{p} \in S_A$ such that (1) holds has a natural density, which is a rational number whose minimal denominator can be bounded in terms of g and ℓ (this generalizes to finitely many primes ℓ, see Proposition 12).

If ℓ is a prime number and G is a finite group, we denote by $\exp_\ell(G)$ the ℓ-adic valuation of the exponent of G. Similarly, if $g \in G$, we write $\mathrm{ord}_\ell(g)$ for the ℓ-adic valuation of the order

of g. We also consider the following condition:

$$\operatorname{ord}_\ell\left(P \bmod \mathfrak{p}\right) = \exp_\ell(A(k_\mathfrak{p}))\,. \tag{2}$$

Similarly to the Lang-Trotter conjecture, considering all primes ℓ at once gives rise to the following conjectures:

Conjecture (Indivisibility/Exponent LT Conjecture)**.** The set of those $\mathfrak{p} \in S_A$ such that Condition (1) (respectively, (2)) holds for every prime number ℓ admits a natural density. This density is the infimum, by varying S over the finite set of prime numbers, of the density that is obtained by considering the condition only for $\ell \in S$.

The main result of this work (which builds on the results in Section 7) is the following:

Theorem 1. *Let A be an elliptic curve. Fixing a prime number ℓ, the set of primes $\mathfrak{p} \in S_A$ such that*

$$\operatorname{ord}_\ell\left(P \bmod \mathfrak{p}\right) = \exp_\ell(A(k_\mathfrak{p}))$$

admits a natural density which is a rational number.

In the above conjectures the upper density is clearly bounded from above by the given infimum. We have the following inequalities for the densities (because the required conditions are here ranked from strongest to weakest):

$$\text{Lang-Trotter} \leq \text{Exponent-LT} \leq \text{Indivisible-LT}\,.$$

We made numerical experiments, see Appendix B, that support the validity of the conjectures. Our results are based on an investigation of the *ℓ-adic* (respectively, *adelic*) torsion-Kummer representation of A, considering the Galois action on the division points over P. Clearly, the above definitions, results and conjectures have an analogue if P is replaced by a subgroup of $A(K)$. Moreover, as observed by Félix Baril Boudreau, many of the arguments do not depend on the fact the ground field is a number field in the sense that they work equally well for global function fields. In particular, similar conclusions are expected to hold for non-CM Abelian varieties over global function fields (given an analogue of [Ber88, Theorem 1]). For precise big image considerations, one should also take into account parity of the power of the prime number p.

Of independent interest is our investigation (see Section 2) of the notion of $\ell\mathbb{Z}$-rank for a matrix with entries modulo ℓ^n. This notion is similar to the usual notion of rank for a matrix, but where we only accept those linear combinations of the columns with integer coefficients that are not all divisible by ℓ. More specifically, in Appendix A we count lifts (from modulo ℓ^n to modulo ℓ^{n+1}) of 2×2 matrices in Cartan groups and their normalizers, according to their $\ell\mathbb{Z}$-rank. These counts are used to prove our main result on the rationality of the density.

Given the oncoming book (edited by the second-listed author and Moree) about Artin's conjecture and the Lang-Trotter conjecture we opted for not presenting a historical account of the latter. We just point out that the known results (for example, those by Gupta and Murty) can probably be adapted, at least to a certain extent, to the variants that we have considered.

Acknowledgements. We thank Félix Baril Boudreau, Fritz Hörmann and Davide Lombardo for helpful discussions and for Theorem 20. This research was funded in whole, or in part, by the Luxembourg National Research Fund (FNR), grant reference PRIDE23/18685085. For the purpose of open access, and in fulfilment of the obligations arising from the grant agreement,

2. The $\ell\mathbb{Z}$-rank of matrices modulo ℓ^n

In this work, ℓ denotes a prime number. If $N > n$ are positive integers, we occasionally identify $\mathbb{Z}/\ell^n\mathbb{Z}$ with the subgroup $[\ell^{N-n}]\mathbb{Z}/\ell^N\mathbb{Z}$ of $\mathbb{Z}/\ell^N\mathbb{Z}$.

Fix a prime number ℓ. We say that the elements $r_1, \ldots, r_m \in \mathbb{Z}/\ell^n\mathbb{Z}$ are $\ell\mathbb{Z}$-linearly dependent if there are integers $a_1, \ldots, a_m$ not all divisible by ℓ such that

$$a_1 r_1 + a_2 r_2 \cdots + a_m r_m = 0\,.$$

Definition 2 ($\ell\mathbb{Z}$-rank)**.** Let d, m be positive integers and consider a matrix $M \in \mathrm{Mat}_{d\times m}(\mathbb{Z}/\ell^n\mathbb{Z})$. The $\ell\mathbb{Z}$-rank of M, denoted by $\mathrm{rk}_{\ell\mathbb{Z}}(M)$, is the maximal number of columns of M that are $\ell\mathbb{Z}$-independent in $(\mathbb{Z}/\ell^n\mathbb{Z})^d$.

For example, the $\ell\mathbb{Z}$-rank of a matrix M is zero if and only if M is the zero matrix.

We can identify $M \in \mathrm{Mat}_{d\times m}(\mathbb{Z}/\ell^n\mathbb{Z})$ with a $\mathbb{Z}/\ell^n\mathbb{Z}$-linear transformation $(\mathbb{Z}/\ell^n\mathbb{Z})^m \to (\mathbb{Z}/\ell^n\mathbb{Z})^d$, and its kernel $\ker(M)$ is a subgroup of $(\mathbb{Z}/\ell^n\mathbb{Z})^m$.

Lemma 3. *Let $M \in \mathrm{Mat}_{d\times d}(\mathbb{Z}/\ell^n\mathbb{Z})$.*

1. *The number of cyclic components of $\ker(M)$ having size ℓ^n is $d - \mathrm{rk}_{\ell\mathbb{Z}}(M)$. In particular, the exponent of $\ker(M)$ equals ℓ^n if and only if $\mathrm{rk}_{\ell\mathbb{Z}}(M) < d$.*
2. *The group structure of $\ker(M)$ determines and it is determined by the numbers*

$$\mathrm{rk}_{\ell\mathbb{Z}}(M \bmod \ell^h) \qquad h = 1, \ldots, n\,.$$

Indeed, for $1 \le h < n$ the number of cyclic components of size ℓ^h is

$$\mathrm{rk}_{\ell\mathbb{Z}}(M \bmod \ell^{h+1}) - \mathrm{rk}_{\ell\mathbb{Z}}(M \bmod \ell^h)\,,$$

while the number of cyclic components of size ℓ^n is $d - \mathrm{rk}_{\ell\mathbb{Z}}(M)$.

Proof. We first prove (1). Let $\vec{c}_1, \ldots, \vec{c}_d$ be the columns of M. For any two distinct integers i and j in $\{1, \ldots, d\}$, let E_{ij} be the elementary matrix corresponding to the column swap $\vec{c}_i \leftrightarrow \vec{c}_j$. For $\lambda \in \mathbb{Z}/\ell^n\mathbb{Z}$, we call $E_{ij}(\lambda)$ the elementary matrix corresponding to the column operation $\vec{c}_i \leftarrow \vec{c}_i + \lambda\vec{c}_j$. If $E \in \{E_{ij}, E_{ij}(\lambda)\}$, then M and ME have the same $\ell\mathbb{Z}$-rank. If $\vec{x}$ is a column vector in $(\mathbb{Z}/\ell^n\mathbb{Z})^d$, then $E^{-1}\vec{x}$ has the same order as $\vec{x}$. Thus, we can perform elementary operations on the columns of M without changing the $\ell\mathbb{Z}$-rank nor the number of cyclic components of size ℓ^n of the kernel. Set $r := \mathrm{rk}_{\ell\mathbb{Z}}(M)$.

A column vector $\vec{x} = (x_1, \ldots, x_d)^\intercal$ in $(\mathbb{Z}/\ell^n\mathbb{Z})^d$ belongs to $\ker(M)$ if and only if $x_1\vec{c}_1 + \ldots + x_d\vec{c}_d = \vec{0}$. If $r = d$, then ℓ must divide all the coordinates x_i because the columns are $\ell\mathbb{Z}$-linearly independent, so $\ker(M)$ has no element of order ℓ^n. Now suppose that $r < d$. By elementary operations on the columns of M, we may replace M by

$$(\vec{b}_1|\cdots|\vec{b}_r|\vec{0}|\cdots|\vec{0}),$$

where the columns $\vec{b}_1, \ldots, \vec{b}_r$ are $\ell\mathbb{Z}$-linearly independent. The kernel of M then consists of vectors $\vec{x} = (x_1, \ldots, x_r, x_{r+1}, \ldots, x_d)^\intercal$ where the r first coordinates are divisible by ℓ (and there is no condition on the last $d - r$ coordinates). Thus, $\ker(M)$ has precisely $d - r$ cyclic components of size ℓ^n.

To prove (2), we apply (1) to $M_h := (M \bmod \ell^h)$ for $1 \leq h < n$. We deduce that $\ker(M_h)$ has $d - r_h$ components of size ℓ^h, where $r_h := \mathrm{rk}_{\ell\mathbb{Z}}(M_h)$. To conclude, it suffices to prove that $d - r_h$ equals the number of cyclic components of $\ker(M)$ of size at least ℓ^h. We may equivalently show that $\ker(M)$ and $\ker(M_h)$ have the same number of vectors of order ℓ^h. Let $\vec{x} \in (\mathbb{Z}/\ell^n\mathbb{Z})^d$ have order ℓ^h. All entries of $\vec{x}$ are divisible by ℓ^{n-h} but they are not all divisible by $\ell^{n-(h-1)}$. Then $\vec{x}$ can be identified with a vector $\vec{x_h} \in (\mathbb{Z}/\ell^h\mathbb{Z})^d$ of order ℓ^h (dividing by ℓ^{n-h} integer representants for the entries of $\vec{x}$). Conversely, starting with a vector $\vec{x_h} \in (\mathbb{Z}/\ell^h\mathbb{Z})^d$ of order ℓ^h (multiplying by ℓ^{n-h} integer representants for the entries of $\vec{x_h}$) we obtain a vector $\vec{x} \in (\mathbb{Z}/\ell^n\mathbb{Z})^d$ of order ℓ^h. We conclude because we have $\vec{x} \in \ker(M)$ if and only if $\vec{x_h} \in \ker(M_h)$. □

For $M \in \mathrm{Mat}_{d\times d}(\mathbb{Z}/\ell^n\mathbb{Z})$, the image of M is the column space of M and it is isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^d/\ker(M)$, hence its group structure can be determined thanks to Lemma 3.

Remark 4. For $M = (\vec{c}_1|\vec{c}_2) \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/\ell^n\mathbb{Z})$ we have $\mathrm{rk}_{\ell\mathbb{Z}}(M) \in \{0, 1, 2\}$. Moreover, we have $\mathrm{rk}_{\ell\mathbb{Z}}(M) = 1$ if and only if M is not the zero matrix and there is some $k \in \mathbb{Z}/\ell^n\mathbb{Z}$ such that $\vec{c}_1 = k\vec{c}_2$ or $\vec{c}_2 = k\vec{c}_1$. By Lemma 3 (2), $\ker(M)$ contains a point of order ℓ^n if and only if $\mathrm{rk}_{\ell\mathbb{Z}}(M) \leq 1$.

Remark 5. Let $A, B \in \mathrm{Mat}_{d\times d}(\mathbb{Z}/\ell^n\mathbb{Z})$ such that B is invertible. The matrices A and $B^{-1}AB$ have isomorphic kernels and hence by Lemma 3 for all $1 \leq h \leq d$ the matrices $(A \bmod \ell^h)$ and $(B^{-1}AB \bmod \ell^h)$ have the same $\ell\mathbb{Z}$-rank.

Now extend A, B, B^{-1} to $A_+, B_+, B_+^{-1} \in \mathrm{Mat}_{d+1\times d+1}(\mathbb{Z}/\ell^n\mathbb{Z})$ as follows. The additional row has zero entries, except the last entry which is 1. The additional column, except the last entry, are vectors $\vec{v}, \vec{v}_B, \vec{v}_{B^{-1}}$ in $(\mathbb{Z}/\ell^n\mathbb{Z})^d$. We impose the condition that $B_+^{-1}B_+ = \mathrm{Id}$, namely that $\vec{v}_{B^{-1}} = -B^{-1}\vec{v}_B$. The matrix $B_+^{-1}A_+B_+$ has the same last row as A_+. The upper left $d \times d$ submatrix is $B^{-1}AB$. We compute that the last column of $B_+^{-1}A_+B_+$, without the last entry, is

$$\vec{w} := B^{-1}(A - \mathrm{Id}_d)\vec{v}_B + B^{-1}\vec{v}.$$

We deduce that $\vec{v} \in \mathrm{Im}(A - \mathrm{Id})$ if and only if $\vec{w} \in \mathrm{Im}(B^{-1}AB - \mathrm{Id})$.

Notice that the effect on A_+ of a base change in $(\mathbb{Z}/\ell^n\mathbb{Z})^d$ is the conjugation with an invertible matrix B_+ such that $\vec{v}_B = \vec{0}$. Also remark for later use that replacing $\vec{v}$ by adding to it an element in $\mathrm{Im}(A - \mathrm{Id})$ does not affect the condition $\vec{v} \in \mathrm{Im}(A - \mathrm{Id})$.

3. Torsion-Kummer representations of abelian varieties

3.1. **Torsion-Kummer representations.** We let K be a number field, and work within a fixed algebraic closure $\bar{K}$ of K. We let A be an abelian variety defined over K and of positive dimension g. We denote by S_A the set of primes of K that are of good reduction for A.

Fix some prime number ℓ. For every $n \geq 1$ we choose a basis for $A[\ell^n]$ such that if $N > n$ then the basis of $A[\ell^n]$ is the image of the basis of $A[\ell^N]$ under multiplication by ℓ^{N-n}. By taking the projective limit of these bases, we get a $\mathbb{Z}_\ell$-basis of the Tate module $T_\ell(A)$.

After having chosen a basis for $A[\ell^n]$ we can identify this group with $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$. Then we can identify the group of automorphisms of $A[\ell^n]$ with $\mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$. Similarly, we can identify the group of $\mathbb{Z}_\ell$-module automorphisms of $T_\ell(A)$ with $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$.

Definition 6 (torsion representations)**.** For every $\sigma \in \mathrm{Gal}(\bar{K}/K)$ the restriction of σ to $A[\ell^n]$ is, with the above identifications, a matrix $M_n \in \mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$. The group homomorphism

$\sigma \mapsto M_n$ is the *torsion representation modulo* ℓ^n. Similarly, by considering the Galois action on $T_\ell(A)$, we obtain the *ℓ-adic torsion representation*.

We will suppose that the Mordell-Weil group $A(K)$ contains a point P of infinite order, which is necessary to formulate the Lang-Trotter conjecture and to consider similar problems.

For every positive integer n we denote by $\frac{1}{\ell^n}P$ the set of points $P' \in A(\overline{K})$ such that $[\ell^n]P' = P$. For every positive integer n we fix a point $Q_n \in \frac{1}{\ell^n}P$ such that $[\ell^{N-n}]Q_N = Q_n$.

We now briefly describe the *torsion-Kummer representations* (also called *arboreal representations*). We refer to [JR10] and [LP21] for an introduction to these representations.

Definition 7 (torsion-Kummer representation modulo ℓ^n)**.** The *torsion-Kummer representation modulo* ℓ^n is a group homomorphism that maps $\sigma \in \mathrm{Gal}(\bar{K}/K)$ to the matrix $M'_n \in \mathrm{GL}_{2g+1}(\mathbb{Z}/\ell^n\mathbb{Z})$ defined as follows: removing the last row and column, we get the image of σ under the $\mathrm{mod}\ell^n$ torsion representation; the last row consists of zeroes, with the exception of the last entry, which is 1; the first $2g$ entries in the last column are the coefficients that express, in the chosen basis of $A[\ell^n]$, the torsion point $\sigma(Q_n) - Q_n$.

The image of the torsion-Kummer representation modulo ℓ^n, by definition, is contained in a group isomorphic to the semi-direct product

$$\mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z}) \ltimes (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}\,.$$

Considering the projective limit of the torsion-Kummer representations modulo ℓ^n we obtain the *ℓ-adic torsion-Kummer representation*, whose image is a subgroup of

$$\mathrm{GL}_{2g}(\mathbb{Z}_\ell) \ltimes (\mathbb{Z}_\ell)^{2g}\,.$$

3.2. **Reduction maps.** We keep the notation from Section 3.1. Let L/K be an extension of number fields. If $\mathfrak{p} \in S_A$ and $\mathfrak{q}$ is a prime of L lying over $\mathfrak{p}$, then $\mathfrak{q}$ is a prime of good reduction for the abelian variety $A \otimes_K L$, and we identify $A(k_\mathfrak{p})$ with the subgroup of $A(k_\mathfrak{q})$ consisting of the elements that are fixed by the Frobenius at $\mathfrak{p}$ (which generates the Galois group of the finite field extension $k_\mathfrak{q}/k_\mathfrak{p}$).

Remark 8. Consider some prime $\mathfrak{p} \in S_A$ that is not over ℓ. The reduction modulo $\mathfrak{p}$ is injective on the torsion points of order a power of ℓ, see [HS00, Theorem C.1.4]. Fix a positive integer n. The prime $\mathfrak{p}$ does not ramify in the Galois extension $K(\frac{1}{\ell^n}P)/K$ (the absence of ramification for the subextension $K(A[\ell^n])/K$ is due to the Néron-Ogg-Shafarevic criterion, while for the subextension $K(\frac{1}{\ell^n}P)/K(A[\ell^n])$ is due to [HS00, Proposition C.1.5]). Let σ be in the conjugacy class of the Frobenius at $\mathfrak{p}$ for the extension $K(\frac{1}{\ell^n}P)/K$, and let M_n be the image of σ under the $\mathrm{mod}\ell^n$ torsion representation. We denote by Id_n the identity matrix of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Then with the reduction map modulo $\mathfrak{p}$ we can identify $A[\ell^n](k_\mathfrak{p})$ with $\ker(M_n - \mathrm{Id}_n)$ (which, with our identifications, is the subgroup of $A[\ell^n](\overline{K})$ consisting of the points fixed by σ). Notice that the group structure of $\ker(M_n - \mathrm{Id}_n)$ does not depend on the choice of σ.

In the following result we keep the above notation, and we let $T_{i,n}$ (for $i = 1, \dots, 2g$) be the chosen basis of $A[\ell^n]$. Notice that the statement does not depend on the choice of σ in the conjugacy class of the Frobenius at $\mathfrak{p}$, nor on the choice of the point Q_n.

