New York Journal of Mathematics

New York J. Math. **23** (2017) 897–925.

The 1-eigenspace for matrices in $\mathrm{GL}_2(\mathbb{Z}_\ell)$

Davide Lombardo and Antonella Perucca

Abstract. Fix some prime number ℓ and consider an open subgroup G either of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or of the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. The elements of G act on $(\mathbb{Z}/\ell^n\mathbb{Z})^2$ for every $n \geqslant 1$ and also on the direct limit, and we call 1-eigenspace the group of fixed points. We partition G by considering the possible group structures for the 1-eigenspace and show how to evaluate with a finite procedure the Haar measure of all sets in the partition. The results apply to all elliptic curves defined over a number field, where we consider the image of the ℓ-adic representation and the Galois action on the torsion points of order a power of ℓ.

Contents

1. Introduction

Fix a prime number ℓ, and let G be an open subgroup of either $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or the normalizer of a (possibly ramified) Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. This general framework can be applied to elliptic curves defined over a number field, where G is the image of the ℓ-adic representation. We identify an element of G with an automorphism of the direct limit in n of $(\mathbb{Z}/\ell^n\mathbb{Z})^2$: for elliptic curves this means considering the Galois action on the group of torsion points whose order is a power of ℓ.

Received January 29, 2017. Revised July 22, 2017.

2010 *Mathematics Subject Classification.* 28C10, 16S50, 11G05, 11F80.

Key words and phrases. Haar measure, general linear group, Cartan subgroup, ℓ-adic representation, elliptic curve.

The second author gratefully acknowledges financial support from the SFB-Higher Invariants at the University of Regensburg.

ISSN 1076-9803/2017

We equip G with its Haar measure, normalized so as to assign volume one to G, and we compute the measure of subsets of G of arithmetic interest. For $M \in G$, we call 1-*eigenspace of* M the subgroup of fixed points of M for its action on the direct limit $\varinjlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^2$. This leads to partitioning G into subsets according to the group structure of the 1-eigenspace. More specifically, the matrices whose 1-eigenspace is an infinite group form a subset of G that has Haar measure zero, so we only investigate the possible finite group structures. For all integers $a, b \geqslant 0$ we consider the set

$$\mathcal{M}_{a,b} := \{M \in G : \ker(M - I) \simeq \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^{a+b}\mathbb{Z}\}$$

and its Haar measure in G, which is well-defined for each pair (a, b) and that we call $\mu_{a,b}$. The aim of this paper is to show that the whole countable family $\mu_{a,b}$ can be effectively computed:

Theorem 1. *Fix a prime number ℓ and an open subgroup G either of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or of the normalizer of one of its (possibly ramified) Cartan subgroups. It is possible to compute the whole family $\{\mu_{a,b}\}$ for $(a, b) \in \mathbb{N}^2$ with a finite procedure. More precisely, we can partition $\mathbb{N}^2$ in finitely many subsets S (as in Definition 42 and explicitly computable) such that the following holds: there is some (explicitly computable) rational number $c_S \geqslant 0$ such that for every $(a, b) \in S$ we have*

$$\mu_{a,b} = c_S \cdot \ell^{-(\dim(G)a+b)}$$

where the dimension of G is either 4 or 2, according to whether G is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or in the normalizer of a Cartan subgroup. The sets S and the constants c_S may depend on ℓ and G.

Some explicit results are as follows:

Theorem 2. *For $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we have:*

$$\mu_{a,b} = \begin{cases} \dfrac{\ell^3 - 2\ell^2 - \ell + 3}{(\ell-1)^2 \cdot (\ell+1)} & \text{if } a = 0, b = 0 \\ \dfrac{\ell^2 - \ell - 1}{\ell(\ell-1)} \cdot \ell^{-b} & \text{if } a = 0, b > 0 \\ \ell^{-4a} & \text{if } a > 0, b = 0 \\ (\ell+1) \cdot \ell^{-4a-b-1} & \text{if } a > 0, b > 0. \end{cases}$$

Theorem 3. *For a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ which is either split or nonsplit (see Definition 6) we respectively have:*

$$\mu_{a,b} = \begin{cases} \dfrac{(\ell-2)^2}{(\ell-1)^2} & \text{if } a = 0, b = 0 \\ \dfrac{2(\ell-2)}{\ell-1} \cdot \ell^{-b} & \text{if } a = 0, b > 0 \\ \ell^{-2a} & \text{if } a > 0, b = 0 \\ 2 \cdot \ell^{-2a-b} & \text{if } a > 0, b > 0 \end{cases} \qquad \mu_{a,b} = \begin{cases} \dfrac{\ell^2 - 2}{\ell^2 - 1} & \text{if } a = 0, b = 0 \\ \ell^{-2a} & \text{if } a > 0, b = 0 \\ 0 & \text{if } b > 0. \end{cases}$$

Theorem 4. *For the normalizer of a split or nonsplit Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ we have*

$$\mu_{a,b} = \frac{1}{2} \cdot \mu_{a,b}^{C} + \frac{1}{2} \cdot \mu_{a,b}^{*}$$

where $\mu_{a,b}^{C}$ is the Haar measure in C of $\mathcal{M}_{a,b} \cap C$ (which can be read off Theorem 3) and where we set

$$\mu_{a,b}^{*} = \begin{cases} \dfrac{\ell-2}{\ell-1} & \text{if } a = 0, b = 0 \\ \ell^{-b} & \text{if } a = 0, b > 0 \\ 0 & \text{if } a > 0 \ . \end{cases}$$

The Haar measure $\mu_{a,b}$ can computed as the limit in n of the ratio $\#\mathcal{M}_{a,b}(n)/\#G(n)$, where for a subset X of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ the symbol $X(n)$ denotes the image of X in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. For fixed a and b, the quantity $\#\mathcal{M}_{a,b}(n)/\#G(n)$ stabilizes for n sufficiently large by the higher-dimensional version of Hensel's Lemma. However, since we cannot fix a single value of n which is good for every pair (a, b), we need technical results about counting the number of lifts of any given matrix in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ to $\mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$.

The structure of the paper is as follows. In Section 2 we define Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ in full generality and prove a classification result which might be of independent interest. In Section 3 we prove general results about the group structure of the 1-eigenspace and set the notation for the subsequent sections. These contain further results, in particular Theorem 28 (about the reductions of $\mathcal{M}_{a,b}$) and the two technical results Theorems 27 and 31. Finally, the last section is devoted to the proof of Theorems 1 to 4. In [LP16] we apply the results of this paper to solve a problem about elliptic curves:

Remark 5. Let E be an elliptic curve defined over a number field K. If ℓ is a prime number and $E[\ell^\infty]$ is the group of $\overline{K}$-points on E of order a power of ℓ, we have general results and a computational strategy for:

- classifying the elements in the image of the ℓ-adic representation according to the group structure of the fixed points in $E[\ell^\infty]$;
- computing the density of reductions such that the ℓ-part of the group of local points has some prescribed group structure, for the whole family of possible group structures.

2. Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$

2.1. General definition of Cartan subgroups. Classical references are [Bor91, Chapter 4] and [Ser72, Section 2]. Let ℓ be a prime number and F be a reduced $\mathbb{Q}_\ell$-algebra of degree 2 with ring of integers $\mathcal{O}_F$. Concretely, F is either a quadratic extension of $\mathbb{Q}_\ell$, or the ring $\mathbb{Q}_\ell^2$ (in the latter case we define the ℓ-adic valuation as the minimum of those of the two coordinates and by $\mathcal{O}_F$ we mean the valuation ring $\mathbb{Z}_\ell^2$). Let furthermore R be a $\mathbb{Z}_\ell$-order

in F, by which we mean a subring of F (containing 1) which is a finitely generated $\mathbb{Z}_\ell$-module and satisfies $\mathbb{Q}_\ell R = F$ (i.e., R spans F over $\mathbb{Q}_\ell$).

The *Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ associated with R* is the group of units of R: the embedding $R^\times \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ is given by fixing a $\mathbb{Z}_\ell$-basis of R and considering the left multiplication action of $R^\times$. The Cartan subgroup is only well-defined up to conjugation in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ because of the choice of the basis. Writing $C_R := \mathrm{Res}_{R/\mathbb{Z}_\ell}(\mathbb{G}_m)$, where Res is the Weil restriction of scalars, we have $C = C_R(\mathbb{Z}_\ell)$, provided that the Weil restriction is computed using the same $\mathbb{Z}_\ell$-basis for R.

Equivalently, a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ can be described as follows: there exists a maximal torus $\mathcal{T}$ of $\mathrm{GL}_{2,\mathbb{Z}_\ell}$, flat over $\mathbb{Z}_\ell$, such that $C = \mathcal{T}(\mathbb{Z}_\ell)$.

Definition 6. We shall say that the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ associated with R is:

- *maximal*, if ℓ does not divide the index of R in $\mathcal{O}_F$;
- *split*, if it is maximal and furthermore ℓ is split in F;
- *nonsplit*, if it is maximal and furthermore ℓ is inert in F;
- *ramified*, if it is neither split nor nonsplit.

Notice in particular that *unramified* means the same as *either split or nonsplit*. Thus a Cartan subgroup is either split, nonsplit or ramified: a Cartan subgroup can be ramified because

(1) it is not maximal (ℓ divides $[\mathcal{O}_F : R]$), or
(2) ℓ ramifies in F.

Note that we always understand 'maximal' in the sense of the above definition (in particular, even if a Cartan subgroup is not maximal, it is still the group of $\mathbb{Z}_\ell$-points of a maximal subtorus of GL_2). A proper subgroup of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is not a Cartan subgroup in our terminology.

Remark 7. A strict inclusion of quadratic rings $R \hookrightarrow S$ over $\mathbb{Z}_\ell$ does not induce an inclusion of Cartan subgroups according to our definition. This is because the multiplication action of $R^\times$ on R (resp. of $S^\times$ on S) is represented with respect to a $\mathbb{Z}_\ell$-basis of R (resp. S), and the base-change matrix relating a basis of R with a basis of S is not ℓ-integral. More concretely, write $S = \mathbb{Z}_\ell[\omega]$ and $R = \mathbb{Z}_\ell[\ell^k\omega]$ for some $k > 0$. Suppose for simplicity that $\ell \neq 2$ and $\omega^2 = d \in \mathbb{Z}_\ell$, and consider the bases $\{1, \omega\}$ and $\{1, \ell^k\omega\}$ of S, R respectively. An element $a + b\ell^k\omega$ (where $a, b \in \mathbb{Z}_\ell$) corresponds to

$$\begin{pmatrix} a & b\ell^k d \\ b\ell^k & a \end{pmatrix} \in C_S(\mathbb{Z}_\ell) \quad \text{and} \quad \begin{pmatrix} a & b\ell^{2k} d \\ b & a \end{pmatrix} \in C_R(\mathbb{Z}_\ell).$$

One can check that for $b \neq 0$ there is no $\mathbb{Z}_\ell$-integral change of basis relating these two matrices, and a similar conclusion holds for any choice of $\mathbb{Z}_\ell$-bases of R, S.

