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. For one of them, we require that the group $E(\mathbb{F}_p)$ and its subgroup $\langle (P \bmod p) \rangle$ have the same exponent, namely the cyclic subgroup is as large as possible. We conjecture that the set of primes p such that this condition holds admits a natural density, whose value is a rational multiple of the product over all primes ℓ of the natural densities (which we prove to exist and be rational) of those p such that the exponents of $E(\mathbb{F}_p)$ and $\langle (P \bmod p) \rangle$ have the same ℓ-adic valuation. Numerical examples support the validity of our conjectures.

1. INTRODUCTION

1.1. The Lang-Trotter conjecture.

Let S be a set of primes, and call $\mathcal{P}$ the set of all primes. The natural density of S is defined, provided that the limit exists, as

$$\mathrm{dens}(S) := \lim_{x\to\infty} \frac{\#\{p \le x : p \in S\}}{\#\{p \le x : p \in \mathcal{P}\}}\,.$$

Artin's conjecture on primitive roots predicts the natural density of the set of primes p for which a given integer a is a primitive root (which means that $(a \bmod p)$ generates $\mathbb{F}_p^\times$). It has been proven by Hooley in 1967 under the Generalized Riemann Hypothesis (GRH). In 1976, Lang and Trotter [LT77] formulated an elliptic-curve analogue of Artin's conjecture. Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})$ be a point of infinite order. The Lang-Trotter conjecture on primitive points predicts the natural density of the set of primes p (of good reduction for E) such that P is *primitive* modulo p: this condition means that $(P \bmod p)$ generates the group $E(\mathbb{F}_p)$ and in particular it requires $E(\mathbb{F}_p)$ to be cyclic.

Let $m > 1$ be a square-free integer. We define $\mathrm{dens}_{\mathrm{index}}(m)$ as the natural density of the set of primes p of good reduction for E such that, for all primes $\ell \mid m$, the following holds:

(1) the index of the subgroup $\langle (P \bmod p) \rangle$ in $E(\mathbb{F}_p)$ is not divisible by ℓ.

We observe that this natural density exists by the Chebotarev density theorem because we may study the condition via the $\bmod m$ torsion-Kummer representation for $E/\mathbb{Q}$ and P.

Conjecture (Lang-Trotter)**.** The set of primes p of good reduction for E such that $(P \bmod p)$ generates $E(\mathbb{F}_p)$ admits a natural density. Moreover, there exists a square-free integer $m > 1$

2020 *Mathematics Subject Classification.* 11G05,11R45.

Key words and phrases. Elliptic curves, primitive points, Lang-Trotter conjecture, matrix groups.

such that this natural density is the convergent product

$$\mathrm{dens}_{\mathrm{index}}(m) \cdot \prod_{\ell \nmid m} \mathrm{dens}_{\mathrm{index}}(\ell).$$

Contrarily to Artin's conjecture, the Lang-Trotter conjecture is not proven conditionally under GRH. However, for example, adapting the method by Hooley for Artin's conjecture, Gupta and Murty proved in [GRM86] that if $E/\mathbb{Q}$ has CM by the ring of integers of an imaginary quadratic field K, then under GRH the natural density in question exists, and it is positive if 2 and 3 are inert in K, or $K = \mathbb{Q}(\sqrt{-11})$. Moreover, there are unconditional results if the point P is replaced by a subgroup of $E(\mathbb{Q})$ of sufficiently large rank, see for example [Mel15] (also for elliptic curves without CM). For one point P, the natural density is positive only if there is a positive natural density of primes p such that the group $E(\mathbb{F}_p)$ is cyclic. The related problem of cyclicity was studied by several authors: Serre [Ser78] showed under GRH that the natural density of *cyclic reductions* (namely, of those p such that $E(\mathbb{F}_p)$ is cyclic) exists, and it is positive if and only if not all 2-torsion points are defined over $\mathbb{Q}$ (and Murty in [Mur83] proved the result unconditionally for curves with CM). We remark that Meleleo in [Mel15] also considers the alternative condition that the quotient of $E(\mathbb{F}_p)$ by $\langle (P \bmod p) \rangle$ is cyclic. Moreover, Jones, Pappalardi and Stevenhagen [JPS23] recently proved that there are elliptic curves $E/\mathbb{Q}$ and points $P \in E(\mathbb{Q})$ of infinite order such that for every prime p of good reduction the point $(P \bmod p)$ doesn't generate $E(\mathbb{F}_p)$ (beyond the trivial examples where e.g. $E(\mathbb{Q})$ contains a point of order 2 and a point whose double is P). Given the oncoming book about Artin's conjecture and the Lang-Trotter conjecture [MPe27] we have opted for not presenting a complete historical account on them.

1.2. **The Exponent LT conjecture and the Indivisibility LT conjecture.** We formulate and 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, which means that the order of $(P \bmod p)$ equals the exponent of $E(\mathbb{F}_p)$. This is equivalent to requiring for all primes ℓ, denoting by ord_ℓ (respectively, $\exp_\ell$) the ℓ-adic valuation of the order (respectively, exponent), that we have

$$\mathrm{ord}_\ell\big(P \bmod p\big) = \exp_\ell(E(\mathbb{F}_p))\,. \tag{2}$$

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 $\#E(\mathbb{F}_p)$:

$$\ell \mid \#E(\mathbb{F}_p) \quad \Rightarrow \quad (P \bmod p) \notin [\ell]E(\mathbb{F}_p)\,. \tag{3}$$

Our two conditions are equivalent to Condition (1) if $E(\mathbb{F}_p)$ is cyclic.

Call S_E the set of primes of good reduction for E. For any finite non-empty set L of prime numbers, the set of primes $p \in S_E$ such that Condition (2) (respectively, (3)) holds for every $\ell \in L$ admits a natural density (see Theorems 3 and 1 respectively), that we call $\mathrm{dens}_{\mathrm{exp}}(L)$ (respectively, $\mathrm{dens}_{\mathrm{indiv}}(L)$). For a square-free integer, we define

$$\mathrm{dens}_{\mathrm{exp}}(m) := \mathrm{dens}_{\mathrm{exp}}(\{\ell : \ell \mid m\})$$

(respectively, $\mathrm{dens}_{\mathrm{indiv}}(m) := \mathrm{dens}_{\mathrm{indiv}}(\{\ell : \ell \mid m\})$). If S is a (not necessarily finite) non-empty set of prime numbers, we similarly define the natural density $\mathrm{dens}_{\mathrm{exp}}(S)$ (respectively, $\mathrm{dens}_{\mathrm{indiv}}(S)$) — provided that this natural density exists. In the spirit of the Lang-Trotter conjecture, we state:

Conjecture (Exponent LT conjecture)**.** Let S be a non-empty set of prime numbers. The natural density $\mathrm{dens}_{\mathrm{exp}}(S)$ exists and it is the infimum, by varying L over the finite non-empty subsets of S, of $\mathrm{dens}_{\mathrm{exp}}(L)$.

Conjecture (Indivisibility LT conjecture)**.** Let S be a non-empty set of prime numbers. The natural density $\mathrm{dens}_{\mathrm{indiv}}(S)$ exists and it is the infimum, by varying L over the finite non-empty subsets of S, of $\mathrm{dens}_{\mathrm{indiv}}(L)$.

We point out that the existence of the natural density is part of the conjectures, as it is not clear why the given set of primes should admit a density in case S is not finite: we would expect the argument to involve deep results from analytic number theory.

We may take in particular $S = \mathcal{P}$ in the above conjectures. Notice that the upper natural density (with the limit superior in place of the limit) is clearly bounded from above by the given infimum. As Conditions (1), (2), and (3) go from strongest to weakest, we have

$$\mathrm{dens}_{\mathrm{index}}(L) \leq \mathrm{dens}_{\mathrm{exp}}(L) \leq \mathrm{dens}_{\mathrm{indiv}}(L)$$

for every finite non-empty set L of primes (and, provided that the densities exist, the same holds for an infinite set of primes).

Our results are based on an investigation of the *ℓ-adic* (respectively, *adelic*) torsion-Kummer representation of E, considering the Galois action on the division points over P.

For the Indivisibility LT conjecture we prove the following:

Theorem 1. *For any finite non-empty set L of primes, the natural density* $\mathrm{dens}_{\mathrm{indiv}}(L)$ *exists and it is a rational number. If ℓ is a sufficiently large prime, then the following holds: if E is without complex multiplication,*

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

while if E has CM by an order contained in the imaginary quadratic field of discriminant $-D$, then for ℓ big enough we have

$$\mathrm{dens}_{\mathrm{indiv}}(\ell) = \begin{cases} 1 - \dfrac{3\ell^2 - 5\ell + 1}{2\ell^2(\ell-1)^2} & \textit{if } \left(\frac{-D}{\ell}\right) = 1 \\ 1 - \dfrac{\ell^2 + \ell + 1}{2\ell^2(\ell-1)(\ell+1)} & \textit{if } \left(\frac{-D}{\ell}\right) = -1. \end{cases}$$

If m is a positive integer, we denote by $\frac{1}{m}P$ the set of preimages of P in $E(\bar{\mathbb{Q}})$ under the multiplication by m. Relying on the open image theorem for the adelic torsion-Kummer representation (see Proposition 7), we have:

Theorem 2. *Let E be without complex multiplication and let B be a positive integer such that for every prime $\ell \nmid B$ the following holds: the extension $\mathbb{Q}(\frac{1}{\ell}P)$ is linearly disjoint from $\mathbb{Q}(\frac{1}{m}P)$ for all positive square-free integers m coprime to ℓ. Then, assuming the Indivisibility LT conjecture, we can write*

$$\mathrm{dens}_{\mathrm{indiv}}(\mathcal{P}) = \mathrm{dens}_{\mathrm{indiv}}(\{\ell : \ell \mid B\}) \cdot \prod_{\ell \nmid B} \mathrm{dens}_{\mathrm{indiv}}(\ell)\,.$$

Moreover, there exists a rational number Q such that

$$\mathrm{dens}_{\mathrm{indiv}}(\mathcal{P}) = Q \cdot \prod_{\ell \in \mathcal{P}} \Big(1 - \frac{\ell^4 - 2\ell^2 - \ell + 1}{\ell^3(\ell-1)^2(\ell+1)}\Big)\,.$$

We also have a similar result if E has CM after extending the base field, see Theorems 22 and 24.

Our main result on the Exponent LT conjecture (which builds on the results in Section 5 and on Proposition 28 by Hörmann and Lombardo) is the following:

Theorem 3. *For any finite non-empty set L of primes, $\mathrm{dens}_{\exp}(L)$ exists and it is a rational number.*

The proof of this result stems from explicit matrix counts in the image of the modulo ℓ^n torsion-Kummer representation of $E/\mathbb{Q}$ and P by varying $n \geq 1$. The intuition that certain quantities stabilize or have a regular growth in n for $n \gg 0$ is correct, and indeed we prove rationality by showing that the natural density is a finite sum of rational terms and geometric series with rational ratios. The matrix counts are of independent interest and, in particular, they can be useful to understand the minimal denominator of the natural density (leading to a positive lower bound for a non-zero natural density, and to the possibility of identifying the natural density with great certainty by numerical experiments). Notice that it may be difficult to tell whether a natural density is rational or not: for example, the generic natural density in Artin's conjecture is the Artin constant $\prod_{\ell\in\mathcal{P}}(1-\frac{1}{\ell^2-\ell})$ and it is not known whether this is rational.

The natural density $\mathrm{dens}_{\exp}(\ell)$ for a prime ℓ is computed explicitly for certain images of the ℓ-adic torsion-Kummer representation of $E/\mathbb{Q}$ and P, see Appendix B.1. If m is a positive integer, we denote by $\mathbb{Q}(\frac{1}{m^\infty}P)$ the union of all fields $\mathbb{Q}(\frac{1}{m^n}P)$ for $n \geq 1$. We then have the analogue of Theorem 2:

Theorem 4. *Let E be without complex multiplication and let B be a positive integer such that for every prime $\ell \nmid B$ the following holds: the extension $\mathbb{Q}(\frac{1}{\ell^\infty}P)$ is linearly disjoint from $\mathbb{Q}(\frac{1}{m^\infty}P)$ for all positive square-free integers m coprime to ℓ. Then, assuming the Exponent LT conjecture, we can write*

$$\mathrm{dens}_{\exp}(\mathcal{P}) = \mathrm{dens}_{\exp}(\{\ell : \ell \mid B\}) \cdot \prod_{\ell \nmid B} \mathrm{dens}_{\exp}(\ell)\,.$$

Moreover, there exists a rational number Q such that

$$\mathrm{dens}_{\exp}(\mathcal{P}) = Q \cdot \prod_{\ell\in\mathcal{P}} \Big(1 - \frac{\ell^5-\ell^3-\ell^2-1}{\ell^7-\ell^6-\ell^3+\ell^2}\Big)\,.$$

We also have a similar result if E has CM after extending the base field, see Theorems 50 and 52.

Similarly to the original Lang-Trotter conjecture, our two conjectures have been stated over $\mathbb{Q}$ for concreteness, but they are meant for any number field. Moreover, they can also be considered for abelian varieties. In any case, we prove our results more generally for any number field in place of $\mathbb{Q}$.

The above conjectures and results also have an analogue if P is replaced by a subgroup Γ of $E(\mathbb{Q})$. Indeed, Condition (2) can be generalized by considering $\exp_\ell(\Gamma \bmod p)$, while Condition (3) can be generalized as follows: a point in $(\Gamma \bmod p)$ is an ℓ-multiple in $E(\mathbb{F}_p)$ only if it is an ℓ-multiple in $(\Gamma \bmod p)$.

Moreover, as observed by Baril Boudreau, many of the arguments work equally well for global function fields and similar conclusions are expected to hold (given an analogue of [Ber88, Theorem 1]).

The overview of the paper is as follows: In Section 2, we give the necessary background on torsion-Kummer representations. Of independent interest is our investigation in Section 2.6 of the notion of *$\ell\mathbb{Z}$-rank* for a matrix with entries modulo ℓ^n (for which we only accept linear combinations of the columns with coefficients not all divisible by ℓ). We then provide some counts of matrices with a given $\ell\mathbb{Z}$-rank, considering the possible generic images of the torsion representation modulo ℓ^n. In Section 3, we investigate Condition (3) and prove Theorems 1 and 2. Theorems 3 and 4 are proven in Sections 4 and 5. More precisely, in Section 4 we prove the existence of $\mathrm{dens}_{\mathrm{exp}}(L)$ while in Section 5 we show that this is rational, relying on results from the first appendix. In Appendix A we count lifts from modulo ℓ^n to modulo ℓ^{n+1} of matrices in GL_2, Cartan groups and their normalizers, according to their $\ell\mathbb{Z}$-rank. In Appendix B we compute $\mathrm{dens}_{\mathrm{exp}}(\ell)$ for some possible images of the ℓ-adic torsion-Kummer representation and we give numerical examples supporting the validity of our conjectures. Finally, in Appendix C (building on Lemmas 82 and 83 by Hörmann) we prove two results on the torsion-Kummer extensions of elliptic curves, which are of independent interest and that we have applied to investigate our examples.

Acknowledgements. We thank Félix Baril Boudreau, Fritz Hörmann, Davide Lombardo and Pieter Moree for helpful discussions and especially for Proposition 28 and Lemmas 82 and 83. This research was funded 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, the author has applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

Data availability statement and Declarations. The source code used for the numerical experiments is available as a supplementary file to the paper at `https://alexandrebenoist.github.io`. The authors declare no competing interests.

2. Preliminaries (torsion and Kummer representations)

In this section we introduce the general notation of the paper and then describe the theoretical framework of the torsion-Kummer representations. We have opted to focus on elliptic curves for concreteness: the definitions and results which do not rely on the explicit description of the image (up to a finite index) of the torsion representation also hold for abelian varieties, straight-forwardly generalized and with the same proof.

2.1. Notation.

The general notation that we make use of is collected here — grouping related notions — for the convenience of the reader.

- We let K be a number field, and we fix an algebraic closure $\bar{K}$. We denote by $\mathfrak{p}$ a prime of K, and we write $k_{\mathfrak{p}}$ for the residue field at $\mathfrak{p}$ (fixing an algebraic closure $\bar{k}_{\mathfrak{p}}$). All densities of primes of K mentioned in this paper are natural densities. For a set S of primes of K, the natural density of S is defined, provided that the limit exists, as
$$\mathrm{dens}(S) := \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in S : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}},$$
where $N_{K/\mathbb{Q}}$ is the norm from K to $\mathbb{Q}$. If L/K is a finite Galois extension of K and $\mathfrak{p}$ does not ramify in L, then we write $\mathrm{Frob}_{\mathfrak{p}}$ for the conjugacy class of the Frobenius elements at $\mathfrak{p}$.

- We let ℓ be a prime number. We write $\mathbb{Z}_\ell$ for the ring of ℓ-adic integers and $\mathbb{Z}/\ell^n\mathbb{Z}$ for the ring of the integers modulo ℓ^n (for some positive integer n). We denote by v_ℓ the ℓ-adic valuation defined for non-zero elements of $\mathbb{Z}_\ell$ or $\mathbb{Z}/\ell^n\mathbb{Z}$. If G is a group we let $\exp_\ell(G)$ (respectively, $\mathrm{ord}_\ell(G)$) be the ℓ-adic valuation of the exponent (respectively, the order) of G. We do not distinguish between the order of an element and the order of the cyclic subgroup that it generates.
- We let E/K be an elliptic curve defined over K and we denote by S_E the set of primes of K that are of good reduction for E. We let $P \in E(K)$ be a point of infinite order. Then, if L is a non-empty set of prime numbers, we write $\mathrm{dens}_{\mathrm{index}}(L)$ (respectively, $\mathrm{dens}_{\mathrm{exp}}(L)$ and $\mathrm{dens}_{\mathrm{indiv}}(L)$) to mean the natural density – provided it exists – of the subset of S_E consisting of the primes $\mathfrak{p}$ of K which, for every $\ell \in L$, satisfy Condition (1) (respectively, (2) and (3)), expressed similarly in the setting of prime ideals. Moreover, if ℓ is fixed, we write $S_{\exp}$ for the subset of S_E consisting of the primes $\mathfrak{p}$ for which $\exp_\ell(E(k_\mathfrak{p})) = \mathrm{ord}_\ell(P \bmod \mathfrak{p})$ and also define its subset $S_{\exp,n}$ with the condition $\exp_\ell(E(k_\mathfrak{p})) = \mathrm{ord}_\ell(P \bmod \mathfrak{p}) = n$.
- We denote the semi-direct product of groups with the symbol $\ltimes$. We denote by π_1 the projection onto the former group and π_2 the projection onto the latter group.
- We denote by μ the normalized Haar measure.
- If R is a ring, we denote by $\mathrm{GL}_2(R)$ the group of 2×2 invertible matrices with coefficients in R (and we similarly define $\mathrm{GL}_3(R)$). If M is a matrix with entries in $\mathbb{Z}/\ell^n\mathbb{Z}$, we denote by $\mathrm{rk}_{\ell\mathbb{Z}}(M)$ the $\ell\mathbb{Z}$-rank of the matrix M (see Definition 13). If ℓ is fixed, the identity matrix of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is denoted by Id_n.
- We usually denote by G a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell) \ltimes \mathbb{Z}_\ell^2$ (for example, the image of the ℓ-adic torsion-Kummer representation attached to E and P). We then write $G(n)$ for the reduction of G modulo ℓ^n.