Lemma 9. *Fix $\mathfrak{p} \in S_A$ not over ℓ and let $\sigma \in \mathrm{Frob}_\mathfrak{p}$ with respect to the Galois extension $K(\frac{1}{\ell^n}P)/K$. The following conditions are equivalent:*

(1) The point $(P \bmod \mathfrak{p})$ is ℓ^n-divisible in $A(k_\mathfrak{p})$.
(2) There is $Q \in \frac{1}{\ell^n}P$ such that $(\sigma - \mathrm{Id})(Q) = 0$.
(3) We have $(\sigma - \mathrm{Id})(Q_n) \in (\sigma - \mathrm{Id})(A[\ell^n])$.
(4) The last column of M'_n, removing the last entry, is in the column space of $M_n - \mathrm{Id}_n$.
(5) For all $N \geq n$, the ℓ^{N-n} multiple of the last column of M'_N, removing the last entry, is in the column space of $M_N - \mathrm{Id}_N$.

Proof. (1) $\Leftrightarrow$ (2). Suppose that there is $R \in A(k_\mathfrak{p})$ such that $\ell^n R = (P \bmod \mathfrak{p})$. Let $\mathfrak{q}$ be a prime of $K(\frac{1}{\ell^n}P)$ lying over $\mathfrak{p}$. Then there is $Q \in \frac{1}{\ell^n}P$ such that $(Q \bmod \mathfrak{q}) = R$. Since R is defined over $k_\mathfrak{p}$, it is fixed by the Frobenius element of $\mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p})$ and we deduce that $\sigma(Q) = Q$. Conversely, if Q as in (2) exists, then $(Q \bmod \mathfrak{q}) \in A(k_\mathfrak{p})$ and it satisfies $[\ell^n](Q \bmod \mathfrak{q}) = (P \bmod \mathfrak{p})$.

(2) $\Leftrightarrow$ (3). If Q exists, we can write $Q = Q_n - T$ for some $T \in A[\ell^n]$, so the condition $(\sigma - \mathrm{Id})(Q) = 0$ is equivalent to $(\sigma - \mathrm{Id})(Q_n) = (\sigma - \mathrm{Id})(T)$. Conversely, if Q_n satisfies this last condition for some $T \in A[\ell^n]$, then the point $Q := Q_n - T$ satisfies $(\sigma - \mathrm{Id})(Q) = 0$.

(3) $\Leftrightarrow$ (4). Call $\vec{c}_i$ the column vectors of $M_n - \mathrm{Id}_n$, and let $\vec{v}$ be the last column of M'_n, removing the last entry. We can identify these column vectors of length $2g$ with the corresponding torsion points (choosing the torsion point that, written in the basis $T_{1,n}, \dots, T_{2g,n}$, has the vector components as coordinates). So we have $\vec{c}_i = \sigma(T_{i,n}) - T_{i,n}$ and $\vec{v} = \sigma(Q_n) - Q_n$.

Suppose that we can write $\vec{v} = \sum_i \alpha_i \vec{c}_i$ for some integers α_i. Consider the torsion point $T := \sum_i \alpha_i T_{i,n}$. Then we have

$$\sigma(Q_n) - Q_n = \vec{v} = \sum_i \alpha_i \vec{c}_i = \sum_i \alpha_i (\sigma(T_{i,n}) - T_{i,n}) = \sigma(T) - T$$

and hence (3) holds. Conversely, if $T \in A[\ell^n]$ is such that $\sigma(T) - T = \sigma(Q_n) - Q_n$, then we can write $T := \sum_i \alpha_i T_{i,n}$ for some integers α_i and we deduce that

$$\vec{v} = \sigma(Q_n) - Q_n = \sigma(T) - T = \sum_i \alpha_i (\sigma(T_{i,n}) - T_{i,n}) = \sum_i \alpha_i \vec{c}_i \,.$$

(5) $\Rightarrow$ (4). This is immediate by setting $N = n$.

(1) $\Rightarrow$ (5). We know that the point $\tilde{P} = \ell^{N-n}P$ is such that $(\tilde{P} \bmod \mathfrak{p})$ is ℓ^N-divisible in $A(k_\mathfrak{p})$. Applying (4) to $\tilde{P}$ and N (choosing the point Q_n in $\frac{1}{\ell^N}\tilde{P}$ and letting $\tilde{M}'_N$ be the analogue of M'_N for $\tilde{P}$) we deduce that the last column of $\tilde{M}'_N$, removing the last entry, is in the column space of $M_N - \mathrm{Id}_N$. We may conclude because (removing the last entries) the last column of $\tilde{M}'_N$ is the ℓ^{N-n}-multiple of the last column of M'_N. □

We will be interested in the points in $A(k_\mathfrak{p})$ that are *indivisible* in this group, namely that are not ℓ multiples for any prime ℓ dividing $\#A(k_\mathfrak{p})$.

Remark 10. The prime ℓ divides $\#A(k_\mathfrak{p})$ if and only if $v_\ell(\det(M_1 - \mathrm{Id}_1)) > 0$, see Remark 8. Moreover, the point $(P \bmod \mathfrak{p})$ is ℓ^n-divisible in $A(k_\mathfrak{p})$ if and only if any of the equivalent conditions in Lemma 9 holds. Observe that, if $(P \bmod \mathfrak{p})$ is not ℓ^n-divisible in $A(K_\mathfrak{p})$ for some n, then ℓ divides $\#A(k_\mathfrak{p})$.

Remark 11. We describe some special cases related to Lemma 9.

• Suppose that $M_n = \mathrm{Id}_n$ (which means that $A(k_\mathfrak{p})$ contains $A[\ell^n](\overline{k_\mathfrak{p}})$). In this case, the point Q_n is fixed by σ if and only if the last column of M'_n, without the last entry, is zero. Thus, $(P \bmod \mathfrak{p})$ is ℓ^n-divisible in $A(k_\mathfrak{p})$ if and only if M'_n is the identity matrix.

• Suppose that $M_n - \mathrm{Id}_n$ is invertible. Then the last column of M'_n, removing the last entry, is of the form $\vec{c} = \sum_{i=1}^{2g} \alpha_i \vec{c}_i$, where the $\vec{c}_i$'s are the columns of $M_n - \mathrm{Id}_n$. Thus, the point $Q_n - \sum_{i=1}^{2g} \alpha_i T_{i,n}$ is fixed by σ and hence $(P \bmod \mathfrak{p})$ is ℓ^n-divisible in $A(k_\mathfrak{p})$.

• Suppose that the finite abelian group $\ker(M_n - \mathrm{Id}_n)$ has $2g-1$ cyclic components of order ℓ^n and possibly one additional component of strictly lower order. For a suitable choice of the basis of $A[\ell^n]$ we have

$$M'_n - \mathrm{Id}_n = \begin{pmatrix} 0 & \dots & 0 & a_1 & b_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & a_{2g-1} & b_{2g-1} \\ 0 & \dots & 0 & a_{2g} & b_{2g} \\ 0 & \dots & 0 & 0 & 0 \end{pmatrix}.$$

Thus $(P \bmod \mathfrak{p})$ is ℓ^n-divisible in $A(k_\mathfrak{p})$ if and only if $\begin{pmatrix} b_1 \\ \vdots \\ b_{2g} \end{pmatrix}$ is a multiple of $\begin{pmatrix} a_1 \\ \vdots \\ a_{2g} \end{pmatrix}$. More generally, suppose that $\ker(M_n - \mathrm{Id}_n)$ has $2g-r$ cyclic components of order ℓ^n for some $r \geq 1$ and possibly additional components of strictly lower order. Similarly, the point $(P \bmod \mathfrak{p})$ is ℓ^n-divisible in $A(k_\mathfrak{p})$ if and only if the last column of M'_n, without the last entry, is a linear combination of the r non-zero columns of $M_n - \mathrm{Id}_n$.

4. The Indivisibility-LT conjecture

In this section we collect results related to the Indivisibility-LT conjecture.

Proposition 12. *Let S be a finite and non-empty set of prime numbers, and call m the product of the elements of S. The set of primes $\mathfrak{p} \in S_A$ such that Condition 1 holds for all $\ell \in S$ admits a natural density, which is the proportion of Galois automorphisms $\sigma \in \mathrm{Gal}(K(\frac{1}{m}P)/K)$ satisfying the following condition for each $\ell \in S$: σ does not fix any torsion point of order ℓ, or σ does not fix any point in $\frac{1}{\ell}P$. In particular, the density is a rational number whose minimal denominator divides $m^{2g} \cdot \#\mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$.*

Proof. The last assertion is because the degree of $K(\frac{1}{m}P)/K$ divides $m^{2g} \cdot \#\mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$. For each $\ell \in S$ we restrict σ to $K(\frac{1}{\ell}P)$ and apply Lemma 9 with $n = 1$, thus determining a subset of $\mathrm{Gal}(K(\frac{1}{m}P)/K)$ of suitable automorphisms. The statement then follows from the Chebotarev density theorem because we count the primes $\mathfrak{p} \in S_A$, not over any prime in S, whose Frobenius conjugacy class with respect to $K(\frac{1}{m}P)/K$ is contained in the above subset. □

In the following result we may observe that the expression for the density is a rational function in ℓ (where the polynomials in the numerator and denominator have degree 4 or 6 according to whether the elliptic curve is with or without CM), possibly with a case distinction about whether ℓ splits or not in the CM field. We also remark that the Euler product $\prod_{\ell \gg 0} \mathrm{dens}(\ell)$ is strictly positive.

Theorem 13. *Consider the density $\mathrm{dens}(\ell)$ of the set of primes $\mathfrak{p} \in S_A$ such that Condition 1 holds for ℓ. If A is an elliptic curve without complex multiplication, then for every $\ell \gg 0$ we*

have

$$\mathrm{dens}(\ell) = 1 - \frac{\ell^4 - 2\ell^2 - \ell + 1}{\ell^3(\ell-1)(\ell^2-1)}.$$

Now suppose that A is an elliptic curve with complex multiplication by an order contained in the imaginary quadratic field of discriminant $-D$. Then for every $\ell \gg 0$ we have

$$\mathrm{dens}(\ell) = \begin{cases} \dfrac{2\ell^4 - 4\ell^3 - \ell^2 + 5\ell - 1}{2\ell^2(\ell-1)^2} & \text{if the CM is not over } K \text{ and } \left(\frac{-D}{\ell}\right) = 1 \\ \dfrac{2\ell^4 - 3\ell^2 - \ell - 1}{2\ell^2(\ell^2-1)} & \text{if the CM is not over } K \text{ and } \left(\frac{-D}{\ell}\right) = -1 \\ \dfrac{\ell^4 - 2\ell^3 - \ell^2 + 4\ell - 1}{\ell^2(\ell-1)^2} & \text{if the CM is over } K \text{ and } \left(\frac{-D}{\ell}\right) = 1 \\ \dfrac{\ell^4 - \ell^2 - 1}{\ell^4 - \ell^2} & \text{if the CM is over } K \text{ and } \left(\frac{-D}{\ell}\right) = -1\,. \end{cases}$$

Proof. We make use of the adelic open image theorem ([Ser72, Théorème 3], [CP22b, Lemma 2.2]) and of Betrand's Theorem [Ber88, Theorem 1]. If the elliptic curve is without CM, then for every $\ell \gg 0$ the image of the $\mathrm{mod}\ell$ torsion representation is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. If the elliptic curve has CM, then for $\ell \gg 0$ the image of the $\mathrm{mod}\ell$ torsion representation is isomorphic to the group of $\mathbb{Z}/\ell\mathbb{Z}$-points of a Cartan subgroup of GL_2 or the normalizer of a Cartan subgroup of GL_2 (and we are in the former case if and only if the CM is defined over K). The Cartan group is split if $\left(\frac{-D}{\ell}\right) = 1$ and nonsplit if $\left(\frac{-D}{\ell}\right) = -1$. Moreover, for $\ell \gg 0$ the Kummer representation $\mathrm{mod}\ell$ is surjective, and the image of the torsion-Kummer representation $\mathrm{mod}\ell$ is as large as possible. The density (which exists by Proposition 12) can easily be computed thanks to Proposition 12, Proposition 15 and Proposition 26. □

Remark 14. Let M_1 vary in the image of the $\mathrm{mod}\ell$ torsion representation of A. If for some M_1 we have $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2g$, then the density $\mathrm{dens}(\ell)$ is strictly positive. Now suppose that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) < 2g$ holds for all M_1. Then $\mathrm{dens}(\ell)$ is zero if P is an ℓ-multiple in $A(K)$. For elliptic curves, this last condition is necessary to have $\mathrm{dens}(\ell) = 0$ by the results on the local-global principle for divisibility, see [Won00].

In the following result, we denote by G the image of the ℓ-adic torsion-Kummer representation and we denote by μ the normalized Haar measure on G. In the following proposition, we make use of the notation introduced in Section 6.

Proposition 15. *Let A be an elliptic curve. The density $\mathrm{dens}(\ell)$ is the Haar measure of the set*

$$\{(M, v) \in G \mid \mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2 \text{ or } v_1 \notin \mathrm{Im}(M_1 - \mathrm{Id}_1)\}\,.$$

If $[K(A(\frac{1}{\ell}P) : K(A[\ell])] = \ell^2$, this Haar measure is $1 - \frac{R_1'(1)\ell + 1}{R_1(1)\ell^2}$.

Proof. The first assertion is a consequence of Proposition 12. Our assumption on the $\mathrm{mod}\ell$ torsion-Kummer representation implies that $R(1) = R_1(1)\ell^2$. The number of $(M_1, v_1) \in G(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2$ is ℓ^2 times $R_1(1) - R_1'(1) - 1$, as the latter is the number of matrices $M_1 \in \pi_1(G)(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2$. Similarly, the number of $(M_1, v_1) \in G(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 1$ and $v_1 \notin \mathrm{Im}(M_1 - \mathrm{Id}_1)$ is $\ell^2 - \ell$ times $R_1'(1)$. Finally, there are $\ell^2 - 1$ elements $(M_1, v_1) \in G(1)$ such that $M_1 = \mathrm{Id}_1$ and $v_1 \neq 0$. □

As a consequence of the adelic open image theorem ([Ser72, Théorème 3], [CP22b, Lemma 2.2]) and of Betrand's Theorem [Ber88, Theorem 1], the assumption on the torsion-Kummer

representation in the following theorem is known to hold for elliptic curves without CM or with CM that is defined over the base field.

Theorem 16. *Suppose that there is some positive integer B such that for every prime $\ell \nmid B$ the following holds: the extension $K(\frac{1}{\ell}P)$ is linearly disjoint from $K(\frac{1}{m}P)$ for all positive square-free integers m coprime to ℓ. Then the density in the Indivisibility-LT conjecture is a rational multiple of the product over all primes ℓ of the density that considers Condition 1 only for ℓ.*

Proof. For any finite and non-empty set S of prime numbers denote by $\mathrm{dens}(S)$ the density from Proposition 12. We simply write $\mathrm{dens}(\ell)$ if $S = \{\ell\}$. Let S_B be the set of prime divisors of B. First, $\mathrm{dens}(S_B)$ is a rational multiple of $\prod_{\ell \in S_B} \mathrm{dens}(\ell)$. This is because we compare two rational numbers and $\mathrm{dens}(S_B)$ is zero whenever $\mathrm{dens}(\ell)$ is zero for some $\ell \in S_B$. Then it suffices to observe that the following holds, by our assumption on B, for any finite set S' of prime numbers that do not divide B:

$$\mathrm{dens}(S') = \prod_{\ell \in S'} \mathrm{dens}(\ell)$$

$$\mathrm{dens}(S' \cup S_B) = \mathrm{dens}(S') \cdot \mathrm{dens}(S_B) \qquad \prod_{\ell \in S' \cup S_B} \mathrm{dens}(\ell) = \mathrm{dens}(S') \cdot \prod_{\ell \in S_B} \mathrm{dens}(\ell)\,.$$

We conclude by considering the infimum of the given quantities by increasing S'. □

5. The ℓ-adic valuation of the exponent

Fix some prime ℓ. We study the set S of primes $\mathfrak{p} \in S_A$, not over ℓ, such that Condition 2 holds. We write $S = \cup_{n \geq 0} S_n$, where

$$S_n = \{\mathfrak{p} \in S : \mathrm{ord}_\ell(P \bmod \mathfrak{p}) = \exp_\ell A(k_\mathfrak{p}) = n\}\,.$$

Call $\rho_{\ell^n} : \mathrm{Gal}(K(A[\ell^n])/K) \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$ the torsion representation $\bmod \ell^n$.

Remark 17. The set S_0 consists of the primes $\mathfrak{p} \in S_A$, not over ℓ, such that $\ell \nmid \#A(k_\mathfrak{p})$. This set has a natural density which is a rational number. By Lemma 3 we have

$$\mathrm{dens}(S_0) = \frac{\#\{M_1 \in \mathrm{Im}(\rho_\ell) \mid \mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2g\}}{\#\{M_1 \in \mathrm{Im}(\rho_\ell)\}}\,.$$

Remark 18. For $n > 0$, the set S_n has a natural density which is a rational number because it can be described in terms of the $\bmod \ell^{n+1}$ torsion-Kummer representation. Let $M_{n+1} \in \mathrm{Im}(\rho_{\ell^{n+1}})$ and write $M_n := M_{n+1} \bmod \ell^n$. Let $\sigma \in \mathrm{Gal}(K(A[\ell^n])/K)$ be the preimage of M_n under ρ_{ℓ^n}. Suppose that $\mathfrak{p}$ is such that σ is in the conjugacy class of the Frobenius at $\mathfrak{p}$. Then by Lemma 3 the condition $\exp_\ell(A(k_\mathfrak{p})) = n$ is equivalent to the following:

$$\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) < 2g \qquad \text{and} \qquad \mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2g\,.$$

Remark that $\mathrm{ord}_\ell(P \bmod \mathfrak{p}) = n$ is equivalent to $\ell^{n-1}(P \bmod \mathfrak{p})$ being not ℓ^n-divisible in $A(k_\mathfrak{p})$. By applying Lemma 9 to the point $\ell^{n-1}P$ this condition is equivalent to the following:

$$[\ell^{n-1}](\sigma(Q_n) - Q_n) \notin \mathrm{Im}(M_n - \mathrm{Id}_n)$$

where we here extend σ to a Galois automorphism of $K(\frac{1}{\ell^n}P)/K$. Notice that the above conditions do not depend on the choice of σ nor on the choice of its extension because they ultimately depend only on $\mathfrak{p}$. This independence can also be verified directly, see Remark 5.

Notice that $\{\mathfrak{p} : \exp_\ell A(k_\mathfrak{p}) \geq n\}$ can be described in terms of the $\mathrm{mod}\ell^n$ torsion representation of A. Moreover, the set $\{\mathfrak{p} \in S_A : \exp_\ell(A(k_\mathfrak{p})) < n\}$ and hence also its complementary set $\{\mathfrak{p} \in S_A : \exp_\ell(A(k_\mathfrak{p})) \geq n\}$ admits a natural density that is a rational number. The density is non-decreasing (respectively, non-increasing) with n.

Lemma 19 (Hörmann-Lombardo)**.** *A monic polynomial $f(x)$ of degree d with coefficients in $\mathbb{Z}/\ell^n\mathbb{Z}$ can have at most*

$$d \cdot \ell^{n(1-\frac{1}{d})}$$

roots in $\mathbb{Z}/\ell^n\mathbb{Z}$.