For a maximal Cartan subgroup we have $R = \mathcal{O}_F$ and for a split Cartan subgroup we have $R \cong \mathbb{Z}_\ell^2$ and hence $C \cong (\mathbb{Z}_\ell^\times)^2$.

2.2. A classification for quadratic rings. It is apparent from the previous discussion that classifying the Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ up to conjugacy is equivalent to classifying the *quadratic rings* over $\mathbb{Z}_\ell$ (i.e., the orders in integral quadratic $\mathbb{Q}_\ell$-algebras) up to a $\mathbb{Z}_\ell$-linear ring isomorphism. A Cartan subgroup is maximal if and only if the corresponding quadratic ring R is the maximal order; a maximal Cartan subgroup is unramified if and only if the corresponding $\mathbb{Q}_\ell$-algebra is étale, i.e., it is either $\mathbb{Q}_\ell^2$ (in the split case) or the unique unramified quadratic extension of $\mathbb{Q}_\ell$ (in the non-split case). We have an étale $\mathbb{Q}_\ell$-algebra if and only if the ℓ-adic valuation on R, normalized so that $v_\ell(\ell) = 1$, takes integer values.

Theorem 8 (Classification of quadratic rings)**.** *If R is a quadratic ring over $\mathbb{Z}_\ell$ then there exist a $\mathbb{Z}_\ell$-basis $(1, \omega)$ of R and parameters (c, d) in $\mathbb{Z}_\ell$ satisfying $\omega^2 = c\omega + d$ and such that one of the following holds: $c = 0$ (and hence $d \neq 0$); $\ell = 2$, $c = 1$, and d is either zero or odd.*

Proof. Let $(1, \omega_0)$ be a $\mathbb{Z}_\ell$-basis of R and write $\omega_0^2 = c_0\omega_0 + d_0$ for some $c_0, d_0 \in \mathbb{Z}_\ell$. If ℓ is odd or c_0 is even, we set $\omega = \omega_0 - c_0/2$ and have parameters $(0, d_0 + c_0^2/4)$. If $\ell = 2$ and c_0 is odd, we set $\omega = \omega_0 - (c_0 - 1)/2$ and $d_1 = d_0 + (c_0^2 - 1)/4$. If d_1 is odd, we are done because we have $\omega^2 = \omega + d_1$. If d_1 is even, the quadratic equation $\omega^2 = \omega + d_1$ has solutions in $\mathbb{Q}_2$ because its discriminant $1 - 4d_1 \equiv 1 \pmod 8$ is a square. Thus R is an order in $\mathbb{Q}_2^2$ and hence it is of the form $\mathbb{Z}_2(1, 1) \oplus \mathbb{Z}_2(0, \beta)$ for some $\beta \in \mathbb{Z}_2$. If β is odd, we have $R = \mathbb{Z}_2^2$ so we set $\omega = (0, 1)$ and have parameters $(1, 0)$. If β is even, we set $\omega = (-\beta/2, \beta/2)$ and have parameters $(0, \beta^2/4)$. □

2.3. Parameters for a Cartan subgroup. We call the parameters (c, d) as in Theorem 8 *parameters for the Cartan subgroup* of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to R: they are in general not uniquely determined.

Remark 9. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_\ell$ we may assume that the parameters (c, d) are integers. Indeed, one can prove that the isomorphism class of the ring $\mathbb{Z}_\ell[x]/(x^2 - cx - d)$ is a locally constant function of $(c, d) \in \mathbb{Z}_\ell^2$ (this property is closely related to Krasner's Lemma [The17, Tag 0BU9]). We also give a direct argument. Consider first a Cartan subgroup C with parameters $(0, d)$. If u is an ℓ-adic unit, $(0, u^2 d)$ are also parameters for C. Thus C depends on d only through its class in $(\mathbb{Z}_\ell \setminus \{0\})/\mathbb{Z}_\ell^{\times 2}$ (quotient as multiplicative monoids): this is isomorphic to $\mathbb{N} \times \mathbb{Z}_\ell^\times/\mathbb{Z}_\ell^{\times 2}$, where the first factor is the valuation and the second factor is finite (indeed $\mathbb{Z}_\ell^\times/\mathbb{Z}_\ell^{\times 2} \cong \mathbb{F}_\ell^\times/\mathbb{F}_\ell^{\times 2}$ if ℓ is odd, and $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2} \cong (\mathbb{Z}/8\mathbb{Z})^\times$). With powers of ℓ we can realize every integral valuation (recall that d is an element of $\mathbb{Z}_\ell$), and the integers coprime to ℓ represent all elements of $\mathbb{Z}_\ell^\times/\mathbb{Z}_\ell^{\times 2}$, thus there is an integer representative. Now suppose $\ell = 2$ and consider a Cartan subgroup with parameters $(1, d)$ where d is odd: in Proposition 11 we show that the quadratic ring is $\mathbb{Z}_2[\zeta_6]$ and hence we can take as parameters $(1, -1)$.

Proposition 10 (Classification of Cartan subgroups for ℓ odd)**.** *Suppose that ℓ is odd, and consider a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with parameters $(0,d)$. It is maximal if and only if $v_\ell(d) \leqslant 1$. It is unramified if and only if $\ell \nmid d$: it is then split if d is a square in $\mathbb{Z}_\ell^\times$, and nonsplit otherwise.*

Proof. If $v_\ell(d) = 1$ then $v_\ell(\omega) = 1/2$ and hence F is a ramified extension of $\mathbb{Q}_\ell$. If $v_\ell(d) \geqslant 2$ then C is not maximal because $(\omega/\ell)^2 = d/\ell^2 \in \mathbb{Z}_\ell$ and hence ω/ℓ is in $\mathbb{Z}_\ell$. If $v_\ell(d) \leqslant 1$ then R is a maximal order. Indeed, let R' be an order in F containing R and choose a $\mathbb{Z}_\ell$-basis $(1, \omega_1)$ of R' satisfying $\omega_1^2 = d_1 \in \mathbb{Z}_\ell$: writing $\omega = a\omega_1 + b$ for some $a, b \in \mathbb{Z}_\ell$, we have

$$d = \omega^2 = (a^2 d_1 + b^2) \cdot 1 + (2ab) \cdot \omega_1$$

which implies $b = 0$, thus $v_\ell(d) = 2v_\ell(a) + v_\ell(d_1)$ and hence $v_\ell(a) = 0$ and $R' = R$.

Now suppose $v_\ell(d) = 0$. If d is not a square, then $F = \mathbb{Q}_\ell(\sqrt{d})$ is an unramified extension of $\mathbb{Q}_\ell$ while if d is a square the map

$$a + b\omega \mapsto (a + b\sqrt{d}, a - b\sqrt{d})$$

identifies R and $\mathbb{Z}_\ell^2$. □

Proposition 11 (Classification of Cartan subgroups for $\ell = 2$)**.** *Suppose that $\ell = 2$, and consider a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with parameters (c,d). It is unramified if and only if $c = 1$: it is then split for $d = 0$ and nonsplit for d odd. It is maximal and ramified if and only if $c = 0$ and either $v_2(d) = 1$ or $v_2(d) = 0$ and $d \equiv 3 \pmod 4$.*

Proof. We keep the notation of the previous proof. If $c = 1$ and $d = 0$ then $a + b\omega \mapsto (a, a + b)$ is an isomorphism between R and $\mathbb{Z}_2^2$, so that C is split. If $c = 1$ and d is odd then up to isomorphism we may suppose $\omega^2 = \omega + d$. This equation is separable over $\mathbb{Z}/2\mathbb{Z}$, so R is contained in the unique unramified quadratic extension of $\mathbb{Q}_2$, which is $\mathbb{Q}_2(\zeta_6)$. Since 2 is inert, we will have shown that C is nonsplit once we prove $R = \mathbb{Z}_2[\zeta_6]$. To show $\zeta_6 \in R$, we write $\omega = a + b\zeta_6$ (with $a, b \in \mathbb{Z}_2$) and prove that b is a unit: the equation $\omega^2 = \omega + d$ gives

$$(a^2 - b^2) + \zeta_6(b^2 + 2ab) = (a + d) + \zeta_6 b,$$

so $a + d$ has the same parity as $a^2 - b^2$ and we deduce that b is odd.

Conversely, if C is unramified then no $\mathbb{Z}_2$-basis $(1, \omega)$ of R satisfies $\omega^2 \in \mathbb{Z}_2$ and we must have $c = 1$. Since $t^2 = t + d$ has no solutions in $\mathbb{Z}_2^2$ for d odd while it has solutions in $\mathbb{Q}_2$ if $d = 0$, we deduce that $d = 0$ (resp. d is odd) for a split (resp. nonsplit) Cartan subgroup. If $c = 1$ we have seen that C is maximal, so suppose $c = 0$ and hence $\omega^2 = d \in \mathbb{Z}_2$. Analogously to the previous remark we have $v_2(d) \leqslant 1$ if C is maximal. By Remark 9 we only need to consider those d in $(\mathbb{Z}_2 \setminus \{0\})/\mathbb{Z}_2^{\times 2} \cong (\mathbb{N} \times \mathbb{Z}_2^\times)/\mathbb{Z}_2^{\times 2}$ with valuation 0 or 1, namely $d = 1, 3, 5, 7$ and $d = 2, 6, 10, 14$. We may conclude because it is known whether $\mathbb{Z}_2[\sqrt{d}]$ has index 1 or 2 in the ring of integers of $\mathbb{Q}_2(\sqrt{d})$, where for $d = 1$ we set $\sqrt{d} = (1, -1) \in \mathbb{Z}_2^2$. □

2.4. A concrete description of Cartan subgroups. Let (c,d) be parameters as in Theorem 8; we can then give a precise description for $C_R := \mathrm{Res}_{R/\mathbb{Z}_\ell}(\mathbb{G}_m) \subset \mathrm{GL}_{2,\mathbb{Z}_\ell}$ as follows. For every $\mathbb{Z}_\ell$-algebra A, the A-points of C_R are the subgroup of $\mathrm{GL}_{2,\mathbb{Z}_\ell}(A)$ given by:

$$C_R(A) = \left\{ \begin{pmatrix} x & dy \\ y & x+yc \end{pmatrix} : x,y \in A,\ \det \begin{pmatrix} x & dy \\ y & x+yc \end{pmatrix} \in A^\times \right\}.$$