2.2. **Torsion-Kummer representations of elliptic curves.** We fix a number field K and an elliptic curve E/K. We suppose that the Mordell-Weil group $E(K)$ contains a point P of infinite order, as this is necessary to formulate the Lang-Trotter conjecture and to consider similar problems.

Fix some prime number ℓ. For every $n \geq 1$ we choose an ordered basis for $E[\ell^n]$ such that if $N > n$ then the basis of $E[\ell^n]$ is the image of the basis of $E[\ell^N]$ under multiplication by ℓ^{N-n}. By taking the projective limit of these bases, we get an ordered $\mathbb{Z}_\ell$-basis of the Tate module $T_\ell(E)$. After having chosen an ordered basis for $E[\ell^n]$ we can identify this group with $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. Then we can identify the group of automorphisms of $E[\ell^n]$ with $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Similarly, we can identify the group of $\mathbb{Z}_\ell$-module automorphisms of $T_\ell(E)$ with $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

Definition 5 (torsion representations)**.** For every $\sigma \in \mathrm{Gal}(\bar{K}/K)$ the restriction of σ to $E[\ell^n]$ is, with the above identifications, a matrix $M_n \in \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. The group homomorphism $\sigma \mapsto M_n$ is the *torsion representation modulo* ℓ^n. Similarly, by considering the Galois action on $T_\ell(E)$, we obtain the *ℓ-adic torsion representation.*

For every positive integer n we denote by $\frac{1}{\ell^n}P$ the set of points $P' \in E(\bar{K})$ such that$[\ell^n]P' = P$ and by $K(\frac{1}{\ell^n}P)$ the field obtained by adding the coordinates of the points of $\frac{1}{\ell^n}P$ to K. For every positive integer n we fix a point $Q_n \in \frac{1}{\ell^n}P$ such that $[\ell^{N-n}]Q_N = Q_n$ holds for all $N > n$.

We now describe the *torsion-Kummer representations* (also called *arboreal representations*), referring to [JR10] and [LP21] for a more detailed introduction to these representations.

Definition 6 (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 $\mathrm{GL}_3(\mathbb{Z}/\ell^n\mathbb{Z})$ which is

$$M_n' := \begin{pmatrix} M_n & \vec{v_n} \\ 0 & 1 \end{pmatrix}$$

where $M_n \in \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is the image of σ under the $\mathrm{mod}\ \ell^n$ torsion representation, 0 is the zero row vector with two entries and $\vec{v_n}$ is the column vector with two entries whose coordinates are the coordinates of the torsion point $\sigma(Q_n) - Q_n$ in the chosen ordered basis of $E[\ell^n]$.

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

$$\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \ltimes (\mathbb{Z}/\ell^n\mathbb{Z})^2 .$$

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

$$\mathrm{GL}_2(\mathbb{Z}_\ell) \ltimes (\mathbb{Z}_\ell)^2 .$$

2.3. **On the image of the torsion representation.** We first consider the possible images of the ℓ-adic torsion representation for a prime number ℓ. We say that E/K doesn't have complex multiplication (abbreviated CM) if the endomorphism ring $\mathrm{End}_{\bar{K}}(E)$ is isomorphic to $\mathbb{Z}$. Before considering the CM case, we recall some facts on the Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. They are groups $C_{(c,d)}$ described by two suitably chosen parameters $c, d \in \mathbb{Z}_\ell$, see [LP17, Propositions 10 and 11]. We have

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

and

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

For ℓ odd, we can take $c = 0$ and the Cartan group is said to be ramified if $\ell \mid d$ (and unramified otherwise). If $\ell \nmid d$, then the Cartan subgroup is said to be split if d is a square in $\mathbb{Z}_\ell^\times$, otherwise it is said to be 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 $d \neq 0$, we call $v := v_\ell(d)$.

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, we will use the diagonal model: it is isomorphic to

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

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

If E has CM by an order contained in the imaginary quadratic field of discriminant $-D$, then for every $\ell \gg 0$ the image of the ℓ-adic torsion representation is isomorphic to a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ if the CM field of E is defined over K and to the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ if the CM field is not defined over K. The underlying Cartan subgroup is split if $\left(\frac{-D}{\ell}\right) = 1$ and nonsplit if $\left(\frac{-D}{\ell}\right) = -1$, see [Ser78, Section 4.5] and the proof of [Zyw15, Lemma 7.3].

2.4. On the image of the torsion-Kummer representation.

Call ρ_n (respectively, ρ'_n) the torsion (respectively, the torsion-Kummer) representation modulo n.

Proposition 7. *There exists a positive integer N such that for every $n \geq 1$ we have*

$$[W_n \ltimes (\mathbb{Z}/n\mathbb{Z})^2 : \mathrm{Im}(\rho'_n)] = [W_{\gcd(n,N)} \ltimes (\mathbb{Z}/\gcd(n,N)\mathbb{Z})^2 : \mathrm{Im}(\rho'_{\gcd(n,N)})]$$

where the group W_n is as follows:

- *if E is without CM, $W_n = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$;*
- *if E has CM defined over K, then $W_n = C(\mathbb{Z}/n\mathbb{Z})$ for some Cartan subgroup scheme C of GL_2 defined over $\mathbb{Z}$ and independent of n;*
- *if E has CM not defined over K, we may take*
$$W_n = \langle C(\mathbb{Z}/n\mathbb{Z}), (M \bmod n)\rangle$$
where $(M \bmod n)$ is the reduction modulo n of a specific matrix $M \in \mathrm{GL}_2(\mathbb{Z})$ such that M^2 is the identity, and C is as above.

Thus $\mathrm{Im}(\rho'_n)$ is the preimage in $W_n \ltimes (\mathbb{Z}/n\mathbb{Z})^2$ of $\mathrm{Im}(\rho'_{\gcd(n,N)})$ under the reduction modulo $\gcd(n,N)$.

Proof. The result can be obtained by combining a result by Ribet [Rib79] (see [Ber88, Theorem 1]) with an appropriate open image theorem on the adelic torsion representation, as explained in [PP24]. If E is without CM, we rely on Serre's open image theorem [Ser72, Théorème 3]. If E has CM defined over K, the open image theorem is a Corollary in [Ser72, Section 4.5]. If E has CM not defined over K, references for the open image theorem are [CP22b, Lemma 2.2] and [LR22, Theorem 1.1]. □

Corollary 8. *With the notation of Proposition 7, for all positive integers n coprime to N (in particular, for all primes $n \gg 0$) we have*

$$[K(E[n]) : K] = \#W_n \qquad \text{and} \qquad \left[K\left(\frac{1}{n}P\right) : K(E[n])\right] = n^2 .$$

Moreover, for every $n \geq 1$, the positive integer

$$f(n) := \frac{n^2}{\left[K\left(\frac{1}{n}P\right) : K(E[n])\right]}$$

divides $f(N)$.

Proof. If $\gcd(n,N) = 1$, by the above theorem $\mathrm{Im}(\rho'_n)$ is the preimage of $\mathrm{Im}(\rho'_1)$ hence

$$\mathrm{Im}(\rho'_n) = W_n \ltimes (\mathbb{Z}/n\mathbb{Z})^2 .$$

The image of the torsion representation is then W_n and hence $[K(E[n]) : K] = \#W_n$. Moreover, the degree of $K\left(\frac{1}{n}P\right)/K(E[n])$ equals n^2 because it is the size of the intersection of $\mathrm{Im}(\rho'_n)$ with the subgroup of $W_n \ltimes (\mathbb{Z}/n\mathbb{Z})^2$ consisting of the elements whose first component is the identity.

For the last assertion, we may suppose without loss of generality that n is a multiple of N (because $f(m)$ divides $f(n)$ if m divides n), and we apply the above theorem to conclude. □

2.5. **Reduction maps.** We keep the notation from Section 2.2. Let L/K be an extension of number fields. If $\mathfrak{p} \in S_E$ and $\mathfrak{q}$ is a prime of L lying over $\mathfrak{p}$, then $\mathfrak{q}$ is a prime of good reduction for the elliptic curve $E \otimes_K L$, and (choosing $k_\mathfrak{q} \subseteq \bar{k}_\mathfrak{p}$) we identify $E(k_\mathfrak{p})$ with the subgroup of $E(k_\mathfrak{q})$ consisting of the points that are defined over k_p. If $\mathfrak{p}$ does not ramify in L, $E(k_\mathfrak{p})$ is the subgroup consisting of the elements that are fixed by the Frobenius element of $\mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p})$.

Remark 9. Consider some prime $\mathfrak{p} \in S_E$ 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 $K(\frac{1}{\ell^n}P)/K$ by [HS00, Proposition C.1.5]. Let σ be in the conjugacy class $\mathrm{Frob}_\mathfrak{p}$ 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 $\bmod \ell^n$ torsion representation. Then with the reduction map modulo $\mathfrak{p}$ we can identify $E[\ell^n](k_\mathfrak{p})$ with $\ker(M_n - \mathrm{Id}_n)$ (which is the subgroup of $E[\ell^n](\bar{K})$ consisting of the points fixed by σ). In particular, the group structure of $\ker(M_n - \mathrm{Id}_n)$ does not depend on the choice of σ inside $\mathrm{Frob}_\mathfrak{p}$.

In the following result we let $T_{1,n}, T_{2,n}$ be the chosen ordered basis of $E[\ell^n]$. Notice that the statement does not depend on the choice of σ in the conjugacy class of the Frobenius at $\mathfrak{p}$ in $\mathrm{Gal}(K(\frac{1}{\ell^n}P)/K)$, nor on the choice of the point Q_n.

Lemma 10. *Fix $\mathfrak{p} \in S_E$ 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 $E(k_\mathfrak{p})$.
(2) There is $Q \in \frac{1}{\ell^n}P$ such that $(\sigma - \mathrm{Id})(Q) = 0$.
(3) We have $(\sigma - \mathrm{Id})(Q_n) \in (\sigma - \mathrm{Id})(E[\ell^n])$.
(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) ⇔ (2). Suppose that there is $R \in E(k_\mathfrak{p})$ such that $[\ell^n]R = (P \bmod \mathfrak{p})$. Let $\mathfrak{q}$ be a prime of $K(\frac{1}{\ell^n}P)$ lying over $\mathfrak{p}$ such that σ is the Frobenius automorphism for $\mathfrak{q}$. Let $Q_0 \in \frac{1}{\ell^n}P$. We have $[\ell^n](Q_0 \bmod \mathfrak{q}) = (P \bmod \mathfrak{p})$. Let $T = R - (Q_0 \bmod \mathfrak{q}) \in E(k_\mathfrak{q})$. Then, $[\ell^n]T = 0$ so $T \in E[\ell^n](\overline{k_\mathfrak{q}})$. Since the reduction map $\mathrm{red}_\mathfrak{q} : E[\ell^n](\overline{K}) \to E[\ell^n](\overline{k_\mathfrak{q}})$ is bijective (see Remark 9), we can lift T in $S \in E[\ell^n](\overline{K})$. We define $Q = Q_0 + S$, which is an element of $\frac{1}{\ell^n}P$ 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 $(Q \bmod \mathfrak{q}) \in E(k_\mathfrak{p})$ and it satisfies $[\ell^n](Q \bmod \mathfrak{q}) = (P \bmod \mathfrak{p})$.

(2) ⇔ (3). If Q exists, then we write $Q = Q_n - T$ for some $T \in E[\ell^n]$, 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 $T \in E[\ell^n]$, then the point $Q := Q_n - T$ is in $\frac{1}{\ell^n}P$ and satisfies $(\sigma - \mathrm{Id})(Q) = 0$.

(3) ⇔ (4). Call $\vec{c_i}$ (for $i = 1, 2$) 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 with the corresponding torsion points (choosing the torsion point that, written in the basis $T_{1,n}, T_{2,n}$, 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 $T \in E[\ell^n]$ 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) ⇒ (4). This is immediate by setting $N = n$.

(1) and (4) ⇒ (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 $E(k_\mathfrak{p})$. Applying (4) to $\tilde{P}$ and N (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 $E(k_\mathfrak{p})$ that are *indivisible* in this group, namely that are not ℓ-multiples for any prime ℓ dividing $\#E(k_\mathfrak{p})$.

Remark 11. The prime ℓ divides $\#E(k_\mathfrak{p})$ if and only if $\det(M_1 - \mathrm{Id}_1) = 0$ in $\mathbb{F}_\ell$, see Remark 9. Moreover, if there is no $X \in E(k_\mathfrak{p})$ such that $[\ell^n]X = (P \bmod \mathfrak{p})$, then the map $[\ell^n] : E(k_\mathfrak{p}) \to E(k_\mathfrak{p})$ is not surjective: in particular, $\ell \mid \#E(k_\mathfrak{p})$. This explains why the notion of ℓ-divisibility is relevant only for primes dividing $\#E(k_\mathfrak{p})$.

Remark 12. We describe some special cases related to Lemma 10.

• Suppose that $M_n = \mathrm{Id}_n$ (which means that $E(k_\mathfrak{p})$ contains $E[\ell^n](\bar{k}_\mathfrak{p})$). 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 $E(k_\mathfrak{p})$ 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 $\vec{c} = \sum_i \alpha_i \vec{c_i}$ for some integers α_i, where the $\vec{c_i}$'s are the columns of $M_n - \mathrm{Id}_n$. Thus, the point $Q_n - \sum_i \alpha_i T_{i,n}$ is fixed by σ and hence $(P \bmod \mathfrak{p})$ is ℓ^n-divisible in $E(k_\mathfrak{p})$.

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

$$M'_n - \mathrm{Id}_n = \begin{pmatrix} 0 & a_1 & b_1 \\ 0 & a_2 & b_2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Thus $(P \bmod \mathfrak{p})$ is ℓ^n-divisible in $E(k_\mathfrak{p})$ if and only if $\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ is a multiple of $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$.

2.6. **The $\ell\mathbb{Z}$-rank of matrices modulo ℓ^n.** We fix a prime number ℓ and, 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 positive integers m and d. We say that the elements $r_1, \ldots, r_m \in (\mathbb{Z}/\ell^n\mathbb{Z})^d$ 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 13 ($\ell\mathbb{Z}$-rank)**.** The $\ell\mathbb{Z}$-rank of a matrix $M \in \mathrm{Mat}_{d\times m}(\mathbb{Z}/\ell^n\mathbb{Z})$, 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 0 if and only if M is the zero matrix.

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

Lemma 14. *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 $d - rk_{\ell\mathbb{Z}}(M)$. In particular, the exponent of $\ker(M)$ equals ℓ^n if and only if $rk_{\ell\mathbb{Z}}(M) < d$.

(2) The group structure of $\ker(M)$ determines and it is determined by the numbers

$$rk_{\ell\mathbb{Z}}(M \bmod \ell^h) \qquad h = 1, \dots, n\,.$$

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

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

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

Proof. Proof of (1). Let $\vec{c}_1, \dots, \vec{c}_d$ be the columns of M and set $r := \mathrm{rk}_{\ell\mathbb{Z}}(M)$. We consider the matrices E that act as the following elementary column operations when multiplied on the right: swapping two columns, multiplying a column by an integer coprime to ℓ, or adding to a column the multiple of another column. Then M and ME have the same $\ell\mathbb{Z}$-rank, so we can perform the above elementary column operations without changing the $\ell\mathbb{Z}$-rank. Moreover, 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 $\vec{x}$ hence we can perform the above elementary column operations without changing the number of cyclic components of size ℓ^n of the kernel.

Consider a column vector $\vec{x} \in (\mathbb{Z}/\ell^n\mathbb{Z})^d$ with components x_1 to x_d. We have $\vec{x} \in \ker(M)$ if and only if $x_1\vec{c}_1 + \ldots + x_d\vec{c}_d = \vec{0}$. If $r = d$, this condition implies that ℓ divides all components of $\vec{x}$ hence $\ker(M)$ has no element of order ℓ^n. Now suppose that $r < d$. With elementary columnn operations as above, we may replace M by

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

where the columns $\vec{b}_1, \dots, \vec{b}_r$ are $\ell\mathbb{Z}$-linearly independent columns from the original matrix M. Then $\vec{x} \in \ker(M)$ implies that x_1 to x_r are divisible by ℓ and there is no condition on the last $d - r$ components. We deduce that $\ker(M)$ has precisely $d - r$ cyclic components of size ℓ^n.

Proof of (2). We can apply (1) to $M_h := (M \bmod \ell^h)$ for $1 \leq h < n$. Thus $\ker(M_h)$ 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, namely 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 representatives for the components 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 representatives for the components 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 $\vec{x_h} \in \ker(M_h)$. Indeed, using integer representatives, we have $M\vec{x} = M\ell^{n-h}\vec{x_h}$ and hence this vector is zero modulo ℓ^n if and only if $M\vec{x_h}$ is zero modulo ℓ^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 14.

Remark 15. The $\ell\mathbb{Z}$-rank of a matrix $M = (\vec{c}_1|\vec{c}_2) \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/\ell^n\mathbb{Z})$ can only be 0, 1, or 2. 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 14 (2), $\ker(M)$ contains a point of order ℓ^n if and only if $\mathrm{rk}_{\ell\mathbb{Z}}(M) \leq 1$.

Remark 16. Let $A_+ = \begin{pmatrix} A & \vec{v}_A \\ 0 & 1 \end{pmatrix}$ and $B_+ = \begin{pmatrix} B & \vec{v_B} \\ 0 & 1 \end{pmatrix}$ be elements of $\mathrm{Mat}_{d+1\times d+1}(\mathbb{Z}/\ell^n\mathbb{Z})$ with $A, B \in \mathrm{Mat}_{d\times d}(\mathbb{Z}/\ell^n\mathbb{Z})$, $\vec{v}_A$ and $\vec{v}_B$ column vectors, and 0 denoting the zero matrix in $\mathrm{Mat}_{d\times 1}(\mathbb{Z}/\ell^n\mathbb{Z})$. Suppose that B is invertible, thus B_+ is invertible with inverse

$$B_+^{-1} = \begin{pmatrix} B^{-1} & -B^{-1}\vec{v_B} \\ 0 & 1 \end{pmatrix}.$$

The matrices A and $B^{-1}AB$ have isomorphic kernels and hence by Lemma 14 for all $1 \leq h \leq n$ the matrices $(A \bmod \ell^h)$ and $(B^{-1}AB \bmod \ell^h)$ have the same $\ell\mathbb{Z}$-rank. We have

$$B_+^{-1}A_+B_+ = \begin{pmatrix} B^{-1}AB & \vec{w} \\ 0 & 1 \end{pmatrix} \qquad \text{with} \qquad \vec{w} = B^{-1}(A - \mathrm{Id})\vec{v}_B + B^{-1}\vec{v}_A\,.$$

We deduce that $\vec{v}_A \in \mathrm{Im}(A-\mathrm{Id})$ if and only if $\vec{w} \in \mathrm{Im}(B^{-1}AB-\mathrm{Id})$. Indeed, if $\vec{v}$ is a vector, then $\vec{v}_A = A\vec{v} - \vec{v}$ implies $\vec{w} = (B^{-1}AB - \mathrm{Id})(B^{-1}\vec{v}_B + B^{-1}\vec{v})$ while $\vec{w} = B^{-1}AB\vec{v} - \vec{v}$ implies $\vec{v}_A = (A - \mathrm{Id})(B\vec{v} - \vec{v}_B)$.

We remark 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 $\vec{v}_B = \vec{0}$. Moreover, replacing $\vec{v}_A$ by adding to it an element in $\mathrm{Im}(A - \mathrm{Id})$ does not affect whether $\vec{v}_A \in \mathrm{Im}(A - \mathrm{Id})$.