Proof. Fix a monic polynomial $\tilde{f}(x) \in \mathbb{Z}_\ell[x]$ that is congruent to $f(x)$ modulo ℓ^n. Let K be a splitting field of $\tilde{f}(x)$ over $\mathbb{Q}_\ell$ and write $\mathcal{O}_K$ for the ring of integers of K and π for a uniformiser. By construction, $\tilde{f}(x)$ factors in $\mathcal{O}_K[x]$ as $\prod_{i=1}^d (x - x_i)$ for certain $x_i \in \mathcal{O}_K$. Note that every $\alpha \in \mathbb{Z}/\ell^n\mathbb{Z}$ such that $f(\alpha) \equiv 0 \pmod{\ell^n}$ lifts to $\tilde{\alpha} \in \{0, 1, \ldots, \ell^n - 1\} \subset \mathcal{O}_K$ with $v_\pi(\tilde{f}(\tilde{\alpha})) \geq v_\pi(\ell^n) = ne$, where $e := v_\pi(\ell)$ is the ramification index of K over $\mathbb{Q}_\ell$. If $v_\pi(\tilde{f}(\tilde{\alpha})) \geq ne$, there is an index i such that $v_\pi(\tilde{\alpha} - x_i) \geq \frac{ne}{d}$. For each root α of $f(x)$ consider the lift $\tilde{\alpha}$ and the index i such that $v_\pi(\tilde{\alpha} - x_i)$ is maximal (if more than one such index i exists, take the smallest one). If α_1, α_2 both correspond to the same index i, then

$$v_\pi(\tilde{\alpha}_1 - \tilde{\alpha}_2) = v_\pi((\tilde{\alpha}_1 - x_i) - (\tilde{\alpha}_2 - x_i)) \geq \min\{v_\pi(\tilde{\alpha}_1 - x_i), v_\pi(\tilde{\alpha}_2 - x_i)\} \geq \frac{ne}{d}.$$

Since $\tilde{\alpha}_1, \tilde{\alpha}_2$ are in $\mathbb{Z}$, we also have $v_\pi(\tilde{\alpha}_1 - \tilde{\alpha}_2) = e \cdot v_\ell(\tilde{\alpha}_1 - \tilde{\alpha}_2)$, and therefore $v_\ell(\tilde{\alpha}_1 - \tilde{\alpha}_2) \geq \frac{n}{d}$, that is, $\alpha_1 \equiv \alpha_2 \pmod{\ell^{\lceil n/d \rceil}}$. In particular, there are at most $\ell^{n - \lceil n/d \rceil} \leq \ell^{n(1-1/d)}$ roots α corresponding to a given index i. The claim follows from the fact that there are d possible values for i. □

Notice that the following result, in case of elliptic curves, can be deduced from the explicit computations carried out in this paper:

Theorem 20 (Hörmann-Lombardo)**.** *For any abelian variety, the density of the set*

$$\{\mathfrak{p} \in S_A \mid \exp_\ell(A(k_\mathfrak{p})) \geq n\}$$

goes to 0 *when n goes to infinity.*

Proof. We may suppose that $\mathfrak{p}$ is not over ℓ. By Remark 8 and by the Chebotarev Density Theorem, we may equivalently show that $\#H_n/\#G_n$ goes to 0 when n goes to infinity, where $G_n := \mathrm{Gal}(K(A[\ell^n])/K)$ and

$$H_n := \{\sigma \in G_n \mid \exists\, T \in A[\ell^n] \setminus A[\ell^{n-1}] : \sigma(T) = T\}.$$

As usual, we can identify G_n with a subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$. By a result of Serre and Wintenberger (see the proof of [LP21, Lemma 31]) we know that G_n contains at least $c\ell^n$ scalar matrices, where c is a positive constant that depends only on A/K. We claim that in each coset of G_n modulo the scalar matrices there are at most $2g \cdot \ell^{n(1-1/(2g))}$ elements M for which there exists a primitive vector $v \in (\mathbb{Z}/\ell^n\mathbb{Z})^{2g} \setminus (\ell\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ (corresponding to a torsion point $T \in A[\ell^n] \setminus A[\ell^{n-1}]$) with $Mv = v$. Indeed, if M_0 is a fixed representative of the coset, the matrix M is of the form $M = \lambda M_0$ for some $\lambda \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$, hence the equation $Mv = v$ becomes $M_0 v = (\lambda^{-1})v$. As v is primitive, this implies that λ^{-1} is a root in $\mathbb{Z}/\ell^n\mathbb{Z}$ of the characteristic polynomial of M_0 (see [Bro93, Lemma 17.3]). By Lemma 19, the (monic) characteristic polynomial of M_0 has at most $2g \cdot \ell^{n(1-1/(2g))}$ roots in $\mathbb{Z}/\ell^n\mathbb{Z}$, which proves the

claim. Letting $t := \#\{\lambda \cdot \mathrm{Id} \mid \lambda \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times, \lambda \cdot \mathrm{Id} \in G_n\}$ and summing over the cosets, we obtain $\#H_n \leq (\#G_n/t) \cdot \ell^{n(1-1/(2g))}$. As $t \geq c\ell^n$, we conclude because we then have

$$\frac{\#H_n}{\#G_n} \leq \frac{2g \cdot \ell^{n-n/(2g)}}{c\ell^n} = \frac{2g}{c} \cdot \ell^{-n/(2g)}.$$

□

Consider the above statement. The same holds replacing the density by the Haar measure of the corresponding elements in the image of the ℓ-adic torsion-Kummer representation (we study those sets in Section 6).

Remark 21. With the notation of Section 6, for every $n \geq 0$ we have $\mathrm{dens}(S_n) = \mu(E_n)$.

Remark 22. From Theorem 20 we deduce that $\mathrm{dens}(S)$ exists and that we have

$$\mathrm{dens}(S) = \sum_{n \geq 0} \mathrm{dens}(S_n)\,.$$

Similarly, if we consider Condition (2) for finitely many prime numbers ℓ, we deduce that we have a natural density, which is the sum of the densities where we restrict to the primes $\mathfrak{p}$ such that $\exp_\ell(A(k_\mathfrak{p}))$ is prescribed for the finitely many primes ℓ.

Proof of Theorem1. The statement is true because the corresponding sets of matrices have rational Haar measures, see Section 7. □

Corollary 23. *Let $\ell_1, \ldots, \ell_r$ be distinct primes. If A is an elliptic curve, then the set*

$$\{\mathfrak{p} \in S_A \mid \mathrm{ord}_{\ell_i}\left(P \bmod \mathfrak{p}\right) = \exp_{\ell_i}(A(k_\mathfrak{p})) \ \forall i = 1, \ldots, r\}$$

has a natural density which is a rational number.

Proof. By Remark 22 we only have to prove the rationality of the density. Let $m = \prod_i \ell_i$. We may select n_0 such that the image of the m-adic torsion-Kummer representation is the preimage of the image of the $\mathrm{mod}m^{n_0}$ torsion-Kummer representation. We then partition the primes $\mathfrak{p}$ according to the $\mathrm{mod}m^{n_0}$ torsion-Kummer representation. This is a finite partition, so to prove the rationality it suffices to fix a matrix M_0 in the image of the $\mathrm{mod}m^{n_0}$ torsion-Kummer representation. Call $M_{0,i}$ the image of M_0 in the $\mathrm{mod}\ell_i^{n_0}$ torsion-Kummer representation. The density d_i concerning only ℓ_i and fixing $M_{0,i}$ is rational (see Section 7). So the density concerning ℓ_i and fixing M_0 is rational because it equals $\prod_i d_i$. □

As a consequence of the adelic open image theorem ([Ser72, Théorème 3], [CP22b, Lemma 2.2]) and of Betrand's Theorem [Ber88, Theorem 1], the assumption on the torsion-Kummer representation in the following theorem is known to hold for elliptic curves without CM or with CM that is defined over the base field. The assumption on the density is known for elliptic curves as a consequence of Corollary 23.

Theorem 24. *Assume that the density, considering Condition 2 for ℓ in a finite set, exists and it is rational. Moreover, suppose that there is some positive integer B such that for every prime $\ell \nmid B$ the following holds: the extension $K(\frac{1}{\ell^\infty}P)$ is linearly disjoint from $K(\frac{1}{m^\infty}P)$ for all positive square-free integers m coprime to ℓ. The density in the Exponent-LT conjecture is then a rational multiple of the product over all ℓ of the density that considers only Condition 2 at ℓ.*

Proof. The proof is analogous to the one of Theorem 16. □

6. The matrices corresponding to the exponent condition at ℓ

6.1. **Setup.** Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell) \ltimes (\mathbb{Z}_\ell)^2$ and call π_1, π_2 the projections onto the two factors. We suppose that $\pi_1(G)$ is a finite index subgroup of a group $\pi_1(G)'$ that is either $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or (the normalizer of) a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. We also suppose that G has finite index in $\pi_1(G)' \ltimes (\mathbb{Z}_\ell)^2$. We let n_0 be a positive integer such that the index of $G(n_0)$ in $\pi_1(G)'(n_0) \ltimes (\mathbb{Z}/\ell^{n_0}\mathbb{Z})^2$ is the same as the index of G in $\pi_1(G)' \ltimes (\mathbb{Z}_\ell)^2$. We let $d_G = 4$ if $\pi_1(G)$ has finite index in $\mathrm{GL}(\mathbb{Z}_\ell)$, and $d_G = 2$ otherwise.

We equip G with its normalized Haar measure μ. For $n \geq 1$, we set $G(n) = G \bmod \ell^n$. For an element $(M, v) \in G$ and a positive integer n, we set $(M_n, v_n) := (M, v) \bmod \ell^n \in G(n)$. Similarly, for a positive integer N and an element $(M_N, v_N) \in G(N)$, for $n \leq N$, we set $(M_n, v_n) := (M_N, v_N) \bmod \ell^n$.

We define

$$E_0 = \{(M, v) \in G \mid \mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2\}$$

and, for $n \geq 1$, we define

$$E_n = \{(M, v) \in G \mid \mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2, \mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) \leq 1, [\ell^{n-1}]v_n \notin \mathrm{Im}(M_n - \mathrm{Id}_n)\}.$$

Definition 25. We define $R_1(n) = \#\pi_1(G)(n)$, $R(n) = \#G(n)$ and

$$R_1'(n) = \#\{M_n \in \pi_1(G)(n) \mid \mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1\}.$$

If $n \geq 2$, we also define

$$R_1''(n) = \#\{M_n \in \pi_1(G)(n) \mid \mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1 \text{ and } M_n \equiv \mathrm{Id}_{n-1} \bmod \ell^{n-1}\}.$$

Proposition 26. *The quantities $R_1(1)$ and $R_1'(1)$ are as follows:*

	$R_1(1)$	$R_1'(1)$
$\mathrm{GL}_2(\mathbb{Z}_\ell)$	$(\ell^2-1)(\ell^2-\ell)$	$\ell^3 - 2\ell - 1$
Split Cartan	$(\ell-1)^2$	$2\ell - 4$
Nonsplit Cartan	$\ell^2 - 1$	0
Normalizer of a split Cartan	$2(\ell-1)^2$	$3\ell - 5$
Normalizer of a nonsplit Cartan	$2(\ell^2-1)$	$\ell + 1$
Normalizer of a ramified Cartan (ℓ odd)	$2\ell(\ell-1)$	$3\ell - 1$
Normalizer of a ramified Cartan ($\ell = 2$)	2	1

Proof. The case of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. The matrices M_1 in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that $\det(M_1 - \mathrm{Id}_1) = 0 \bmod \ell$ are those matrices of the form $\begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix}$ such that $ad - bc = 0$ and $1 + a + d \neq 0$. We distinguish the cases $a, d \notin \{0, -1\}$, $a = 0$ and $d \neq -1$ (or conversely), $a = -1$ and $d \neq 0$ (or conversely). A straightforward count gives $(\ell-2)(\ell-3)(\ell-1)$ respectively $(2\ell-1)(2\ell-3)$ respectively $(2\ell-3)(\ell-1)$, with a total of $\ell^3 - 2\ell$ matrices. Excluding the identity from this count gives $R_1'(1) = \ell^3 - 2\ell - 1$.

The (normalizer of a) split Cartan. We use the diagonal model. A matrix $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \beta_1 \end{pmatrix} \in C(1)$ has a 1-eigenvector if and only if $\alpha_1 = 1$ or $\beta_1 = 1$. There are $2\ell - 4$ such elements different from the identity. Let $M_1 = \begin{pmatrix} 0 & \beta_1 \\ \alpha_1 & 0 \end{pmatrix} \in C'(1)$. Then, $\det(M_1 - \mathrm{Id}_1) = 0$ if and only

if $1-\alpha_1\beta_1=0$, so there are $\ell-1$ elements M_1 in $C'(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1-\mathrm{Id}_1)=1$. Therefore, $R_1'(1)=3\ell-5$.

The (normalizer of a) nonsplit Cartan for ℓ odd. For $M_1=\begin{pmatrix}\alpha_1 & \beta_1 d\\ \beta_1 & \alpha_1\end{pmatrix}\in C(1)$, $\mathrm{rk}(M_1-\mathrm{Id}_1)=2$ except if $\beta_1=0$ and $\alpha_1=1$ (which corresponds to $M_1=\mathrm{Id}_1$). For $\begin{pmatrix}\alpha_1 & \beta_1 d\\ \beta_1 & \alpha_1\end{pmatrix}\in C(1)$, we have $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\cdot\begin{pmatrix}\alpha_1 & \beta_1 d\\ \beta_1 & \alpha_1\end{pmatrix}=\begin{pmatrix}\alpha_1 & \beta_1 d\\ -\beta_1 & -\alpha_1\end{pmatrix}$. We have $\mathrm{rk}\left(\begin{pmatrix}\alpha_1-1 & \beta_1 d\\ -\beta_1 & -\alpha_1-1\end{pmatrix}\right)=1$ if and only if $\beta_1^2 d+1=\alpha_1^2$. For $\alpha_1=\pm1$, there is only one possibility for β_1 ($\beta_1=0$). Else, the previous equation has solutions if and only if $\left(\frac{\alpha_1^2-1}{\ell}\right)=-1$. We know from [PP18, Theorem 1] that $\sum_{a\in\mathbb{Z}/\ell\mathbb{Z}}\left(\frac{a^2-1}{\ell}\right)=-1$, so the number of coefficients α_1 such that $\left(\frac{\alpha_1^2-1}{\ell}\right)=-1$ is $\frac{\ell-1}{2}$. Each value of α_1 gives two possibilities for β_1, so the number of elements of $C'(1)$ such that $\mathrm{rk}(M_1-\mathrm{Id}_1)=1$ is $\ell+1$, which implies $R_1'(1)=\ell+1$.

The (normalizer of a) nonsplit Cartan for $\ell=2$. Consider that the elements $M_1\in N(1)$ different from Id_1 such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1-\mathrm{Id}_1)\leq 1$ are

$$M_{1,1}=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, M_{1,2}=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, M_{1,3}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

Notice that they all belong to $C'(1)$.

The (normalizer of a) ramified Cartan. The case $\ell=2$ is a small calculation, so suppose that ℓ is odd. For $M_1=\begin{pmatrix}\alpha_1 & 0\\ \beta_1 & \alpha_1\end{pmatrix}\in C(1)$, M_1 admits a 1-eigenvector if and only if $\alpha_1=1$ (there are $\ell-1$ ways to choose β_1, $\beta_1=0$ corresponds to the identity). For $M_1=\begin{pmatrix}\alpha_1 & 0\\ -\beta_1 & -\alpha_1\end{pmatrix}\in C'(1)$, M_1 admits a 1-eigenvector if and only if $\alpha_1=\pm1$ (there are two possible choices for α_1, and ℓ choices for β_1). So $R_1'(1)=3\ell-1$. □

Remark 27. We have

$$\mu(E_0)=1-\frac{R_1'(1)+1}{R_1(1)}$$

as the number of $M_1\in\pi_1(G)(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1-\mathrm{Id}_1)=2$ is $R_1(1)-(R_1'(1)+1))$.

Proposition 28. *Suppose that $[K(\frac{1}{\ell^n}P):K(A[\ell^n])]=\ell^{2n}$ holds for all $n\geq 1$ (equivalently, suppose that this holds for n_0). For $n\geq n_0$ we have*

$$\mu(E_n)=\frac{(R_1'(n)\ell^{d_G}-R_1'(n+1))\frac{\ell-1}{\ell}+(\ell^{d_G}-R_1''(n+1)-1)\frac{\ell^2-1}{\ell^2}}{R_1(n+1)}.$$

Proof. For $n\geq 1$, there are $\ell^{d_G}-R_1''(n+1)-1$ matrices $M_{n+1}\in\pi_1(G)(n+1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1}-\mathrm{Id}_{n+1})=2$ and $M_n=\mathrm{Id}_n$. The proportion of vectors $v_n\in\pi_2(\pi_1^{-1}(M_n))$ such that $[\ell^{n-1}]v_n\notin\mathrm{Im}(M_n-\mathrm{Id}_n)$ is $\frac{\ell^2-1}{\ell^2}$. The number of matrices $M_{n+1}\in\pi_1(G)(n+1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1}-\mathrm{Id}_{n+1})=2$ and $\mathrm{rk}_{\ell\mathbb{Z}}(M_n-\mathrm{Id}_n)=1$ is $R_1'(n)\ell^{d_G}-R_1'(n+1)$. The proportion of vectors $v_n\in\pi_2(\pi_1^{-1}(M_n))$ such that $[\ell^{n-1}]v_n\notin\mathrm{Im}(M_n-\mathrm{Id}_n)=1$ is $\frac{\ell-1}{\ell}$. □

Lemma 29. *Let $M_{n+1}\in\mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$ be such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1}-\mathrm{Id}_{n+1})=1$ and $v_{n+1}\in(\mathbb{Z}/\ell^{n+1}\mathbb{Z})^2$. Assume that $M_n\neq\mathrm{Id}_n$. Then*

$$[\ell^n]v_{n+1}\in\mathrm{Im}_{\ell\mathbb{Z}}(M_{n+1}-\mathrm{Id}_{n+1})\iff[\ell^{n-1}]v_n\in\mathrm{Im}_{\ell\mathbb{Z}}(M_n-\mathrm{Id}_n).$$

Proof. Call $\vec{c}_{n+1}$ one non-zero column of $M_{n+1} - \mathrm{Id}_{n+1}$ that generates the column space. Assume that $[\ell^n]v_{n+1} = \lambda_{n+1}\vec{c}_{n+1}$. If λ_{n+1} is not divisible by ℓ, then, the coefficients of $\vec{c}_{n+1}$ are both divisible by ℓ^n, which means that $\vec{c}_{n+1} \bmod \ell^n$ is zero, contradicting that $M_n \neq \mathrm{Id}_n$. We deduce that $[\ell^{n-1}]v_n = \frac{\lambda_{n+1}}{\ell}\vec{c}_n$. Conversely, if $[\ell^{n-1}]v_n = k_n\vec{c}_n$, then $[\ell^n]v_{n+1} = \ell k_{n+1}\vec{c}_{n+1}$ where k_{n+1} is any lift of k_n. □

Lemma 30. *Let $n > n_0$. Let $M_n \in \pi_1(G)(n)$ be such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $M_n \equiv \mathrm{Id}_{n_0} \bmod \ell^{n_0}$. There is $\mathcal{C} \in \{0, 1 - \frac{1}{\ell}\}$ such that, in the set $\pi_2(\pi^{-1}(M_n))$, the proportion of elements v_n such that $[\ell^{n-1}]v_n \notin \mathrm{Im}(M_n - \mathrm{Id}_n)$ is $\mathcal{C}$. Consider the group $H := [\ell^{n_0-1}]\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$. If H is trivial (for example, if $\pi_2(\pi^{-1}(\mathrm{Id}_1))$ is trivial), then $\mathcal{C} = 0$. If H has two components, then $\mathcal{C} = 1 - \frac{1}{\ell}$. If H has one component, we are in the former case if and only if $H = \mathrm{Im}(M_h - \mathrm{Id}_h)$, where $M_h = M_n \bmod \ell^h$ and $h > n_0$ is the smallest integer such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_h - \mathrm{Id}_h) = 1$. If $N \geq n$ is such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_N - \mathrm{Id}_N) = 1$ and $M_N \equiv M_n \bmod \ell^n$, then $\mathcal{C}(M_n) = \mathcal{C}(M_N)$.*

Proof. We know that $\pi_2(\pi_1^{-1}(M_n))$ is the preimage under the multiplication by ℓ^{n-n_0} of $\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$. Moreover, $[\ell^{n-1}]\pi_2(\pi^{-1}(M_n))$ is contained in $\pi_2(\pi_1^{-1}(\mathrm{Id}_1))$.