In particular the Cartan subgroup $C = C_R(\mathbb{Z}_\ell)$ is the set

$$C = \left\{ \begin{pmatrix} x & dy \\ y & x+yc \end{pmatrix} : x,y \in \mathbb{Z}_\ell,\ v_\ell(x(x+yc) - dy^2) = 0 \right\}. \tag{2.1}$$

Remark 12 (Diagonal model for a split Cartan subgroup)**.** For the parameters (c,d) of a split Cartan subgroup C we have shown: if ℓ is odd, we have $c = 0$ and d is a square in $\mathbb{Z}_\ell^\times$; if $\ell = 2$, we have $(c,d) = (1,0)$. We deduce the existence of an isomorphism between C and the group of diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}_\ell)$:

$$\left\{ \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} :\ X,Y \in \mathbb{Z}_\ell^\times \right\}. \tag{2.2}$$

We can define such an isomorphism for ℓ odd and for $\ell = 2$ respectively as:

(2.3)

$$\varphi_\ell : \begin{pmatrix} x & dy \\ y & x \end{pmatrix} \mapsto \begin{pmatrix} x - y\sqrt{d} & 0 \\ 0 & x + y\sqrt{d} \end{pmatrix} \quad \varphi_2 : \begin{pmatrix} x & 0 \\ y & x+y \end{pmatrix} \mapsto \begin{pmatrix} x & 0 \\ 0 & x+y \end{pmatrix}.$$

We have $\det(\varphi_\ell(M) - I) = \det(M - I)$ and for any $n \geqslant 1$ we have

$$\varphi_\ell(M) - I \equiv 0 \pmod{\ell^n} \iff M - I \equiv 0 \pmod{\ell^n}.$$

Notation. For a subset X of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ we denote by $X(n)$ the image of X in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

Lemma 13. *If C is a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ we have*

$$\#C(1) = \begin{cases} (\ell-1)^2 & \text{if } C \text{ is split} \\ (\ell-1)\cdot(\ell+1) & \text{if } C \text{ is nonsplit} \\ (\ell-1)\cdot\ell & \text{if } C \text{ is ramified} \end{cases}$$

and for any $n \geqslant 1$ we have $\#C(n) = \#C(1)\cdot\ell^{2n-2}$.

Proof. The assertion for $n = 1$ is a straightforward computation, while for $n > 1$ it follows from the (higher-dimensional version of) Hensel's Lemma [Nek, Proposition 7.8] because the Zariski closure of C in $\mathrm{GL}_{2,\mathbb{Z}_\ell}$ is smooth of relative dimension 2. □

2.5. Normalizers of Cartan subgroups.

Lemma 14. *A Cartan subgroup of* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *has index* 2 *in its normalizer. If* C *is as in* (2.1)*, its normalizer* N *in* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *is the disjoint union of* C *and*

$$C' := \begin{pmatrix} 1 & c \\ 0 & -1 \end{pmatrix} \cdot C.$$

We have instead $C' := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot C$ *for a split Cartan subgroup as in* (2.2)*.*

Proof. An easy verification shows $C' \subset N$. If $A \in N$, there exist $x, y \in \mathbb{Z}_\ell$ such that we have

$$A \begin{pmatrix} 0 & d \\ 1 & c \end{pmatrix} A^{-1} = \begin{pmatrix} x & yd \\ y & x + yc \end{pmatrix}.$$

If $c = 0$, by comparing traces we find $x = 0$ and hence by comparing determinants we have $(x, y) = (0, \pm 1)$. If $\ell = 2$ and $c = 1$, by comparing traces we find $y = 1 - 2x$ and hence by comparing determinants we have $-x^2 + x = 0$, so (x, y) is either $(0, 1)$ or $(1, -1)$. We compute

$$A \begin{pmatrix} 0 & d \\ 1 & c \end{pmatrix} = \begin{pmatrix} x & yd \\ y & x + yc \end{pmatrix} A$$

for any explicit value of (x, y) as above, finding in each case $A \in C \cup C'$. The last assertion about a split Cartan subgroup is well-known and easy to prove. □

Remark 15. If one considers a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ as the $\mathbb{Z}_\ell$-valued points of a maximal torus of GL_2, the previous lemma also follows from the fact that any maximal torus in GL_2 has index 2 in its normalizer (the Weyl group of GL_2 is $\mathbb{Z}/2\mathbb{Z}$).

Lemma 16. *If* C *is as in* (2.1) *and* N *is its normalizer then we have*

$$N \setminus C = \left\{ \begin{pmatrix} z & -dw + cz \\ w & -z \end{pmatrix} : z, w \in \mathbb{Z}_\ell,\ v_\ell(-z^2 + dw^2 - czw) = 0 \right\}. \tag{2.4}$$

Consider $M \in N \setminus C$*. If* ℓ *is odd, we have* $M \not\equiv I \pmod{\ell}$*; if* $\ell = 2$*, we have* $M \not\equiv I \pmod{4}$*, and if* C *is unramified we also have* $M \not\equiv I \pmod{2}$*.*

Proof. The first assertion follows from the previous lemma and (2.1). Since M has trace zero, we have $M \not\equiv I \pmod{\ell}$ for ℓ odd and $M \not\equiv I \pmod{4}$ for $\ell = 2$. If $\ell = 2$ and C is unramified we know $c = 1$ thus $M \equiv I \pmod{2}$ is impossible. □

Remark 17. By comparing (2.1) and (2.4), we see that the sets $C(n)$ and $(N \setminus C)(n)$ are disjoint for $n \geqslant 2$ (if ℓ is odd or C is unramified, for $n \geqslant 1$). By Lemma 14 we then have $\#N(n) = 2 \cdot \#C(n)$.

2.6. The tangent space of a Cartan subgroup. Let G be an open subgroup of either $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or of the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Then G is an ℓ-adic manifold, and there is a well-defined notion of a tangent space $T_I G$ at the identity. This is a $\mathbb{Q}_\ell$-vector subspace of $\mathrm{Mat}_2(\mathbb{Q}_\ell)$, of dimension equal to the dimension of G as a manifold (in particular, if $G = \mathrm{GL}_2(\mathbb{Z}_\ell)$ we have $T_I G = \mathrm{Mat}_2(\mathbb{Q}_\ell)$). For our lifting questions, however, we are more interested in the 'mod-ℓ' tangent space, which can be defined either as the reduction modulo ℓ of the intersection of $T_I G$ with $\mathrm{Mat}_2(\mathbb{Z}_\ell)$, or as the tangent space to the modulo-ℓ fiber of the Zariski closure of G in $\mathrm{GL}_{2,\mathbb{Z}_\ell}$. More concretely, the next two definitions describe the tangent space explicitly:

Definition 18. If C is as in (2.1), its tangent space is

$$\mathbb{T} := \left\{ \begin{pmatrix} x & dy \\ y & x + cy \end{pmatrix} : x, y \in \mathbb{Z}/\ell\mathbb{Z} \right\}$$

where (c, d) are here the reductions modulo ℓ of the parameters of C. Write $\mathbb{T}^\times = C(1)$ for the subset of $\mathbb{T}$ consisting of the invertible matrices.

We clearly have $\#\mathbb{T} = \ell^2$ and by Lemma 13 we also know $\#\mathbb{T}^\times$. So we get:

(2.5)

Type of C	$\#\mathbb{T}$	$\#\mathbb{T}^\times$	$\#\mathbb{T} - \#\mathbb{T}^\times - 1$
split	ℓ^2	$(\ell-1)^2$	$2(\ell-1)$
nonsplit	ℓ^2	$\ell^2 - 1$	0
ramified	ℓ^2	$\ell(\ell-1)$	$\ell - 1$

We define the tangent space of an open subgroup of the normalizer of C as the tangent space of C. We also define the tangent space of an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ as follows:

Definition 19. Let G be an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. The tangent space of G is $\mathbb{T} := \mathrm{Mat}_2(\mathbb{Z}/\ell\mathbb{Z})$ and we write $\mathbb{T}^\times = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

For $\mathrm{GL}_2(\mathbb{Z}_\ell)$ we have

$$\#\mathbb{T} = \ell^4, \quad \#\mathbb{T}^\times = \ell(\ell-1)^2(\ell+1) \quad \text{and} \quad \#\mathbb{T} - \#\mathbb{T}^\times - 1 = (\ell+1)(\ell^2-1).$$

3. The group structure of the 1-eigenspace

3.1. The level. Let G' be either $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let G be an open subgroup of G' of finite index $[G' : G]$. Call $G'(n)$ and $G(n)$ the reductions of G' and G modulo ℓ^n, that is their respective images in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

If n is the smallest positive integer such that we have

$$[G'(n) : G(n)] = [G' : G],$$

we define the *level* n_0 of G as

$$n_0 = \begin{cases} \max\{n, 2\} & \text{if } \ell = 2 \text{ and } G' \text{ is the normalizer of a ramified Cartan} \\ n & \text{otherwise.} \end{cases}$$

Remark 20. It is easy to check that all our statements involving the notion of *level* remain true if n_0 is replaced by any larger integer.

All matrices in G' that are congruent to the identity modulo ℓ^{n_0} belong to G. In other words, G is the inverse image of $G(n_0)$ for the reduction map $G' \to G'(n_0)$. Consequently we have

$$[G'(n) : G(n)] = [G' : G] \quad \text{for every } n \geqslant n_0. \tag{3.1}$$

The dimension of G' is 4 if $G' = \mathrm{GL}_2(\mathbb{Z}_\ell)$ and is 2 otherwise, and we have

$$[G(n+1) : G(n)] = [G'(n+1) : G'(n)] = \ell^{\dim G'} \quad \text{for every } n \geqslant n_0. \tag{3.2}$$

Remark 21. Let G be an open subgroup of either $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let n_0 be the level of G. For any $n \geqslant n_0$ the map $M \mapsto \ell^{-n}(M-I)$ identifies the tangent space of G with the kernel of $G(n+1) \to G(n)$. This is immediate for $\mathrm{GL}_2(\mathbb{Z}_\ell)$, and for Cartan subgroups it follows from (2.1). The assertion also holds for normalizers of Cartan subgroups because by Lemma 16 all matrices reducing to the identity in $G(n)$ are contained in the Cartan subgroup.

3.2. The 1-eigenspace. We identify an element of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with an automorphism of the direct limit in n of $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. For all integers $a, b \geqslant 0$, if $X \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ we define

$$\mathcal{M}_{a,b}(X) := \{M \in X : \ker(M - I) \simeq \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^{a+b}\mathbb{Z}\} \tag{3.3}$$

and call $\mathcal{M}_{a,b}(X; n)$ the reduction of $\mathcal{M}_{a,b}(X)$ modulo ℓ^n. To ease notation, we write $\mathcal{M}_{a,b} := \mathcal{M}_{a,b}(G)$ and $\mathcal{M}_{a,b}(n) := \mathcal{M}_{a,b}(G; n)$.