2.7. **Matrix-counting.**

We fix a prime number ℓ: the densities $\mathrm{dens}_{\text{indiv}}(\ell)$ and $\mathrm{dens}_{\exp}(\ell)$ will be computed thanks to the Chebotarev density theorem by counting suitable matrices in the image of the $\bmod \ell$ (respectively, $\bmod \ell^n$ for $n \geq 1$) torsion-Kummer representations. We introduce the notation and present some preliminary results.

Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell) \ltimes (\mathbb{Z}_\ell)^2$. We define G_ℓ to be one of the following groups: $\mathrm{GL}_2(\mathbb{Z}_\ell)$, a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. We suppose that the first projection $\pi_1(G)$ is a finite index subgroup of G_ℓ. We also suppose that G has finite index in $G_\ell \ltimes (\mathbb{Z}_\ell)^2$. We let n_0 be a positive integer such that the index of $G(n_0)$ in $G_\ell(n_0) \ltimes (\mathbb{Z}/\ell^{n_0}\mathbb{Z})^2$ is the same as the index of G in $G_\ell \ltimes (\mathbb{Z}_\ell)^2$. Moreover, 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 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 $N \geq n$ and an element $(M_N, v_N) \in G(N)$ we set $(M_n, v_n) := (M_N, v_N) \bmod \ell^n$. Then we call (M_N, v_N) a *lift* of (M_n, v_n).

Definition 17. We define $R(n) = \#G(n)$, $R_1(n) = \#\pi_1(G)(n)$ and

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

If $n \geq 2$, we also define

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

Proposition 18. *The quantities $R_1(1)$ and $R_1'(1)$ are as follows in the special case where $\pi_1(G) = G_\ell$:*

$\pi_1(G)$	$R_1(1)$	$R'_1(1)$
$\mathrm{GL}_2(\mathbb{Z}_\ell)$	$\ell(\ell-1)^2(\ell+1)$	$\ell^3-2\ell-1$
Split Cartan	$(\ell-1)^2$	$2\ell-4$
Nonsplit Cartan	ℓ^2-1	0
Normalizer of a split Cartan	$2(\ell-1)^2$	$3\ell-5$
Normalizer of a nonsplit Cartan	$2(\ell^2-1)$	$\ell+1$
Ramified Cartan (ℓ odd)	$\ell(\ell-1)$	$\ell-1$
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 quantities $R_1(1)$ are well known or clear from the description of the Cartan subgroups provided in Section 2.3. As we are working modulo ℓ, the notion of $\ell\mathbb{Z}$-rank coincides with the usual notion of rank.

The case of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. For $M_1 \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, one has $\det(M_1-\mathrm{Id}_1) = 1-\mathrm{tr}(M_1)+\det(M_1)$, so the condition $\det(M_1-\mathrm{Id}_1)=0$ is equivalent to $d=t-1$ where $t=\mathrm{tr}(M_1)$ and $d=\det(M_1)$. By [CFRM05, Lemma 2.7], one has

$$\#\{M_1 \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(M_1)=d, \mathrm{tr}(M_1)=t\} = \ell^2+\ell\left(\frac{t^2-4d}{\ell}\right).$$

The condition $t=d+1$ gives $t^2-4d=(d-1)^2$, so

$$\#\{M_1 \in \mathrm{GL}_2(\mathbb{Z}_\ell) : \det(M_1)=d, \mathrm{tr}(M_1)=t\} = \begin{cases} \ell^2+\ell, & d\neq 1 \\ \ell^2, & d=1. \end{cases}$$

Summing over $d\in\mathbb{F}_\ell^\times$ and excluding the identity matrix from this count, one obtains

$$R'_1(1) = (\ell-2)(\ell^2+\ell)+\ell^2-1 = \ell^3-2\ell-1.$$

The (normalizer of a) split Cartan. We use the diagonal model. A matrix $M_1 = \begin{pmatrix}\alpha_1 & 0\\ 0 & \beta_1\end{pmatrix}$ in $C(1)$ has a 1-eigenvector if and only if $\alpha_1=1$ or $\beta_1=1$. There are $2(\ell-2)$ such matrices M_1 different from the identity. If $M_1 = \begin{pmatrix}0 & \beta_1\\ \alpha_1 & 0\end{pmatrix} \in C'(1)$, then $\det(M_1-\mathrm{Id}_1)=0$ if and only if $1-\alpha_1\beta_1=0$, so there are $\ell-1$ matrices M_1 in $C'(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1-\mathrm{Id}_1)=1$. Summing the contributions from $C(1)$ and $C'(1)$ gives $R'_1(1)$ for the normalizer of a split Cartan.

The (normalizer of a) nonsplit Cartan. The case $\ell=2$ is a small calculation, so suppose that ℓ is odd. For $M_1 = \begin{pmatrix}\alpha_1 & \beta_1 d\\ \beta_1 & \alpha_1\end{pmatrix} \in C(1)$, as d is not a square modulo ℓ, we have $\mathrm{rk}(M_1-\mathrm{Id}_1)=2$ except for the identity matrix. The matrices in $C'(1)$ are obtained by multiplying the matrices in $C(1)$ by $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ so they are of the form $M'_1 = \begin{pmatrix}\alpha_1 & \beta_1 d\\ -\beta_1 & -\alpha_1\end{pmatrix}$. As M'_1 is not the identity, the rank of $M'_1-\mathrm{Id}_1$ equals 1 if and only if $\beta_1^2 d = \alpha_1^2-1$. For $\alpha_1=\pm1$ this gives $\beta_1=0$. Else, this 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 α_1's 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 $\ell+1$.

The (normalizer of a) ramified Cartan. The case $\ell = 2$ is a small calculation (in that case, $N(1) = C(1)$), 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 $\alpha_1 = 1$ (and then $\beta_1 = 0$ gives the identity matrix). 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 $\alpha_1 = \pm 1$ (and the matrix is not the identity). So $R_1'(1)$ is $\ell - 1$ for the Cartan subgroup and $(\ell-1)+2\ell$ for its normalizer. □

3. The Indivisibility LT conjecture

In this section we collect results related to the Indivisibility LT conjecture, which is based on Condition (3).

Proposition 19. *Let L be a finite and non-empty set of prime numbers, and call m the product of the elements of L. The set of primes $\mathfrak{p} \in S_E$ such that Condition* (3) *holds for all $\ell \in L$ admits a natural density* $\mathrm{dens}_{\mathrm{indiv}}(L)$*. This natural density is the proportion of Galois automorphisms $\sigma \in \mathrm{Gal}(K(\frac{1}{m}P)/K)$ satisfying the following condition for each $\ell \in L$: σ does not fix any torsion point of order ℓ, or σ does not fix any point in $\frac{1}{\ell}P$. In particular,* $\mathrm{dens}_{\mathrm{indiv}}(L)$ *is a rational number whose minimal denominator divides $m^2 \cdot \#\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.*

Proof. The last assertion is because the degree of $K(\frac{1}{m}P)/K$ divides $m^2\cdot\#\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. For each prime $\ell \in L$, Condition (3) is equivalent to the condition

$$\ell \nmid \#E(k_{\mathfrak{p}}) \text{ or } (P \bmod \mathfrak{p}) \notin [\ell]E(k_{\mathfrak{p}})\,.$$

We consider the primes $\mathfrak{p} \in S_E$ that are not over the primes in L and do not ramify in $K(\frac{1}{m}P)/K$ (we are excluding only finitely many primes of K). We let $\sigma \in \mathrm{Gal}(K(\frac{1}{m}P)/K)$. If $\sigma \in \mathrm{Frob}_{\mathfrak{p}}$, then we have $\ell \nmid \#E(k_{\mathfrak{p}})$ if and only if σ doesn't fix any torsion point of order ℓ in $E(\bar{K})$. Moreover, by Lemma 10 we have $(P \bmod \mathfrak{p}) \notin [\ell]E(k_{\mathfrak{p}})$ if and only if σ does not fix any point in $\frac{1}{\ell}P$. The statement then follows from the Chebotarev density theorem because the suitable primes $\mathfrak{p}$ correspond (up to the finite set of excluded primes) to suitable automorphisms σ. □

We are now going to prove Theorem 1. In fact, we will prove the following result for a general number field K. For every sufficiently large prime ℓ the natural density $\mathrm{dens}_{\mathrm{indiv}}(\ell)$ is a rational function in ℓ (where the polynomials in both the numerator and the denominator have degree 4 (resp. 6) if E has CM (resp. non-CM). We deduce that the Euler product $\prod_{\ell\gg 0}\mathrm{dens}_{\mathrm{indiv}}(\ell)$ is strictly positive.

Theorem 20. *The natural density* $\mathrm{dens}_{\mathrm{indiv}}(\ell)$ *is the Haar measure of the set*

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

and, if $[K(E(\frac{1}{\ell}P)) : K(E[\ell])] = \ell^2$, we also have $\mathrm{dens}_{\mathrm{indiv}}(\ell) = 1 - \frac{R_1'(1)\ell+1}{R_1(1)\ell^2}$.

If E is without complex multiplication, then for every $\ell \gg 0$ we have

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

If E has complex multiplication by an order contained in the imaginary quadratic field of discriminant $-D$, then for every $\ell \gg 0$ we have

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

Proof. The fact that $\mathrm{dens}_{\mathrm{indiv}}(\ell)$ is the Haar measure of the given set follows from Proposition 19. Now we may suppose that the degree of $K(E(\frac{1}{\ell}P))/K(E[\ell])$ is maximal, which holds in particular for all $\ell \gg 0$ by Corollary 8. Then, with the notation of Section 2.7 and letting G be the image of the ℓ-adic torsion-Kummer representation, we have $R(1) = R_1(1)\ell^2$. The number of matrices $M_1 \in \pi_1(G)(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1)$ equals 1 (respectively, 2) is $R_1'(1)$ (respectively, $R_1(1) - R_1'(1) - 1$). So the number of elements $(M_1, v_1) \in G(1)$ such that $v_1 \notin \mathrm{Im}(M_1 - \mathrm{Id}_1)$ is the sum of $\ell^2 - 1$ (for $M_1 = \mathrm{Id}_1$) and $(\ell^2 - \ell)R_1'(1)$ (for $M_1 - \mathrm{Id}_1$ with $\ell\mathbb{Z}$-rank 1). The number of elements $(M_1, v_1) \in G(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2$ is $\ell^2(R_1(1) - R_1'(1) - 1)$. The natural density $\mathrm{dens}_{\mathrm{indiv}}(\ell)$ is then by Proposition 19

$$\frac{\Big(\ell^2 - 1 + (\ell^2 - \ell)R_1'(1) + \ell^2(R_1(1) - R_1'(1) - 1)\Big)}{\ell^2 R_1(1)}\,.$$

For $\ell \gg 0$ the fields $K(E[\ell])/K$ have maximal degree hence the explicit expressions for $\mathrm{dens}_{\mathrm{indiv}}(\ell)$ follow from Proposition 18. □

Remark 21. Recall Proposition 19 and Lemma 10, and let M_1 vary in the image of the $\bmod \ell$ torsion representation of E. If for some M_1 we have $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2$, then (as no point in $E[\ell](\bar{K})$ of order ℓ is fixed by M_1) we have $\mathrm{dens}_{\mathrm{indiv}}(\ell) > 0$. Else, all matrices M_1 fix at least one point of order ℓ in $E[\ell](\bar{K})$. Then we have $\mathrm{dens}_{\mathrm{indiv}}(\ell) = 0$ if and only if $E(K) \cap \frac{1}{\ell}P$ is non-empty: the latter condition is clearly sufficient, and it is necessary by the results on the local-global principle for divisibility, see [Won00, Theorem 1].

Notice that, in the following result, the integer B exists by Proposition 7. Moreover, the rational number Q could be zero, even if $\mathrm{dens}_{\mathrm{indiv}}(\ell) > 0$ holds for every $\ell \in \mathcal{P}$. This is due to the so-called *entanglement* between the torsion-Kummer extensions $K(\frac{1}{\ell}P)/K$ at different primes ℓ. To showcase such entanglement phenomena we refer the reader to the related example by Nathan Jones mentioned by Zywina in [Zyw11, Section 1].

We are now going to prove Theorem 2. In fact, we will prove the following result for a general number field K. We call $\mathrm{SplitCM}$ (respectively, $\mathrm{InertCM}$) the set of prime numbers that split (respectively, are inert) in the CM field.

Theorem 22. *Suppose that E is without CM, or that it has CM defined over K. We assume the Indivisibility LT conjecture for $S = \mathcal{P}$. Let B be a positive integer 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. Calling L_B the set of prime divisors of B we have*

$$\mathrm{dens}_{\mathrm{indiv}}(\mathcal{P}) = \mathrm{dens}_{\mathrm{indiv}}(L_B) \cdot \prod_{\ell \in \mathcal{P} \setminus L_B} \mathrm{dens}_{\mathrm{indiv}}(\ell)\,. \tag{4}$$

Moreover, there exists a rational number Q such that the following holds: if E is without CM, then

$$\mathrm{dens}_{\mathrm{indiv}}(\mathcal{P}) = Q \cdot \prod_{\ell \in \mathcal{P}} \Big(1 - \frac{\ell^4 - 2\ell^2 - \ell + 1}{\ell^3(\ell-1)^2(\ell+1)}\Big)$$

while if E has CM defined over K, then we have

$$\mathrm{dens}_{\mathrm{indiv}}(\mathcal{P}) = Q \cdot \prod_{\ell \in \mathrm{SplitCM}} \Big(1 - \frac{2\ell^2 - 4\ell + 1}{\ell^2(\ell-1)^2}\Big) \cdot \prod_{\ell \in \mathrm{InertCM}} \Big(1 - \frac{1}{\ell^2(\ell+1)(\ell-1)}\Big)\,.$$

Proof. By our assumption on B and Proposition 19, for any finite set L' of prime numbers that do not divide B we have

$$\mathrm{dens}_{\mathrm{indiv}}(L_B \cup L') = \mathrm{dens}_{\mathrm{indiv}}(L_B) \cdot \prod_{\ell \in L'} \mathrm{dens}_{\mathrm{indiv}}(\ell)\,.$$

By the Indivisibility LT conjecture with $S = \mathcal{P}$, taking the infimum of both sides (by enlarging L') we obtain (4).

We observe that $\mathrm{dens}_{\mathrm{indiv}}(L_B)$ is a rational multiple of $\prod_{\ell \in L_B} \mathrm{dens}_{\mathrm{indiv}}(\ell)$. Indeed, by Proposition 19 we are comparing two rational numbers and $\mathrm{dens}_{\mathrm{indiv}}(L_B)$ is zero if $\mathrm{dens}_{\mathrm{indiv}}(\ell)$ is zero for some $\ell \in L_B$. We may then conclude because the rational number $\mathrm{dens}_{\mathrm{indiv}}(\ell)$ is a rational multiple of and (by the description of the torsion-Kummer representations in Section 2) for $\ell \gg 0$ is equal to the non-zero generic natural density described in Theorem 20. □

In the following result we write $\mathrm{dens}_{\mathrm{indiv},K'}$ to specify the base field K'. Moreover, we write $\mathrm{dens}_{\mathrm{indiv},\mathrm{Split}}$ (respectively, $\mathrm{dens}_{\mathrm{indiv},\mathrm{Inert}}$) if we restrict to the primes of K that split (respectively, are inert) in K'.

Lemma 23. *Suppose that E has CM that is not defined over K but over a quadratic extension K' of K. Let S be a non-empty set of prime numbers and assume the Indivisibility LT conjecture for S over K and over K'. The set of primes $\mathfrak{p}$ of K that split (respectively, are inert) in K' and that satisfy Condition* (3) *for all $\ell \in S$ has a natural density and we have*

$$\mathrm{dens}_{\mathrm{indiv}}(S) = \mathrm{dens}_{\mathrm{indiv},\mathrm{Split}}(S) + \mathrm{dens}_{\mathrm{indiv},\mathrm{Inert}}(S)\,.$$

Moreover, we have

$$\mathrm{dens}_{\mathrm{indiv},\mathrm{Split}}(S) = \frac{1}{2}\,\mathrm{dens}_{\mathrm{indiv},K'}(S)$$

and the existence of one of these two densities implies the existence of the other.

Proof. Consider a prime $\mathfrak{p}$ of K that splits in K' and a prime $\mathfrak{q}$ of K' over $\mathfrak{p}$. Since the residue fields at $\mathfrak{p}$ and at $\mathfrak{q}$ are the same, Condition (3) holds for $\mathfrak{p}$ if and only if it holds for $\mathfrak{q}$. The last assertion then follows by combining the following observations: the ideals $\mathfrak{p}$ and $\mathfrak{q}$ have the same norm; there are precisely two primes of K' over $\mathfrak{p}$; the set of primes of K' that lie over the primes of K that split completely in K' has natural density 1.

We may ignore the finitely many primes of K that ramify in K and hence partition the primes of K according to whether they are split or inert in K'. We observe that if two sets $T' \subseteq T$ of primes of K both have a natural density, then the complement $T \setminus T'$ also has a natural density and we have $\mathrm{dens}(T \setminus T') = \mathrm{dens}(T) - \mathrm{dens}(T')$. The existence of $\mathrm{dens}_{\mathrm{indiv}}(S)$ follows from the Indivisibility LT Conjecture over K. Thus we are left to prove that $\mathrm{dens}_{\mathrm{indiv},\mathrm{Split}}(S)$ is well-defined: this is a consequence of the last assertion because $\mathrm{dens}_{\mathrm{indiv},K'}(S)$ exists by the Indivisibility LT Conjecture over K'. □

Theorem 24. *Suppose that E has CM that is not defined over K but over a quadratic extension K' of K. We assume the Indivisibility LT conjecture for $S = \mathcal{P}$ over K and over K'. Then there exist two rational numbers Q_1 and Q_2 such that*

$$\mathrm{dens}_{\mathrm{indiv,Split}}(\mathcal{P}) = Q_1 \cdot \prod_{\ell \in \mathrm{SplitCM}} \Big(1 - \frac{2\ell^2 - 4\ell + 1}{\ell^2(\ell-1)^2}\Big) \cdot \prod_{\ell \in \mathrm{InertCM}} \Big(1 - \frac{1}{\ell^4 - \ell^2}\Big)$$

and

$$\mathrm{dens}_{\mathrm{indiv,Inert}}(\mathcal{P}) = Q_2 \cdot \prod_{\ell \in \mathrm{SplitCM}} \Big(1 - \frac{2\ell - 1}{\ell(\ell-1)^2}\Big) \cdot \prod_{\ell \in \mathrm{InertCM}} \Big(1 - \frac{\ell + 1}{\ell(\ell^2 - 1)}\Big) .$$

Proof. The assertion for $\mathrm{dens}_{\mathrm{indiv,Split}}$ follows by combining Lemma 23 for $S = \mathcal{P}$ and Theorem 22 over K'. Now we consider $\mathrm{dens}_{\mathrm{indiv,Inert}}$, which means that we have to restrict to the Galois automorphisms $\sigma \in \mathrm{Gal}(\bar{K}/K)$ that are not the identity on K'. The analogue of Proposition 7 consists then in replacing W_n by the complement of the Cartan group $C(\mathbb{Z}/n\mathbb{Z})$ in W_n. This adelic open image theorem then guarantees that, for all $\ell \gg 0$, these restricted mod ℓ representations are independent and their images are as large as possible. We conclude (similarly as in the proof of Theorem 22) thanks to the explicit counts in Theorem 20, noticing that suitable elements stemming from the complement of the Cartan subgroup in the normalizer can be computed as a difference, comparing the Cartan and its normalizer. For the case where ℓ is split in the CM field we have

$$\big(2\ell^2(\ell-1)^2 - (3\ell^2 - 5\ell + 1)\big) - \big(\ell^2(\ell-1)^2 - (\ell^2 - 4\ell + 1)\big) = \ell^2(\ell-1)^2 - (2\ell^2 - \ell)$$

suitable elements out of $\ell^2(\ell-1)^2$, and in the respective case

$$(2\ell^2(\ell^2-1) - (\ell^2 + \ell + 1)) - (\ell^2(\ell^2 - 1) - 1) = \ell^2(\ell^2-1) - (\ell^2 + \ell)$$

suitable elements out of $\ell^2(\ell^2 - 1)$. The condition of splitting (respectively, being inert) in K' is independent of ℓ and for this reason we count for each ℓ the proportion of elements considering the Cartan group (respectively, its complement) and not the normalizer of the Cartan. In other words, we should consider one single factor $1/2$ as done in Lemma 23, as the $\mathrm{mod}\ell$ representations are not independent (this factor is included in Q_1 and Q_2 respectively). □

4. The existence of the natural density for Condition (2)

We fix some prime ℓ and study the set $S_{\exp}$ of primes in S_E, not over ℓ, such that Condition (2) holds. We consider the partition $S_{\exp} = \cup_{n \geq 0} S_{\exp,n}$, where

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

Recall that ρ_{ℓ^n} is the torsion representation $\mathrm{mod}\ell^n$.