Recall the identification of $([\ell^{m-1}]\mathbb{Z}/\ell^m\mathbb{Z})^2$ with $(\mathbb{Z}/\ell\mathbb{Z})^2$ for every $m \geq 2$. By the assumption on the $\ell\mathbb{Z}$-rank we know that the group

$$W_{M_n} := \mathrm{Im}(M_n - \mathrm{Id}_n) \cap (\mathbb{Z}/\ell\mathbb{Z})^2$$

has ℓ elements. The ratio between the cardinality of the groups H and $H \cap W_{M_n}$ could then be 1 or ℓ, leading to $\mathcal{C} = 0$ and $\mathcal{C} = 1 - \frac{1}{\ell}$ respectively. If H is trivial (respectively, $H = (\mathbb{Z}/\ell\mathbb{Z})^2$), the ratio is clearly 1 (respectively, ℓ). Now suppose that H has ℓ elements. We conclude by observing that $W_{M_n} = W_{M_h} = \mathrm{Im}(M_h - \mathrm{Id}_h)$.

The last assertion is clear because $W_{M_n} = W_{M_N}$. □

Definition 31. For $n \geq n_0$ and $M_{n_0} \in \pi_1(G)(n_0)$, we define

$$E_{n,M_{n_0}} = \{(M, v) \in E_n \mid M_n \equiv M_{n_0} \bmod \ell^{n_0}\}. \tag{3}$$

Thus, for $n \geq n_0$, we have

$$\mu(E_n) = \sum_{M_{n_0} \in \pi_1(G)(n_0)} \mu(E_{n,M_{n_0}}). \tag{4}$$

Remark 32. Fix a subgroup H of $(\mathbb{Z}/\ell\mathbb{Z})^2$ with ℓ elements. For an integer $t \geq n_0 + 1$, consider the set H' of all $M_t \in \pi_1(G)(t)$ such that $M_{t-1} = \mathrm{Id}_{t-1}$, $\mathrm{rk}_{\ell\mathbb{Z}}(M_t - \mathrm{Id}_t) = 1$ and $\mathrm{Im}(M_t - \mathrm{Id}_t) = H$. If $\pi_1(G)$ is a finite index subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, then $\#H' = \ell^2 - 1$. If $\pi_1(G)$ is a finite index subgroup of the normalizer of a split Cartan subgroup, then $\#H' = \ell - 1$ or $\#H' = 0$ (and we are in the former case if and only if H is the group generated by one of the two vectors of the basis diagonalizing the Cartan). Recall that there is no matrix M_t above the identity such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_t - \mathrm{Id}_t) = 1$ (see Table 46) for a nonsplit Cartan subgroup.

Remark 33. Let $n \geq n_0$ and set $H := [\ell^{n_0-1}]\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$. There is $\mathcal{C} \in \{0, \frac{\ell^2-1}{\ell^2}, \frac{\ell-1}{\ell}\}$ such that in the set $\pi_2(\pi_1^{-1}(\mathrm{Id}_n))$, the proportion of elements v_n such that $[\ell^{n-1}]v_n \neq 0$ equals $\mathcal{C}$. If H is trivial, then $\mathcal{C} = 0$. If H has two components, then $\mathcal{C} = \frac{\ell^2-1}{\ell^2}$. If H has one component, then $\mathcal{C} = \frac{\ell-1}{\ell}$. This is because the set $\pi_2(\pi_1^{-1}(\mathrm{Id}_n))$ is the preimage in $(\mathbb{Z}/\ell^n\mathbb{Z})^2$ of $\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$ under $[\ell^{n-n_0}]$.

Definition 34. Let $n \geq n_0$. If $M_n \equiv M_{n_0} \bmod \ell^{n_0}$ and $M_n - \mathrm{Id}_n$ and $M_{n_0} - \mathrm{Id}_{n_0}$ have both $\ell\mathbb{Z}$-rank 1, by Lemma 29, the number of pairs $(M_N, v_N) \in G(N)$ such that $[\ell^{N-1}]v_N$ is in the column space of $M_N - \mathrm{Id}_N$ divided by the number of pairs $(M_N, v_N) \in G(N)$ is the same for $N = n_0$ and $N = n$. We denote this ratio by $c_{M_{n_0}}$.

Definition 35. Suppose that $\pi_1(G)$ has finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or the normalizer of an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let $n \geq n_0$, and let $M_n \in \pi_1(G)(n)$ be such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) \leq 1$. If $M_n \neq \mathrm{Id}_n$, we define L_1 (respectively, L_2) as the number of lifts M_{n+1} of M_n to $\pi_1(G)(n+1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$ (respectively, $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$). If $M_n = \mathrm{Id}_n$, we similarly define $L_{\mathrm{Id},1}$ and $L_{\mathrm{Id},2}$.

Suppose that we are in the case of GL_2 or an unramified Cartan or the normalizer of an unramified Cartan. Then our explicit computations in Appendix A show that L_1, L_2, $L_{\mathrm{Id},1}$ and $L_{\mathrm{Id},2}$ don't depend on $n \geq n_0$ and L_1, L_2 do not depend on the choice of the matrix $M_n \neq \mathrm{Id}_n$.

7. On the rationality of certain Haar measures

We make use of the notation from Section 6. Observe that the set $\cup_{n\geq 0} E_n$ admits a Haar measure and we have

$$\mu(\cup_{n\geq 0} E_n) = \sum_{n\geq 0} \mu(E_n)\,.$$

7.1. GL_2 and normalizers of unramified Cartan subgroups.

Theorem 36. *Let $\pi_1(G)$ have finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or in the normalizer of an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Moreover, suppose that the group $[\ell^{n_0-1}]\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$ is cyclic. Then $\mu(\bigcup_{n\geq 0} E_n)$ is a rational number.*

Proof. For every $1 \leq n < n_0$, $\mu(E_n)$ exists and it is a rational number, so we restrict to $n \geq n_0$. Consider that the sets E_n are pairwise disjoint, each of them admits a Haar measure (because they are the preimage in G of a subset of $G(n+1)$) and $\mu(\cup_{m\geq n} E_m) \to 0$ for $n \to \infty$ by Theorem 20. We are left to prove the rationality of the Haar measure. We make use of (4).

If $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 2$, then $\mu(E_{n,M_{n_0}}) = 0$ for all $n \geq n_0$. If $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 1$, then we have

$$\mu(E_{n,M_{n_0}}) = \frac{c_{M_{n_0}} \cdot L_1^{-n_0} L_2}{R_1(n_0)\ell^{(1-n_0)d_G}} \cdot (L_1 \ell^{-d_G})^n$$

and in particular $\mu(E_{n,M_{n_0}})$ for $n \geq n_0$ is a geometric sequence. Finally, suppose that $M_{n_0} = \mathrm{Id}_{n_0}$.

If $[\ell^{n_0-1}]\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$ is trivial, we conclude because we have $\mu(E_{n,M_{n_0}}) = 0$ for all $n \geq n_0$ by Remark 33. Now suppose that $H := [\ell^{n_0-1}]\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$ has ℓ elements. We partition $E_{n,\mathrm{Id}_{n_0}} = E'_{n,\mathrm{Id}_{n_0}} \cup E''_{n,\mathrm{Id}_{n_0}}$ where the former subset consists of the elements (M, v) such that $M \equiv \mathrm{Id}_n \bmod \ell^n$. The set $\pi_1(E'_{n,\mathrm{Id}_{n_0}})(n+1)$ has $L_{\mathrm{Id},2}$ elements, so we have

$$\mu(E'_{n,\mathrm{Id}_{n_0}}) = \frac{(1-\frac{1}{\ell})L_{\mathrm{Id},2}}{R_1(n_0)\ell^{(1-n_0)d_G}} \cdot (\ell^{-d_G})^n\,.$$

Now we study $E''_{n,\mathrm{Id}_{n_0}}$ and partition this set according to $r \in \{n_0, \ldots, n-1\}$ which is the largest index for which $M \equiv \mathrm{Id}_r \bmod \ell^r$. The number of lifts of Id_r to a matrix M_{r+1} such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{r+1} - \mathrm{Id}_{r+1}) = 1$ and $\mathrm{Im}(M_{r+1} - \mathrm{Id}_{r+1}) \neq H$ is $L_{\mathrm{Id},1} - \#H'$, where H' was

introduced in Remark 32. The number of lifts M_{n+1} of M_{r+1} such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1}-\mathrm{Id}_{n+1}) = 2$ and $\mathrm{rk}_{\ell\mathbb{Z}}(M_n-\mathrm{Id}_n)=1$ is $L_1^{n-(r+1)}L_2$. In the set $\pi_2(\pi_1^{-1}(M_n))$, the proportion of elements v_n that satisfy $[\ell^{n-1}]v_n \notin \mathrm{Im}(M_n-\mathrm{Id}_n)$ is $1-\frac{1}{\ell}$ by Lemma 30 (recall that for elements such that $\mathrm{Im}(M_{r+1}-\mathrm{Id}_{r+1})=H$, this proportion is 0). Thus,

$$\mu(E''_{n,\mathrm{Id}_{n_0}}) = \frac{(1-\frac{1}{\ell})\sum_{r=n_0}^{n-1}(L_{\mathrm{Id},1}-\#H')L_1^{n-(r+1)}L_2}{R_1(n_0)\ell^{(n+1-n_0)d_G}} = D(L_1^{-n_0}(\ell^{-d_G}L_1)^n-(\ell^{-d_G})^n).$$

where $D=\frac{(1-\frac{1}{\ell})(L_{\mathrm{Id},1}-\#H')L_2}{R_1(n_0)\ell^{(1-n_0)d_G}(L_1-1)}$ is a constant. Therefore, $\sum_{n\geq n_0}\mu(E_{n,M_{n_0}})$ is a sum of geometric series. □

Theorem 37. *Let $\pi_1(G)$ have finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or in the normalizer of an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Moreover, suppose that the group $[\ell^{n_0-1}]\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$ is not cyclic. Then $\mu(\cup_{n\geq 0}E_n)$ is a rational number. More precisely, for every $h\geq 0$ we have*

$$\mu(E_{n_0+h}) = \frac{L_{\mathrm{Id},2}\frac{\ell^2-1}{\ell^2}+R'_1(n_0)L_2\frac{\ell-1}{\ell}L_1^h+L_{\mathrm{Id},1}L_2\frac{\ell-1}{\ell}(L_1^h-1)/(L_1-1)}{R_1(n_0)(\ell^{d_G})^{h+1}}.$$

Proof. The explicit expression for $\mu(E_{n_0+h})$ implies the rationality of $\mu(\cup_{n\geq n_0}E_n)$ and hence of $\mu(\cup_{n\geq 0}E_n)$.

Let $n=n_0+h$ and remark that $\#\pi_1(G)(n+1)=R_1(n_0)\ell^{(h+1)d_G}$. The matrices $M_{n+1}\in\pi_1(E_n)(n+1)$ and that are the identity modulo ℓ^n are $L_{\mathrm{Id},2}$. In the set $\pi_2(\pi_1^{-1}(\mathrm{Id}_n))$, the proportion of elements v_n such that $[\ell^{n-1}]v_n\neq 0$ is $\frac{\ell^2-1}{\ell^2}$ by Remark 33.

Now suppose that $M_{n+1}\not\equiv \mathrm{Id}_n \bmod \ell^n$. By Lemma 30 the above proportion is $\frac{\ell-1}{\ell}$ instead. There are $R'_1(n_0)L_1^hL_2$ matrices $M_{n+1}\in\pi_1(E_n)(n+1)$ such that $M_{n+1}\not\equiv \mathrm{Id}_{n_0}\bmod\ell^{n_0}$. Finally, fix $n_0\leq r<n$. The number of matrices $M_{n+1}\in\pi_1(E_n)(n+1)$ such that r is the largest integer such that $M_r\equiv \mathrm{Id}_r \bmod \ell^r$ is $L_{\mathrm{Id},1}L_1^{n-r-1}L_2$ (observe that $\sum_{r=n_0}^{n-1}L_1^{n-r-1}=(L_1^h-1)/(L_1-1)$). □

7.2. **Normalizers of ramified Cartan subgroups (for ℓ odd).**

Remark 38. Let ℓ be odd. Write $d=d'\ell^{2\nu}$ for some positive integer ν and let $m>2\nu$. Suppose that $d' \bmod \ell$ is a non-zero square. Let $k \bmod \ell^m$ be a square root of $d \bmod \ell^m$. Let $\pm s$ be the two square roots of d' in $\mathbb{Z}_\ell$ and write $s=\sum_{i=0}^{+\infty}s_i\ell^i$. With the correct sign choice we may write

$$k=\ell^\nu\left(\sum_{i=0}^{m-2\nu-1}s_i\ell^i+\sum_{i=m-2\nu}^{m-\nu-1}a_i\ell^i\right)$$

where the coefficients a_i can be arbitrarily chosen (because k^2 is a multiple of $\ell^{2\nu}$). Suppose that there is $m-2\nu\leq t\leq m-\nu-1$ such that $a_t\neq s_t$ and suppose that t is minimal. Then all lifts of k modulo $\ell^{t+2\nu}$ are square roots of $d \bmod \ell^{t+2\nu}$ while no lift of k modulo $\ell^{t+2\nu+1}$ is a square root of $d \bmod \ell^{t+2\nu+1}$. Let $N>m+\nu$. If $k\equiv \ell^\nu s \bmod \ell^m$ then the amount of lifts of k modulo ℓ^N such that $k^2\equiv d \bmod \ell^N$ equals ℓ^ν (choosing a lift consists in choosing coefficients a_i for $N-2\nu\leq i\leq N-\nu-1$). Among those, there are $\ell^{\nu-1}$ lifts that can be

lifted modulo ℓ^{N+1} keeping this property (because this amounts to the coefficient $a_{N-2\nu}$ being $s_{N-2\nu}$).

Theorem 39. *Suppose that ℓ is odd, and that $\pi_1(G)$ has finite index in the normalizer of a ramified Cartan. Then $\sum_{n\geq n_0} \mu(E_{n,M_{n_0}})$ is a rational number for any $M_{n_0} \in \pi_1(G)(n_0)$.*

Proof. If $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 2$, the statement is clear because $\mu(E_{n,M_{n_0}}) = 0$ for every $n \geq n_0$. The case $M_{n_0} = \mathrm{Id}_{n_0}$ is the content of Lemma 40. Now we may suppose that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 1$.

Call C the Cartan group and C' its complement in the normalizer. If $M_{n_0} \in C'(n_0)$, we have

$$\mu(E_{n,M_{n_0}}) = c_{M_{n_0}} \frac{\ell^{n-n_0}(\ell^2-\ell)}{\#\pi_1(G)(n+1)} = c'_{M_{n_0}} \ell^{-n}$$

for some rational number $c'_{M_{n_0}}$ depending only on n_0 and M_{n_0} and we may conclude. This is because the number of lifts M_{n+1} of an element $M_n \in C'(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = \mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ is equal to ℓ (see Proposition 48).

If $M_{n_0} \in C(n_0)$, write $M_{n_0} - \mathrm{Id}_{n_0} = \begin{pmatrix} \alpha_{n_0} - 1 & d\beta_{n_0} \\ \beta_{n_0} & \alpha_{n_0} - 1 \end{pmatrix}$ and set $b := v_\ell(\beta_{n_0}) < n_0$. Let n_1 be such that $b < n_1 - v$ (in particular, $d \not\equiv 0 \bmod \ell^{n_1-b}$). We may study instead $\sum_{n>n_1} \mu(E_{n,M_{n_0}})$. In turn, this amounts to proving the rationality (for every fixed $M_{n_1} \in \pi_1(G)$ such that $M_{n_1} \equiv M_{n_0} \bmod \ell^{n_0}$ and $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_1} - \mathrm{Id}_{n_1}) = 1$) for the quantity $\sum_{n>n_1} \mu(E_{n,M_{n_1}})$. Indeed, $E_{n,M_{n_0}}$ is the disjoint union of $E_{n,M_{n_1}}$ by varying M_{n_1} in the finite set of lifts of M_{n_0} modulo ℓ^{n_1} when $n \geq n_1$.

We can write $M_{n_1} - \mathrm{Id}_{n_1} = \begin{pmatrix} \alpha_{n_1} - 1 & d\beta_{n_1} \\ \beta_{n_1} & \alpha_{n_1} - 1 \end{pmatrix}$ with $v_\ell(\beta_{n_1}) = b$. Let $n \geq n_1$ and consider $M_n \equiv M_{n_1} \bmod \ell^{n_1}$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$. By comparing the valuations of the elements we see that the second column must be $(k_n \bmod \ell^n)$ times the first for some suitable choice of k_n. Remark that knowing (α_n, β_n) is equivalent to knowing $(k_n \bmod \ell^{n-b}, \beta_n)$ and we must have $k_n^2 \equiv d \bmod \ell^{n-b}$.

We now investigate how to lift M_n to $M_{n+1} \in C(n+1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$. We choose arbitrarily a lift β_{n+1} of β_n and choose (if it exists) a lift k_{n+1} of k_n such that $k_{n+1}^2 \equiv d \bmod \ell^{n+1-b}$.