We consider the normalized Haar measure on G and call $\mu_{a,b}$ the measure of the set $\mathcal{M}_{a,b}$. Since $\mathcal{M}_{a,b}(n)$ is a subset of $G(n)$, we may consider its measure

$$\mu_{a,b}(n) := \#\mathcal{M}_{a,b}(n)/\#G(n).$$

The sets $\mathcal{M}_{a,b}$ are pairwise disjoint, but the same is not necessarily true for the sets $\mathcal{M}_{a,b}(n)$. The sequence $\mu_{a,b}(n)$ is constant for $n > a + b$: this shows that $\mu_{a,b}$ is well-defined and that we have $\mu_{a,b} = \mu_{a,b}(n)$ for every $n > a + b$.

Remark 22. We clearly have $\mathcal{M}_{a,b} = G \cap \mathcal{M}_{a,b}(G')$. Moreover, we have

$$\mathcal{M}_{a,b} = \emptyset \quad \Leftrightarrow \quad G(n_0) \cap \mathcal{M}_{a,b}(G'; n_0) = \emptyset.$$

Indeed we know $\mathcal{M}_{a,b}(n_0) \subseteq G(n_0) \cap \mathcal{M}_{a,b}(G'; n_0)$ so if the latter is empty so is $\mathcal{M}_{a,b}$. Conversely, matrices in $\mathcal{M}_{a,b}(G')$ whose reduction modulo ℓ^{n_0} lies in $G(n_0)$ are in $\mathcal{M}_{a,b}$ because G is the inverse image in G' of $G(n_0)$.

3.3. Additional notation. We write $\det_\ell$ for the *ℓ-adic valuation of the determinant*. If M is in $\mathrm{Mat}_2(\mathbb{Z}/\ell^n\mathbb{Z})$, then $\det(M)$ is well-defined modulo ℓ^n so we can write $\det_\ell(M) \geqslant n$ if the determinant is zero modulo ℓ^n. Notice that the matrices in $\mathrm{Mat}_2(\mathbb{Z}_\ell)$ that are zero modulo ℓ^a for some $a \geqslant 0$ and with a given reduction modulo ℓ^n for some $n > a$ have a determinant which is well-defined modulo ℓ^{a+n}. More generally, if p is a polynomial with integer coefficients and z_1, z_2 are in $\mathbb{Z}/\ell^n\mathbb{Z}$ then we write $v_\ell(p(z_1, z_2))$ for the minimum of $v_\ell(p(Z_1, Z_2))$ over all lifts Z_1, Z_2 of z_1, z_2 to $\mathbb{Z}_\ell$. For example, if $z \equiv \ell^t \pmod{\ell^n}$ with $t < n$ then we have $v_\ell(z^2) = 2t$ because all lifts Z of z satisfy $v_\ell(Z^2) = 2t$.

3.4. Conditions related to the group structure of the 1-eigenspace.

Lemma 23. *The set $\mathcal{M}_{a,b}$ consists of the matrices $M \in G$ that satisfy*

$$\begin{aligned} M - I &\equiv 0 \pmod{\ell^a}, \\ M - I &\not\equiv 0 \pmod{\ell^{a+1}}, \\ \det_\ell(M - I) &= 2a + b. \end{aligned} \tag{3.4}$$

For every $n > a + b$ the set $\mathcal{M}_{a,b}$ is the preimage of $\mathcal{M}_{a,b}(n)$ in G, and $\mathcal{M}_{a,b}(n)$ consists of the matrices $M \in G(n)$ satisfying (3.4).

Proof. Necessity of (3.4) follows because for $A \in \mathrm{Mat}_2(\mathbb{Z}_\ell)$ the order of the kernel of A (considered as acting on the direct limit $\varinjlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^2$) equals $\ell^{\det_\ell A}$, that is, there are $\ell^{\det_\ell A}$ points x in $\varinjlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^2$ such that $Ax = 0$. Now suppose that $M \in G$ satisfies (3.4), and write $M = I + \ell^a A$ for some $A \in \mathrm{Mat}_2(\mathbb{Z}_\ell)$ which is nonzero modulo ℓ. We have $\det_\ell(A) = b$. Since A is nonzero modulo ℓ, the kernel of A is cyclic. Thus $\ker(A) \simeq \mathbb{Z}/\ell^b\mathbb{Z}$ and hence $\ker(M - I) \simeq \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^{a+b}\mathbb{Z}$. If $n > a + b$, (3.4) holds for the matrices in $\mathcal{M}_{a,b}(n)$ and their preimages in G. □

By Remark 12 and Lemma 23, the maps in (2.3) preserve $\mathcal{M}_{a,b}$ and $\mathcal{M}_{a,b}(n)$, thus for a split Cartan subgroup we can indifferently use the general model (2.1) or the diagonal model (2.2).

3.5. Existence of the Haar measure. A fundamental tool in dealing with Haar measures on profinite groups is the following simple lemma:

Lemma 24. [FJ08, Lemma 18.1.1] *Let $\mathcal{G}_1$ be a profinite group equipped with its normalized Haar measure, and let $\mathcal{G}_2$ be an open normal subgroup of $\mathcal{G}_1$. Call π the natural projection $\mathcal{G}_1 \to \mathcal{G}_1/\mathcal{G}_2$. For any subset S of the finite group $\mathcal{G}_1/\mathcal{G}_2$, the set $\pi^{-1}(S)$ is measurable in $\mathcal{G}_1$, and its Haar measure is $\#S/\#(\mathcal{G}_1/\mathcal{G}_2)$.*

Lemma 25. *For all integers $a, b \geqslant 0$ the set $\mathcal{M}_{a,b}$ is measurable in G and we have $\mu_{a,b} = \mu_{a,b}(n)$ whenever $n > a + b$. In particular we have $\mu_{a,b} = 0$ if and only if $\mathcal{M}_{a,b} = \emptyset$. The set $\bigcup_{a,b\in\mathbb{N}} \mathcal{M}_{a,b}$ is measurable in G, and its complement has measure zero.*

Proof. For the first assertion apply Lemma 24 to G, $\ker(G \to G(n))$ and $\mathcal{M}_{a,b}(n)$, noticing that $\mathcal{M}_{a,b}$ is the preimage of $\mathcal{M}_{a,b}(n)$ in G by Lemma 23. The set $\mathcal{M} := \bigcup_{a,b\in\mathbb{N}} \mathcal{M}_{a,b}$ is measurable because it is a countable union of measurable sets. We now prove $\mu(G \setminus \mathcal{M}) = 0$. Fix n_0 as in (3.1) and for $n \geqslant n_0$ call $\pi_n : G \to G(n)$ the reduction modulo ℓ^n. We have $G \setminus \mathcal{M} \subseteq \pi_n^{-1}(\pi_n(G \setminus \mathcal{M}))$, so by Lemma 24 it suffices to show that

$$\mu(\pi_n(G \setminus \mathcal{M})) = \frac{\#\pi_n(G \setminus \mathcal{M})}{\#G(n)} \tag{3.5}$$

tends to 0 as n tends to infinity. By (3.2) we know that $\#G(n)$ is a constant times $\ell^{n \dim G'}$. Let G'_∞ be the closed ℓ-adic analytic subvariety of G' defined by $\det(M - I) = 0$. We have $G \setminus \mathcal{M} \subseteq G'_\infty$ because for any $M \in G$ with $\det(M - I) \neq 0$ there exists n such that

$$M \not\equiv I \pmod{\ell^n} \quad \text{and} \quad \det_\ell(M - I) \leqslant n,$$

whence $M \in \mathcal{M}$. Thus the numerator in (3.5) is at most $\#\pi_n(G'_\infty)$, which by [Oes82, Theorem 4] is at most a constant times $\ell^{n \dim(G'_\infty)} = \ell^{n(\dim G' - 1)}$. □

3.6. The complement of a Cartan subgroup in its normalizer. Fix a Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and denote by N its normalizer. If G is an open subgroup of N, set

$$\mathcal{M}^*_{a,b} := (N \setminus C) \cap \mathcal{M}_{a,b}.$$

We denote by $\mathcal{M}^*_{a,b}(n)$ the reduction of $\mathcal{M}^*_{a,b}$ modulo ℓ^n, that is its image in $G(n)$.

If G is not contained in C, the sets $G \cap C$ and $G \cap (N \setminus C)$ are measurable and have measure $1/2$ in G because of Lemma 24 applied to the canonical projection $G \to G/(G \cap C) \cong \mathbb{Z}/2\mathbb{Z}$. In particular we have

$$\mu(\mathcal{M}_{a,b}) = \mu(\mathcal{M}_{a,b} \cap C) + \mu\left(\mathcal{M}^*_{a,b}\right).$$

Since $\mu_N(\mathcal{M}_{a,b} \cap C) = 1/2 \cdot \mu_C(\mathcal{M}_{a,b} \cap C)$, to determine $\mu_{a,b}$ we are reduced to computing $\mu(\mathcal{M}^*_{a,b})$ and studying $G \cap C$, which is open in the Cartan subgroup C.

Proposition 26. *We have $\mathcal{M}^*_{a,b} = \emptyset$ for $a > 1$ (if ℓ is odd or C is unramified, for $a > 0$).*

Proof. This is a consequence of Lemma 16. □

4. First results on the cardinality of $\mathcal{M}_{a,b}(n)$

Theorem 27. *Let G' be either $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or the normalizer of an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let G be an open subgroup of G' of level n_0. Call $\mathcal{H}_{a,b}(n)$ the set of matrices M in $G(n)$ satisfying the following conditions:*

(1) *If $a > 0$, $M \equiv I \pmod{\ell^a}$; if $n > a$, $M \not\equiv I \pmod{\ell^{a+1}}$.*

(2) *If* $a < n \leqslant a+b$, $\det_\ell(M-I) \geqslant a+n$.
If $n > a+b$, $\det_\ell(M-I) = 2a+b$.

For every integer $n \geqslant 1$ *define*

$$f(n) = \begin{cases} 1 & \text{if } n < a \\ \#\mathbb{T}^\times & \text{if } n = a, b = 0 \\ \#\mathbb{T} - \#\mathbb{T}^\times - 1 & \text{if } n = a, b > 0 \\ \#\mathbb{T} \cdot \ell^{-1} & \text{if } a < n < a+b \\ \#\mathbb{T} \cdot (1-\ell^{-1}) & \text{if } n = a+b,\ b > 0 \\ \#\mathbb{T} & \text{if } n > a+b. \end{cases}$$

Then the following hold:

(i) *For every* $n \geqslant n_0$ *we have* $\#\mathcal{H}_{a,b}(n+1) = f(n) \cdot \#\mathcal{H}_{a,b}(n)$. *For each* $M \in \mathcal{H}_{a,b}(n)$ *the number of matrices* $M' \in \mathcal{H}_{a,b}(n+1)$ *such that* $M' \equiv M \pmod{\ell^n}$ *equals* $f(n)$.