Remark 25. The set $S_{\exp,0}$ consists of the primes $\mathfrak{p} \in S_E$, not over ℓ, such that $\ell \nmid \#E(k_\mathfrak{p})$. This set has a natural density $\mathrm{dens}(S_{\exp,0})$ which is a rational number because this is the proportion of the matrices that do not fix any point in $E[\ell]$ of order ℓ (see Remark 9). As already given in [Coj03, Theorem 1], we have

$$\mathrm{dens}(S_{\exp,0}) = \frac{\#\{M_1 \in \mathrm{Im}(\rho_\ell) : \mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2\}}{\#\{M_1 \in \mathrm{Im}(\rho_\ell)\}} .$$

Remark 26. For $n \geq 1$, the set $S_{\exp,n}$ admits a natural density which is a rational number because, as we now explain, this set can be described in terms of the $\mathrm{mod}\ell^{n+1}$ 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 $\sigma \in \mathrm{Gal}(K(\frac{1}{\ell^{n+1}}P)/K)$ vary in the preimage of M_{n+1} under $\rho_{\ell^{n+1}}$. If $\mathfrak{p} \in S_E$ is not over ℓ

and it is such that $\sigma \in \mathrm{Frob}_{\mathfrak{p}}$, then by Lemma 14 the condition $\exp_\ell(E(k_{\mathfrak{p}})) = n$ is equivalent to the following:

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

Moreover, if $\exp_\ell(E(k_{\mathfrak{p}})) = n$, then the condition $\mathrm{ord}_\ell(P \bmod \mathfrak{p}) = n$ is equivalent to $[\ell^{n-1}](P \bmod \mathfrak{p})$ being not ℓ^n-divisible in $E(k_{\mathfrak{p}})$. By applying Lemma 10 to $[\ell^{n-1}]P$, this is equivalent to

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

where we here extend σ to a Galois automorphism of $K(\frac{1}{\ell^n}P)/K$. Notice that the choice of $\sigma \in \mathrm{Frob}_{\mathfrak{p}}$ is irrelevant, see also Remark 16.

Consider the primes in S_E not over ℓ, and fix a positive integer n. The set

$$\{\mathfrak{p} : \exp_\ell E(k_{\mathfrak{p}}) < n\}$$

and hence its complement

$$\{\mathfrak{p} : \exp_\ell(E(k_{\mathfrak{p}})) \geq n\}$$

can be described in terms of the $\bmod \ell^n$ torsion representation of E/K and it admits a natural density that is a rational number. the natural density is non-decreasing (for the complement, non-increasing) with n.

Lemma 27 (Hörmann and Lombardo)**.** *Fix a prime number ℓ and positive integers n and d. 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 $g(x) \in \mathbb{Z}_\ell[x]$ that is congruent to $f(x)$ modulo ℓ^n. Let K be a splitting field of $g(x)$ over $\mathbb{Q}_\ell$ and write $\mathcal{O}_K$ for the ring of integers of K and π for a uniformiser. We consider the valuation v_π and also the ℓ-adic valuation v_ℓ. By construction, $g(x)$ 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 $f(\alpha) = 0$ lifts to $\beta \in \{0, 1, \ldots, \ell^n - 1\} \subset \mathcal{O}_K$ with $v_\pi(g(\beta)) \geq v_\pi(\ell^n) = ne$, where $e := v_\pi(\ell)$ is the ramification index of K over $\mathbb{Q}_\ell$. For each α we consider the lift β and the index i such that $v_\pi(\beta - x_i)$ is maximal (selecting the smallest possible index) and hence $v_\pi(\beta - x_i) \geq \frac{ne}{d}$. If two distinct roots α and α' give the same index i, then we have

$$v_\pi(\beta - \beta') = v_\pi((\beta - x_i) - (\beta' - x_i)) \geq \min\{v_\pi(\beta - x_i), v_\pi(\beta' - x_i)\} \geq \frac{ne}{d}.$$

Since β, β' are in $\mathbb{Z}$, we have $v_\pi(\beta - \beta') = e \cdot v_\ell(\beta - \beta')$ and hence $\beta \equiv \beta' \pmod{\ell^{\lceil n/d \rceil}}$. 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. We conclude because there are at most d possible values for i. □

The following result can be generalized to abelian varieties with a similar proof:

Proposition 28 (Hörmann-Lombardo)**.** *The natural density of the set*

$$\{\mathfrak{p} \in S_E : \exp_\ell(E(k_{\mathfrak{p}})) \geq n\}$$

goes to 0 when n goes to infinity.

Proof. We may suppose that $\mathfrak{p}$ is not over ℓ. By Remark 9 and by the Chebotarev density theorem, we may equivalently show that $\#H_n/\#G_n$ goes to 0 when n goes to infinity, where $G_n := \mathrm{Gal}(K(E[\ell^n])/K)$ and

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

We identify G_n as usual with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ and we call G'_n the subgroup of G_n consisting of the scalar matrices. By a result of Serre and Wintenberger (see the proof of [LP21, Lemma 31]) we have $\#G'_n \geq c\ell^n$, where c is a positive constant that depends only on E/K. We claim that in each coset of G_n modulo G'_n there are at most $2 \cdot \ell^{n/2}$ elements M for which there exists a primitive vector $v \in (\mathbb{Z}/\ell^n\mathbb{Z})^2 \setminus (\ell\mathbb{Z}/\ell^n\mathbb{Z})^2$ (corresponding to a torsion point $T \in E[\ell^n] \setminus E[\ell^{n-1}]$) such that $Mv = v$. Summing over the cosets, we may conclude because we have

$$\#H_n \leq (\#G_n/\#G'_n) \cdot 2\ell^{n/2} \leq \#G_n \cdot \frac{2}{c} \cdot \ell^{-n/2}\,.$$

To prove the claim, let M_0 be a representative of the coset, and write $M = \alpha M_0$ for some $\alpha \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$. So the equation $Mv = v$ becomes $M_0 v = (\alpha^{-1})v$. As v is primitive, this implies that α^{-1} is a root of the characteristic polynomial of M_0 (see [Bro93, 17.3]), which is monic and of degree 2. So we may conclude by Lemma 27. □

Remark 29. From Proposition 28 we deduce that the natural density $\mathrm{dens}(S_{\mathrm{exp}})$ exists and that we have

$$\mathrm{dens}(S_{\mathrm{exp}}) = \sum_{n\geq 0} \mathrm{dens}(S_{\mathrm{exp},n})\,.$$

If we consider Condition (2) for a finite non-empty set of primes L we similarly have that the natural density $\mathrm{dens}_{\mathrm{exp}}(L)$ exists. Moreover, calling ℓ_i for $i = 1, \ldots, r$ the elements of L and letting n_i vary in the set of the non-negative integers we have that $\mathrm{dens}_{\mathrm{exp}}(L)$ is the sum of the natural densities of the sets

$$\{\mathfrak{p} \in S_E : \mathrm{ord}_{\ell_i}(P \bmod \mathfrak{p}) = \exp_{\ell_i} E(k_{\mathfrak{p}}) = n_i \text{ for all } i\}\,.$$

5. The rationality of the natural density for Condition (2)

The aim of this section is proving Theorem 3. To do so, we fix a prime number ℓ and show that the natural density $\mathrm{dens}_{\mathrm{exp}}(\ell)$ is a finite sum of rational numbers and geometric series with rational ratios.

5.1. **Setup.** We fix a prime number ℓ, and we call G the image of the ℓ-adic torsion-Kummer representation. We define

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

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

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

By Remarks 25 and 26, for every $n \geq 0$ the natural density of $S_{\mathrm{exp},n}$ equals $\mu(E_n)$, so by Remark 29 we have

$$\mathrm{dens}_{\mathrm{exp}}(\ell) = \sum_{n\geq 0} \mu(E_n)\,.$$

We make use of the notation introduced in Section 2.7. We let n_0 be a positive integer such that the index of $G(n_0)$ in $G_\ell(n_0) \ltimes (\mathbb{Z}/\ell^{n_0}\mathbb{Z})^2$ is the same as the index of G in $G_\ell \ltimes (\mathbb{Z}_\ell)^2$, where $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ if E is without CM, and G_ℓ is a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (respectively, the normalizer thereof) if E has CM that is defined (respectively, not defined) over K. We let $d_G = 4$ if E is without CM and $d_G = 2$ otherwise.

Remark 30. 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 31. *If we have* $[K(\frac{1}{\ell^{n_0}}P) : K(E[\ell^{n_0}])] = \ell^{2n_0}$*, then for any* $n \geq n_0$ *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. By the definition of n_0 we deduce that $[K(\frac{1}{\ell^n}P) : K(E[\ell^n])] = \ell^{2n}$ holds for all $n \geq n_0$. The number of matrices $M_{n+1} \in \pi_1(G)(n+1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ and $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ is $R_1'(n)\ell^{d_G} - R_1'(n+1)$, for which 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 $\frac{\ell-1}{\ell}$. 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 $M_n = \mathrm{Id}_n$, for which 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 $\frac{\ell^2-1}{\ell^2}$. □

Definition 32. For $n \geq n_0$ and for $M_{n_0} \in \pi_1(G)(n_0)$, we define

$$E_{n,M_{n_0}} = \{(M, v) \in E_n : M_n \equiv M_{n_0} \bmod \ell^{n_0}\}. \tag{5}$$

With the above notation, for $n \geq n_0$ we have

$$\mu(E_n) = \sum_{M_{n_0} \in \pi_1(G)(n_0)} \mu(E_{n,M_{n_0}}). \tag{6}$$

Remark 33. If $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 2$, then $\mu(E_{n,M_{n_0}}) = 0$ for $n \geq n_0$.

5.2. **General strategy for computing $\mu(E_{n,M_{n_0}})$.** Let us fix a matrix $M_{n_0} \in \pi_1(G)(n_0)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) \leq 1$. In the next subsections, we will show that $(\mu(E_{n,M_{n_0}}))$ is a geometric sequence or the sum of two geometric sequences with rational ratios for n large enough.

As a preliminary result, in Section 5.3 we show that for $n \geq n_0$ the proportion of vectors $v_n \in \pi_2(\pi_1^{-1}(M_n))$ such that $[\ell^{n-1}]_n \notin \mathrm{Im}(M_n - \mathrm{Id}_n)$ doesn't depend on n nor on $M_n \equiv M_{n_0} \bmod \ell^{n_0}$ if $M_{n_0} \neq \mathrm{Id}_{n_0}$. Indeed, if $n \geq n_0$, the structure of $[\ell^{n-1}]\pi_2(\pi_1^{-1}(M_n))$ is known from the group $[\ell^{n_0-1}]\pi_2(\pi_1^{-1}(M_{n_0}))$ and the proportion of suitable Kummer vectors only depends on the structure of this group. A similar result is established for $M_{n_0} = \mathrm{Id}_{n_0}$.

Then, starting from M_{n_0}, we only have to count the matrices $M_{n+1} \in \pi_1(G)(n+1)$ such that $M_{n+1} \equiv M_{n_0} \bmod \ell^{n_0}$, $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ and $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) \leq 1$. Since $n \geq n_0$, the matrices $M_{n+1} \equiv M_{n_0} \bmod \ell^{n_0}$ are in $\pi_1(G)(n+1)$.

- *For* GL_2 *and (normalizers) of unramified Cartan subgroups.* For $k \geq n_0$ and $\mathrm{rk}_{\ell\mathbb{Z}}(M_k - \mathrm{Id}_k) = 1$, we define L_1 as the number of lifts M_{k+1} of M_k modulo ℓ^{k+1} such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{k+1} - \mathrm{Id}_{k+1}) = 1$ (see Section 5.4). If $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 1$, we obtain the number of suitable matrices M_{n+1} in terms of L_1. It is crucial that L_1 does not depend on M_k nor on k. For the case $M_{n_0} = \mathrm{Id}_{n_0}$ we partition over the first index $n_0 < k \leq n$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_k - \mathrm{Id}_k) = 1$ if it exists.

- *For ramified Cartan subgroups.* The reasoning is more involved, because L_1 is not well-defined: for instance, if $C(n)$ is the reduction modulo ℓ^n of a ramified Cartan subgroup $C_{(0,d)}$ and if $M_n = \begin{pmatrix} \alpha_n & d\beta_n \\ \beta_n & \alpha_n \end{pmatrix}$ in $C(n)$ satisfy $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$, then the number of lifts M_{n+1} of M_n such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$ depends on $v_\ell(\beta_n)$ and $v_\ell(\alpha_n - 1)$. Choosing a lift M_{n+1} involves lifting a square root of d: lifting square roots is more convenient if n is large enough, and we may assume this condition without loss of generality. The case $\ell = 2$ is different because we have different numbers of lifts of the square roots (compare Remarks 43 and 47) and because for $\ell = 2$ it may not hold that ℓ divides the parameter d of the Cartan subgroup.

5.3. **Counting Kummer vectors.** Let (M_n, v_n) be in the image of the torsion-Kummer representation modulo ℓ^n. Fixing the matrix M_n, we count the vectors v_n as such which are in the image of $M_n - \mathrm{Id}_n$.

Lemma 34. *Let $(M_{n+1}, v_{n+1}) \in \mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \ltimes (\mathbb{Z}/\ell^{n+1}\mathbb{Z})^2$ be such that $M_n \neq \mathrm{Id}_n$ and $rk_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 1$. Then we have*

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

Proof. Let $\vec{c}_{n+1}$ be a column of $M_{n+1} - \mathrm{Id}_{n+1}$ that generates the column space, and call $\vec{c}_n$ its reduction modulo ℓ^n. If $[\ell^n]v_{n+1} = \alpha\vec{c}_{n+1}$ holds for some integer α, then ℓ divides α (else $\vec{c}_n$ is zero, contradicting that $M_n \neq \mathrm{Id}_n$) and hence $[\ell^{n-1}]v_n = \frac{\alpha}{\ell}\vec{c}_n$. Conversely, if $[\ell^{n-1}]v_n = \beta\vec{c}_n$ holds for some integer β, then we have $[\ell^n]v_{n+1} = \ell\beta\vec{c}_{n+1}$. □

Lemma 35. *Let $n > n_0$ and let $M_n \in \pi_1(G)(n)$ be such that $rk_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $M_{n_0} = \mathrm{Id}_{n_0}$. Call $\mathcal{C}_{M_n}$ the proportion, in the set $\pi_2(\pi_1^{-1}(M_n))$, of the elements v_n such that $[\ell^{n-1}]v_n \notin \mathrm{Im}(M_n - \mathrm{Id}_n)$. Then $\mathcal{C}_{M_n}$ is either 0 or $1 - \frac{1}{\ell}$. Considering the group $H := [\ell^{n_0-1}]\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$ we have:*
• if H is trivial (for example, if $\pi_2(\pi_1^{-1}(\mathrm{Id}_1))$ is trivial), then $\mathcal{C}_{M_n} = 0$;
• if H has two cyclic components, then $\mathcal{C}_{M_n} = 1 - \frac{1}{\ell}$;
• if H has one cyclic component, then we have $\mathcal{C}_{M_n} = 0$ if and only if $H = \mathrm{Im}(M_h - \mathrm{Id}_h)$, where $h > n_0$ is the smallest integer such that $rk_{\ell\mathbb{Z}}(M_h - \mathrm{Id}_h) = 1$.
If $N \geq n$ and $M_N \in \pi_1(G)(N)$ is a lift of M_n such that $rk_{\ell\mathbb{Z}}(M_N - \mathrm{Id}_N) = 1$, then we have $\mathcal{C}_{M_N} = \mathcal{C}_{M_n}$.

Proof. Recall the identification of $(\ell^{m-1}\mathbb{Z}/\ell^m\mathbb{Z})^2$ with $(\mathbb{Z}/\ell\mathbb{Z})^2$ for any $m \geq 2$. 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, $[\ell^{n-1}]\pi_2(\pi_1^{-1}(M_n))$ and H are contained in $\pi_2(\pi_1^{-1}(\mathrm{Id}_1))$. By the assumption on the $\ell\mathbb{Z}$-rank, the group

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

has ℓ elements. The ratio $\#(H \cap W_{M_n})/\#H$ is either 1 or $\frac{1}{\ell}$, leading to $\mathcal{C}_{M_n} = 0$ or $\mathcal{C}_{M_n} = 1 - \frac{1}{\ell}$ respectively. If H is trivial (respectively, $H = (\mathbb{Z}/\ell\mathbb{Z})^2$), the ratio is 1 (respectively, $\frac{1}{\ell}$). If H has ℓ elements, we conclude by observing that $W_{M_n} = W_{M_h} = \mathrm{Im}(M_h - \mathrm{Id}_h)$. Finally, the last assertion follows from $W_{M_N} = W_{M_n}$. □

Remark 36. Fix a subgroup H of $(\mathbb{Z}/\ell\mathbb{Z})^2$ with ℓ elements and, for an integer $t \geq n_0 + 1$, consider the set H' of all $M_t \in \pi_1(G)(t)$ such that

$$M_{t-1} = \mathrm{Id}_{t-1}, \quad \mathrm{rk}_{\ell\mathbb{Z}}(M_t - \mathrm{Id}_t) = 1 \quad \text{and} \quad \mathrm{Im}(M_t - \mathrm{Id}_t) = H\,.$$

If $\pi_1(G)$ has finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$, then $\#H' = \ell^2 - 1$. If $\pi_1(G)$ has finite index in 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). As we will see in Proposition 40, there is no matrix M_t above the identity such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_t - \mathrm{Id}_t) = 1$ for the normalizer of a nonsplit Cartan subgroup.