Set $m := n - b$ and $m_1 := n_1 - b$, which are positive by the choice of n_1. We apply Remark 38 to lift $k_{n_1} \bmod \ell^{m_1}$. With the notation of this remark, if $a_i \neq s_i$ holds for some i, then $\mu(E_{n,M_{n_1}}) = 0$ holds for all sufficiently large n and we conclude. Now we may suppose that $k_{n_1} \equiv \ell^\nu s \bmod \ell^{m_1}$.

We can lift β_{n_1} to β_{n+1} in ℓ^{n-n_1+1} possible ways while we can lift k_{n_1} in $(\ell-1)\ell^{\nu-1}$ ways such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ (in other words, the lift of k_{n_1} is suitable modulo ℓ^m but not modulo ℓ^{m+1}). We deduce that $\mu(E_{n,M_{n_1}})$ is a constant times ℓ^{-n} and we conclude. □

Lemma 40. *With the notation of* (3)*, the sum $\sum_{n\geq n_0} \mu(E_{n,\mathrm{Id}_{n_0}})$ is a rational number.*

Proof. Let $n \geq n_0$ and call c the number of elements in $G(n_0)$ whose first projection is Id_{n_0}. Consider the matrices $M_n \bmod \ell^n$ such that $M_n \equiv \mathrm{Id}_{n_0} \bmod \ell^{n_0}$. If $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$,

then there is a smallest integer $n' \leq n$ such that we have $M_n - \mathrm{Id}_n \equiv \begin{pmatrix} 0 & 0 \\ \beta_{n'} & 0 \end{pmatrix} \bmod \ell^{n'}$ for some $\beta_{n'} \neq 0$. For all M_n as such, the number of v_n such that $[\ell^{n-1}]v_n \notin \mathrm{Im}(M_n - \mathrm{Id}_n)$ and $(M_n, v_n) \in G(n)$ divided by the number of v_n such that $(M_n, v_n) \in G(n)$ does not depend on n and does not depend on M_n. Call it c'. The former property follows from Lemma 29, the latter then is because the vectors $v_{n'}$ such that $[\ell^{n'-1}]v_{n'} \in \mathrm{Im}(M_{n'} - \mathrm{Id}_{n'})$ are the preimage under the multiplication by $\ell^{n'-n_0}$ of the vectors $\begin{pmatrix} \ell x \\ y \end{pmatrix} \in (\mathbb{Z}/\ell^{n_0}\mathbb{Z})^2$ and $\pi_2(\pi_1^{-1}(M_{n'}))$ is the preimage under the multiplication by $\ell^{n'-n_0}$ of $\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$. The two above quantities only depend on M_n through n' and their ratio does not even depend on n'. We conclude that the ratio does not depend on M_n.

On the other hand, it is easy to see that (for the case $M_n = \mathrm{Id}_n$), the number of $v_n \in \pi_2(\pi_1^{-1}(\mathrm{Id}_n))$ such that $[\ell^{n-1}]v_n \notin \mathrm{Im}(\mathrm{Id}_n - \mathrm{Id}_n)$ divided by the number of $v_n \in \pi_2(\pi_1^{-1}(\mathrm{Id}_n))$ is a constant c_{Id} which doesn't depend on $n \geq n_0$.

Then it suffices to show that $\sum_{n \geq n_0} \mu(\widetilde{E}_{n,\mathrm{Id}_{n_0}})$ is a rational number, where $\mu(\widetilde{E}_{n,\mathrm{Id}_{n_0}})$ is the proportion of matrices in $\pi_1(G)(n+1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2, \mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) \leq 1, M_{n_0} \equiv \mathrm{Id}_{n_0} \bmod \ell^{n_0}$.

Define β_{n+1} as in the proof of Lemma 50 and set $b := v(\beta_{n+1})$. The number of matrices M_{n+1} as requested such that $M_n = \mathrm{Id}_n$ (which means $b = n$) is $\ell^2 - \ell$. Now we suppose that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and we count the matrices M_{n+1} such that $b = n_0 + h$ for $0 \leq h \leq n - n_0 - 1$.

Define $S(n)$ as the number of matrices $M_n \in \pi_1(G)(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $M_n \equiv \mathrm{Id}_{n_0} \bmod \ell^{n_0}$. The number of matrices $M_{n+1} \in \pi_1(G)(n+1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2, \mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $M_n \equiv \mathrm{Id}_{n_0} \bmod \ell^{n_0}$ is then equal to $S(n) \cdot \ell^2 - S(n+1)$.

Fix first $b < n - v$. If v is odd or $d\ell^{-v} \bmod \ell$ is not a square, then there are no matrices as requested. Else, we are in the case (3) of Lemma 50 (where $a = v/2 + n_0 + h$), so there are $2\ell^{v/2+n-n_0-h-1}(\ell - 1)$ matrices. Summing over all $b < n - v$ (which means $0 \leq h < n - v - n_0$) gives the quantity $S_3(n)$, where

$$S_3(n) \in \{0, 2\ell^{n+v/2-n_0}(1 - \ell^{-n+v+n_0})\}.$$

Now consider all $b \geq n - v$ (which means $n - v - n_0 \leq h < n - n_0$). The matrices that fall in case (1) of Lemma 50 are then $S_1(n) = \ell^v - 1$. The matrices that fall in case (2) of Lemma 50 are then

$$S_2(n) = \sum_{h=n-v-n_0}^{n-1-n_0} \sum_{a=\lceil (n+n_0+h)/2 \rceil}^{n-1} \ell^{2n-2-(a+n_0+h)}(\ell-1)^2 = \sum_{i=1}^{v} (\ell-1)\ell^{\lfloor 3i/2 \rfloor - 1} + 1 - \ell^v.$$

We deduce that $S(n)$ is either a rational number independent of n or it is of the form $q_1 + q_2\ell^n$ for some fixed rational numbers q_1 and q_2. We also observe that $\#\pi_1(G)(n) = q_3\ell^{2n}$ for some positive rational number q_3. We may then conclude because we obtain geometric series by summing over $n \geq n_0$ the quantity

$$\mu(E_{n,\mathrm{Id}_{n_0}}) = q_3^{-1}\ell^{-2n} \cdot (c'(S(n)\ell^2 - S(n+1)) + c_{\mathrm{Id}}(\ell^2 - \ell)).$$

□

7.3. **Normalizers of ramified Cartan subgroups (for $\ell = 2$).** Let $\pi_1(G)$ be a finite index subgroup in the normalizer of ramified Cartan subgroup C with $\ell = 2$. If the parameter d is even, we can mimic some arguments of Theorem 39.

Lemma 41. *Let $\pi_1(G)$ be a finite index subgroup in the normalizer of ramified Cartan subgroup C with $\ell = 2$. Then $\sum_{n \geq n_0} \mu(E_{n,\mathrm{Id}_{n_0}})$ is a rational number.*

Proof. Suppose first that d is even. We may reason as for Lemma 40, applying Lemma 52 in place of Lemma 50. Notice that the only quantity that changes is

$$S_3(n) = 2^{n-n_0+v/2+3} - 2^{3v/2+w} \qquad w \in \{3,4,5\}$$

because Case 3 of Lemma 50 is replaced by Cases 3.1,3.2, and 3.3. of Lemma 52 (and the last two cases may occur or not depending on d).

Now suppose that d is odd. Consider the matrices $M_n \bmod 2^n$ such that $M_n \equiv \mathrm{Id}_{n_0} \bmod 2^{n_0}$. The contribution to $\mu(E_{n,\mathrm{Id}_{n_0}})$ given by $M_n = \mathrm{Id}_n$ is $c_{\mathrm{Id}} \cdot 2/\#\pi_1(G)(n+1)$, where c_{Id} is the same constant as in the proof of Lemma 40 and $\#\pi_1(G)(n+1) = \#\pi_1(G)(n_0)2^{2n+2-2n_0}$. Now we may suppose that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$. By inspecting the four lifts of $\mathrm{Id}_{n'-1}$ modulo $2^{n'}$, there is a smallest integer $n' \leq n$ such that we have $M_{n'} - \mathrm{Id}_{n'} = \begin{pmatrix} 2^{n'-1} & 2^{n'-1}d \\ 2^{n'-1} & 2^{n'-1} \end{pmatrix}$.

Since the matrices $M_{n'} - \mathrm{Id}_{n'}$ are of the same form by varying n', as in Lemma 40 we conclude that the number of v_n such that $[2^{n-1}]v_n \notin \mathrm{Im}(M_n - \mathrm{Id}_n)$ and $(M_n, v_n) \in G(n)$ divided by the number of v_n such that $(M_n, v_n) \in G(n)$ is a constant c' independent of n and M_n. So it suffices to show that $\sum_{n \geq n_0} \mu(\widetilde{E}'_{n,\mathrm{Id}_{n_0}})$ is a rational number, where $\mu(\widetilde{E}'_{n,\mathrm{Id}_{n_0}})$ is the proportion of matrices in $\pi_1(G)(n+1)$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$, $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$, $M_{n_0} \equiv \mathrm{Id}_{n_0} \bmod 2^{n_0}$. The number of suitable matrices in $\pi_1(G)(n+1)$ is $4S(n) - S(n+1)$, where $S(n)$ is defined as in the proof of Lemma 40 (we partition the set of matrices according to the valuation $b := v_2(\beta_n)$).

We recall from the proof of Lemma 55 that the number of matrices M_n such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $v_2(\beta_n) = b$ is equal to 1 if $n - b = 1, 4$ if $n - b = 2$ and $d \equiv 1 \bmod 4$, and 2^{n-b+1} if $n - b \geq 3$ and $d \equiv 1 \bmod 8$. So we have, with a case distinction depending only on d and on whether $n - n_0$ is 0, 1, 2, or ≥ 3,

$$S(n) \in \{0, 1, 5, 5 + 2^{n+2}(2^{-n_0} - 2^{-n+2})\}.$$

We may conclude because for $n \geq n_0 + 3$ the number $S(n)$ is of the form $q_1 + q_2 \cdot 2^n$ where q_1, q_2 are rational numbers independent of n. □

The following remark is the analogue of Remark 38 for $\ell = 2$.

Remark 42. Suppose that $d = 2^{2\nu}d'$, where $d' \equiv 1 \bmod 8$ and $\nu \geq 0$ is an integer. Let d'_0 be one of the two 2-adic square roots of d'. For every $m \geq 3$, 1 admits four square roots modulo 2^m (namely, ± 1 and $\pm 1 + 2^{m-1}$ modulo 2^m) and only ± 1 can be lifted to square roots of 1 modulo 2^{m+1}.

If $\nu = 0$, the four square roots of d modulo 2^m are $\pm d'_0 \bmod 2^m$, $(d'_0 \bmod 2^m)(\pm 1 + 2^{m-1})$. Only the two first two can be lifted to square roots modulo 2^{m+1}. If $\nu \geq 1$ and $m - 2\nu \geq 2$, the square roots $\hat{d}$ of d modulo 2^m are of the form

$$\hat{d} = \pm 2^\nu d'_0 \left(1 + \varepsilon_{m-2\nu-1}2^{m-2\nu-1} + \sum_{i=m-2\nu}^{m-\nu-1} a_i 2^i\right) \bmod 2^m$$

where $\varepsilon_{m-2\nu-1} \in \{0,1\}$ and the coefficients $a_i \in \{0,1\}$ can be chosen arbitrarily. We deduce that $\hat{d}$ can be lifted to a square root modulo 2^{m+1} if and only if $\varepsilon_{m-2\nu-1} = 0$. Suppose that this last condition holds and that there is some minimal integer t with $m-2\nu \leq t \leq m-\nu-1$ such that $a_t = 1$. Then, all lifts of $\hat{d}$ modulo $2^{t+2\nu+1}$ are square roots of $d \bmod 2^{t+2\nu+1}$ while no lift of $\hat{d}$ modulo $2^{t+2\nu+2}$ is a square root of $d \bmod 2^{t+2\nu+2}$.

Lemma 43. *If d is even and and $M_{n_0} \neq \mathrm{Id}_{n_0}$, then $\sum_{n \geq n_0} \mu(E_{n,M_{n_0}})$ is a rational number.*

Proof. We can write

$$\mu(E_{n,M_{n_0}}) = c_{M_{n_0}} \frac{p(n)}{\#\pi_1(G)(n_0) \cdot 2^{2(n+1-n_0)}},$$

where $c_{M_{n_0}}$ is the constant of Definition 34 and $p(n)$ is the number of matrices $M_n \equiv M_{n_0} \bmod 2^{n_0}$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$.

Suppose first that $M_{n_0} \in C'(n_0)$ and that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$. Then we have $p(n) = 2^{n+1-n_0}$ because (see the proof of Lemma 54) for every $n_0 \leq n' \leq n$ two out of the four lifts of $M_{n'} - \mathrm{Id}_{n'}$ from modulo $2^{n'}$ to modulo $2^{n'+1}$ have $2\mathbb{Z}$-rank 1.

Now suppose that $M_{n_0} \in C(n_0)$ and write $M_{n_0} - \mathrm{Id}_{n_0} = \begin{pmatrix} \alpha_{n_0} - 1 & d\beta_{n_0} \\ \beta_{n_0} & \alpha_{n_0} - 1 \end{pmatrix}$. Set $b := v_2(\beta_{n_0}) < n_0$. We may restrict to consider $n > n_1$ and $\mu(E_{n,M_{n_1}})$, where $n_1 \geq n_0$ is such that $b < n_1 - 2\nu$ and $n_1 - 2\nu \geq 2$ and M_{n_1} varies in the finitely many lifts of M_{n_0}.

We write $M_{n_1} - \mathrm{Id}_{n_1} = \begin{pmatrix} \alpha_{n_1} - 1 & d\beta_{n_1} \\ \beta_{n_1} & \alpha_{n_1} - 1 \end{pmatrix}$ with $v_2(\beta_{n_1}) = b$. As in the proof of Theorem 39, knowing the coefficients (α_n, β_n) of M_n is equivalent to knowing $(k_n \bmod 2^{n-b}, \beta_n)$ where k_n is a square root of d modulo 2^{n-b}.

We may suppose that $d = 2^{2\nu} d'$ with $2 \nmid d'$. This is because, if $v_2(d)$ is odd or $d' \not\equiv 1 \bmod 8$, then d is not a square modulo 2^{n-b} if $n - b - 2\nu \geq 3$ and hence $\mu(E_{n,M_{n_1}}) = 0$ for every $n \geq b + 5 + 2\nu$.

We apply Remark 42 to lift $k_{n_1} \bmod 2^{n_1-b}$. With the notation of this remark, if $\varepsilon_{n_1-b-2\nu-1} = 1$ or $a_i = 1$ for some i, then $\mu(E_{n,M_{n_1}}) = 0$ holds for sufficiently large n and we conclude. Now we may suppose that $k_{n_1} = \pm 2^\nu d'_0 \bmod 2^{n_1-b}$.

We can lift β_{n_1} to β_{n+1} in 2^{n-n_1+1} possible ways. We can lift $(k_{n_1} \bmod 2^{n_1-b})$ modulo 2^{n+1-b} in $2^{\nu+1}$ ways: by Remark 42 we can write the lift as

$$\pm 2^\nu d'_0 \Big(1 + 2^{n-b-2\nu-1} + \sum_{i=n-b-2\nu}^{n-b-\nu} a_i 2^i\Big)$$

with arbitrary a_i's because the lift must be a square root of d modulo 2^{n-b} but not modulo 2^{n+1-b}. In this way, $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$. Making use of the constant $c_{M_{n_1}}$ from Definition 34, we deduce that $\mu(E_{n,M_{n_1}})$ is a constant times 2^{-n} and we conclude. □

Lemma 44. *If d is odd and $M_{n_0} \neq \mathrm{Id}_{n_0}$, then $\sum_{n \geq n_0} \mu(E_{n,M_{n_0}})$ is a rational number.*

Proof. Without loss of generality we may assume that $n_0 \geq 3$. By making use of the constant $c_{M_{n_0}}$ from Definition 34, it suffices to prove that the number of lifts M_{n+1} of M_{n_0} such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ is a constant or a constant times 2^n.

We first consider the case $M_{n_0} \in C(n_0)$. With our usual notation, we suppose that α_{n_0} is even and β_{n_0} is odd (the other case α_{n_0} odd and β_{n_0} even being analogous). We refer to the proof of Lemma 55. For $n \geq 3$, we can have $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ only if $d \equiv 1 \bmod 8$ (because $d \equiv k_n^2 \bmod 2^n$) so suppose that this is the case. Moreover, choosing a lift of M_n amounts to choosing a lift of β_n and, if it exists, a suitable lift of $k_n \bmod 2^{n-b}$. By Remark 42, $k_n \bmod 2^n$ cannot be lifted to a square root of d modulo 2^{n+1} if and only if $k_n \bmod 2^n = \pm d_0(1 + 2^{n-1}) \bmod 2^n$ and the sign is determined by k_{n_0} (this corresponds to $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$). We deduce that the number of suitable matrices is 2^{n+1-n_0}, namely the number of lifts of β_{n_0} modulo 2^{n+1}.

Now we consider the case $M_{n_0} \in C'(n_0)$ and we refer to the proof of Lemma 55.

If α_n is odd and β_n is even, these coefficients are parametrized by k_n (and for 2 out of the 4 lifts of k_n we preserve the property that the $2\mathbb{Z}$-rank is 1). We deduce that the number of suitable matrices M_{n+1} is 2^{n+1-n_0}.

If α_n is even and β_n is odd, $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if $\frac{4a'^2-1}{d} \equiv (1 + 2b')^2 \bmod 2^n$. This congruence holds modulo 2^{n+1} either for all lifts of a' and b' or for none of them. So there is at most one integer $n' \geq n_0$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_{n'} - \mathrm{Id}_{n'}) = 1$ and $\mathrm{rk}_{2\mathbb{Z}}(M_{n'+1} - \mathrm{Id}_{n'+1}) = 2$. For this integer n' we have $4^{n'+1-n_0}$ suitable matrices, while for $n \neq n_0$ and $n \neq n'$ there are no matrices. □

APPENDIX A. ON THE $\ell\mathbb{Z}$-RANK OF MATRICES IN $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$

Let n be a positive integer. We consider a 2×2 matrix $M_n \in \mathrm{Mat}(\mathbb{Z}/\ell^n\mathbb{Z})$ and its lifts $M_{n+1} \in \mathrm{Mat}(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$. The $\ell\mathbb{Z}$-rank of $(M_{n+1} - \mathrm{Id}_{n+1})$ is at least the one of $(M_n - \mathrm{Id}_n)$.

We consider Cartan subgroups. As the $\ell\mathbb{Z}$-rank is invariant under conjugation (see Remark 5), we may suppose that the Cartan groups have a specific form. In particular, the split Cartan group will be the group of invertible diagonal matrices. If S is a subset of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, then we write $S(n)$ for the image of S under reduction modulo ℓ^n.