(ii) *If* $\mathcal{M}_{a,b} \neq \emptyset$ *and* $n \geqslant n_0$, *or if* $n > a+b$, *we have* $\mathcal{M}_{a,b}(n) = \mathcal{H}_{a,b}(n)$.

(iii) *For* $a \geqslant n_0$ *we have* $\mathcal{M}_{a,b} = \emptyset$ *if and only if*

$$b > 0 \quad \text{and} \quad \#\mathbb{T} - \#\mathbb{T}^\times - 1 = 0.$$

Proof. We first prove (i). Since $n \geqslant n_0$, all lifts to $G'(n+1)$ of matrices in $\mathcal{H}_{a,b}(n)$ are in $G(n+1)$. If $n > a+b$ then clearly every lift to $G(n+1)$ of a matrix in $\mathcal{H}_{a,b}(n)$ belongs to $\mathcal{H}_{a,b}(n+1)$. If $n < a$, the sets $\mathcal{H}_{a,b}(n)$ and $\mathcal{H}_{a,b}(n+1)$ contain only the identity and we are done.

Suppose $n = a$: the only matrix in $\mathcal{H}_{a,b}(a)$ is the identity, so we apply Remark 21. For $b = 0$ we count the matrices of the form $I + \ell^a T$ with $T \in \mathbb{T}$ and $\det_\ell(T) = 0$. For $b > 0$ we count those $M \in \mathcal{H}_{a,b}(a+1)$ that are congruent to the identity modulo ℓ^a but not modulo ℓ^{a+1} and such that $\det_\ell(M-I) \geqslant 2a+1$: this means $M = I + \ell^a T$, where $T \in \mathbb{T}$ with $\det_\ell T \neq 0$, and excluding $T = 0$.

Now consider the case $a < n < a+b$. Let $M \in \mathcal{H}_{a,b}(n)$ and fix some lift L to $G(n+1)$. The lifts of M are those matrices of the form $M' = L + \ell^n T$ with $T \in \mathbb{T}$, unless G' is the normalizer of a Cartan subgroup C and $M \notin C(n)$, for which by Lemma 16 we have $a = 0$ and $T \in \mathbb{T}_1$, where

$$\mathbb{T}_1 := \left\{ \begin{pmatrix} z & -dw + cz \\ w & -z \end{pmatrix} : z, w \in \mathbb{Z}/\ell\mathbb{Z} \right\}. \tag{4.1}$$

Write $L - I = \ell^a N$ for some $N \in \mathrm{Mat}_2(\mathbb{Z}/\ell^{n+1-a}\mathbb{Z})$. Since $b > n-a$, we have $\det(N) = \ell^{n-a} z$ for some $z \in \mathbb{Z}/\ell\mathbb{Z}$. Setting $(N \bmod \ell) = (n_{ij})$ and $T = (t_{ij})$, we get the following congruence modulo ℓ^{n+1-a}:

$$\begin{aligned} \det(M' - I) &\equiv \ell^{2a} \cdot \det(N + \ell^{n-a} T) \\ &\equiv \ell^{n+a} \left(z + n_{11}t_{22} + n_{22}t_{11} - n_{21}t_{12} - n_{12}t_{21} \right). \end{aligned}$$

So the condition for M' to be in $\mathcal{H}_{a,b}(n+1)$ is

$$z + n_{22}t_{11} + n_{11}t_{22} - n_{21}t_{12} - n_{12}t_{21} = 0. \tag{4.2}$$

We conclude by checking that this equation defines an affine subspace of codimension 1 in $\mathbb{T}$ (resp. in $\mathbb{T}_1$, if $M \notin C(n)$). The equation is nontrivial because at least one of the n_{ij} is nonzero, and this remark suffices for $\mathrm{GL}_2(\mathbb{Z}_\ell)$. If G' is the normalizer of a Cartan subgroup, we also have to check that (4.2) is independent from the equations defining $\mathbb{T}$ (resp. $\mathbb{T}_1$), which are

$$\begin{cases} t_{22} = t_{11} + ct_{21} \\ t_{12} = dt_{21}, \end{cases} \qquad \text{resp.} \qquad \begin{cases} t_{22} = -t_{11} \\ t_{12} = -dt_{21} + ct_{11}. \end{cases}$$

For the elements of $\mathbb{T}$, noticing that ($N \bmod \ell$) depends only on ($M \bmod \ell^{a+1}$) and it is in $\mathbb{T} \setminus \{0\}$, we can rewrite (4.2) as

$$z + (2n_{11} + cn_{21})t_{11} + (n_{11}c - 2dn_{21})t_{21} = 0$$

and we can easily check by Proposition 11 that $2n_{11} + cn_{21}$ or $n_{11}c - 2dn_{21}$ is nonzero.

For the elements of $\mathbb{T}_1$, we again conclude by Proposition 11 because $a = 0$ and we have ($N + I \bmod \ell$) $\in \mathbb{T}_1 \setminus \{0\}$, thus (4.2) becomes

$$z - (2(n_{11} + 1) + cn_{21})t_{11} + (2dn_{21} - c(n_{11} + 1))t_{21} = 0. \tag{4.3}$$

If $n = a + b$ and $b > 0$, we can reason as in the previous case. Now the condition for M' to be in $\mathcal{H}_{a,b}(a + b + 1)$ is that (4.2) is *not* satisfied: we conclude because that equation has $\ell^{-1} \cdot \#\mathbb{T}$ solutions.

We now prove (ii). The assertion for $n > a + b$ is the content of Lemma 23, so in particular we know $\mathcal{M}_{a,b}(a+b+1) = \mathcal{H}_{a,b}(a+b+1)$ and we may suppose $n \leqslant a + b$. We clearly have $\mathcal{M}_{a,b}(n) \subseteq \mathcal{H}_{a,b}(n)$ and are left to prove the other inclusion. The assumption $\mathcal{M}_{a,b} \neq \emptyset$ implies that for all $x \geqslant 1$ the sets $\mathcal{M}_{a,b}(x)$ and $\mathcal{H}_{a,b}(x)$ are nonempty and hence by (i) we know $f(x) \neq 0$ for all $x \geqslant n_0$. Thus for any $M \in \mathcal{H}_{a,b}(n)$ there is some $M' \in \mathcal{H}_{a,b}(a + b + 1)$ satisfying $M' \equiv M \pmod{\ell^n}$, and we deduce $M \in \mathcal{M}_{a,b}(n)$.

Finally, we prove (iii). The condition $f(a) = 0$ is equivalent to $b > 0$ and $\#\mathbb{T} - \#\mathbb{T}^\times - 1 = 0$. By (i), if $f(a) = 0$ then $\mathcal{H}_{a,b}(a + 1)$ is empty and hence also $\mathcal{M}_{a,b}(a + 1)$ and $\mathcal{M}_{a,b}$ are empty. If $f(a) \neq 0$ then we have $f(x) \neq 0$ for all $x \geqslant 1$. Since $\mathcal{H}_{a,b}(a)$ contains the identity, we deduce that $\mathcal{H}_{a,b}(a + b + 1) = \mathcal{M}_{a,b}(a + b + 1)$ is nonempty, and hence $\mathcal{M}_{a,b} \neq \emptyset$. □

5. The number of lifts for the reductions of matrices

5.1. Main result. We study the lifts of a given matrix $M \in \mathcal{M}_{a,b}(n)$ to $\mathcal{M}_{a,b}(n+1)$, namely the matrices in $\mathcal{M}_{a,b}(n+1)$ which are congruent to M modulo ℓ^n.

Theorem 28. *Let G be an open subgroup of either $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or the normalizer N of a Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let n_0 be the level of G. For $n \geqslant n_0$ the number of lifts of a matrix $M \in \mathcal{M}_{a,b}(n)$ to $\mathcal{M}_{a,b}(n + 1)$ is independent of M in the first case, while in the second case it depends at most on whether M belongs to either $C(n)$ or $(N \setminus C)(n)$.*

Proof of Theorem 28. If G is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or if C is unramified, the number of lifts of M to $G(n+1)$ is independent of M by Theorem 27(i). If C is ramified the assertion follows from Theorems 30 and 31. □

Example 29. The number of lifts may indeed depend on the coset of N/C. Suppose that ℓ is odd and consider the Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with parameters $(0,\ell)$. If G is the normalizer of C then the matrices

$$\begin{pmatrix} 1 & \ell \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & -\ell \\ 1 & -1 \end{pmatrix}$$

are in $\mathcal{M}_{0,1}$ and their reductions modulo ℓ have respectively ℓ^2 and $\ell^2-\ell$ lifts to $\mathcal{M}_{0,1}(2)$. Indeed, their lifts to $G(2)$ are of the form

$$L = \begin{pmatrix} 1+\ell u & \ell \\ 1+\ell v & 1+\ell u \end{pmatrix} \quad \text{and} \quad L' = \begin{pmatrix} 1+\ell u & -\ell \\ 1+\ell v & -1-\ell u \end{pmatrix}$$

respectively, where $u, v \in \mathbb{Z}/\ell\mathbb{Z}$: we have $\det_\ell(L-I) = 1$ for every u, v while $\det_\ell(L'-I) = 1$ holds if and only if $2u - 1 \not\equiv 0 \pmod{\ell}$.

5.2. Ramified Cartan subgroups.

Theorem 30. *Let G be open in a ramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let n_0 be the level of G. For all $a, b \geqslant 0$ and for all $n \geqslant n_0$ the number of lifts of a matrix $M \in \mathcal{M}_{a,b}(n)$ to $\mathcal{M}_{a,b}(n+1)$ is independent of M.*

Proof. For $n \leqslant a$ the set $\mathcal{M}_{a,b}(n)$ consists at most of the identity matrix, so suppose $n > a$. Let $(0,d)$ be the parameters for the Cartan subgroup (for convenience, we do not use a different notation for d and its reductions modulo powers of ℓ). The matrices in $\mathcal{M}_{a,b}(n)$ are of the form

$$M = I + \ell^a \begin{pmatrix} x & dy \\ y & x \end{pmatrix} \tag{5.1}$$

where $x, y \in \mathbb{Z}/\ell^{n-a}\mathbb{Z}$ are not both divisible by ℓ and have lifts $X, Y \in \mathbb{Z}_\ell$ satisfying $v_\ell(X^2 - dY^2) = b$.