Remark 37. Let $n \geq n_0$ and set $H := [\ell^{n_0-1}]\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$. Call $\mathcal{C}_{\mathrm{Id}}$ the proportion in the set $\pi_2(\pi_1^{-1}(\mathrm{Id}_n))$ of the elements v_n such that $[\ell^{n-1}]v_n \neq 0$. If H is trivial, then $\mathcal{C}_{\mathrm{Id}} = 0$. If H has two components, then $\mathcal{C}_{\mathrm{Id}} = \frac{\ell^2-1}{\ell^2}$. If H has one component, then $\mathcal{C}_{\mathrm{Id}} = \frac{\ell-1}{\ell}$. 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 38. Let $M_{n_0} \in \pi_1(G)(n_0)$ be such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 1$, and consider the elements in $\pi_1^{-1}(M_{n_0}) \subseteq G(n_0)$. We call $c_{M_{n_0}}$ the proportion of the elements (M_{n_0}, v_{n_0}) satisfying

$$[\ell^{n_0-1}]v_{n_0} \notin \mathrm{Im}(M_{n_0} - \mathrm{Id}_{n_0})\,.$$

Let M_{n_0} be as in the above definition. If $n > n_0$ and $M_n \in \pi_1(G)$ is a lift of M_{n_0} such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$, then by Lemma 34 the number $c_{M_{n_0}}$ is also the proportion of the elements (M_n, v_n) in $\pi_1^{-1}(M_n) \subseteq G(n)$ satisfying

$$[\ell^{n-1}]v_n \notin \mathrm{Im}(M_n - \mathrm{Id}_n)\,.$$

5.4. **Lifts of matrices with a given $\ell\mathbb{Z}$-rank.** Let $n \geq n_0$. We consider $M_n \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/\ell^n\mathbb{Z})$ and its lifts $M_{n+1} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$. The $\ell\mathbb{Z}$-rank of $(M_{n+1} - \mathrm{Id}_{n+1})$ is at least that of $(M_n - \mathrm{Id}_n)$. As the $\ell\mathbb{Z}$-rank is invariant under conjugation (see Remark 16), 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.

Definition 39. Suppose that $\pi_1(G)$ has finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$, in an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or a normalizer thereof. If $n \geq n_0$ and $M_n \in \pi_1(G)(n)$ is such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$, 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 $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1})$ equals 1 (respectively, 2). If $M_n = \mathrm{Id}_n$, we similarly define $L_{\mathrm{Id},1}$ (respectively, $L_{\mathrm{Id},2}$) as the number of lifts M_{n+1} of Id_n to $\pi_1(G)(n+1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1})$ equals 1 (respectively, 2).

Proposition 40. *With the notation of Definition 39, the numbers L_1, L_2 do not depend on n nor on M_n, while $L_{\mathrm{Id},1}$, $L_{\mathrm{Id},2}$ do not depend on n. 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	$\ell^4-\ell^3$
(Normalizer of) split Cartan	$2(\ell-1)$	$(\ell-1)^2$	ℓ	$\ell^2-\ell$
(Normalizer of) nonsplit Cartan	0	ℓ^2-1	ℓ	$\ell^2-\ell$

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

$$1 + L_{\mathrm{Id},1} + L_{\mathrm{Id},2} \qquad \text{and} \qquad L_1 + L_2 \qquad \text{respectively}\,. \tag{7}$$

This number is ℓ^4 for $\mathrm{GL}_2(\mathbb{Z}_\ell)$, while in the other cases it is the cardinality of the tangent space from [LP17], namely ℓ^2. □

5.5. **Computation of $\mu(E_{n,M_{n_0}})$ for GL_2 and normalizers of unramified Cartan subgroups.** In this section, we suppose that $\pi_1(G)$ has finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or in the normalizer of an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and we consider the group $H := [\ell^{n_0-1}]\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$. We make use of the rational number $c_{M_{n_0}}$ from Definition 38. We compute the Haar measure of the set $E_{n,M_{n_0}}$ defined in (5).

Lemma 41. *If H is cyclic, then for $n \geq n_0$ we have*

$$\mu(E_{n,M_{n_0}}) = \begin{cases} 0 & \text{if } rk_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 2 \\ \frac{c_{M_{n_0}} \cdot L_1^{-n_0} L_2}{R_1(n_0)\ell^{(1-n_0)d_G}} \cdot (L_1 \ell^{-d_G})^n & \text{if } rk_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 1 \\ D_1 \cdot (\ell^{-d_G})^n + D_2 \cdot (L_1^{-n_0}(\ell^{-d_G} L_1)^n - (\ell^{-d_G})^n) & \text{if } rk_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 0, \end{cases}$$

with $D_1 = \frac{(1-\frac{1}{\ell})L_{\mathrm{Id},2}}{R_1(n_0)\ell^{(1-n_0)d_G}}$ *and* $D_2 = \frac{(1-\frac{1}{\ell})(L_{\mathrm{Id},1} - \#H')L_2}{R_1(n_0)\ell^{(1-n_0)d_G}(L_1-1)}$.

Proof. The first case follows from Remark 33. In the second case, the number of lifts M_{n+1} in $\pi_1(G)(n+1)$ of M_{n_0} 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 $L_1^{n-n_0} \cdot L_2$. Moreover, $\#\pi_1(G)(n+1) = R_1(n_0)\ell^{(n+1-n_0)d_G}$, so we may conclude. Finally, suppose that $M_{n_0} = \mathrm{Id}_{n_0}$.

If H is trivial, we conclude because $\mu(E_{n,M_{n_0}}) = 0$ for all $n \geq n_0$ by Remark 37. Now suppose that H 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 and by Remark 37 the proportion of $v_n \in \pi_2(\pi_1^{-1}(\mathrm{Id}_n))$ such that $[\ell^{n-1}]v_n \neq 0$ is $1 - \frac{1}{\ell}$, so we have

$$\mu(E'_{n,\mathrm{Id}_{n_0}}) = \frac{(1-\frac{1}{\ell})L_{\mathrm{Id},2}}{R_1(n_0)\ell^{(1-n_0)d_G}} \cdot (\ell^{-d_G})^n = D_1 \cdot (\ell^{-d_G})^n .$$

Now we study $E''_{n,\mathrm{Id}_{n_0}}$ and partition this set according to the largest $r \in \{n_0, \ldots, n-1\}$ such that $M \equiv \mathrm{Id}_r \bmod \ell^r$. 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 36. 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 35 (recall that for elements such that $\mathrm{Im}(M_{r+1} - \mathrm{Id}_{r+1}) = H$, this proportion is 0). We may conclude because we have

$$\mu(E''_{n,\mathrm{Id}_{n_0}}) = \frac{(1-\frac{1}{\ell}) \sum_{r=n_0}^{n-1} (L_{\mathrm{Id},1} - \#H')L_1^{n-(r+1)}L_2}{R_1(n_0)\ell^{(n+1-n_0)d_G}} = D_2(L_1^{-n_0}(\ell^{-d_G}L_1)^n - (\ell^{-d_G})^n).$$

□

Lemma 42. *If H is not cyclic, then for $n \geq n_0$ we have*

$$\mu(E_{n,M_{n_0}}) = \begin{cases} 0 & \text{if } rk_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 2 \\ \frac{\frac{\ell-1}{\ell} \cdot L_1^{-n_0} L_2}{R_1(n_0)\ell^{(1-n_0)d_G}} \cdot (L_1 \ell^{-d_G})^n & \text{if } rk_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 1 \\ \frac{L_{\mathrm{Id},2}\frac{\ell^2-1}{\ell^2} + L_{\mathrm{Id},1}L_2\frac{\ell-1}{\ell}(L_1^{n-n_0}-1)/(L_1-1)}{R_1(n_0)(\ell^{d_G})^{n-n_0+1}} & \text{if } rk_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 0 \end{cases}$$

and, 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 case $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 2$ still follows from Remark 33. For M_{n_0} such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 1$, we may argue as in the previous lemma with $c_{M_{n_0}} = \frac{\ell^2-\ell}{\ell^2} = \frac{\ell-1}{\ell}$.

Now suppose that $M_{n_0} = \mathrm{Id}_{n_0}$. There are $L_{\mathrm{Id},2}$ lifts $M_{n+1} \in \pi_1(G)(n+1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ and $M_n = \mathrm{Id}_n$. 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 37. Now fix $n_0 \leq r < n$. The number of matrices $M_{n+1} \in \pi_1(G)(n+1)$ 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 $\sum_{r=n_0}^{n-1} L_1^{n-r-1} = (L_1^{n-n_0}-1)/(L_1-1)$). For these elements M_{n+1}, the proportion of $v_n \in \pi_2(\pi_1^{-1}(M_n))$ such that $[\ell^{n-1}]v_n \notin \mathrm{Im}(M_n - \mathrm{Id}_n)$ is $\frac{\ell-1}{\ell}$ by Lemma 35.

To obtain $\mu(E_{n_0+h})$, we sum $\mu(E_{n_0+h,\mathrm{Id}_{n_0}})$ and $\mu(E_{n_0+h,M_{n_0}})$ by varying M_{n_0} such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 1$, the number of such matrices being $R_1'(n_0)$. □

5.6. Computation of $\mu(E_{n,M_{n_0}})$ for normalizers of ramified Cartan subgroups, ℓ odd.

In this section ℓ is odd, and $\pi_1(G)$ has finite index in the normalizer of a ramified Cartan subgroup. Let

$$C = \left\{ \begin{pmatrix} \alpha & d\beta \\ \beta & \alpha \end{pmatrix} : v_\ell(\alpha^2 - d\beta^2) = 0 \right\}$$

be a ramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with $\ell \mid d$. As in Section 2.3, we call $v := v_\ell(d)$. Let C' be the complement of C in its normalizer N. We recall that $C(n)$ and $C'(n)$ are defined as the reductions of C and C' modulo ℓ^n. We let $M_{n_0} \in \pi_1(G)(n_0)$.

Remark 43. 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 $s = \sum\limits_{i=0}^{+\infty} s_i\ell^i$. 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 $s_{N-2\nu}$).

Lemma 44. *Suppose that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n_0} - \mathrm{Id}_{n_0}) = 1$, and write*

$$M_{n_0} - \mathrm{Id}_{n_0} = \begin{pmatrix} \alpha_{n_0} - 1 & d\beta_{n_0} \\ \beta_{n_0} & \alpha_{n_0} - 1 \end{pmatrix}.$$

There is a rational constant $D_{M_{n_0}}$ such that $\mu(E_{n,M_{n_0}}) = D_{M_{n_0}} \cdot \ell^{-n}$ for all $n \geq n_0$ such that $n > v_\ell(\beta_{n_0}) + v$.

Proof. If $M_{n_0} \in C'(n_0)$, then for all $n \geq n_0$ we have

$$\mu(E_{n,M_{n_0}}) = c_{M_{n_0}} \frac{\ell^{n-n_0}(\ell^2-\ell)}{\#\pi_1(G)(n+1)} = \left(\frac{c_{M_{n_0}}(\ell^2-\ell)\ell^{n_0-2}}{R_1(n_0)}\right)\ell^{-n}.$$

This is because for $n_0 \leq n' \leq n$ the number of lifts $M_{n'+1} \in C'(n')$ 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 58).

If $M_{n_0} \in C(n_0)$, set $b := v_\ell(\beta_{n_0}) < n_0$. Let n_1 be such that $b < n_1 - v$ (in particular, $d \not\equiv 0 \bmod \ell^{n_1-b}$). Then, $E_{n,M_{n_0}}$ 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

$$M_{n_1} - \mathrm{Id}_{n_1} = \begin{pmatrix} \alpha_{n_1}-1 & d\beta_{n_1} \\ \beta_{n_1} & \alpha_{n_1}-1 \end{pmatrix} \qquad \text{with } v_\ell(\beta_{n_1}) = b\,.$$

Let $n \geq n_1$ and consider a lift $M_n \in C(n)$ of M_{n_1} (obtained with lifts α_n, β_n of $\alpha_{n_1}, \beta_{n_1}$) such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$. By comparing the valuations of the elements, its 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 43 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. 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 $\mu(E_{n,M_{n_1}}) = D'_{M_{n_1}}\ell^{-n}$ for a rational constant $D'_{M_{n_1}}$ which doesn't depend on n. We may conclude because

$$\mu(E_{n,M_{n_0}}) = \sum_{M_{n_1} \equiv M_{n_0} \bmod \ell^{n_0}} \mu(E_{n,M_{n_1}}) = \left(\sum_{M_{n_1} \equiv M_{n_0} \bmod \ell^{n_0}} D'_{M_{n_1}}\right) \cdot \ell^{-n}.$$

□

Lemma 45. *There are two rational constants $D_{\mathrm{Id}_{n_0}}$ and $D'_{\mathrm{Id}_{n_0}}$ such that for every $n \geq n_0$ we have*

$$\mu(E_{n,\mathrm{Id}_{n_0}}) = D_{\mathrm{Id}_{n_0}} \cdot \ell^{-2n} + D'_{\mathrm{Id}_{n_0}} \cdot \ell^{-n}.$$

Proof. Consider the matrices $M_n \in \pi_1(G)(n)$ 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

$$M_n - \mathrm{Id}_n \equiv \begin{pmatrix} 0 & 0 \\ \beta_{n'} & 0 \end{pmatrix} \bmod \ell^{n'} \text{ for some } \beta_{n'} \neq 0$$

and the proportion (that we call c') of $v_n \in \pi_2(\pi_1^{-1}(M_n))$ such that $[\ell^{n-1}]v_n \notin \mathrm{Im}(M_n - \mathrm{Id}_n)$ does not depend on $n \geq n_0$ and does not depend on M_n. The former property follows from Lemma 34, 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 $\begin{pmatrix} \ell x \\ y \end{pmatrix} \in (\mathbb{Z}/\ell^{n_0}\mathbb{Z})^2$ while $\pi_2(\pi_1^{-1}(M_{n'}))$ is the preimage under the multiplication by $\ell^{n'-n_0}$ of $\pi_2(\pi_1^{-1}(\mathrm{Id}_{n_0}))$ (the dependency on n' disappears in the ratio).

For the case $M_n = \mathrm{Id}_n$, the proportion (that we call c_{Id}) of $v_n \in \pi_2(\pi_1^{-1}(\mathrm{Id}_n))$ such that $[\ell^{n-1}]v_n \neq 0$ does not depend on $n \geq n_0$.

Then it remains to study the set of elements $M_{n+1} \in \pi_1(G)(n+1)$ such that

$$\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2, \;\; \mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) \leq 1, \;\;\; M_{n_0} = \mathrm{Id}_{n_0} \,.$$

Write $M_{n+1} = \begin{pmatrix} \alpha_{n+1} & d\beta_{n+1} \\ \beta_{n+1} & \alpha_{n+1} \end{pmatrix}$ and set $b := v_\ell(\beta_{n+1})$. 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 $A_n \in \pi_1(G)(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(A_n - \mathrm{Id}_n) = 1$ and $A_{n_0} = \mathrm{Id}_{n_0}$. 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 $M_{n_0} = \mathrm{Id}_{n_0}$ is then equal to $S(n) \cdot \ell^2 - S(n+1)$.

We first fix $b < n - v$. 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 60 (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 number of matrices that fall in Case (1) of Lemma 60 is then $S_1(n) = \ell^v - 1$. The matrices that fall in Case (2) of Lemma 60 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 $S(n) = S_1(n) + S_2(n) + S_3(n)$ 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 know that $\#\pi_1(G)(n+1) = \#\pi_1(G)(n_0) \cdot \ell^{2(n+1-n_0)}$. We may then conclude because

$$\mu(E_{n,\mathrm{Id}_{n_0}})(\#\pi_1(G)(n_0))^{-1}\ell^{-2(n+1-n_0)} \cdot (c'(S(n)\ell^2 - S(n+1)) + c_{\mathrm{Id}}(\ell^2 - \ell)) \,.$$

□

5.7. **Computation of $\mu(E_{n,M_{n_0}})$ for normalizers of ramified Cartan subgroups, $\ell = 2$.**

In this section, we let $\pi_1(G)$ be a finite index subgroup in the normalizer of a ramified Cartan subgroup C with $\ell = 2$. The parameter d from Section 2.3 can be even or odd. If d is even, we can mimic some arguments of Lemma 44.

Lemma 46. *There are two rational constants $D_{\mathrm{Id}_{n_0}}$ and $D'_{\mathrm{Id}_{n_0}}$ such that for $n \geq n_0 + 3$ we have*

$$\mu(E_{n,\mathrm{Id}_{n_0}}) = D_{\mathrm{Id}_{n_0}} \cdot 2^{-2n} + D'_{\mathrm{Id}_{n_0}} \cdot 2^{-n} \,.$$

Proof. Suppose first that d is even. We may reason as for Lemma 45, applying Lemma 62 in place of Lemma 60: 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 60 is replaced by Cases (3.1), (3.2), and (3.3) of Lemma 62 (and the last two cases may occur or not depending on d).

Now suppose that d is odd. Consider the matrices $M_n \in \pi_1(G)(n)$ such that $M_{n_0} = \mathrm{Id}_{n_0}$. 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 as in the proof of Lemma 45 and $\#\pi_1(G)(n+1) = \#\pi_1(G)(n_0) \cdot 2^{2(n+1-n_0)}$. 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 45 we deduce that, fixing M_n, the proportion of $(M_n, v_n) \in G(n)$ such that $[2^{n-1}]v_n \notin \mathrm{Im}(M_n - \mathrm{Id}_n)$ is a constant c' independent of n and M_n. We let $\widetilde{E}_{n,\mathrm{Id}_{n_0}}$ be the set of elements $M_{n+1} \in \pi_1(G)(n+1)$ such that

$$\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2, \quad \mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1 \text{ and } M_{n_0} = \mathrm{Id}_{n_0} .$$

We have $\#\widetilde{E}_{n,\mathrm{Id}_{n_0}} = 4S(n) - S(n+1)$, where $S(n)$ is as in the proof of Lemma 45 (with the notation of that lemma, we partition the matrices according to $b := v_2(\beta_n)$). Moreover, we have

$$\mu(E_{n,\mathrm{Id}_{n_0}}) = (\pi_1(G)(n_0))^{-1} \cdot 2^{-2(n+1-n_0)} \cdot (c' \cdot \#\widetilde{E}_{n,\mathrm{Id}_{n_0}} + 2c_{\mathrm{Id}}).$$

From the proof of Lemma 65, 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 1 if $n - b = 1$, is 4 if $n - b = 2$ and $d \equiv 1 \bmod 4$, and is 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 at least 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 that are independent of n. □

Remark 47. 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 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 48. *If d is even and $M_{n_0} \neq \mathrm{Id}_{n_0}$, there is a rational constant $D_{M_{n_0}}$ such that for $n \gg 0$ we have $\mu(E_{n,M_{n_0}}) = D_{M_{n_0}} \cdot 2^{-n}$.*

Proof. Suppose first that $M_{n_0} \in C'(n_0)$. We refer to the proof of Lemma 64.

If $v_2(\beta_{n_0}) < v_2(\alpha_{n_0}+1)$, then there is k_{n_0} such that

$$(\alpha_{n_0}, \beta_{n_0}) = \left(\frac{1+k_{n_0}^2 d}{1-k_{n_0}^2 d}, \frac{2k_{n_0}}{1-k_{n_0}^2 d}\right)$$

and the lifts M_n of M_{n_0} such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ correspond to lifts k_n of k_{n_0}. So there are 2^{n+1-n_0} matrices $M_{n+1} \in \pi_1(G)(n+1)$ lifting M_{n_0} such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$.