Remark 45. We consider Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. We describe them as $C_{(c,d)}$ with two suitably chosen parameters $c, d \in \mathbb{Z}_\ell$, see [LP17, Propositions 10 and 11]. We have

$$C_{(c,d)} = \left\{ \begin{pmatrix} \alpha & d\beta \\ \beta & \alpha + c\beta \end{pmatrix} \mid \alpha, \beta \in \mathbb{Z}_\ell,\ v_\ell(\alpha(\alpha + c\beta) - d\beta^2) = 0 \right\}$$

and

$$C_{(c,d)}(n) = \left\{ \begin{pmatrix} \alpha_n & d\beta_n \\ \beta_n & \alpha_n + c\beta_n \end{pmatrix} \mid \alpha_n, \beta_n \in \mathbb{Z}/\ell^n\mathbb{Z},\ \alpha_n(\alpha_n + c\beta_n) - d\beta_n^2 \notin \ell\mathbb{Z}/\ell^n\mathbb{Z} \right\}.$$

For ℓ odd, we can take $c = 0$ and we have $\ell \mid d$ if and only if the Cartan group is ramified. If $\ell \nmid d$, then the Cartan subgroup is split if and only if d is a square in $\mathbb{Z}_\ell^\times$, otherwise it is nonsplit. For $\ell = 2$, we can take $c \in \{0, 1\}$. If $c = 0$ the Cartan group is ramified while if $c = 1$ the Cartan group is unramified (it is either split or nonsplit; in the former case we may take $d = 0$ and in the latter case we may take d odd). If C is a Cartan group, the normalizer N of C is the disjoint union of C and $C' := \begin{pmatrix} 1 & c \\ 0 & -1 \end{pmatrix} \cdot C$.

If C is split, it is isomorphic to

$$\left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \mid \alpha, \beta \in \mathbb{Z}_\ell^\times \right\}.$$

The normalizer of C is the disjoint union of C and $C' := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot C$.

Suppose that M_n and M_{n+1} are in GL_2 (respectively, a Cartan or the normalizer of a Cartan). If M_n is the identity, we define $L_{\mathrm{Id},1}$ (respectively, $L_{\mathrm{Id},2}$) as the number of lifts M_{n+1} such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$ (respectively, 2). We similarly define L_1 (respectively, L_2) for a matrix M_n that is not the identity.

Theorem 46. *Suppose that M_n and M_{n+1} are in GL_2 (respectively, an unramified Cartan or the normalizer of an unramified Cartan). The numbers $L_{\mathrm{Id},1}$, $L_{\mathrm{Id},2}$, L_1, L_2 do not depend on n and they are as follows:*

Ambient group	$L_{\mathrm{Id},1}$	$L_{\mathrm{Id},2}$	L_1	L_2
$\mathrm{GL}_2(\mathbb{Z}_\ell)$	$(\ell+1)^2(\ell-1)$	$\ell(\ell+1)(\ell-1)^2$	ℓ^3	$\ell^4 - \ell^3$
Split Cartan	$2(\ell-1)$	$(\ell-1)^2$	ℓ	$\ell^2 - \ell$
Nonsplit Cartan	0	$\ell^2 - 1$	ℓ	$\ell^2 - \ell$

Proof. The proof is based on the explicit computations for each case, which are collected in this section, and on the following observation: the total number T of lifts is

$$T = 1 + L_{\mathrm{Id},1} + L_{\mathrm{Id},2} \qquad \text{and} \qquad T = L_1 + L_2 \qquad \text{respectively}. \tag{5}$$

This number is ℓ^4 for GL_2, while for (the normalizer of) an unramified Cartan subgroup it is the cardinality of the tangent space from [LP17], namely $T = \ell^2$. □

We make use of the following general observation on the number of square roots:

Remark 47. Let ℓ be a prime, m a positive integer and d a non-zero square modulo ℓ^m. Setting $2\nu := v_\ell(d)$, we can write $d \equiv \ell^{2\nu} d' \bmod \ell^m$, where d' is a square modulo $\ell^{m-2\nu}$ not divisible by ℓ. If ℓ is odd, the number of square roots of d is $2\ell^\nu$. For $\ell = 2$, the number of square roots of d is as follows: 2^ν, if $m - 2\nu = 1$; $2^{\nu+1}$, if $m - 2\nu = 2$; $2^{\nu+2}$, otherwise. Indeed, let $\ell^\nu k$ be a square-root of d with $\ell \nmid k$. We have to determine $k \bmod \ell^{m-\nu}$ and the defining condition is $k^2 \equiv d' \bmod \ell^{m-2\nu}$. There are 2 square roots of $d' \bmod \ell^{m-2\nu}$ if ℓ is odd. If $\ell = 2$, the number of square roots is as follows: 1, if $m - 2\nu = 1$; 2, if $m - 2\nu = 2$; 4, otherwise. We conclude because we can lift these square roots in ℓ^ν ways to obtain k.

A.1. **Lifts in GL_2.** We first prove that $L_{\mathrm{Id},2} = \ell(\ell+1)(\ell-1)^2$. To have a lift M_{n+1} of the identity such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$, we can choose the first column of $M_{n+1} - \mathrm{Id}_{n+1}$ to be non-zero in $\ell^2 - 1$ ways, and then we can choose the second column in a way that is not a multiple of the first, namely in $\ell^2 - \ell$ ways. We notice that the value of $L_{\mathrm{Id},1}$ can be obtained by (5).

We prove that $L_1 = \ell^3$. Take $M_n = \begin{pmatrix} 1+\alpha_n & \beta_n \\ \gamma_n & 1+\delta_n \end{pmatrix}$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$. Assume, without loss of generality, that $\begin{pmatrix} \alpha_n \\ \gamma_n \end{pmatrix} = k_n \begin{pmatrix} \beta_n \\ \delta_n \end{pmatrix}$ and that $v_\ell(\beta_n) \leq v_\ell(\delta_n)$. Then we must have $v_\ell(\beta_n) < n$. Remark that k_n is uniquely determined modulo $\ell^{n-v_\ell(\beta_n)}$. We may arbitrarily lift α_n and β_n modulo ℓ^{n+1}, which determines k_{n+1} modulo $\ell^{n+1-v_\ell(\beta_n)}$. We conclude because we can also lift δ_n arbitrarily and then γ_{n+1} is determined. The value of L_2 can be obtained with (5).

A.2. **Lifts in (the normalizer of) a split Cartan.** We have $L_{\mathrm{Id},2} = (\ell-1)^2$ because choosing a lift $M_{n+1} \in C(n+1)$ above the identity such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ consists in choosing independently two non-zero numbers modulo ℓ. We now prove that $L_1 = \ell$. Let $M_n \in C(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$. Up to swapping the elements of the basis, we may assume that the first column of M_n is $\begin{pmatrix}1\\0\end{pmatrix}$. The lifts of $M_n - \mathrm{Id}_n$ are then of the form

$$\begin{pmatrix} a'\ell^n & 0 \\ 0 & b+b'\ell^n \end{pmatrix}$$

where $b \not\equiv 0 \mod \ell^n$ and a', b' are units. There is a linear combination of the columns where not both coefficients are divisible by ℓ if and only if $a'\ell^n = 0$, so the number of suitable lifts is ℓ. Finally, consider $M_n = \begin{pmatrix}0 & a\\ b & 0\end{pmatrix} \in C'(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$. A lift of $M_n - \mathrm{Id}_n$ is of the form $M_{n+1} - \mathrm{Id}_{n+1} = \begin{pmatrix} -1 & a+a'\ell^n \\ b+b'\ell^n & -1 \end{pmatrix}$. The condition for this lift to have $\ell\mathbb{Z}$-rank equal to 1 is that there exists some invertible k such that $\begin{pmatrix}-1\\ b+b'\ell^n\end{pmatrix} = k\begin{pmatrix}a+a'\ell^n\\ -1\end{pmatrix}$. So $a'\ell^n$ can be chosen anyway (ℓ possibilities). Then, k is determined by $-1 = k(a+a'\ell^n)$, which determines $b'\ell^n = -k$, so the number of lifts M_{n+1} with $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$ is ℓ.

A.3. **Lifts in (the normalizer of) a nonsplit Cartan, for ℓ odd.** Let ℓ be an odd prime, and $C = C_{(0,d)}$ be a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (then, d is not a square in $\mathbb{Z}_\ell^\times$).

We prove that $L_{\mathrm{Id},2} = \ell^2 - 1$, deducing from (5) that $L_{\mathrm{Id},1} = 0$. Consider the identity matrix modulo ℓ^n. Its ℓ^2 lifts modulo ℓ^{n+1} that are in $C(n+1)$ are matrices M_{n+1} such that

$$M_{n+1} - \mathrm{Id}_{n+1} = \begin{pmatrix} a'\ell^n & b'\ell^n d \\ b'\ell^n & a'\ell^n \end{pmatrix}$$

where a', b' are units. If $a'\ell^n = b'\ell^n = 0$, then $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 0$. We prove that for all the remaining lifts we have $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$. This is clear if precisely one between $a'\ell^n$ and $b'\ell^n$ is zero. Now suppose that $a'\ell^n$ and $b'\ell^n$ are both non-zero. If the $\ell\mathbb{Z}$-rank is less than 2, then there is some $k \in (\mathbb{Z}/\ell^{n+1}\mathbb{Z})^\times$ such that $\begin{pmatrix}a'\ell^n\\ b'\ell^n\end{pmatrix} = k\begin{pmatrix}b'\ell^n d\\ a'\ell^n\end{pmatrix}$ and we deduce that $k^2 d \equiv 1 \mod \ell$, contradicting that d is not a square modulo ℓ.

We now prove that $L_1 = \ell$, deducing from (5) that $L_2 = \ell(\ell-1)$.

Let $M_n \in C'(n)$ and write $M_n - \mathrm{Id}_n = \begin{pmatrix}\alpha_n - 1 & \beta_n d\\ -\beta_n & -\alpha_n - 1\end{pmatrix}$. Since ℓ is odd, $\alpha_n + 1$ or $\alpha_n - 1$ is invertible.

Suppose first that $\alpha_n + 1$ is invertible. Then we have $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if there is some $k_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ such that

$$\begin{aligned} \alpha_n - 1 &= k_n \beta_n d \\ -\beta_n &= -k_n(\alpha_n + 1). \end{aligned}$$

If such a k_n exists, then $k_n^2 = \frac{1}{d} \cdot \frac{\alpha_n - 1}{\alpha_n + 1}$ and $k_n^2 d - 1$ is invertible (as d is not a square modulo ℓ). We deduce that

$$(\alpha_n, \beta_n) = \left(\frac{-1 - k_n^2 d}{k_n^2 d - 1}, \frac{-2k_n}{k_n^2 d - 1}\right) \tag{6}$$

for some $k_n \in \mathbb{Z}/\ell^n\mathbb{Z}$. If (α_n, β_n) are as in (6), the corresponding matrix $\begin{pmatrix} \alpha_n & \beta_n d \\ -\beta_n & -\alpha_n \end{pmatrix}$ is an element of $C'(n)$ because its determinant is non-zero modulo ℓ. Hence, $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if (α_n, β_n) satisfy (6) for some $k_n \in \mathbb{Z}/\ell^n\mathbb{Z}$. Replacing in (6) k_n by a different value k'_n leads to a different pair (α_n, β_n). Indeed, if k_n and k'_n give the same α_n, we deduce that $k_n^2 \equiv k_n'^2 \bmod \ell^n$. Then, if they give the same β_n, we deduce that $k_n \equiv k'_n \bmod \ell^n$. This shows that lifting M_n to M_{n+1} such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$ consists in choosing a lift $k_{n+1} \in \mathbb{Z}/\ell^{n+1}\mathbb{Z}$ of k_n and, for different choices of k_{n+1}, the lifts of M_n are distinct.

We now assume that $\alpha_n - 1$ is invertible and reason as in the previous case. We have $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if there is some $k_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ such that

$$\begin{aligned} \beta_n d &= k_n(\alpha_n - 1) \\ -(\alpha_n + 1) &= -k_n\beta_n \,. \end{aligned}$$

Then we have $k_n^2 = d\frac{\alpha_n+1}{\alpha_n-1}$ and hence the pairs (α_n, β_n) whose corresponding matrix M_n is such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ are those of the form

$$(\alpha_n, \beta_n) = \left(\frac{d + k_n^2}{k_n^2 - d}, \frac{2k_n}{k_n^2 - d}\right) . \tag{7}$$

We may conclude as above because a different value for k_n leads to a different value for (α_n, β_n).

A.4. **Lifts in (the normalizer of) a nonsplit Cartan, for $\ell = 2$.** Let $C = C_{(c,d)}$ be a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$. Then $c = 1$ and d is odd according to [LP17, Proposition 11]. Consider a matrix $M_{n+1} \in C(n+1)$ such that $M_{n+1} \equiv \mathrm{Id}_n \bmod 2^n$ and such that $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$. The possibilities for $M_{n+1} - \mathrm{Id}_{n+1}$ are

$$\begin{pmatrix} 2^n & 0 \\ 0 & 2^n \end{pmatrix}, \begin{pmatrix} 0 & 2^n d \\ 2^n & 2^n \end{pmatrix}, \begin{pmatrix} 2^n & 2^n d \\ 2^n & 0 \end{pmatrix},$$

so $L_{\mathrm{Id},2} = 3$. We also deduce that a matrix $M_n \in N(n)$ such that $M_n \equiv \mathrm{Id}_1 \bmod 2$ is either the identity or it is such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 2$. Thus the elements $M_n \in N(n)$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ are in $C'(n)$ (because the elements M_1 of $N(1)$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 1$ are the elements of $C'(1)$). Choose

$$M_n = \begin{pmatrix} \alpha_n + \beta_n & (d+1)\beta_n + \alpha_n \\ -\beta_n & -\alpha_n - \beta_n \end{pmatrix} \in C'(n)$$

such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$.

Remark that we cannot have $v_2(\alpha_n) \geq 1$ and $v_2(\beta_n) \geq 1$. Indeed, we don't have a suitable relation between the columns of $M_n - \mathrm{Id}_n$ because

$$v_2(\alpha_n + \beta_n - 1) < v_2((d+1)\beta_n + \alpha_n) \quad \text{and} \quad v_2(-\beta_n) > v_2(-\alpha_n - \beta_n - 1)\,.$$

We prove that $L_1 = 2$.

The case $v_2(\alpha_n) = 0$. We have $v_2(\alpha_n + \beta_n - 1) \geq v_2((d+1)\beta_n + \alpha_n)$, so there is some $k_n \in \mathbb{Z}/2^n\mathbb{Z}$ such that

$$\begin{pmatrix} \alpha_n + \beta_n - 1 \\ -\beta_n \end{pmatrix} = k_n \begin{pmatrix} (d+1)\beta_n + \alpha_n \\ -(\alpha_n + \beta_n) - 1 \end{pmatrix}.$$

If $v_2(\beta_n) = 0$, k_n must be invertible, otherwise it must not be invertible. The second row gives $\alpha_n = \beta_n\left(\frac{1}{k_n} - 1\right) - 1$ and we deduce that

$$(\alpha_n, \beta_n) = \left(\frac{1 - 2k_n + k_n^2(d+1)}{1 - k_n - k_n^2 d}, \frac{2k_n - k_n^2}{1 - k_n - k_n^2 d}\right).$$

Similarly to the case ℓ odd, these pairs correspond to the matrices $M_n \in C'(n)$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and different values of k_n correspond to different pairs. Indeed, if

$$\frac{1 - 2k_n + k_n^2(d+1)}{1 - k_n - k_n^2 d} = \frac{1 - 2k'_n + {k'_n}^2(d+1)}{1 - k'_n - {k'_n}^2 d},$$

we deduce that $k_n = k'_n$ because we have

$$(k_n - k'_n)(-1 - k_n - k'_n - (3d+1)k_n k'_n) = 0$$

and the second factor has 2-adic valuation zero. We deduce that there are 2 lifts M_{n+1} of M_n such that $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$, corresponding to the two possible lifts of k_n.

The case $v_2(\alpha_n) \geq 1$ *and* $v_2(\beta_n) = 0$. Since $v_2(-\beta_n) < v_2(-\alpha_n - \beta_n - 1)$, so there is $k_n \in \mathbb{Z}/2^n\mathbb{Z}$ (not invertible) such that

$$k_n \begin{pmatrix} \alpha_n + \beta_n - 1 \\ -\beta_n \end{pmatrix} = \begin{pmatrix} (d+1)\beta_n + \alpha_n \\ -\alpha_n - \beta_n - 1 \end{pmatrix}.$$

We deduce that

$$(\alpha_n, \beta_n) = \left(\frac{k_n^2 - 2k_n + d + 1}{k_n^2 - k_n - d}, \frac{2k_n - 1}{k_n^2 - k_n - d}\right).$$

Different values of k_n correspond to different pairs: this is because, as above, if

$$\frac{2k_n - 1}{k_n^2 - k_n - d} = \frac{2k'_n - 1}{k'^2_n - k'_n - d},$$

then we have

$$(k'_n - k_n)(2k_n k'_n + 2d + 1 - k_n - k'_n) = 0.$$

Then, as in the previous case, there are 2 lifts M_{n+1} of M_n such that $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$.

A.5. **(Normalizer of) a ramified Cartan with parameters** $(0, d)$ **for** ℓ **odd.** Consider a ramified Cartan subgroup C with parameters $(0, d)$ such that $\ell \mid d$, see Remark 45. For every positive integer n, the group $C(n)$ consists of the matrices of the form

$$\begin{pmatrix} \alpha_n & d\beta_n \\ \beta_n & \alpha_n \end{pmatrix}$$

such that $v_\ell(\alpha_n) = 0$. We first look at elements of $C'(n)$.

Proposition 48. *Let M_n be an element of $C'(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$. The matrix M_n has precisely ℓ lifts $M_{n+1} \in C'(n+1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$.*

Proof. Write $M_n - \mathrm{Id}_n = \begin{pmatrix} \alpha_n - 1 & d\beta_n \\ -\beta_n & -\alpha_n - 1 \end{pmatrix}$. Since ℓ is odd, $\alpha_n + 1$ or $\alpha_n - 1$ is invertible. First assume that $\alpha_n + 1$ is invertible. Then, $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if there is some $k_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ such that

$$\left\{ \begin{array}{ll} \alpha_n - 1 & = k_n d\beta_n \\ -\beta_n & = -k_n(\alpha_n + 1). \end{array} \right. \tag{8}$$

Then we have $k_n^2 d = \frac{\alpha_n - 1}{\alpha_n + 1}$. We deduce that (α_n, β_n) are such that the corresponding matrix M_n is in C'_{ℓ^n} and $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if they are of the form

$$(\alpha_n, \beta_n) = \left(\frac{1 + k_n^2 d}{1 - k_n^2 d}, \frac{2k_n}{1 - k_n^2 d} \right)$$

for some $k_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ (notice that α_n is invertible). We notice that a different value k'_n leads to a different value for (α_n, β_n). Indeed, if k_n and k'_n give the same α_n we deduce that $dk_n^2 \equiv dk_n'^2 \bmod \ell^n$ hence if they also give the same β_n we must have $k_n = k'_n$. Therefore, choosing a lift M_{n+1} of M_n such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$ consists in choosing a lift $k_{n+1} \in \mathbb{Z}/\ell^{n+1}\mathbb{Z}$ of k_n, different choices of k_{n+1} giving different lifts of M_n.