If all matrices in $\mathcal{M}_{a,b}(n)$ satisfy $x \equiv 0 \pmod{\ell^{n-a}}$ then they all have the same number of lifts to $\mathcal{M}_{a,b}(n+1)$. Since y is a unit, for any M_1, M_2 in $\mathcal{M}_{a,b}(n)$ there is an obvious bijection between the lifts of $M_1 - I$ and of $M_2 - I$ given by rescaling by a suitable unit.

If some $M_0 \in \mathcal{M}_{a,b}(n)$ satisfies $x_0 \not\equiv 0 \pmod{\ell^{n-a}}$ and either $v_\ell(x_0^2) \neq v_\ell(d)$ or $v_\ell(x_0^2) = v_\ell(d) = v_\ell(x_0^2 - dy_0^2)$ then every matrix in $\mathcal{M}_{a,b}(n)$ has ℓ^2 lifts to $\mathcal{M}_{a,b}(n+1)$.

It suffices to show that for $M \in \mathcal{M}_{a,b}(n)$ all lifts X, Y of x, y to $\mathbb{Z}_\ell$ satisfy $v_\ell(X^2 - dY^2) = b$ because this implies that all lifts of M to G belong to $\mathcal{M}_{a,b}$.

If $v_\ell(x_0^2) < v_\ell(d)$ then for any X_0, Y_0 lifting x_0, y_0 we have $v_\ell(X_0^2 - dY_0^2) = v_\ell(X_0^2) = v_\ell(x_0^2)$, so this number is independent of the lift and it is equal to b. In particular, we have $b < v_\ell(d)$ and $b < 2(n-a)$. For $M \in \mathcal{M}_{a,b}(n)$ there exist lifts $X, Y \in \mathbb{Z}_\ell$ of x, y that satisfy $v_\ell(X^2 - dY^2) = b$. We deduce

$v_\ell(X^2) = b$ and hence $v_\ell(x^2) \leqslant b$: since $v_\ell(x^2) < v_\ell(d)$ and $x \not\equiv 0 \pmod{\ell^{n-a}}$ we can reason as for M_0 and we conclude.

If $v_\ell(x_0^2) > v_\ell(d)$ then y_0 must be a unit, so we have $v_\ell(d) = v_\ell(x_0^2 - dy_0^2)$, and the same holds for all lifts X_0, Y_0. In particular, we have

$$b = v_\ell(d) < 2(n-a).$$

If $v_\ell(x_0^2) = v_\ell(d) = v_\ell(x_0^2 - dy_0^2)$, we write $x_0 = \ell^k u_0$ and $d = \ell^{2k}\delta$, where u_0, δ are units and $k < n-a$. Then $u_0^2 - \delta y_0^2$ is a unit and hence $v_\ell(U_0^2 - \delta Y_0^2) = 0$ for all lifts U_0, Y_0 of u_0, y_0. We deduce $v_\ell(X_0^2 - dY_0^2) = v_\ell(d)$ for all lifts X_0, Y_0 of x_0, y_0 and again we have $b = v_\ell(d) < 2(n-a)$.

So suppose $b = v_\ell(d) < 2(n-a)$. For $M \in \mathcal{M}_{a,b}(n)$ there are lifts X, Y of x, y satisfying $v_\ell(X^2 - dY^2) = b$ and hence $v_\ell(X^2) \geqslant v_\ell(d)$ and $v_\ell(x^2 - dy^2) \leqslant v_\ell(d)$. If $x \not\equiv 0 \pmod{\ell^{n-a}}$ then either $v_\ell(x^2) \neq v_\ell(d)$ or we have $v_\ell(x^2) = v_\ell(d)$ and $v_\ell(x^2 - dy^2) = v_\ell(d)$, so we can reason as for M_0. If $x \equiv 0 \pmod{\ell^{n-a}}$ then $v_\ell(x^2) > v_\ell(d)$ and y is a unit: we deduce $v_\ell(X^2 - dY^2) = b$ for all lifts X, Y.

If some $M_0 \in \mathcal{M}_{a,b}(n)$ satisfies $x_0 \not\equiv 0 \pmod{\ell^{n-a}}$, $v_\ell(x_0^2) = v_\ell(d)$ and $v_\ell(x_0^2 - dy_0^2) > v_\ell(d)$, then no $M \in \mathcal{M}_{a,b}(n)$ has $x \equiv 0 \pmod{\ell^{n-a}}$. From $v_\ell(x_0^2 - dy_0^2) > v_\ell(d)$ we deduce $b > v_\ell(d)$. Supposing that such an M exists, let X, Y be lifts of x, y to $\mathbb{Z}_\ell$ such that $v_\ell(X^2 - dY^2) = b$. Since y must be a unit, $v_\ell(X^2 - dY^2) > v_\ell(d)$ implies $v_\ell(X^2) = v_\ell(dY^2) = v_\ell(d)$. We deduce $v_\ell(x_0) = v_\ell(X) \geqslant v_\ell(x)$, which contradicts $v_\ell(x_0) < n - a \leqslant v_\ell(x)$.

Finally, if all $M \in \mathcal{M}_{a,b}(n)$ satisfy $x \not\equiv 0 \pmod{\ell^{n-a}}$, $v_\ell(x^2) = v_\ell(d)$ and $v_\ell(x^2 - dy^2) > v_\ell(d)$ then the number of lifts of M to $\mathcal{M}_{a,b}(n+1)$ only depends on G, d, n, a, b. The hypotheses imply $v_\ell(x^2) = v_\ell(dy^2)$ and hence y is a unit, otherwise neither x nor y would be units. We can write $d = \ell^{2k}\delta$, $x = \ell^k u$ and $X = \ell^k U$ where δ, u, U are units. We are counting the reductions modulo ℓ^{n-a+1} of the pairs $(X, Y) \in \mathbb{Z}_\ell^2$ that satisfy:

$$\begin{cases} U \equiv u \pmod{\ell^{n-a-k}} \\ Y \equiv y \pmod{\ell^{n-a}} \\ v_\ell(U^2 - \delta Y^2) = b - 2k. \end{cases} \tag{5.2}$$

Consider the case where ℓ is odd. If $b - 2k \leqslant n - a - k$, the third condition of (5.2) is a consequence of the first two because it only depends on U, Y through u, y (since by assumption it holds for some lifts, it then holds for all lifts). So M has ℓ^2 lifts to $\mathcal{M}_{a,b}(n+1)$. Now suppose that $b - 2k > n - a - k$.

We know that δ is a square in $\mathbb{Z}_\ell^\times$ because $\ell \mid u^2 - \delta y^2$ and $\ell \nmid y$. Since ℓ is odd, we may assume without loss of generality that $u - \sqrt{\delta} y \equiv 0 \pmod{\ell}$ and $u + \sqrt{\delta} y \not\equiv 0 \pmod{\ell}$. We may then rewrite the third condition of (5.2) as

$$U - \sqrt{\delta}\, Y \equiv 0 \pmod{\ell^{b-2k}}, \quad U - \sqrt{\delta}\, Y \not\equiv 0 \pmod{\ell^{b-2k+1}}. \tag{5.3}$$

If we choose $(Y \bmod \ell^{n-a+1})$ arbitrarily among the lifts of y, (5.3) uniquely determines the value of $(U \bmod \ell^{n-a-k+1})$, so M has ℓ lifts to $\mathcal{M}_{a,b}(n+1)$.

Now consider the case $\ell = 2$. If $b - 2k \leqslant n - a - k + 1$ there are 4 lifts for M to $\mathcal{M}_{a,b}(n+1)$ because again the third condition of (5.2) is a consequence of the first two: notice that $(u \bmod 2^{n-a-k})$ determines $(u^2 \bmod 2^{n-a-k+1})$, and likewise for y. Suppose instead that $b - 2k > n - a - k + 1$. If δ is a square in $\mathbb{Z}_2^\times$ we can proceed as for ℓ odd, where we may suppose $v_2(U - \sqrt{\delta}Y) = b - 2k - 1$ and $v_2(U + \sqrt{\delta}Y) = 1$ because $U - \sqrt{\delta}Y$ and $U + \sqrt{\delta}Y$ are even and not both divisible by 4. Thus M has 2 lifts to $\mathcal{M}_{a,b}(n+1)$. Finally, suppose that δ is not a square in $\mathbb{Z}_2^\times$, i.e., $\delta \not\equiv 1 \pmod 8$. For all $X, Y \in \mathbb{Z}_2$ lifting x, y we know that Y is odd, and we have

$$v_2(X^2 - dY^2) = 2k + v_2(U^2 - \delta Y^2) = 2k + \begin{cases} 1, & \text{if } \delta \equiv 3 \pmod 4 \\ 2, & \text{if } \delta \equiv 5 \pmod 8. \end{cases}$$

Since $v_2(X^2 - dY^2)$ is independent of X, Y, the matrix M has 4 lifts to $\mathcal{M}_{a,b}(n+1)$. □

5.3. Normalizers of ramified Cartan subgroups. Recall from Proposition 26 that $\mathcal{M}^*_{a,b} = \emptyset$ if ℓ is odd and $a > 0$, or if $\ell = 2$ and $a > 1$.

Theorem 31. *Let G be open in the normalizer of a ramified Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let n_0 be the level of G. Assume $a = 0$ if ℓ is odd, and $a \in \{0, 1\}$ if $\ell = 2$. Let $n \geqslant 1$.*

If ℓ is odd, define $\mathcal{N}_{a,b}(n)$ as the subset of $G(n) \setminus C(n)$ consisting of those matrices M that satisfy the following conditions:

- *$\det_\ell(M - I) \geqslant n$, if $n \leqslant b$; $\det_\ell(M - I) = b$, if $n > b$.*

If $\ell = 2$, define $\mathcal{N}_{a,b}(n)$ as the subset of $G(n) \setminus C(n)$ consisting of those matrices M that satisfy the following conditions:

- *$M \equiv I \pmod{2^a}$, $M \not\equiv I \pmod{2^{a+1}}$;*
- *$\det_2(M-I) \geqslant n+1$, if $n < 2a+b$; $\det_2(M-I) = 2a+b$, if $n \geqslant 2a+b$.*

Define for ℓ odd and $\ell = 2$ respectively:

$$f(n) = \begin{cases} \ell & \text{if } n < b \\ \ell(\ell-1) & \text{if } n = b \\ \ell^2 & \text{if } n > b, \end{cases} \qquad f(n) = \begin{cases} 2 & \text{if } n < 2a + b \\ 4 & \text{if } n \geqslant 2a + b. \end{cases}$$

(i) *For every $n \geqslant n_0$ we have $\#\mathcal{N}_{a,b}(n+1) = f(n) \cdot \#\mathcal{N}_{a,b}(n)$. More precisely, for every matrix in $\mathcal{N}_{a,b}(n)$ the number of lifts to $\mathcal{N}_{a,b}(n+1)$ is $f(n)$.*

(ii) *If $n \geqslant n_0$ or if $n > a + b$ we have $\mathcal{M}^*_{a,b}(n) = \mathcal{N}_{a,b}(n)$.*

Proof. We first prove (i). The parameters for C are $(0, d)$, where $\ell \mid d$ if ℓ is odd, and by Lemma 16 any matrix in $G \setminus C$ is of the form

$$M = \begin{pmatrix} x & dy \\ -y & -x \end{pmatrix}. \tag{5.4}$$

The case ℓ odd ($n \geqslant n_0$ and $a = 0$). If $b < n$, every lift of a matrix in $\mathcal{N}_{0,b}(n)$ to $G(n+1)$ is in $\mathcal{N}_{0,b}(n+1)$. If $b \geqslant n > 0$ we proceed as for

Theorem 27, noticing two facts: by Proposition 26 no matrix in $G \setminus C$ is congruent to the identity modulo ℓ; the coefficient of t_{11} in (4.3) is nonzero because $\det_\ell(M-I) > 0$ gives $x^2 \equiv 1 \pmod{\ell}$, and we have $n_{11} + 1 \equiv x \pmod{\ell}$.