If $v_2(\beta_{n_0}) = 0$, then $\alpha_{n_0}^2 = 1 + d\beta_{n_0}^2$ and, for $n \geq n_0$, a lift M_n of M_{n_0} satisfies $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ if and only if $\alpha_n^2 = 1 + d\beta_n^2$. Set $n_1 := \max(3, n_0)$ and take M_{n_1} such that $\mathrm{rk}_{2\mathbb{Z}}(M_{n_1} - \mathrm{Id}_{n_1}) = 1$ (if there is no such M_{n_1}, then $\mu(E_{n,M_{n_0}}) = 0$ for $n \geq n_1$). For $n \geq n_1$, if $\alpha_n^2 = 1 + d\beta_n^2$, then $\alpha_{n+1}^2 = 1 + d\beta_{n+1}^2$ for all lifts $(\alpha_{n+1}, \beta_{n+1})$ of (α_n, β_n) or for none of them. If $\alpha_{n_1+1}^2 \neq 1 + d\beta_{n_1+1}^2$ for all lifts of $(\alpha_{n_1}, \beta_{n_1})$, then $\mu(E_{n,M_{n_1}}) = 0$ for every $n > n_1 + 1$. Assume that $\alpha_{n_1+1}^2 = 1 + d\beta_{n_1+1}^2$ for all lifts of $(\alpha_{n_1}, \beta_{n_1})$ (which implies that $d \equiv 0 \bmod 8$). Then, first choosing a lift β_{n_1+1} of β_{n_1}, there is exactly one way to lift α_{n_1} such that $\alpha_{n_1+2}^2 = 1 + d\beta_{n_1+2}^2$ for all lifts $(\alpha_{n_1+2}, \beta_{n_1+2})$ of $(\alpha_{n_1+1}, \beta_{n_1+1})$. Indeed, as $d \equiv 0 \bmod 8$, the value of $1 + d\beta_{n_1+2}^2$ is independent of the lift β_{n_1+2} of β_{n_1}. Call D a square root of $1 + d\beta_{n_1+2}^2$. Then, for $n = n_1, n_1+1, n_1+2$, the four square roots of $1 + d\beta_n^2$ are $D \bmod 2^n$, $-D \bmod 2^n$, $(D \bmod 2^n) \cdot (1 + 2^{n-1})$, $(-D \bmod 2^n) \cdot (1 + 2^{n-1})$ and for $n = n_1, n_1+1$, only the two first ones are liftable to a square root of $1 + d\beta_{n+1}^2$ modulo 2^{n+1} (and the sign is determined by α_{n_1}). Repeating this argument, for $n > n_1$ the number of elements M_{n+1} above M_{n_1} such that $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ and $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ is 2^{n+1-n_1}.

If $0 < v_2(\beta_{n_0}) < v_2(\alpha_{n_0}+1)$, then (with the notation of the proof of Lemma 64) a matrix M_n above M_{n_0} has $2\mathbb{Z}$-rank equal to 1 if and only if $a'^2 - a' \equiv db'^2 \bmod 2^{n-1}$. To choose a lift M_{n+1} of M_n of $2\mathbb{Z}$-rank equal to 1, one might first lift b' to b'_{n+1}, which fixes a'_{n+1} through the condition $a'^2_{n+1} - a'_{n+1} \equiv db'^2_{n+1} \bmod 2^n$ (and we can check that a'_{n+1} is a lift of a'). So the number of elements M_{n+1} above M_{n_1} such that $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ and $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ is 2^{n+1-n_0}.

Now suppose that $M_{n_0} \in C(n_0)$ and write

$$M_{n_0} - \mathrm{Id}_{n_0} = \begin{pmatrix} \alpha_{n_0} - 1 & d\beta_{n_0} \\ \beta_{n_0} & \alpha_{n_0} - 1 \end{pmatrix} \quad \text{and} \quad b := v_2(\beta_{n_0}) < n_0.$$

We may restrict to consider $n > n_1$ and $\mu(E_{n,M_{n_1}})$, where $n_1 \geq n_0$ is such that $b < n_1 - 2\nu$, $n_1 - 2\nu \geq 2$ and M_{n_1} varies in the finitely many lifts of M_{n_0} modulo ℓ^{n_1}. We write

$$M_{n_1} - \mathrm{Id}_{n_1} = \begin{pmatrix} \alpha_{n_1} - 1 & d\beta_{n_1} \\ \beta_{n_1} & \alpha_{n_1} - 1 \end{pmatrix} \quad \text{with} \quad v_2(\beta_{n_1}) = b\,.$$

As in the proof of Theorem 44, knowing the entries (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 47 to lift $k_{n_1} \bmod 2^{n_1-b}$: with its notation, 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 $n \gg 0$ 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 47 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 it 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 38, we deduce that $\mu(E_{n,M_{n_1}})$ is a constant times 2^{-n} and we conclude. □

Lemma 49. *If d is odd and $M_{n_0} \neq \mathrm{Id}_{n_0}$, there is a rational constant $D_{M_{n_0}}$ such that for $n \gg 0$ we have $\mu(E_{n,M_{n_0}}) = D_{M_{n_0}} \cdot 2^{-n}$.*

Proof. We first consider the case $M_{n_0} \in C(n_0)$. With the notation from Section 2.3, 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 65. 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 $k_n \bmod 2^n$. By Remark 47, $k_n \bmod 2^n$ 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 matrices $M_{n+1} \in C(n+1)$ above M_{n_0} with $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ is 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 refer to the proof of Lemma 65 and the corresponding notation. If α_n is odd and β_n is even, these numbers are parametrized by k_n (and for two out of the four lifts of k_n we preserve the property that the $2\mathbb{Z}$-rank is 1). We deduce that there are 2^{n+1-n_0} matrices $M_{n+1} \in C'(n+1)$ above M_{n_0} such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $\mathrm{rk}_{2\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$. 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 and we may reason as in Lemma 48. □

5.8. **The rationality of the natural density for Condition** (2).

We can finally prove that for any finite non-empty set L of primes, $\mathrm{dens}_{\exp}(L)$ is a rational number. We keep the above notation.

Proof of Theorem 3 (where the base field can be any number field K). By Remark 29, the existence of the density is guaranteed. It therefore suffices to prove that this density is rational.

Suppose first that $L = \{\ell\}$. The sets E_n are pairwise disjoint, each of them admits a Haar measure which is a rational number (because they are the preimage in G of a subset of $G(n+1)$) and we have $\mu(\cup_{m\geq n} E_m) \to 0$ for $n \to \infty$ by Proposition 28. So we have

$$\mathrm{dens}_{\exp}(\ell) = \sum_{n\geq 1} \mu(E_n)\,.$$

For every $1 \leq n < n_0$, $\mu(E_n)$ is a rational number, so we may restrict to $n \geq n_0$. In turn, by (6) it suffices to show that for every $M_{n_0} \in \pi_1(G)(n_0)$ the sum $\sum\limits_{n \geq n_0} \mu(E_{n,M_{n_0}})$ is rational. This is the case because by Lemmas 41, 42 (for $\pi_1(G)$ having finite index in GL_2 or in an unramified Cartan) by Lemmas 44, 45 (for $\pi_1(G)$ having finite index in a ramified Cartan with ℓ odd) and by Lemmas 46, 48, 49 (for $\pi_1(G)$ having finite index in a ramified Cartan with $\ell = 2$), up to a finite number of rational terms, this is a sum of finitely many geometric series with rational ratios.

Now let $L = \{\ell_1, \dots, \ell_r\}$ and set $m = \prod_{i=1}^r \ell_i$. By Proposition 7 we may select n_0 such that the image of the m-adic torsion-Kummer representation is the preimage of the image of the $\bmod m^{n_0}$ torsion-Kummer representation. We then partition the primes $\mathfrak{p}$ according to the $\bmod m^{n_0}$ torsion representation. This is a finite partition, so it suffices to fix a matrix A in the image of the $\bmod m^{n_0}$ torsion representation and prove the existence and rationality of the restricted natural density. Calling A_i the image of A in the $\bmod \ell_i^{n_0}$ torsion representation, the restricted natural density considering only the prime ℓ_i (and the matrix A_i) exists and it is rational by the first part of the proof. We conclude because (by the definition of n_0) we are asking for the existence and rationality of the Haar measure of a set that is the product of its projections, each of which admits a rational Haar measure with respect to the ambient group of the projection. □

Theorem 50. *Suppose that E is without CM, or that it has CM defined over K. We assume the Exponential LT conjecture for $S = \mathcal{P}$. Let B be a positive integer 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. Calling L_B the set of prime divisors of B we have*

$$\mathrm{dens}_{\exp}(\mathcal{P}) = \mathrm{dens}_{\exp}(L_B) \cdot \prod_{\ell \in \mathcal{P} \setminus L_B} \mathrm{dens}_{\exp}(\ell)\,. \tag{8}$$

Moreover, there exists a rational number Q such that the following holds: if E is without CM, then

$$\mathrm{dens}_{\exp}(\mathcal{P}) = Q \cdot \prod_{\ell \in \mathcal{P}} \Big(1 - \frac{\ell^5 - \ell^3 - \ell^2 - 1}{\ell^7 - \ell^6 - \ell^3 + \ell^2}\Big)$$

while if E has CM defined over K, then we have

$$\mathrm{dens}_{\exp}(\mathcal{P}) = Q \cdot \prod_{\ell \in \mathrm{SplitCM}} \Big(1 - \frac{2\ell^3 - 2\ell^2 - \ell - 1}{(\ell+1)(\ell-1)^2\ell^2}\Big) \cdot \prod_{\ell \in \mathrm{InertCM}} \Big(1 - \frac{1}{(\ell+1)(\ell-1)\ell^2}\Big)\,.$$

Proof. The proof is analogous to the one of Theorem 22, making use of Theorem 3 in place of Proposition 19. The local densities are computed in Examples 66, 67 and 68 in Appendix B. □

Proof of Theorem 4. This is a special case of Theorem 50. □

In the following result we write $\mathrm{dens}_{\exp,K'}$ to specify the base field K'. Moreover, we write $\mathrm{dens}_{\exp,\mathrm{Split}}$ (respectively, $\mathrm{dens}_{\exp,\mathrm{Inert}}$) if we restrict to the primes of K that split (respectively, are inert) in K'.

Lemma 51. *Suppose that E has CM that is not defined over K but over a quadratic extension K' of K. Let S be a non-empty set of prime numbers and assume the Exponent LT conjecture* *for S over K and over K'. The set of primes $\mathfrak{p}$ of K that split (respectively, are inert) in K' and that satisfy Condition (2) for all $\ell \in S$ has a natural density and we have*

$$\mathrm{dens}_{\exp}(S) = \mathrm{dens}_{\exp,\mathrm{Split}}(S) + \mathrm{dens}_{\exp,\mathrm{Inert}}(S)\,.$$

Moreover, we have

$$\mathrm{dens}_{\exp,\mathrm{Split}}(S) = \frac{1}{2}\,\mathrm{dens}_{\exp,K'}(S)$$

and the existence of one of these two densities implies the existence of the other.

Proof. The argument is similar to that of Lemma 23. □

Theorem 52. *Suppose that E has CM that is not defined over K but over a quadratic extension K' of K. We assume the Exponent LT conjecture for $S = \mathcal{P}$ over K and over K'. Then there exist two rational numbers Q_1 and Q_2 such that*

$$\mathrm{dens}_{\exp,\mathrm{Split}}(\mathcal{P}) = Q_1 \cdot \prod_{\ell\in \mathrm{SplitCM}} \Big(1 - \frac{2\ell^3-2\ell^2-\ell-1}{(\ell+1)(\ell-1)^2\ell^2}\Big) \cdot \prod_{\ell \in \mathrm{InertCM}} \Big(1 - \frac{1}{(\ell+1)(\ell-1)\ell^2}\Big)$$

and

$$\mathrm{dens}_{\exp,\mathrm{Inert}}(\mathcal{P}) = Q_2 \cdot \prod_{\ell\in \mathrm{SplitCM}} \Big(1 - \frac{1}{\ell(\ell-1)}\Big) \cdot \prod_{\ell\in \mathrm{InertCM}} \Big(1 - \frac{1}{\ell(\ell-1)}\Big)\,.$$

Proof. The argument is similar to that of Theorem 24. For $\mathrm{dens}_{\exp,\mathrm{Split}}$ we can make use of Theorem 50 and Lemma 51. We now explain how to compute the factors for $\mathrm{dens}_{\exp,\mathrm{Inert}}$. We work in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Recall from Section 2.3 that for $\ell \gg 0$ the image of the ℓ-adic torsion representation is the normalizer of a Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. We call C' the complement of the Cartan subgroup C in its normalizer, see Section 2.3.

Assume that C is split. By Proposition 18, the number of elements M_1 in the normalizer of the Cartan such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1)$ is $3\ell - 5$ and the number of elements $M_1 \in C(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 1$ is $2\ell - 4$, so $M_1 \in C'(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 1$ is $\ell - 1$. Then, the number of elements $M_1 \in C'(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2$ is $(\ell-1)^2 - (\ell-1)$. So, with the notation of Section 4 (but measuring only the Galois automorphisms stemming from the complement of the Cartan and also restricting the ambient space to this complement) we have

$$\begin{aligned}\mathrm{dens}(S_{\exp,0}) &= \frac{(\ell-1)^2-(\ell-1)}{(\ell-1)^2}\\ &= 1 - \frac{1}{\ell-1}.\end{aligned}$$

The number of elements $M_{n+1} \in C'(n+1)$ 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 $(\ell-1)L_1^{n-1}L_2$, and hence for $n \geq 1$,

$$\begin{aligned}\mathrm{dens}(S_{\exp,n}) &= \frac{\frac{\ell-1}{\ell}\cdot(\ell-1)L_1^{n-1}L_2}{(\ell-1)^2\cdot \ell^{2n}}\\ &= \frac{\ell-1}{\ell}\cdot\frac{1}{\ell^n}.\end{aligned}$$

Summing the above contributions gives

$$\begin{aligned}\operatorname{dens}(S_{\exp}) &= \operatorname{dens}(S_{\exp,0}) + \sum_{n\geq 1}\operatorname{dens}(S_{\exp,n})\\ &= 1 - \frac{1}{\ell-1} + \frac{\ell-1}{\ell}\cdot\frac{1}{\ell-1}\\ &= 1 - \frac{1}{\ell(\ell-1)}.\end{aligned}$$

When C is nonsplit, Proposition 18 gives that the number of $M_1 \in C'(1)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 2$ is $\ell^2 - 1 - (\ell+1)$, so we have

$$\begin{aligned}\operatorname{dens}(S_{\exp,0}) &= \frac{\ell^2-1-(\ell+1)}{\ell^2-1}\\ &= 1 - \frac{1}{\ell-1}\end{aligned}$$

The number of $M_{n+1} \in C'(n+1)$ 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 $(\ell+1)L_1^{n-1}L_2$ so for $n \geq 1$ we have

$$\begin{aligned}\operatorname{dens}(S_{\exp,n}) &= \frac{\frac{\ell-1}{\ell}\cdot(\ell+1)L_1^{n-1}L_2}{(\ell^2-1)\cdot\ell^{2n}}\\ &= \frac{\ell-1}{\ell}\cdot\frac{1}{\ell^n}.\end{aligned}$$

Summing the above contributions gives $\operatorname{dens}(S_{\exp}) = 1 - \frac{1}{\ell(\ell-1)}$.

□

Appendix A. On the $\ell\mathbb{Z}$-rank of matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$

In this appendix, we prove Proposition 40. Let G_ℓ be $\mathrm{GL}_2(\mathbb{Z}_\ell)$, an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or the normalizer of an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Given a matrix $M_n \in G_\ell \bmod \ell^n$ with $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$, for $i = 1, 2$ we let L_i be the number of its lifts $M_{n+1} \in G_\ell \bmod \ell^{n+1}$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = i$. Moreover, if $M_n = \mathrm{Id}_n$ we similarly define $L_{\mathrm{Id},i}$, see Definition 39.

We remark that L_1 can be obtained from L_2 and conversely (respectively, $L_{\mathrm{Id},1}$ can be obtained from $L_{\mathrm{Id},2}$ and conversely) by (7).

For ramified Cartan subgroups, the quantities $L_1, L_2, L_{\mathrm{Id},1}, L_{\mathrm{Id},2}$ are not well-defined, but we give the counts to calculate the quantities

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

and

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

which can be used to compute $\mu(E_n)$ through Proposition 31. We also give ingredients to prove some of the lemmas of Section 5.

The following remark will be very useful for the case of ramified Cartan subgroups (paragraphs A.5 and A.6).

Remark 53. 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. The number of square roots of d in $\mathbb{Z}/\ell^m\mathbb{Z}$ is as follows:

$$\begin{cases} 2\ell^\nu & \text{if } \ell \text{ is odd} \\ 2^\nu & \text{if } \ell = 2 \text{ and } m - 2\nu = 1 \\ 2^{\nu+1} & \text{if } \ell = 2 \text{ and } m - 2\nu = 2 \\ 2^{\nu+2} & \text{if } \ell = 2 \text{ and } m - 2\nu \geq 3\,. \end{cases}$$

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.**

Lemma 54. *If $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$, then $L_{\mathrm{Id},2} = \ell(\ell+1)(\ell-1)^2$ and $L_1 = \ell^3$.*

Proof. We have $L_{\mathrm{Id},2} = \ell(\ell+1)(\ell-1)^2$. Indeed, 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 now 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. □

A.2. **Lifts in (the normalizer of) a split Cartan.**

Lemma 55. *If G_ℓ is a split Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or the normalizer $N = C \cup C'$ of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, then $L_{\mathrm{Id},2} = (\ell-1)^2$ and $L_1 = \ell$.*

Proof. We have $L_{\mathrm{Id},2} = (\ell-1)^2$ because choosing a lift $M_{n+1} \in C(n+1)$ above the identity modulo ℓ^n such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_{n+1} - \mathrm{Id}_{n+1}) = 2$ amounts to 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 taken modulo ℓ. 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 in any way (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.**

Lemma 56. *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 $\mathbb{Z}_\ell^\times$). If $G_\ell = C$ or $G_\ell = N = C \cup C'$ is the normalizer of C, then $L_{\mathrm{Id},2} = \ell^2 - 1$ and $L_1 = \ell$.*

We prove that $L_{\mathrm{Id},2} = \ell^2 - 1$. 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 taken from $\mathbb{F}_\ell$. If $a' = b' = 0$, 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 $k^2 d \equiv 1 \bmod \ell$, contradicting that d is not a square modulo ℓ.

We now prove that $L_1 = \ell$. From Proposition 18, all the matrices $M_n \in N(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ are in $C'(n)$.

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, $\alpha_n + 1$ and $\alpha_n - 1$ cannot be both invertible.

Let us assume 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

$$(\alpha_n, \beta_n) = \left(\frac{-1 - k_n^2 d}{k_n^2 d - 1}, \frac{-2k_n}{k_n^2 d - 1} \right) \tag{9}$$

for some $k_n \in \mathbb{Z}/\ell^n\mathbb{Z}$. If (α_n, β_n) are as in (9), 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 (9) for some $k_n \in \mathbb{Z}/\ell^n\mathbb{Z}$. Replacing in (9) 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.

If $\alpha_n + 1$ is not invertible, then $\alpha_n - 1$ must be invertible and a similar same argument applies: 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

$$(\alpha_n, \beta_n) = \left(\frac{d + k_n^2}{k_n^2 - d}, \frac{2k_n}{k_n^2 - d}\right)\,. \tag{10}$$

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 $\ell = 2$.**

Lemma 57. *Let $C = C_{(c,d)}$ be a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$. If $G_2 = C$ or $G_2 = N = C \cup C'$ is the normalizer of C, then $L_{\mathrm{Id},2} = 3$ and $L_1 = 2$.*

Proof. The parameters of C are $c = 1$ and d is odd according to [LP17, Proposition 11]. The elements of C and C' are respectively of the form

$$\begin{pmatrix} \alpha & d\beta \\ \beta & \alpha+\beta \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} \alpha+\beta & (d+1)\beta+\alpha \\ -\beta & -\alpha-\beta \end{pmatrix}\,.$$

The four lifts of Id_n in $C(n+1)$ and $N(n+1)$ are

$$\mathrm{Id}_{n+1}, \begin{pmatrix} 1+2^n & 0 \\ 0 & 1+2^n \end{pmatrix}, \begin{pmatrix} 1 & 2^n d \\ 2^n & 1+2^n \end{pmatrix}, \begin{pmatrix} 1+2^n & 2^n d \\ 2^n & 1 \end{pmatrix}$$

and in particular $L_{\mathrm{Id},2} = 3$. We deduce that a matrix $M_n \in N(n)$ such that $M_n \equiv \mathrm{Id}_1 \bmod 2$ is either Id_n or satisfies $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 2$. 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 $C'(1)$ consists of the elements $M_1 \in N(1)$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_1 - \mathrm{Id}_1) = 1$.