Now assume that $\alpha_n - 1$ is invertible. Then, $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if there is some $k_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ such that

$$\begin{cases} k_n(\alpha_n - 1) & = d\beta_n \\ -k_n\beta_n & = -(\alpha_n + 1). \end{cases}$$

Since $k_n = \frac{\beta_n d}{\alpha_n - 1}$, this system amounts to the equation $\alpha_n^2 = 1 + d\beta_n^2$. Supposing that (α_n, β_n) satisfy this equation, lifting M_n to a matrix M_{n+1} whose parameters $(\alpha_{n+1}, \beta_{n+1})$ satisfy $\alpha_{n+1}^2 = 1 + d\beta_{n+1}^2$ amounts to lifting β_n freely, and then α_{n+1} is determined. Indeed, $1 + d\beta_{n+1}^2$ is a square in $\mathbb{Z}/\ell^{n+1}\mathbb{Z}$. By Hensel's lemma $c_{n+1} \in \mathbb{Z}/\ell^{n+1}\mathbb{Z}$ is a square in $\mathbb{Z}/\ell^{n+1}\mathbb{Z}$ if and only if $c_{n+1} \bmod \ell$ is a square in $\mathbb{Z}/\ell\mathbb{Z}$. Moreover, the sign choice for α_{n+1} is determined by α_n. □

Remark 49. As seen in the proof of Proposition 26 the number of matrices $M_1 \in C'(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 1$ is 2ℓ. Then from Proposition 48 we deduce that the number of matrices $M_n \in C'(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ is $2\ell^n$.

Now assume that $M_n = \begin{pmatrix} \alpha_n & d\beta_n \\ \beta_n & \alpha_n \end{pmatrix}$ is in $C(n)$. If $\alpha_n - 1$ is invertible we deduce that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 2$ because the determinant of $M_n - \mathrm{Id}_n$ is non-zero modulo ℓ. Now suppose that $\alpha_n - 1$ is not invertible. If $\alpha_n - 1 = 0$, then $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) \leq 1$ if and only if $d\beta_n = 0$. If $\alpha_n - 1 \neq 0$, then $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if there is some $k_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ such that

$$\begin{cases} \beta_n d & = k_n(\alpha_n - 1) \\ \alpha_n - 1 & = k_n\beta_n \,. \end{cases} \tag{9}$$

We may replace the first equation by $\beta_n d = k_n^2 \beta_n$, and notice that $k_n\beta_n \neq 0$. We must have $v_\ell(k_n) > 0$ because $\ell \mid d$.

Lemma 50. *Let $v := v_\ell(d) > 0$. Fixing $a := v_\ell(\alpha_n - 1)$ and $b := v_\ell(\beta_n)$, the number of matrices $M_n \in C(n)$, such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ is as follows:*

(1) $\ell^{n-b-1}(\ell - 1)$, for $a = n$ and $n - v \leq b < n$;
(2) $\ell^{2n-2-(a+b)}(\ell - 1)^2$, for $n - v \leq b < n$ and $(n + b)/2 \leq a < n$;
(3) $2\ell^{\frac{v}{2}+n-b-1}(\ell - 1)$, for $b < n - v$ and $a = v/2 + b$, v is even and $d\ell^{-v} \bmod \ell$ is a square;
(4) 0, otherwise.

Moreover, for $n \geq 2$ there are $\ell - 1$ matrices M_n such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $M_n \equiv \mathrm{Id}_{n-1} \bmod \ell^{n-1}$, so $R''_1(n) = \ell - 1$.

Proof. Notice that, if $a > 0$, the necessary condition $v_\ell(\alpha_n) = 0$ is satisfied.

Suppose first that $a = n$ (which implies $\beta_n \neq 0$ to avoid $M_n = \mathrm{Id}_n$). The requested condition then amounts to $d\beta_n = 0$ and we easily conclude. Remark that, for $n \geq 2$, $\ell - 1$ of these matrices are congruent to the identity modulo ℓ^{n-1}. Now suppose that $a < n$. To have suitable matrices, the system (9) must be solvable, and we have in particular $a = v_\ell(k_n) + b$ (as $\ell \mid k_n$, we deduce that $a > 0$). We cannot have $a = n - 1$ and $b \geq n - 1$ and hence the last assertion of the statement follows ($M_n \equiv \mathrm{Id}_{n-1} \bmod \ell^{n-1}$ means $a, b \geq n - 1$).

Now suppose that $a < n$ and $b \geq n - v$. The equation $k_n^2\beta_n = \beta_n d$ is equivalent to $v_\ell(k_n) \geq (n - b)/2$. We deduce that (9) is solvable if and only if $a \geq (n + b)/2$ (in particular we must have $b < n$) and we find the requested expression fixing a and b.

Finally suppose that $a < n$ and $b < n - v$. If $k_n^2\beta_n = \beta_n d$ is solvable, then $d \bmod \ell^{n-b}$ is a square (which means $d\ell^{-v} \bmod \ell$ is a square) and $k_n \bmod \ell^{n-b}$ can be any of its $2\ell^{v/2}$ square-roots (see Remark 47). These values, according to (9) and fixing β_n, lead to distinct values for α_n (and $a = v/2 + b$ follows from $a = v_\ell(k_n) + b$) and we conclude. □

Remark 51. Let X_i (for $i = 1, 2, 3$) be the number of matrices $M_n \in C(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ from case (i) of the previous lemma (the total number of matrices $M_n \in C(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ is then $X_1 + X_2 + X_3$). Call $m := \min(n, v)$.

We have $X_1 = \sum_{b=n-m}^{n-1} \ell^{n-b-1}(\ell-1) = \ell^m - 1$ and this quantity does not depend on n provided that $n \geq v$. The quantity X_2 also does not depend on n for $n \geq v$ because we have

$$\begin{aligned} X_2 &= \ell^{2n-2}(\ell-1)^2 \sum_{b=n-m}^{n-1} \Big(\sum_{a=\lceil (n+b)/2 \rceil}^{n-1} \ell^{-a-b} \Big) \\ &= \ell^{2n-1}(\ell-1) \sum_{b=n-m}^{n-1} \Big(-\ell^{-n-b} + \ell^{-\lceil (n+b)/2 \rceil - b} \Big) \\ &= 1 - \ell^m + (\ell-1)\ell^{-1} \sum_{i=1}^{m} \ell^{\lfloor 3i/2 \rfloor} . \end{aligned}$$

We have $X_3 = 0$ if v is not even or $d\ell^{-v} \bmod \ell$ is not a square or $n \leq v$. In the remaining case, we have

$$X_3 = 2\ell^{v/2+n-1}(\ell-1) \sum_{b=0}^{n-m-1} \ell^{-b} = 2\ell^{v/2}(\ell^n - \ell^m) .$$

We have $R_1'(n) = X_1 + X_2 + X_3 + 2\ell^n$.

A.6. **(Normalizer of) a ramified Cartan for $\ell = 2$.** Suppose that $\ell = 2$. Consider the normalizer $N = C \cup C'$ of a ramified Cartan subgroup C noticing that $C(1) = C'(1)$ if the parameter c is zero. The parameter d can be even or odd (which means that an integer representant for $(d \bmod 2^n)$ has this parity for all $n \geq 1$).

Lemma 52. *Assume that d is even, and call $v := v_2(d)$. The number of matrices $M_n \in C(n)$, fixing a and b, such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ is as follows:*

(1) 2^{n-b-1}*, for $a = n$ and $n - v \leq b < n$;*
(2) $2^{2n-2-(a+b)}$*, for $n - v \leq b < n$ and $(n + b)/2 \leq a < n$;*
(3.1) $2^{\frac{v}{2}+n-b-1}$*, for $b = n - v - 1$ and $a = v/2 + b$, v is even;*

(3.2) $2^{\frac{v}{2}+n-b}$*, for* $b = n-v-2$ *and* $a = v/2+b$*,* v *is even and* $2^{-v}d \bmod 4$ *is a square;*
(3.3) $2^{\frac{v}{2}+n-b+1}$*, for* $b \leq n-v-3$ *and* $a = v/2+b$*,* v *is even and* $2^{-v}d \bmod 8$ *is a square;*
(4) 0*, otherwise.*

Moreover, for $n \geq 2$ *there is only one matrix* M_n *such that* $rk_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ *and* $M_n \equiv \mathrm{Id}_n \bmod 2^{n-1}$*, so* $R_1''(n) = 1$.

Proof. We may proceed as in Lemma 50, applying Remark 47 while taking square roots. □

Remark 53. As in Remark 51, we can compute the quantities X_1, X_2, X_3, which are defined similarly. We have $X_1 = 2^m - 1$ and $X_2 = 1 - 2^m + \frac{1}{2}\sum_{i=1}^{m} 2^{\lfloor 3i/2 \rfloor}$. We have $X_{33} = 0$ if $n-b-3 < 0$ or if v is not even or $2^{-v}d \bmod 8$ is not a square, else $X_{33} = 2^{v/2+n+2}(1-2^{-(n-v-2)})$.

Lemma 54. *Assume that* d *is even and consider the matrices* $M_n \in C'(n)$ *such that* $rk_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$*. For* $n = 1$ *we have* $C'(n) = C(n)$ *and there is* 1 *matrix. For* $n = 2$*, there are* 8 *matrices if* $4 \mid d$ *and* 4 *matrices otherwise. For* $n \geq 3$ *the number of matrices is* $3 \cdot 2^n$ *if* $8 \mid d$ *and* 2^n *otherwise.*

Proof. The two cases $n = 1$ and $n = 2$ can be checked by hand, so suppose that $n \geq 3$.

Write $M_n = \begin{pmatrix} \alpha_n & d\beta_n \\ -\beta_n & -\alpha_n \end{pmatrix}$ and notice that α_n must be odd.

Suppose first that $v_2(\beta_n) \geq v_2(\alpha_n + 1)$. In that case, $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if there is some $k_n \in \mathbb{Z}/2^n\mathbb{Z}$ such that the system (8) holds, and we can write

$$(\alpha_n, \beta_n) = \left(\frac{1+k_n^2 d}{1-k_n^2 d}, \frac{2k_n}{1-k_n^2 d}\right).$$

Distinct values of (α_n, β_n) correspond to distinct values of $(k_n \bmod 2^{n-1})$, so we find 2^{n-1} matrices.

Now suppose that $v_2(\beta_n) < v_2(\alpha_n + 1)$. We have $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if there is $k_n \in \mathbb{Z}/2^n\mathbb{Z}$ such that $\begin{pmatrix} d\beta_n \\ \alpha_n + 1 \end{pmatrix} = k_n \begin{pmatrix} \alpha_n - 1 \\ \beta_n \end{pmatrix}$.

Assume that $v_2(\beta_n) = 0$. Since $k_n = \frac{\alpha_n+1}{\beta_n}$, the system is equivalent to $\alpha_n^2 = 1 + d\beta_n^2$. Since $1 + d\beta_n^2 \equiv 1 + d \bmod 8$, there are solutions only if $8 \mid d$. In this case one can choose β_n freely (2^{n-1} possibilities), and there are 4 possible values for α_n, giving 2^{n+1} matrices.

Assume that $v_2(\beta_n) > 0$ and set $\beta_n := 2b'$ and $\alpha_n + 1 := 2a'$. We have to count the solutions $(a', b') \bmod 2^{n-1}$ of the system

$$\begin{cases} db' &= k_n(a'-1) \\ a' &= k_n b'. \end{cases}$$

We have $n - 1 \geq v_2(a') > v_2(b')$. Since $k_n \equiv \frac{db'}{a'-1} \bmod 2^{n-1}$ this system is equivalent to $a'^2 - a' \equiv db'^2 \bmod 2^{n-1}$. We choose b' (2^{n-1} possibilities), which uniquely determines a' (because $a' \mapsto a'^2 - a'$ is a bijection on $2\mathbb{Z}/2^{n-1}\mathbb{Z}$ that preserves the valuation) so we find 2^{n-1} matrices. □

The formulas of Lemmas 52 and 54 allow us to compute $R_1'(n)$ when d is even. We now take d odd.

Lemma 55. *Assume that d is odd, and consider the matrices $M_n \in N(n)$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) \leq 1$. For $n = 1$ there are 2 matrices. For $n = 2$, there are 8 matrices. For $n \geq 3$, the number of matrices is*

- $9 \cdot 2^{n-1} - 10$, *if* $d \equiv 1 \bmod 8$,
- $2^{n-1} + 6$, *if* $d \equiv 5 \bmod 8$,
- $3 \cdot 2^{n-1} + 2$ *otherwise*.

Moreover, for $n \geq 3$, $R_1''(n) = 1$ and for $n = 2$ we have $R_1''(2) = 3$.

Proof. For $n \leq 2$, one may compute the number of matrices by hand, so now suppose that $n \geq 3$. Consider first $M_n \in C(n)$ and write $M_n - \mathrm{Id}_n = \begin{pmatrix} \alpha_n - 1 & d\beta_n \\ \beta_n & \alpha_n - 1 \end{pmatrix}$. Suppose first that α_n is even (hence β_n is odd) and write

$$M_n - \mathrm{Id}_n = \begin{pmatrix} -1 + 2a' & d(1 + 2b') \\ 1 + 2b' & -1 + 2a' \end{pmatrix} \neq 0\,.$$

The requested condition means that there is k (invertible) such that

$$k \begin{pmatrix} -1 + 2a' \\ 1 + 2b' \end{pmatrix} = \begin{pmatrix} d(1 + 2b') \\ -1 + 2a' \end{pmatrix},$$

so k must satisfy $k^2 \equiv d \bmod 2^n$. There are no solutions if $d \not\equiv 1 \bmod 8$. If $d \equiv 1 \bmod 8$, then there are 4 square roots of d modulo 2^n. We choose such a square root and $2b'$ ($4 \cdot 2^{n-1}$ possibilities) and the value of $2a'$ is determined, giving 2^{n+1} matrices.

Now suppose that α_n is odd (hence β_n is even) and write $M_n - \mathrm{Id}_n = \begin{pmatrix} 2a' & 2db' \\ 2b' & 2a' \end{pmatrix}$.

There is precisely one matrix $M_n \equiv \mathrm{Id}_{n-1} \bmod 2^{n-1}$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$, namely $M_n - \mathrm{Id}_n = \begin{pmatrix} 2^{n-1} & 2^{n-1}d \\ 2^{n-1} & 2^{n-1} \end{pmatrix}$. Furthermore, $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) \leq 1$ if and only if there is k (invertible) such that $k2a' = 2db'$ and $k^2 2b' = d2b'$. If $M_n \neq \mathrm{Id}_n$, we may choose β_n of a given 2-adic valuation $1 \leq b < n$ (2^{n-b-1} possibilities). Then we consider $k \bmod 2^{n-b}$ such that $k^2 \equiv d \bmod 2^{n-b}$, the number of possibilities being as follows: 1, if $n - b = 1$; 2 (respectively, 0), if $n - b = 2$ and $d \equiv 1 \bmod 4$ (respectively, $d \not\equiv 1 \bmod 4$); 4 (respectively, 0) if $n - b \geq 3$ and $d \equiv 1 \bmod 8$ (respectively, $d \not\equiv 1 \bmod 8$). The total number of matrices as requested is then as follows: 2, if $d \not\equiv 1 \bmod 4$; 6, if $d \equiv 5 \bmod 8$; $6 + 16(2^{n-3} - 1)$, if $d \equiv 1 \bmod 8$.

Now consider $M_n \in C'(n)$ and write $M_n = \begin{pmatrix} \alpha_n & d\beta_n \\ -\beta_n & -\alpha_n \end{pmatrix}$.

Suppose first that α_n is odd (hence β_n is even) and write $M_n - \mathrm{Id}_n = \begin{pmatrix} 2a' & 2db' \\ -2b' & -2 - 2a' \end{pmatrix}$.

The requested condition means that there exists k such that

$$k \begin{pmatrix} 2a' \\ -2b' \end{pmatrix} = \begin{pmatrix} 2db' \\ -2 - 2a' \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} 2a' \\ -2b' \end{pmatrix} = k \begin{pmatrix} 2db' \\ -2 - 2a' \end{pmatrix}.$$

Suppose first that $v_2(a') = 0$. We are in the former case and we remark that $k \bmod 2^{n-1}$ must be even. The system is then equivalent to $a' \equiv \frac{1}{\frac{k^2}{d} - 1} \bmod 2^{n-1}$ and $b' = \frac{k}{d} a'$, with $k \bmod 2^{n-1}$ even. There are 2^{n-2} possible choices for $k \bmod 2^{n-1}$ and such choices lead to

distinct values for (a', b') because $v_2(a') = 0$. Thus, there are 2^{n-2} matrices M_n such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $v_2(a') = 0$.

Now suppose that $v_2(a') \geq 1$. We are in the latter case and again $k \bmod 2^{n-1}$ must be even. The system is then equivalent to $a' \equiv \frac{dk^2}{1-dk^2} \bmod 2^{n-1}$ and $b' = k(1 + a')$, with $k \bmod 2^{n-1}$ even. Different choices of $k \bmod 2^{n-1}$ lead to distinct values for (a', b') because $v_2(1 + a') = 0$. Thus, there are 2^{n-2} matrices M_n such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $v_2(a') \geq 1$.

Finally suppose that α_n is even (hence β_n is odd). We write $M_n - \mathrm{Id}_n = \begin{pmatrix} -1 + 2a' & d(1 + 2b') \\ -1 - 2b' & -1 - 2a' \end{pmatrix}$. We have $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if there is some invertible $k \in \mathbb{Z}/2^n\mathbb{Z}$ such that $\begin{pmatrix} -1 + 2a' \\ -1 - 2b' \end{pmatrix} = k \begin{pmatrix} d(1 + 2b') \\ -1 - 2a' \end{pmatrix}$. Since $k = \frac{1+2b'}{1+2a'}$, the system is equivalent to the equation $\frac{4a'^2-1}{d} = (1 + 2b')^2$.

By Hensel's lemma (and studying this equation modulo 8) this equation is solvable modulo 2^n if and only if either $d \equiv 3 \bmod 8$ and $2 \nmid a'$ or $d \equiv 7 \bmod 8$ and $2 \mid a'$.