The case $\ell = 2$ ($n \geqslant n_0$ and $a \in \{0,1\}$). Remark that $(M \bmod 2^n)$ determines $\det(M-I)$ modulo 2^{n+1}. In particular, $\mathcal{N}_{a,b}(n)$ is well-defined. Fix $M \in \mathcal{N}_{a,b}(n)$, and let L be a lift of M to $G(n+1)$. Since $n \geqslant 2$, we know $L \equiv I \pmod{2^a}$ and $L \not\equiv I \pmod{2^{a+1}}$. If $n \geqslant 2a+b$, by the above remark all 4 lifts of M to $G(n+1)$ are in $\mathcal{N}_{a,b}(n+1)$. If $n < 2a+b$, we have $\det_2(M-I) \geqslant n+1$ and hence $\det_2(L-I) \geqslant n+1$: writing any lift of M in the form $L' = L + 2^n T$ with T as in (4.1), we are left to verify $\det_2(L'-I) \geqslant n+2$ for $n+1 < 2a+b$ and $\det_2(L'-I) = n+1$ for $n+1 = 2a+b$. We thus study the inequality $\det_2\left((L-I) + 2^n T\right) \geqslant n+2$ and an explicit verification (by Lemma 16 and because $2^{n+2} \mid 2^{2n}$) shows that there are precisely two lifts in $\mathcal{N}_{a,b}(n+1)$ as claimed.

We can prove (i)⇒(ii) as in Theorem 27: we clearly have $f(n) \neq 0$ for all $n \geqslant 1$, and we have $\mathcal{N}_{a,b}(2a+b+1) = \mathcal{M}^*_{a,b}(2a+b+1)$ because the defining conditions hold for a matrix if and only if they hold for its lifts to G. □

6. Measures related to the 1-eigenspace

6.1. The case of $\mathbf{GL_2}(\mathbb{Z}_\ell)$ and unramified Cartan subgroups.

Proposition 32. *Suppose that G is open either in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or in the normalizer of an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Suppose $\mathcal{M}_{a,b} \neq \emptyset$. We have $\mathcal{M}_{a,b}(n_0) = \{I\}$ if $n_0 \leqslant a$; moreover $\mathcal{M}_{a,b}(n_0) = \mathcal{M}_{a,n_0-a}(n_0)$ if $a < n_0 \leqslant a+b$, and in particular we have:*

$$\mu_{a,b}(n_0) = \begin{cases} \#G(n_0)^{-1} & \text{if } n_0 \leqslant a \\ \mu_{a,n_0-a}(n_0) & \text{if } a < n_0 \leqslant a+b. \end{cases}$$

Proof. For $n_0 \leqslant a$ the set $\mathcal{M}_{a,b}(n_0)$ contains at most the identity and it is nonempty by the assumption on $\mathcal{M}_{a,b}$. Now suppose $a < n_0 \leqslant a+b$. We claim that $\mathcal{M}_{a,n_0-a} \neq \emptyset$: the statement then follows from Theorem 27(ii) because by definition $\mathcal{H}_{a,b}(n_0) = \mathcal{H}_{a,n_0-a}(n_0)$.

We prove the claim by making use of Theorem 27. The assumption $\mathcal{M}_{a,b} \neq \emptyset$ implies that the set $\mathcal{M}_{a,b}(n_0) = \mathcal{H}_{a,b}(n_0) = \mathcal{H}_{a,n_0-a}(n_0)$ is nonempty. Since $n_0 > a$ we have $f(n_0) \neq 0$ and hence $\mathcal{H}_{a,n_0-a}(n_0+1)$ is nonempty. This set equals $\mathcal{M}_{a,n_0-a}(n_0+1)$ because $n_0+1 > a+(n_0-a)$. □

Proposition 33. *Let G' be either $\mathrm{GL}_2(\mathbb{Z}_\ell)$, an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, or the normalizer of an unramified Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.*

If G is open in G', we have:

$$\mu_{a,b} = \mu_{a,b}(n_0) \cdot \begin{cases} \#\mathbb{T}^{-(a+1-n_0)} \cdot \#\mathbb{T}^\times & n_0 \leqslant a, b = 0 \\ \#\mathbb{T}^{-(a+1-n_0)}(\#\mathbb{T} - \#\mathbb{T}^\times - 1)\,\dfrac{(\ell-1)}{\ell^b} & n_0 \leqslant a, b > 0 \\ \ell^{-(a+b+1-n_0)}(\ell-1) & a < n_0 \leqslant a+b \\ 1 & n_0 > a+b. \end{cases}$$

We also have

$$\mu_{a,b} = [G' : G] \cdot \#\mathbb{T}^{-a} \cdot \varepsilon \cdot \begin{cases} 1 & \text{if } n_0 \leqslant a, b = 0 \\ \dfrac{\#\mathbb{T} - \#\mathbb{T}^\times - 1}{\#\mathbb{T}^\times} \cdot \ell^{-b}(\ell-1) & \text{if } n_0 \leqslant a, b > 0 \end{cases}$$

where $\varepsilon = \frac{1}{2}$ if G' is the normalizer of a Cartan subgroup and $\varepsilon = 1$ otherwise.

Proof. To prove the first assertion we may suppose $\mathcal{M}_{a,b} \neq \emptyset$, because otherwise $\mu_{a,b} = \mu_{a,b}(n_0) = 0$. The formula for $n_0 > a+b$ has been proven in Lemma 25. We have

$$\#\mathcal{M}_{a,b}(a+b+1) = \#\mathcal{M}_{a,b}(n_0) \prod_{j=n_0}^{a+b} \frac{\#\mathcal{M}_{a,b}(j+1)}{\#\mathcal{M}_{a,b}(j)}$$

and by definition of n_0 we know $\#G(a+b+1) = \#G(n_0) \cdot \#\mathbb{T}^{a+b+1-n_0}$. We then obtain

$$\mu_{a,b} = \mu_{a,b}(n_0) \cdot \prod_{j=n_0}^{a+b} \#\mathbb{T}^{-1} \cdot \frac{\#\mathcal{M}_{a,b}(j+1)}{\#\mathcal{M}_{a,b}(j)}$$

and the formulas for $n_0 \leqslant a+b$ can easily be deduced from Theorem 27. We now turn to the second assertion. By Theorem 27(iii), $b = 0$ implies $\mathcal{M}_{a,b} \neq \emptyset$ while $b > 0$ and $\mathcal{M}_{a,b} = \emptyset$ imply $\#\mathbb{T} - \#\mathbb{T}^\times - 1 = 0$. In the latter case the formula for $\mu_{a,b}$ clearly holds, so we can assume $\mathcal{M}_{a,b} \neq \emptyset$ and hence $\mu_{a,b}(n_0) = \#G(n_0)^{-1}$ by Proposition 32. By Remark 17 and Lemma 13 (respectively, by Definition 19) we know that $\#G'(1) = \varepsilon^{-1} \cdot \#\mathbb{T}^\times$ and $\#G'(n_0) = \#G'(1) \cdot \#\mathbb{T}^{n_0-1}$. We conclude because we have

$$\#G(n_0)^{-1} = [G' : G] \cdot (\#G'(n_0))^{-1} = [G' : G] \cdot \varepsilon \cdot (\#\mathbb{T}^\times)^{-1} \cdot \#\mathbb{T}^{1-n_0}. \quad \square$$

Example 34. Let G be the inverse image in $\mathrm{GL}_2(\mathbb{Z}_2)$ of

$$G(2) = \left\langle \begin{pmatrix} 3 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 3 & 0 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}).$$

Since G has index 8 and level 2 in $\mathrm{GL}_2(\mathbb{Z}_2)$, by Proposition 32 we get $\mu_{a,b}(2) = 1/12$ if $a \geqslant 2$ and $\mu_{a,b}(2) = \mu_{a,2-a}(2)$ if $a = 0, 1$ and $a+b \geqslant 2$. A direct computation gives $\mu_{0,0}(2) = 1/3$, $\mu_{1,0}(2) = 1/12$, $\mu_{0,2}(2) = 1/2$ and

$\mu_{0,1}(2) = \mu_{1,1}(2) = 0$. So by Proposition 33 we have:

$$\mu_{a,b} = \begin{cases} 0 & \text{if } a \in \{0,1\}, b = 1 \\ 1/3 & \text{if } a = b = 0 \\ 1/12 & \text{if } a = 1, b = 0 \\ 2^{-b} & \text{if } a = 0, b \geqslant 2 \\ 8 \cdot 2^{-4a} & \text{if } a \geqslant 2, b = 0 \\ 12 \cdot 2^{-4a-b} & \text{if } a \geqslant 2, b > 0. \end{cases}$$

Lemma 35. *Suppose that G is open in a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let n_0 be the level of G. For all $a \geqslant n_0$ we have $\mu_{a,b} = \ell^{-2(a-n_0)}\mu_{n_0,b}$.*

Proof. We prove that for all $a \geqslant n_0$ we have $\mu(\mathcal{M}_{a+1,b}) = \ell^{-2}\mu(\mathcal{M}_{a,b})$. We claim that the map

$$\begin{aligned} \phi : \mathcal{M}_{a,b}(a+b+2) &\to \mathcal{M}_{a+1,b}(a+b+2) \\ M &\mapsto I + \ell(M - I) \end{aligned}$$

is well-defined, surjective and ℓ^2-to-1, so we have:

$$\mu(\mathcal{M}_{a+1,b}) = \frac{\#\mathcal{M}_{a+1,b}(a+b+2)}{\#G(a+b+2)} = \frac{\ell^{-2}\#\mathcal{M}_{a,b}(a+b+2)}{\#G(a+b+2)} = \ell^{-2}\mu(\mathcal{M}_{a,b}).$$