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 $v_2(\beta_n) \geq 1$ because in that case $v_2(\alpha_n+\beta_n-1) = v_2(-\alpha_n - \beta_n - 1) = 0$. Therefore, we cannot 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 $v_2(\alpha_n) = 0$. Since d is odd, we have $v_2((d+1)\beta_n + \alpha_n) = 0$, so $v_2(\alpha_n + \beta_n - 1) \geq v_2((d+1)\beta_n + \alpha_n)$. 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. 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.

If $v_2(\beta_n) > 0$, then k_n must not be invertible. The first row gives

$$\alpha_n(1 - k_n) = \beta_n(k_n d + k_n - 1) + 1$$

so we also deduce that

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

and we can conclude as in the case $v_2(\beta_n) = 0$. *The case $v_2(\alpha_n) \geq 1$ and $v_2(\beta_n) = 0$.* Since $v_2(-\beta_n) < v_2(-\alpha_n - \beta_n - 1)$, 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

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

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.** Let ℓ be odd and consider a ramified Cartan subgroup C with parameters $(0, d)$ such that $\ell \mid d$. 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 58. *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, $\alpha_n + 1$ and $\alpha_n - 1$ cannot be both invertible. Let us 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

$$\left\{ \begin{array}{ll} \alpha_n - 1 & = k_n d\beta_n \\ -\beta_n & = -k_n(\alpha_n + 1). \end{array} \right. \tag{11}$$

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 $C'(n)$ 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 $dk_n^2 \equiv dk_n'^2 \mod \ell^n$ 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.

If $\alpha_n + 1$ is not invertible, then $\alpha_n - 1$ must be 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

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

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 $c_{n+1} \mod \ell$ is a square in $\mathbb{Z}/\ell\mathbb{Z}$. Moreover, the sign choice for α_{n+1} is determined by α_n. □

Remark 59. As seen in the proof of Proposition 18, 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 58 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

$$\left\{ \begin{array}{ll} \beta_n d & = k_n(\alpha_n - 1) \\ \alpha_n - 1 & = k_n\beta_n\,. \end{array} \right. \tag{12}$$

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 $\ell \mid d$.

In Lemma 45, to count the matrices above Id_{n_0}, it is useful to know the number of $M_n \in C(n)$ that satisfy $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ such that $v_\ell(\alpha_n - 1) \geq n_0$ and $v_\ell(\beta_n) \geq n_0$, so we rely on the following result:

Lemma 60. *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 and the element $\begin{pmatrix} \alpha_n & d\beta_n \\ \beta_n & \alpha_n \end{pmatrix}$ is in $C(n)$.

The proof consists in counting the number of solutions of the system (12) imposing the valuations.

Suppose first that $a = n$ (which implies $\beta_n \neq 0$ to avoid $M_n = \mathrm{Id}_n$). The requested condition then amounts to $d\beta_n = 0$, so β_n can be chosen anyway as long as $b \geq n - v$ 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 $a < n$. We have $a = v_\ell(k_n) + b$ (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 (12) 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 53). These values, according to (12) 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 61. Let X_i (for $i = 1, 2, 3$) be the total 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, summed over all possible values of a and b. 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 $X_1 = \sum\limits_{b=n-m}^{n-1} \ell^{n-b-1}(\ell-1) = \ell^m - 1$ 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

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

By Remark 59, there are $2\ell^n$ elements $M_n \in C'(n)$ such that $\mathrm{rk}_{\ell\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$, so 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 representative for $(d \bmod 2^n)$ has this parity for all $n \geq 1$).

Lemma 62. *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, where the parameters a and b are defined as in Lemma 60:*

(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 $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ and $M_n \equiv \mathrm{Id}_n \bmod 2^{n-1}$, so $R''_1(n) = 1$ for C.

Proof. We may proceed as in Lemma 60, applying Remark 53 while taking square roots. □

Remark 63. As in Remark 61, we can compute the quantities X_1, X_2, X_3, which are defined similarly (here, X_3 is the total number of matrices $M_n \in C(n)$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$ from cases (3.1), (3.2) and (3.3)). 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 $X_3 = 0$ if $n - b - 3 < 0$ or if v is not even or $2^{-v}d \bmod 8$ is not a square, else $X_3 = 2^{v/2+n+2}(1 - 2^{-(n-v-2)})$.

Lemma 64. *Assume that d is even and consider the matrices $M_n \in C'(n)$ such that $\mathrm{rk}_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) = 1$. 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 (11) 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 62 and 64 allow us to compute $R_1'(n)$ when d is even. We now take d odd.

Lemma 65. *Assume that d is odd, and consider the matrices $M_n \in N(n)$ such that $rk_{2\mathbb{Z}}(M_n - \mathrm{Id}_n) \leq 1$. 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 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 $2b'$ (there are $4 \cdot 2^{n-1}$ 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. **Examples concerning the Exponent LT condition.** Considering Remark 30 to compute $\mu(E_0)$ and Proposition 40 and Lemma 42 to compute $\mu(E_n)$ for $n \geq 1$, we can evaluate $\mathrm{dens}_{\exp}(\ell)$ if the image of the ℓ-adic torsion-Kummer representation is $G_\ell \ltimes (\mathbb{Z}_\ell)^2$ where G_ℓ is one of the following groups: $\mathrm{GL}_2(\mathbb{Z}_\ell)$, an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or the normalizer of an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

G_ℓ	$\mathrm{GL}_2(\mathbb{Z}_\ell)$	Split Cartan	Nonsplit Cartan	Nor. split Cartan	Nor. non-split Cartan
$\mu(E_0)$	$1-\frac{\ell^2-2}{(\ell-1)^2(\ell+1)}$	$1-\frac{2\ell-3}{(\ell-1)^2}$	$1-\frac{1}{\ell^2-1}$	$1-\frac{3\ell-4}{2(\ell-1)^2}$	$1-\frac{\ell+2}{2(\ell^2-1)}$
$\frac{L_{\mathrm{Id},2}\frac{\ell^2-1}{\ell^2}}{R_1(1)(\ell^d G)^{h+1}}$	$\frac{\ell^2-1}{\ell^6}\cdot\frac{1}{\ell^{4h}}$	$\frac{\ell^2-1}{\ell^4}\cdot\frac{1}{\ell^{2h}}$	$\frac{\ell^2-1}{\ell^4}\cdot\frac{1}{\ell^{2h}}$	$\frac{\ell^2-1}{2\ell^4}\cdot\frac{1}{\ell^{2h}}$	$\frac{\ell^2-1}{2\ell^4}\cdot\frac{1}{\ell^{2h}}$
$\frac{R_1'(1)L_2\frac{\ell-1}{\ell}L_1^h}{R_1(1)(\ell^d G)^{h+1}}$	$\frac{(\ell^3-2\ell-1)}{\ell^3(\ell+1)}\cdot\frac{1}{\ell^h}$	$\frac{2\ell-4}{\ell^2}\cdot\frac{1}{\ell^h}$	0	$\frac{3\ell-5}{2\ell^2}\cdot\frac{1}{\ell^h}$	$\frac{\ell-1}{2\ell^2}\cdot\frac{1}{\ell^h}$
$\frac{L_{\mathrm{Id},1}L_2\frac{\ell-1}{\ell}L_1^h}{(L_1-1)R_1(1)(\ell^d G)^{h+1}}$	$\frac{(\ell+1)(\ell-1)}{\ell^3(\ell^3-1)}\cdot\frac{1}{\ell^h}$	$\frac{2}{\ell^2}\cdot\frac{1}{\ell^h}$	0	$\frac{1}{\ell^2}\cdot\frac{1}{\ell^h}$	0
$\frac{L_{\mathrm{Id},1}L_2\frac{\ell-1}{\ell}}{(L_1-1)R_1(1)(\ell^d G)^{h+1}}$	$\frac{(\ell+1)(\ell-1)}{(\ell^3-1)\ell^3}\cdot\frac{1}{\ell^{4h}}$	$\frac{2}{\ell^2}\cdot\frac{1}{\ell^{2h}}$	0	$\frac{1}{\ell^2}\cdot\frac{1}{\ell^{2h}}$	0
$\sum_{h\geq 0}\frac{L_{\mathrm{Id},2}\frac{\ell^2-1}{\ell^2}}{R_1(1)(\ell^d G)^{h+1}}$	$\frac{1}{\ell^2(\ell^2+1)}$	$\frac{1}{\ell^2}$	$\frac{1}{\ell^2}$	$\frac{1}{2\ell^2}$	$\frac{1}{2\ell^2}$
$\sum_{h\geq 0}\frac{R_1'(1)L_2\frac{\ell-1}{\ell}L_1^h}{R_1(1)(\ell^d G)^{h+1}}$	$\frac{\ell^3-2\ell-1}{\ell^2(\ell-1)(\ell+1)}$	$\frac{2\ell-4}{\ell(\ell-1)}$	0	$\frac{3\ell-5}{2\ell(\ell-1)}$	$\frac{1}{2\ell}$
$\sum_{h\geq 0}\frac{L_{\mathrm{Id},1}L_2\frac{\ell-1}{\ell}L_1^h}{(L_1-1)R_1(1)(\ell^d G)^{h+1}}$	$\frac{\ell+1}{\ell^2(\ell^3-1)}$	$\frac{2}{\ell(\ell-1)}$	0	$\frac{1}{\ell(\ell-1)}$	0
$\sum_{h\geq 0}\frac{L_{\mathrm{Id},1}L_2\frac{\ell-1}{\ell}}{(L_1-1)R_1(1)(\ell^d G)^{h+1}}$	$\frac{\ell}{(\ell^3-1)(\ell^2+1)}$	$\frac{2}{\ell^2-1}$	0	$\frac{1}{\ell^2-1}$	0

Example 66. If the image of the ℓ-adic torsion-Kummer representation is $\mathrm{GL}_2(\mathbb{Z}_\ell)\ltimes(\mathbb{Z}_\ell)^2$, we have

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

Example 67. If the image of the ℓ-adic torsion-Kummer representation is $C\ltimes(\mathbb{Z}_\ell)^2$, where C is a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we have

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

Example 68. If the image of the ℓ-adic torsion-Kummer representation is $C\ltimes(\mathbb{Z}_\ell)^2$, where C is a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we have

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

Example 69. 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

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

Example 70. 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

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

Consider an elliptic curve $E/\mathbb{Q}$ and a point $P \in E(\mathbb{Q})$ of infinite order. We compute $\mathrm{dens}_{\exp}(\ell)$ in some specific examples. The rational densities (computed exactly) have been tested with SageMath [Sag24] by computing the proportion of the suitable primes up to 10^5.

Example 71. Let $E/\mathbb{Q}$ be $y^2 = x^3 - x^2 - 6x$ (LMFDB label 480.b3). The point $P = (-1, 2)$ is not divisible in $E(\mathbb{Q})$. For any odd prime ℓ the ℓ-adic torsion-Kummer representation is surjective (the ℓ-adic torsion representation is surjective according to [LMF25] and we can apply [JR10, Theorem 5.2]). the natural density computed in Example 66 is compared to the experimental natural density considering the primes of good reduction p up to 10^5:

ℓ	$\mathrm{dens}_{\exp}(\ell)$ rounded	experimental
3	0.85694	0.85734
5	0.95234	0.95818
7	0.97674	0.97810
11	0.99099	0.99197

Example 72. Let $E/\mathbb{Q}$ be $y^2 = x^3 - 2x$ (LMFDB label 256.b1). The point $P = (2, 2)$ is not divisible in $E(\mathbb{Q})$. The CM field is $\mathbb{Q}(i)$. For every odd prime ℓ, according to [LMF25], the image of the ℓ-adic representation is the normalizer of a split (respectively, nonsplit) Cartan if $\ell \equiv 1 \bmod 4$ (respectively, $\ell \equiv 3 \bmod 4$). Then by [JR10, Theorem 5.8] the extension $\mathbb{Q}(\frac{1}{\ell^n}P)/\mathbb{Q}(E[\ell^n])$ has maximal degree ℓ^{2n} for every $n \geq 1$. the natural density computed in Examples 69 (respectively, 70) is compared to the experimental natural density considering the primes of good reduction p up to 10^5:

ℓ	$\mathrm{dens}_{\exp}(\ell)$ rounded	experimental
5	0.93458	0.93755
13	0.99086	0.99228
17	0.99470	0.99531

ℓ	$\mathrm{dens}_{\exp}(\ell)$ rounded	experimental
3	0.90972	0.91117
7	0.98788	0.98822
11	0.99542	0.99468

Example 73. Let $E/\mathbb{Q}$ be $y^2 + y = x^3 - 34$ (LMFDB label 225.c1) and let $P = (6, 13)$. According to [LMF25], the image of the 2-adic representation is the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ hence by [JR10, Theorem 5.8] the extension $\mathbb{Q}(\frac{1}{2^n}P)/\mathbb{Q}(E[2^n])$ has maximal degree 2^{2n} for every $n \geq 1$. By Example 70 we have $\mathrm{dens}_{\exp}(2) = 17/24 \approx 0.70833$. The experimental natural density considering the primes of good reduction p up to 10^5 is 0.70938.

Remark 74. Consider a CM elliptic curve E defined over a number field K, and a point $P \in E(K)$ of infinite order. Let ℓ be an odd prime number such that

$$[K(\frac{1}{\ell}P) : K(E[\ell])] = [K(E[\ell^2]) : K(E[\ell])] = \ell^2 \quad \text{and} \quad [K\Big(\frac{1}{\ell}P, E[\ell^2]\Big) : K(E[\ell^2])] = \ell^2 \, .$$

This implies $[K(\frac{1}{\ell^2}P) : K(E[\ell^2])] = \ell^4$ because a subgroup H of $(\mathbb{Z}/\ell^2\mathbb{Z})^2$ such that $[\ell]H = [\ell](\mathbb{Z}/\ell^2\mathbb{Z})^2$ must be $(\mathbb{Z}/\ell^2\mathbb{Z})^2$ (preimages for $(1,0)$ and $(0,1)$ are independent modulo ℓ^2). We then have $[K(\frac{1}{\ell^2}P) : K(\frac{1}{\ell}P)] = \ell^4$ hence by [LP21, Theorem 1.4(ii)] for $n \geq 1$ we have $[K(\frac{1}{\ell^n}P) : K(E[\ell^n])] = \ell^{2n}$.

Example 75. Let $E/\mathbb{Q}$ be $y^2 = x^3 - 735x - 7546$ (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 [GJLRY25, Table 4]). In particular we have $[K(E[9]) : K(E[3])] = 9$. We have checked with [BCP97] that $\mathbb{Q}(\frac{1}{3}P, E[9])/\mathbb{Q}(E[9])$ has degree 9 (the polynomial defining the x-coordinates of $\frac{1}{3}P$ has degree 9 also over $\mathbb{Q}(E[9])$). Then by Remark 74 the extension $\mathbb{Q}(\frac{1}{3^n}P)/\mathbb{Q}(E[3^n])$ has maximal degree 3^{2n} for every $n \geq 1$. By Proposition 18, Lemma 60 and Remark 61, 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 $n > 0$ by Proposition 31 we have

$$\mu(E_n) = \frac{((2 + 2 \cdot 3^n) \cdot 9) - (2 + 2 \cdot 3^{n+1}))\frac{2}{3} + (9 - 3)\frac{8}{9}}{12 \cdot 9^n}.$$

Then $\mathrm{dens}_{\exp}(3) = \sum_{n \geq 0} \mu(E_n) = \frac{3}{4}$.

Finally, the following example supports the Exponent LT conjecture:

Example 76. Let $E/\mathbb{Q}$ be the Serre curve $y^2 = x^3 + 5x + 10$ (LMFDB label 400h1) and let $P = (1, 4)$. For every odd prime ℓ, the ℓ-adic torsion representation is surjective, so is the ℓ-adic torsion-Kummer representation by [JR10, Theorem 5.8]. Moreover, the 2-adic Kummer map is surjective because $\mathbb{Q}(\frac{1}{2}P) \not\subseteq \mathbb{Q}(E[4])$.

We can apply Theorem 84 with ℓ odd and $B = 5$: if m is an odd integer, by Proposition 85, the $\bmod m$ torsion-Kummer representation is surjective.

We impose that $\mathrm{ord}_\ell\big(P \bmod p\big) = \exp_\ell(E(\mathbb{F}_p))$ for every prime $\ell \neq 2$: the conjectural density is

$$\prod_{\substack{\ell \text{ prime} \\ \ell \neq 2}} \left(1 - \frac{\ell^5 - \ell^3 - \ell^2 - 1}{\ell^7 - \ell^6 - \ell^3 + \ell^2}\right) \approx 0.772.$$

The experimental density considering the primes $p < 10^4$ (and $p \neq 2, 5$) is 0.769.

B.2. **Examples concerning the Indivisibility LT condition.** The following examples support the validity of the Indivisibility LT conjecture. We consider an elliptic curve $E/\mathbb{Q}$ and a point $P \in E(\mathbb{Q})$ of infinite order.

Example 77. Let $E/\mathbb{Q}$ be $y^2 = x^3 + x^2 - 9x + 7$ (LMFDB label 128.a1) and consider the point $P = (3, 4)$. Let m be an odd positive squarefree integer. We know that the image of the $\bmod m$ torsion representation is $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. So for any odd prime ℓ the $\bmod \ell$ torsion-Kummer representation is surjective by [JR10, Theorem 5.8]. For any prime divisor ℓ of m we can apply Theorem 84 (with $B = 1$) to ℓ and m/ℓ. Then by Proposition 85 the $\bmod m$ torsion-Kummer representation is surjective.

We impose Condition (3) for $\ell \neq 2$: the conjectural density is

$$\prod_{\substack{\ell \text{ prime} \\ \ell \neq 2}} \mathrm{dens}_{\mathrm{indiv}}(\ell) = \prod_{\substack{\ell \text{ prime} \\ \ell \neq 2}} \left(1 - \frac{\ell^4 - 2\ell^2 - \ell + 1}{\ell^3(\ell-1)(\ell^2-1)}\right) \approx 0.773$$

while the experimental density by considering the primes $p < 10^4$ (and $p \neq 2$) is 0.790.