In both cases, the number of choices for $(2a' \bmod 2^n)$ is 2^{n-2} and there are 4 choices for the square-root of $(\frac{4a'^2-1}{d} \bmod 2^n)$. So in both cases we find 2^n (respectively, 0) matrices whose $2\mathbb{Z}$-rank is 1 if $d \equiv 3 \bmod 4$ (respectively, $d \equiv 1 \bmod 4$). □

APPENDIX B. EXAMPLES

B.1. **Example concerning the Exponential LT condition.** We write dens_ℓ for the density of primes $\mathfrak{p}$ of K that satisfy Condition 2 for the prime ℓ. Considering Table 46 and Theorem 37, we can evaluate dens_ℓ in some cases:

Example 56. If the image of the ℓ-adic torsion-Kummer representation is $\mathrm{GL}_2(\mathbb{Z}_\ell) \ltimes (\mathbb{Z}_\ell)^2$, we have

$$\begin{aligned}\mathrm{dens}_\ell &= 1 - \frac{\ell^2 - 2}{(\ell-1)^2(\ell+1)} + \frac{\ell^2 - 1}{\ell^2(\ell^4 - 1)} + \frac{(\ell^3 - 2\ell - 1)}{\ell^2(\ell-1)(\ell+1)} + \frac{\ell + 1}{\ell^2(\ell^3 - 1)} - \frac{\ell}{(\ell^3 - 1)(\ell^2 + 1)} \\ &= 1 - \frac{\ell^5 - \ell^3 - \ell^2 - 1}{\ell^7 - \ell^6 - \ell^3 + \ell^2}.\end{aligned}$$

Example 57. If the image of the ℓ-adic torsion-Kummer representation is $N \ltimes (\mathbb{Z}_\ell)^2$, where N is the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we have

$$\begin{aligned}\mathrm{dens}_\ell &= 1 - \frac{3\ell - 4}{2(\ell-1)^2} + \frac{1}{2\ell^2} + \frac{3\ell - 5}{2\ell(\ell-1)} + \frac{1}{\ell(\ell-1)} - \frac{1}{\ell^2 - 1} \\ &= 1 - \frac{3\ell^3 - 2\ell^2 - 2\ell - 1}{2\ell^5 - 2\ell^4 - 2\ell^3 + 2\ell^2}.\end{aligned}$$

Example 58. If the image of the ℓ-adic torsion-Kummer representation is $N \ltimes (\mathbb{Z}_\ell)^2$, where N is the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we have

$$\mathrm{dens}_\ell = 1 - \frac{\ell + 2}{2(\ell^2 - 1)} + \frac{1}{2\ell^2} + \frac{1}{2\ell} = 1 - \frac{\ell^2 + \ell + 1}{2\ell^4 - 2\ell^2}.$$

Consider an elliptic curve E over a number field $\mathbb{Q}$ and a point $P \in E(\mathbb{Q})$ of infinite order. We compute in some examples the density dens_ℓ of primes p such that $\mathrm{ord}_\ell(P \bmod p) = \exp_\ell(E(\mathbb{F}_p))$. The rational densities (computed exactly) have been tested with SageMath by computing the proportion of the suitable primes up to 10^5.

Example 59. Let E be defined by $y^2 = x^3 - x^2 - 6x$ (LMFDB label 480.b3) and let $P = (-1, 2)$. For primes $\ell \neq 2$, the ℓ-adic torsion-Kummer representation is surjective. We have

ℓ	dens_ℓ rounded
3	0.857
5	0.952
7	0.978
11	0.991

Example 60. Let E be defined by $y^2 = x^3 - 2x$ (LMFDB label 256.b1) and let $P = (2, 2)$. The CM field is $\mathbb{Q}(i)$. The image of the ℓ-adic representation is the normalizer of a split (respectively, nonsplit) Cartan if $\ell \equiv 1 \bmod 4$ (respectively, $\ell \equiv 3 \bmod 4$). The ℓ-adic Kummer map is surjective. We have

ℓ	dens_ℓ rounded
5	0.935
13	0.991
17	0.995

ℓ	dens_ℓ rounded
3	0.910
7	0.988
11	0.995

Example 61. Let E be defined by $y^2+y = x^3-34$ (LMFDB label 225.c1) and let $P = (6, 13)$. The image of the 2-adic representation is the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ and the 2-adic Kummer map is surjective. We have $\mathrm{dens}_2 = 17/24 \approx 0.708$.

Example 62. Let E be defined by $y^2 = x^3 - 735x - 7546$ (LMFDB label 1764.e2) and let $P = (-17, 6)$. The image of the 3-adic representation is the normalizer of the ramified Cartan subgroup with parameters $(c, d) = (0, -3)$ (see [GJLRY24, Table 4]) and the 3-adic Kummer map is surjective. According to Proposition 26, Lemma 50 and Remark 51, we have $R_1(n) = 12{\cdot}9^{n-1}$, $R_1'(n) = 2{+}2{\cdot}3^n$ for $n \geq 1$ and $R_1''(n) = 2$ for $n \geq 2$. We have $\mu(E_0) = \frac{1}{4}$ and for $n > 0$ we have $\mu(E_n) = \frac{((2+2\cdot3^n)\cdot9)-(2+2\cdot3^{n+1}))\frac{2}{3}+(9-3)\frac{8}{9}}{12\cdot9^n}$. Then $\sum_{n\geq0}\mu(E_n) = \frac{3}{4}$.

B.2. **Example concerning the Indivisibility LT condition.** Let E be an elliptic curve over a number field K, and let $P \in E(K)$ be a point of infinite order. If ℓ is a prime number, we denote by $\mathrm{dens}(\ell)$ the density of the primes $\mathfrak{p}$ of K of good reduction for E, not over ℓ, and such that we have $\ell \nmid \#E(K)$ or the point $(P \bmod \mathfrak{p})$ is an ℓ-multiple in $E(k_\mathfrak{p})$. Similarly, if L is a non-empty set of primes, we denote by $\mathrm{dens}(L)$ the analogue density, requiring that the above condition holds for all primes in L. We write $\mathcal{P}$ for the set of all primes.

Example 63. Let E be the elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation $y^2 = x^3 - x^2 - 6x$ (LMFDB label 480.b3). Its point $P = (-1, 2)$ has infinite order. The adelic torsion representation of E has index 48, and the loss of surjectivity is only due to the 2-adic torsion representation (if m and m' are coprime square-free integers, the m-adic and the m'-adic torsion representations are independent, and the former is surjective if m is odd). By Theorem 5.2 of [JR10], the $\mathrm{mod}\ell$ torsion-Kummer representation has maximal image for every $\ell \neq 2$. If ℓ_1 and ℓ_2 are odd primes, then $\mathbb{Q}(\frac{1}{\ell_1}P)$ and $\mathbb{Q}(E[\ell_2])$ are linearly disjoint (see [BP25]). Since $\mathbb{Q}(E[2]) = \mathbb{Q}$, the mod2 representation has trivial image. With SageMath we found that $P = [2](-3 - 3i, 9 - 3i)$ hence $\mathbb{Q}(\frac{1}{2}P) = \mathbb{Q}(i)$. The non-trivial element of

$\mathrm{Gal}(\mathbb{Q}(\frac{1}{2}P)/\mathbb{Q})$, with the notation of the torsion-Kummer representation $\mathrm{mod}2$, is a matrix $M' \neq \mathrm{Id}$ whose torsion minor M is the identity and hence $\mathrm{rk}(M' - \mathrm{Id}) > \mathrm{rk}(M - \mathrm{Id})$. We deduce that $\mathrm{dens}(2) = \frac{1}{2}$. Now let m be an odd prime. The quotients of order 2 of $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ factor through $\mathrm{GL}_2(m)/\mathrm{SL}_2(m)$ (see [BP25]) hence they correspond to some subextensions of $\mathbb{Q}(\zeta_m)$. Since $\mathbb{Q}(i) \not\subseteq \mathbb{Q}(\zeta_m)$ we deduce that $\mathbb{Q}(\frac{1}{2}P)$ is independent from any torsion field. Hence, for any finite set L of primes, we have

$$\mathrm{dens}(L) = \prod_{\ell \in L} \mathrm{dens}(\ell)\,.$$

Thus the Indivisible LT conjecture predicts that, calling $\mathcal{P}$ the set of all primes, we have

$$\mathrm{dens}(\mathcal{P}) = \frac{1}{2} \cdot \prod_{\substack{\ell \text{ prime} \\ \ell > 2}} \left(1 - \frac{\ell^4 - 2\ell^2 - \ell + 1}{\ell^3(\ell-1)(\ell^2-1)}\right) \approx 0.387\,.$$

For the 200 first primes of good reduction, the experimental density computed with SageMath is equal to 0.410, and by removing the first 20 primes of good reduction we obtain 0.394.

Now we consider Condition 1 for all $\ell \neq 2$. The analogue of the Indivisible LT conjecture would predict the density (approximated by restricting to $\ell < 10^5$)

$$\prod_{\substack{\ell \text{ prime} \\ \ell \neq 2}} \left(1 - \frac{\ell^4 - 2\ell^2 - \ell + 1}{\ell^3(\ell-1)(\ell^2-1)}\right) \approx 0.773\,.$$

The experimental density (testing the reductions modulo p for p up to 10^4) is 0.777.

Example 64. Let E be the elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation $y^2 = x^3 - 1196x + 15920$ (LMFDB label 448.d1) and consider the point $P = (29, 75)$. The adelic torsion representation has index 48 and the loss of surjectivity is only due to the 2-adic torsion representation. We have $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{14})$ and $\mathbb{Q}(\frac{1}{2}P) = \mathbb{Q}(\sqrt{2}, \sqrt{7})$ and

$$\mathrm{Gal}(\mathbb{Q}(2^{-1}P)/\mathbb{Q}) \cong \left\{ \mathrm{Id}_3, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

So $\mathrm{dens}(2) = \frac{1}{4}$. For any odd m, since $\sqrt{2}, \sqrt{7}, \sqrt{14}$ are not contained in $\mathbb{Q}(\zeta_m)$, the 2-division field is linearly disjoint from $\mathbb{Q}(E[m])/\mathbb{Q}$. Hence, the conjectural density is

$$\prod_{\ell \text{ prime}} \mathrm{dens}(\ell) = \frac{1}{4} \cdot \prod_{\substack{\ell \text{ prime} \\ \ell > 2}} \left(1 - \frac{\ell^4 - 2\ell^2 - \ell + 1}{\ell^3(\ell-1)(\ell^2-1)}\right) \approx 0.19$$

The experimental density obtained considering the first 200 primes of good reduction is 0.19.

Now consider the point $P' = 3P$. We have $\mathbb{Q}(\frac{1}{3}P') = \mathbb{Q}(E[3])$. We compute $\mathrm{dens}(3) = \frac{27}{48}$, so the conjectural density for P' is

$$\frac{1}{4} \cdot \frac{27}{48} \cdot \prod_{\substack{\ell \text{ prime} \\ \ell > 3}} \left(1 - \frac{\ell^4 - 2\ell^2 - \ell + 1}{\ell^3(\ell-1)(\ell^2-1)}\right) \approx 0.125\,.$$

The experimental density obtained considering the first 200 primes of good reduction is 0.14.

Example 65. Let E be given by the Weierstrass equation $y^2 = x^3 - 2x$ and defined over its CM field $\mathbb{Q}(i)$. The only prime of bad reduction is $(1 + i)$. Considering that the curve can

also be defined over $\mathbb{Q}$, the image of the $\mathrm{mod}\ell$ torsion representation is a split (respectively, nonsplit) Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for $\ell \equiv 1 \bmod 4$ (respectively, $\ell \equiv 3 \bmod 4$).

Consider the point $P = (2, 2)$. By [JR10, Theorem 5.8], we have $[\mathbb{Q}(\frac{1}{\ell}P) : \mathbb{Q}(E[\ell]] = \ell^2$ for every $\ell \neq 2$. We impose Condition 1 for all $\ell \neq 2$: according to [CP22a, Theorem 1.1], the conjectural density (with a minor adaptation of the Exponential LT conjecture) is then

$$\prod_{\substack{\ell \text{ prime} \\ \ell \neq 2}} \mathrm{dens}(\ell) = \prod_{\substack{\ell \text{ prime} \\ \ell \equiv 1 \bmod 4}} \frac{\ell^4 - 2\ell^3 - \ell^2 + 4\ell - 1}{\ell^2(\ell^2 - 1)} \cdot \prod_{\substack{\ell \text{ prime} \\ \ell \equiv 3 \bmod 4}} \frac{\ell^4 - \ell^2 - 1}{\ell^4 - \ell^2} \approx 0.884\,.$$

Taking into account that rational primes congruent to 1 (respectively, 3) modulo 4 have two (respectively 1) prime above in $\mathbb{Q}(i)$, we compute that the approximated density, by considering the primes in $\mathbb{Q}(i)$ above the first 60 odd rational primes is 0.910.

Example 66. Let E be the Serre curve over $\mathbb{Q}$ given by the Weierstrass equation $y^2 + y = x^3 + x^2$ (LMFDB label 344.a1) and consider the point $P = (0, 0)$, which has infinite order. By [BP21, Example 7.2] the degree of $\mathbb{Q}(\frac{1}{\ell^n}P)/\mathbb{Q}(E[\ell^n])$ equals ℓ^{2n} for every prime ℓ. The minimal discriminant of E is $\Delta = -43$. We make use of the notation from [BP21]. Let $d_\pm(\ell, 0)$ be the number of matrices $M_1 \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1) = 2$ and, if $\ell = 43$, $\varepsilon_{-43}(M_1) = \pm 1$ and, if $\ell = 2$, $\psi(M_1) = \pm 1$. By [BP21, Lemmas 25 and 26] we have

$$d_+(2, 0) = 2; \quad d_-(2, 0) = 0; \quad d_+(43, 0) = 1629055; \quad d_-(43, 0) = 129591321552\,.$$

For $n \geq 1$ and $\ell = 2$, let $d_\pm(\ell, n)$ be the weighted number of matrices $M_{n+1} \in \mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ and $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) \leq 1$ and $\psi(M_{n+1}) = \pm 1$. The weight for a matrix M_{n+1} is $\frac{3}{4}$ if $M_n = \mathrm{Id}_n$ and $\frac{1}{2}$ otherwise. For $\ell = 43$, we analogously define $d_\pm(\ell, n)$ by replacing the condition on ψ with $\varepsilon_{-43}(M_{n+1}) = \pm 1$, and where the weight for a matrix M_{n+1} is $1 - \frac{1}{43^2}$ if $M_n = \mathrm{Id}_n$ and $1 - \frac{1}{43}$ otherwise.

We define $R'_{1,\pm}(1)$ as the number of matrices $M_1 \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 1$ and, if $\ell = 43$, $\varepsilon_{-43}(M_1) = \pm 1$ and, if $\ell = 2$, $\psi(M_1) = \pm 1$. For $n \geq 1$, we have

$$d_+(\ell, n) = L_{\mathrm{Id},2} \cdot \frac{\ell^2 - 1}{\ell^2} + R'_{1,+}(1) L_1^{n-1} L_2 \cdot \frac{\ell - 1}{\ell} + L_{\mathrm{Id},1} L_2 \frac{L_1^{n-1} - 1}{L_1 - 1} \cdot \frac{\ell - 1}{\ell}$$

and

$$d_-(\ell, n) = R'_{1,-}(1) L_1^{n-1} L_2 \cdot \frac{\ell - 1}{\ell}.$$

By [BP21, Lemmas 25 and 26], we get $R'_{1,+}(1) = 0$ and $R'_{1,-}(1) = 3$ for $\ell = 2$, while for $\ell = 43$, we have $R'_{1,+}(1) = 39688$ and $R'_{1,-}(1) = 39732$. Given integers $n_2, n_{43} \geq 0$, we define

$$S_{n_2,n_{43}} = \{p \in S \mid \exp_\ell(E(\mathbb{F}_p)) = \mathrm{ord}_\ell(P \bmod p) = n_\ell \text{ for } \ell = 2, 43\}.$$

We then obtain

$$\mathrm{dens}(S_{n_2,n_{43}}) = \frac{d_+(2, n_2) \cdot d_+(43, n_{43}) + d_-(2, n_2) \cdot d_-(43, n_{43})}{\frac{1}{2} \cdot \#\mathrm{GL}_2(\mathbb{Z}/2^{n_2+1}\mathbb{Z}) \cdot \#\mathrm{GL}_2(\mathbb{Z}/43^{n_{43}+1}\mathbb{Z})}$$

and hence

$$\sum_{n_2,n_{43} \geq 0} \mathrm{dens}(S_{n_2,n_{43}}) \cdot \prod_{\ell \neq 2,43} \mathrm{dens}(\ell) = \frac{1359920108791}{1991228778000} \cdot \prod_{\ell \neq 2,43} \left(1 - \frac{\ell^5 - \ell^3 - \ell^2 - 1}{\ell^7 - \ell^6 - \ell^3 + \ell^2}\right).$$

This number is approximately 0.527, and the density obtained by restricting to the primes $p < 10^5$ (and $p \neq 43$) is 0.530.

REFERENCES

[Ber88] Daniel Bertrand. Galois representations and transcendental numbers. pages 37–55, 1988. in: A. Baker (Ed.), New Advances in Transcendence Theory (Durham 1986).

[BP21] P. Bruin and A. Perucca. Reductions of points on algebraic groups, II. *Glasg. Math. J.*, 63(2):484–502, 2021.

[BP25] A. Benoist and A. Perucca. Entanglement for torsion-Kummer extensions of elliptic curves. In preparation, 2025.

[Bro93] William C. Brown. *Matrices over commutative rings*, volume 169 of *Pure and Applied Mathematics*. New York, Marcel Dekker, 1993.

[CP22a] F. Campagna and R. Pengo. Entanglement in the family of division fields of elliptic curves with complex multiplication. *Pacific J. Math.*, 317(1):21–66, 2022.

[CP22b] F. Campagna and R. Pengo. How big is the image of the Galois representations attached to CM elliptic curves? *Proceedings of the 18th Conference on Arithmetic, Geometry, Cryptography, and Coding Theory, AMS Contemporary Mathematics*, 2022.

[GJLRY24] E. González-Jiménez, Á Lozano-Robledo, and B. York. Models of CM elliptic curves with a prescribed ℓ-adic Galois image. `https://arxiv.org/abs/2408.04159`, 2024.

[HS00] M. Hindry and J. H. Silverman. *Diophantine geometry: an introduction*. Springer-Verlag, 2000.

[JR10] R. Jones and J. Rouse. Galois theory of iterated endomorphisms. *Proc. Lond. Math. Soc.*, 100(3):763–794, 2010.

[LP17] D. Lombardo and A. Perucca. The 1-eigenspace for matrices in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. *New York J. Math.*, 23:897–925, 2017.

[LP21] D. Lombardo and A. Perucca. Reductions of points on algebraic groups. *J. Inst. Math. Jussieu*, 20(5):1637–1669, 2021.

[LT77] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Amer. Math. Soc.*, 83(2):289–292, 1977.

[PP18] R. K. Pandey and A. Parashar. On certain sums with quadratic expressions involving the Legendre symbol. *J. Integer Seq.*, 21, article 18.4.7, 2018.

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

[Won00] Siman Wong. Power residues on Abelian varieties. *Manuscripta Math.*, 102:129–137, 2000.