Example 78. Let $E/\mathbb{Q}$ be $y^2 = x^3 - 9x - 12$ (LMFDB label 7776.m1) and consider the point $P = (4, 4)$. With [BCP97], we found the following (see also [BBP25]): the image of the $\mathrm{mod} 2$ and of the $\mathrm{mod} 3$ torsion-Kummer representations are surjective; the field $\mathbb{Q}(\frac{1}{2}P)$ is contained in $\mathbb{Q}(E[3])$; the image of the $\mathrm{mod} 6$ torsion-Kummer representation has index 24 in $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) \ltimes (\mathbb{Z}/6\mathbb{Z})^2$; up to choosing a suitable basis of $E[6]$, $\mathrm{Gal}(\mathbb{Q}(\frac{1}{6}P)/\mathbb{Q})$ is the subgroup of index 24 of $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) \ltimes (\mathbb{Z}/6\mathbb{Z})^2$ generated by the matrices

$$\begin{pmatrix}1&0&0\\0&1&4\\0&0&1\end{pmatrix}, \begin{pmatrix}1&0&2\\0&1&4\\0&0&1\end{pmatrix}, \begin{pmatrix}5&0&0\\0&5&0\\0&0&1\end{pmatrix}, \begin{pmatrix}5&0&0\\5&1&0\\0&0&1\end{pmatrix} \begin{pmatrix}1&3&0\\1&4&0\\0&0&1\end{pmatrix}, \begin{pmatrix}3&4&3\\2&3&0\\0&0&1\end{pmatrix}, \begin{pmatrix}1&4&0\\4&5&3\\0&0&1\end{pmatrix}.$$

In this subgroup, there are 282 elements (M, v) satisfying $\mathrm{rk}_{\ell\mathbb{Z}}(M - \mathrm{Id}) = 2$ or $v \notin \mathrm{Im}(M - \mathrm{Id})$ for $\ell \in \{2, 3\}$, so $\mathrm{dens}_{\mathrm{indiv}}(6) = \frac{282}{432}$. For any odd positive integer m the $\mathrm{mod} m$ torsion representation is surjective and by [JR10, Theorem 5.8], the $\mathrm{mod} \ell$ torsion-Kummer representation is surjective for any prime $\ell \geq 5$.

We can apply Theorem 84 with $B = 3$: if m is a positive integer coprime to 6, by Proposition 85 the $\mathrm{mod} m$ torsion-Kummer representation is surjective. We prove that the $\mathrm{mod} 6$ torsion-Kummer representation is independent from the $\mathrm{mod} m$ torsion-Kummer representation by showing that $\mathbb{Q}(\frac{1}{m}P)$ and $\mathbb{Q}(\frac{1}{6}P) = \mathbb{Q}(\frac{1}{3}P)$ are linearly disjoint over $\mathbb{Q}$. Considering that the degree of $\mathbb{Q}(\frac{1}{3}P)/\mathbb{Q}$ divides a power of 6, we have

$$\mathbb{Q}\left(\frac{1}{3}P\right) \cap \mathbb{Q}\left(\frac{1}{m}P\right) \subseteq \mathbb{Q}(E[m]).$$

Applying Theorem 84 with $\ell = 3$ and $n = m$ (hence $\gcd(B, n) = 1$) we deduce that

$$\mathbb{Q}\Big(\frac{1}{3}P\Big) \cap \mathbb{Q}(E[3m]) = \mathbb{Q}(E[3])$$

and we conclude because $\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[m]) = \mathbb{Q}$.

Thus, the Indivisible LT conjecture predicts

$$\mathrm{dens}_{\mathrm{indiv}}(\mathcal{P}) = \frac{282}{432} \cdot \prod_{\substack{\ell \text{ prime} \\ \ell \geq 5}} \left(1 - \frac{\ell^4 - 2\ell^2 - \ell + 1}{\ell^3(\ell-1)(\ell^2-1)}\right) \approx 0.588$$

while the experimental natural density considering the primes $p < 10^4$ (and $p \neq 2, 3$) is 0.606.

In this last example the elliptic curve is not defined over $\mathbb{Q}$ so that the CM is defined over the base field:

Example 79. Let $E/\mathbb{Q}(i)$ be $y^2 = x^3 - 2x$, which is a curve with CM defined over $\mathbb{Q}(i)$. 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, $\ell \equiv 3 \bmod 4$). For 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 all odd primes ℓ. The images of the $\mathrm{mod}\ \ell$ representations for the odd primes ℓ are linearly disjoint over K by Remark 80 and by [CP22a, Theorem 1.1] (to apply this result, observe that 2 is the only prime of good reduction and that E has complex multiplication by $\mathbb{Z}[i]$ as the map $(x,y)\to(-x,iy)$ has order 4). We then impose Condition (3) for $\ell\neq 2$: the conjectural natural density is

$$\begin{aligned}\prod_{\substack{\ell \text{ prime}\\ \ell\neq 2}} \mathrm{dens}_{\mathrm{indiv}}(\ell) &= \prod_{\substack{\ell \text{ prime}\\ \ell\equiv 1 \bmod 4}} \left(1-\frac{2\ell^3-2\ell^2-\ell-1}{(\ell+1)(\ell-1)^2\ell^2}\right)\cdot \prod_{\substack{\ell \text{ prime}\\ \ell\equiv 3 \bmod 4}} \left(1-\frac{1}{(\ell+1)(\ell-1)\ell^2}\right)\\ &\approx 0.881\,.\end{aligned}$$

The experimental density, considering the primes in $\mathbb{Q}(i)$ above the rational odd primes $p<3000$, is 0.878.

Remark 80. Let K be a number field, and E/K be an elliptic curve with CM defined over K. Let $P\in E(K)$ be a point of infinite order and ℓ an odd prime number such that $\zeta_\ell\notin K$. Then for any odd squarefree integer n coprime to ℓ we have

$$K\Big(\frac{1}{\ell}P\Big)\cap K(E[n\ell])=K(E[\ell])\,.$$

Indeed, the degree of $K(\frac{1}{\ell}P)/K(E[\ell])$ is a power of ℓ, $K(E[n\ell])/K$ is abelian, and $\zeta_\ell\in K(E[\ell])$: we conclude because by Schinzel's theorem on abelian radical extensions [Sch77, Theorem 2] there cannot be a cyclic extension of $K(\zeta_\ell)$ of degree ℓ which is abelian over K.

Appendix C. One result on entanglement

We prove a result on the entanglement of Kummer extensions that we apply in our examples.

Lemma 81. *Let ℓ be a prime number, and let e be a positive integer. Let m be a positive integer, which is odd if $\ell=2$. Then any normal subgroup of index ℓ^e of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ contains $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.*

Proof. By the Chinese remainder theorem, we may suppose without loss of generality that $m=p^n$ is a prime power. If the assertion does not hold (by restricting the quotient map with respect to the given subgroup) $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ would have a quotient of order a power of ℓ. Since this last quotient is solvable by Burnside's theorem, we deduce that $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ would have a cyclic quotient of order ℓ. By Lemma 83 we deduce that $p=\ell\in\{2,3\}$ so by assumption we are left with the case $p=\ell=3$, which is handled by Lemma 82. □

The following two lemmas have been communicated to us by Hörmann:

Lemma 82. *For $n\geq 1$, a normal subgroup of $\mathrm{GL}_2(\mathbb{Z}/3^n\mathbb{Z})$ whose index is a prime power contains $\mathrm{SL}_2(\mathbb{Z}/3^n\mathbb{Z})$.*

Proof. Call N the normal subgroup, let H be the group of 2×2 matrices over $\mathbb{Z}/3\mathbb{Z}$ and set $H':=\mathrm{Id}+3^{n-1}H<\mathrm{GL}_2(\mathbb{Z}/3^n\mathbb{Z})$. We reason by induction on n, the case $n=1$ following by a direct inspection. Let $n>1$ and consider the following diagram in which we let N_{n-1} be the reduction modulo 3^{n-1} of N:

$$\begin{tikzcd}
N \cap H' \arrow[r, hook] \arrow[d, hook] & N \arrow[r, two heads] \arrow[d, hook] & N_{n-1} \arrow[d, hook] \\
H' \arrow[r, hook] \arrow[d, two heads] & \mathrm{GL}_2(\mathbb{Z}/3^n\mathbb{Z}) \arrow[r, two heads] \arrow[d, two heads] & \mathrm{GL}_2(\mathbb{Z}/3^{n-1}\mathbb{Z}) \arrow[d, two heads] \\
H'/(N \cap H') \arrow[r, hook] & \mathrm{GL}_2(\mathbb{Z}/3^n\mathbb{Z})/N \arrow[r, two heads] & \mathrm{GL}_2(\mathbb{Z}/3^{n-1}\mathbb{Z})/N_{n-1}
\end{tikzcd}$$

The group $\mathrm{SL}_2(\mathbb{Z}/3^n\mathbb{Z})$ acts on H' by conjugation: this action consists in the conjugation by the matrix modulo 3 on H. It also acts on $N \cap H'$ by conjugation. We can identify $N \cap H'$ with a subgroup G of H: the action of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ on G is then a subrepresentation with respect to the action on H. So, if G is a non-trivial proper subgroup of H, it consists of the scalar matrices or of the matrices with trace 0.

By induction hypothesis, we have $\mathrm{SL}_2(\mathbb{Z}/3^{n-1}\mathbb{Z}) \subseteq N_{n-1}$.

If $N \cap H'$ contains $\mathrm{Id} + 3^{n-1}H_0$, we may conclude because of the exact sequence

$$\begin{tikzcd}
\mathrm{Id} + 3^{n-1}H_0 \arrow[r, hook] & \mathrm{SL}_2(\mathbb{Z}/3^n\mathbb{Z}) \arrow[r, two heads] & \mathrm{SL}_2(\mathbb{Z}/3^{n-1}\mathbb{Z})\,.
\end{tikzcd}$$

Now suppose that $N \cap H'$ is contained in the subgroup of the scalar matrices, which implies that the intersection of this group with $\mathrm{Id} + 3^{n-1}H_0$ is trivial. We get

$$\begin{tikzcd}
\{\mathrm{Id} \bmod 3^n\} \arrow[r, hook] \arrow[d, hook] & N \cap \mathrm{SL}_2(\mathbb{Z}/3^n\mathbb{Z}) \arrow[r, two heads, "\sim"] \arrow[d, hook] & \mathrm{SL}_2(\mathbb{Z}/3^{n-1}\mathbb{Z}) \arrow[d, equal] \\
\mathrm{Id} + 3^{n-1}H_0 \arrow[r, hook] & \mathrm{SL}_2(\mathbb{Z}/3^n\mathbb{Z}) \arrow[r, two heads] & \mathrm{SL}_2(\mathbb{Z}/3^{n-1}\mathbb{Z})
\end{tikzcd}$$

Thus the quotient map $\mathrm{SL}_2(\mathbb{Z}/3^n\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/3^{n-1}\mathbb{Z})$ would have a section, which is impossible because the element $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ modulo 3^{n-1} has order 3^{n-1} while modulo 3^n, even multiplied with an element in $\mathrm{Id} + 3^{n-1}H_0$, it has order 3^n. □

Lemma 83. *Let ℓ be a prime, and $n \geq 1$. If there is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ whose quotient is cyclic of prime order p, we must have $p = \ell \in \{2, 3\}$.*

Proof. Call N the normal subgroup. If $\ell \geq 5$ there is a $\alpha \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ such that $\alpha^2 \neq 1 \bmod \ell$. For any $\beta \in (\mathbb{Z}/\ell^n\mathbb{Z})$ we have

$$\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix}\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix}^{-1}\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & (\alpha^2-1)\beta\\ 0 & 1\end{pmatrix}.$$

Thus the matrix $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and similarly $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$ are commutators. Thus $\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is generated by commutators hence does not have any abelian non-trivial quotient. If $\ell \in \{2, 3\}$ we proceed by induction on n. The case $n = 1$ follows by direct inspection. If $n > 1$, let H_0 be the group of 2×2 matrices modulo ℓ with trace zero and consider

$$\begin{tikzcd}
N' \arrow[r, hook] \arrow[d, hook] & N \arrow[r, two heads] \arrow[d, hook] & N_{n-1} \arrow[d, hook] \\
1+\ell^{n-1}H_0 \arrow[r, hook] \arrow[d, two heads] & \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \arrow[r, two heads] \arrow[d, two heads] & \mathrm{SL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z}) \arrow[d, two heads] \\
(1+\ell^{n-1}H_0)/N' \arrow[r, hook] & \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})/N \arrow[r, two heads] & \mathrm{SL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z})/N_{n-1}
\end{tikzcd}$$

where $N' = N \cap (1+\ell^{n-1}H_0)$. By induction hypothesis, $\mathrm{SL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z})/N_{n-1}$ is either $\mathbb{Z}/\ell\mathbb{Z}$ or trivial. Moreover, the group $\mathrm{Id} + \ell^{n-1}H_0$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^3$ so the only possible prime divisor for the order of $\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})/N$ is ℓ. □

In the following result, by ℓ-part of an abelian extension we mean the largest subextension which has degree a power of ℓ.

Theorem 84. *Let K be a number field and let E/K be an elliptic curve. Let $P \in E(K)$ be a point of infinite order. Let ℓ be a prime, $e \geq 1$ and n a positive integer coprime to ℓ. Suppose that the image of the $\bmod n'\ell$ torsion representation is $\mathrm{GL}_2(\mathbb{Z}/n'\ell\mathbb{Z})$, where n' is the square-free part of n. Then we have*

$$K\left(\frac{1}{\ell^e}P\right) \cap K(E[\ell^e n]) \subseteq F_{\gcd(n,B)}(E[\ell^e])$$

where B is the product of the odd primes of bad reduction for E and $F_{\gcd(n,B)}/K$ is the ℓ-part of $K(\zeta_{\gcd(n,B)})/K$. In particular, if additionally $\ell \nmid \varphi(\gcd(n,B))$, we have

$$K\left(\frac{1}{\ell^e}P\right) \cap K(E[\ell^e n]) = K(E[\ell^e])\,.$$

Proof. The second assertion is an immediate consequence of the first. Write $K' := K(E[\ell^e])$. The extension $K\left(\frac{1}{\ell^e}P\right)/K'$ is Kummer of exponent dividing ℓ^e. Hence, any subextension is the compositum of finitely many cyclic extensions of degree dividing ℓ^e. Considering that $K\left(\frac{1}{\ell^e}P\right) \cap K(E[\ell^e n]) \subseteq K'$ and that the degree of $K(E[\ell^e n])/K(E[\ell^e n'])$ is coprime to ℓ, we may suppose that n is square-free (and that $n \neq 1$, because the result is evident in that case).

We know that $K\left(\frac{1}{\ell^e}P\right)/K'$ is unramified at the primes that are not over ℓ nor the primes of bad reduction for E by [HS00, Proposition C.1.5]. We claim that we have

$$K\left(\frac{1}{\ell^e}P\right) \cap K(E[\ell^e n]) \subseteq K'(\zeta_r)$$

with $r = n$. Then, if r is even, we may replace it by $r/2$, which is odd; if p is an odd prime divisor of r and $p \nmid B$, as $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is totally ramified at p, we may replace r by r/p. By iteration, we obtain $r = \gcd(n,B)$ and we conclude.

We are left to prove the claim. The Galois group of $K(E[\ell^e n])/K'$ is $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. By Lemma 81, a normal subgroup of index dividing ℓ^e of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ contains $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ and hence (as the determinant of a scalar matrix is related to the cyclotomic character) hence the claim holds by the Galois correspondence. □

Proposition 85. *Let n be a positive integer, and suppose that for every prime $\ell \mid n$ we have*

$$K(E[\ell^{v_\ell(n)}]) \cap K(E[n/\ell^{v_\ell(n)}]) = K \quad \textit{and} \quad K\left(\frac{1}{\ell^{v_\ell(n)}}P\right) \cap K(E[n]) = K(E[\ell^{v_\ell(n)}])\,.$$

Then the image of the $\bmod n$ torsion-Kummer representation is the product of the images of the $\bmod \ell^{v_\ell(n)}$ torsion-Kummer representations.

Proof. By the coprimality of the degrees of the Kummer extensions and by assumption, we have

$$K\left(\frac{1}{\ell^{v_\ell(n)}}P\right) \cap K\left(\frac{1}{n/\ell^{v_\ell(n)}}P\right) = K\left(\frac{1}{\ell^{v_\ell(n)}}P\right) \cap K(E[n]) = K(E[\ell^{v_\ell(n)}])\,.$$

Since this holds for every ℓ we deduce that the fields $K\left(\frac{1}{\ell^{v_\ell(n)}}P\right)$ are linearly disjoint over K if the same holds for the fields $K(E[\ell^{v_\ell(n)}])$, which is true by assumption. □

References

[BBP25] A. Benoist, S. Buzogány, and A. Perucca. On the intertwined divisibility for elliptic curves. `https://hdl.handle.net/10993/66966`, 2025.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

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

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

[CFRM05] A. C. Cojocaru, E. Fouvry, and M. Ram Murty. The square-sieve and the Lang-Trotter conjecture. *Canadian Journal of Mathematics*, 57(6):1155–1177, 2005.

[Coj03] A. C. Cojocaru. Cyclicity of CM elliptic curves modulo p. *Trans. Amer. Math. Soc.*, 355(7):2651–2662, 2003.

[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.

[GJLRY25] E. González-Jiménez, Á Lozano-Robledo, and B. York. Models of CM elliptic curves with a prescribed ℓ-adic Galois image. *J. Number Theory*, 277:19–62, 2025.

[GRM86] R. Gupta and M. Ram Murty. Primitive points on elliptic curves. *Compositio Math.*, 58(1):13–44, 1986.

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

[JPS23] N. Jones, F. Pappalardi, and P. Stevenhagen. Locally imprimitive points on elliptic curves. `https://arxiv.org/pdf/2304.03964`, 2023.

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

[LMF25] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2025.

[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.

[LR22] Á. Lozano-Robledo. Galois representations attached to elliptic curves with complex multiplication. *Algebra and Number Theory*, 16(4):777–837, 2022.

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

[Mel15] G. Meleleo. Cyclicity of quotients of non-CM elliptic curves modulo primes. In *SCHOLAR—a scientific celebration highlighting open lines of arithmetic research*, volume 655 of *Contemp. Math.*, pages 135–142. Amer. Math. Soc., Providence, RI, 2015.

[MPe27] P. Moree, A. Perucca, and M. Ram Murty eds. Artin's conjecture on primitive roots. Contributed volume (work in progress, planned with Springer), to be printed in 2027.

[Mur83] M. Ram Murty. On Artin's conjecture. *J. Number Theory*, 16(2):147–168, 1983.

[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.

[PP24] A. Pajaziti and A. Perucca. One formal result for torsion and arboreal representations of commutative algebraic groups. https://orbilu.uni.lu/handle/10993/61266, 2024.

[Rib79] K. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.*, 46:745–761, 1979.

[Sag24] The SageDevelopers. *SageMath, the Sage Mathematics Software System (Version 10.5)*, 2024. https://www.sagemath.org.

[Sch77] A. Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arith.*, 32:245–274, 1977.

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

[Ser78] J.-P. Serre. Résumé des cours de 1977-1978. *Annuaire du Collège de France, 67-70*, 1978.

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

[Zyw11] D. J. Zywina. A refinment of Koblitz's conjecture. *Int. J. Number Theory*, 7(3):739–769, 2011.

[Zyw15] D. J. Zywina. On the possible images of the $\bmod \ell$ representations associated to elliptic curves over $\mathbb{Q}$. https://arxiv.org/abs/1508.07660, 2015.

(Alexandre Benoist) UNIVERSITY OF LUXEMBOURG, DEPARTMENT OF MATHEMATICS. 6, AVENUE DE LA FONTE, L-4364 ESCH-SUR-ALZETTE, LUXEMBOURG
ORCID: 0009-0002-3942-0961

Email address: alexandre.benoist@uni.lu

(Antonella Perucca) UNIVERSITY OF LUXEMBOURG, DEPARTMENT OF MATHEMATICS. 6, AVENUE DE LA FONTE, L-4364 ESCH-SUR-ALZETTE, LUXEMBOURG
ORCID: 0000-0003-3173-6988

Email address: antonella.perucca@uni.lu