We are left to prove the claim. Since $a \geqslant n_0$, all matrices in the Cartan subgroup that are congruent to the identity modulo ℓ^a are in G thus we may suppose that G is the Cartan subgroup. A matrix $M \in G(a+b+2)$ is in the domain of ϕ if and only if the conditions in (3.4) hold, and these imply that $\phi(M)$ is in $\mathcal{M}_{a+1,b}(a+b+2)$ by (2.1) and because we have:

$$\begin{aligned} \phi(M) &\equiv I \pmod{\ell^{a+1}}, \\ \phi(M) &\not\equiv I \pmod{\ell^{a+2}}, \\ \det_\ell(\phi(M) - I) &= 2(a+1) + b. \end{aligned}$$

If N is in the codomain of ϕ then $I + \ell^{-1}(N - I)$ is well-defined modulo ℓ^{a+b+1}: by Lemma 23 this matrix belongs to $\mathcal{M}_{a,b}(a+b+1)$ and if M is any lift of it to $\mathcal{M}_{a,b}(a+b+2)$ we have $\phi(M) = N$. This proves that ϕ is surjective (we may suppose that domain and codomain are nonempty, otherwise they must both be empty and the statement holds trivially). The set of preimages of N consists of the matrices in $\mathcal{M}_{a,b}(a+b+2)$ congruent to M modulo ℓ^{a+b+1}, thus there are ℓ^2 such preimages by Theorem 27(i)–(ii). □

Remark 36. For every $a, b \geqslant 0$ we have $\mathcal{M}_{a,b}(\mathrm{GL}_2(\mathbb{Z}_\ell)) \neq \emptyset$ because this set contains

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{for } a = b = 0\ , \text{ and } \quad \begin{pmatrix} 1 & \ell^{a+b} \\ \ell^a & 1 \end{pmatrix} \quad \text{otherwise.}$$

If C is a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we have $\mathcal{M}_{a,b}(C) \neq \emptyset$ for every $a, b \geqslant 0$, with the exception of $\ell = 2$ and $a = 0$: considering the diagonal model, if $\ell \neq 2$ or if $a \geqslant 1$ the set $\mathcal{M}_{a,b}(C)$ contains $\begin{pmatrix} 1+\ell^a & 0 \\ 0 & 1+\ell^{a+b} \end{pmatrix}$; however, for $\ell = 2$ every diagonal invertible matrix is congruent to the identity modulo 2.

If C is a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we have $\mathcal{M}_{a,b}(C) = \emptyset$ for every $b > 0$. Indeed, if $M \in \mathcal{M}_{a,b}(C)$ then for ℓ odd (resp. $\ell = 2$) we have

$$\ell^{-a}(M - I) = \begin{pmatrix} z & dw \\ w & z \end{pmatrix} \quad \text{resp.} \quad 2^{-a}(M - I) = \begin{pmatrix} z & dw \\ w & z + w \end{pmatrix}$$

for some $z, w \in \mathbb{Z}_\ell$, and by Propositions 10 and 11 these matrices are invertible unless z and w are zero modulo ℓ.

6.2. Ramified Cartan subgroups.

Lemma 37. *Suppose that G is open in a Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with parameters $(0, d)$. Write $d = m\ell^v$ with $\ell \nmid m$.*

(i) *If v is odd, we have $\mu_{a,b} = 0$ for every $b > v$.*
(ii) *If v is even and m is not a square in $\mathbb{Z}_\ell^\times$, we have $\mu_{a,b} = 0$ for every $b > v + 2$ (if ℓ is odd we have $\mu_{a,b} = 0$ for $b > v$).*
(iii) *If v is even and m is a square in $\mathbb{Z}_\ell^\times$, consider the Cartan subgroup C' of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with parameters $(0, 1)$. There exists a closed subgroup G_1 of C' such that the following holds: there is an explicit isomorphism between G and G_1; the level of G_1 does not exceed the level of G by more than $v/2$; for all $b > v$ the sets $\mathcal{M}_{a,b}(G)$ and $\mathcal{M}_{a+v/2,b-v}(G_1)$ have the same Haar measure in G and G_1 respectively.*

Proof. Fix $n > a + b + 1$. By (2.1) we can write any matrix in $\mathcal{M}_{a,b}(n)$ as

$$M = I + \ell^a \begin{pmatrix} x & dy \\ y & x \end{pmatrix}$$

where $x, y \in \mathbb{Z}/\ell^{n-a}\mathbb{Z}$ satisfy $v_\ell(x^2 - dy^2) = b$ and we have $v_\ell(x) = 0$ or $v_\ell(y) = 0$.

Proof of (i): We have $v_\ell(x^2) \neq v_\ell(dy^2)$ and hence $v_\ell(x^2 - dy^2) \leqslant v$, which implies that $\mathcal{M}_{a,b}(n)$ is empty for $b > v$.

Proof of (ii): For $b > v$ we have $v_\ell(x^2) \geqslant v$ and we can write $b = v + v_\ell(x_1^2 - my^2)$, where $x = \ell^{v/2}x_1$. We must have $x_1^2 \equiv my^2 \pmod{\ell}$, which is impossible for ℓ odd because m is not a square modulo ℓ. If $\ell = 2$ and $b > v + 2$ we should similarly have $x_1^2 \equiv my^2 \pmod{8}$, which is impossible because m is not a square modulo 8.

Proof of (iii): Since d is a square in $\mathbb{Z}_\ell$, we may fix a square root $\sqrt{d}$ of it. Define G_1 to be the image of

$$\phi : G \to C'$$
$$I + \ell^a \begin{pmatrix} x & dy \\ y & x \end{pmatrix} \mapsto I + \ell^a \begin{pmatrix} x & y\sqrt{d} \\ y\sqrt{d} & x \end{pmatrix}.$$

Embedding G in $\mathrm{GL}_2(\mathbb{Q}_\ell)$, the map ϕ can be identified with the conjugation by $\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{d} \end{pmatrix}$, thus ϕ is a continuous group isomorphism between G and G', and for every $M \in G$ we have

$$\det \phi(M) = \det(M) \quad \text{and} \quad \det(\phi(M) - I) = \det(M - I).$$

Let n_0 denote the level of G. The level of G_1 is at most $n_0 + v/2$ because any matrix in C' which is congruent to the identity modulo $\ell^{n_0+v/2}$ is the image via ϕ of a matrix in C that is congruent to the identity modulo ℓ^{n_0}:

$$I + \ell^{n_0} \begin{pmatrix} \ell^{v/2}z & yd \\ y & \ell^{v/2}z \end{pmatrix} \xrightarrow{\phi} I + \ell^{n_0+v/2} \begin{pmatrix} z & y\sqrt{m} \\ y\sqrt{m} & z \end{pmatrix}.$$

If $b > v$, we have $v_\ell(x^2) \geqslant v$ and a straightforward verification shows that ϕ induces a bijection from $\mathcal{M}_{a,b}(G)$ to $\mathcal{M}_{a+v/2,b-v}(G_1)$, and we conclude because a continuous isomorphism of profinite groups preserves the normalized Haar measure, see [FJ08, Proposition 18.2.2]. □

Lemma 38. *If G is open in the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ with parameters $(0,1)$ the sets $\mathcal{M}_{a,1}$ and $\mathcal{M}_{a,2}$ are empty. Moreover, there exists an open subgroup G_1 of the subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}_2)$ such that the following holds: there is an explicit isomorphism between G and G_1; the level of G_1 does not exceed the level of G by more than 1; for all $b > 2$ the sets $\mathcal{M}_{a,b}(G)$ and $\mathcal{M}_{a+1,b-2}(G_1)$ have the same Haar measure in G and G_1 respectively.*

Proof. We can write any matrix in $\mathcal{M}_{a,b}(G)$ as

$$M = I + 2^a \begin{pmatrix} x & y \\ y & x \end{pmatrix} \tag{6.1}$$

where at least one between x and y is a 2-adic unit. Working modulo 8, we see that $b = v_2(x^2 - y^2)$ cannot be 1 or 2.

We sketch the rest of the proof, which mimics Lemma 37(iii). We define a map ϕ from G to $\mathrm{GL}_2(\mathbb{Z}_2)$, denoting G_1 its image:

$$\phi(M) = I + 2^a \begin{pmatrix} x+y & 0 \\ 0 & x-y \end{pmatrix}. \tag{6.2}$$

We clearly have $\det_2(\phi(M) - I) = \det_2(M - I)$. If $b > 2$, then $x + y$ and $x - y$ must be even and not both divisible by 4, and it follows that $\phi(M) \in \mathcal{M}_{a+1,b-2}(G_1)$. □

Lemma 39. *Let G be open in a Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with parameters $(0,d)$, where d is a square in $\mathbb{Z}_\ell$. For any fixed value of a, the set $\mathcal{M}_{a,b}(n_0)$ does not depend on b provided that $b \geqslant b_0$, where*

$$b_0 := \max\{1 + v_\ell(4d), n_0 - a + v_\ell(2d)\}.$$

Proof. Let $b \geqslant b_0 > 0$ and consider a matrix in $\mathcal{M}_{a,b}$: $M = I + \ell^a \begin{pmatrix} x & dy \\ y & x \end{pmatrix}$. It suffices to show that for every $b' \geqslant b_0$ there is $M' \in \mathcal{M}_{a,b'}$ that is congruent to M modulo ℓ^{n_0}. We have $v_\ell(x^2 - dy^2) \geqslant b > v_\ell(d)$ and at least one among x and y is a unit. One checks easily that y cannot be divisible by ℓ, so we have $v_\ell(x^2) = v_\ell(d)$ and we can define $y'' = x/\sqrt{d}$. Given two units in $\mathbb{Z}_\ell$, either their sum or their difference has valuation $v_\ell(2)$, so up to replacing $\sqrt{d}$ by $-\sqrt{d}$ we get $v_\ell(x - \sqrt{d}y) \geqslant b - v_\ell(d)/2 - v_\ell(2) \geqslant n_0 - a + v_\ell(d)/2$ and hence $y'' \equiv y \pmod{\ell^{n_0-a}}$. Defining $B := b' - v_\ell(d)/2 - v_\ell(2) \geqslant n_0 - a$, the matrix

$$M' = I + \ell^a \begin{pmatrix} x + \ell^B & dy'' \\ y'' & x + \ell^B \end{pmatrix}$$

is congruent to M modulo ℓ^{n_0} and we have $\det(M' - I) = \ell^{2a}(2x\ell^B + \ell^{2B})$. Since $B > v_\ell(d)/2 + v_\ell(2) = v_\ell(x) + v_\ell(2)$ we have $\det_\ell(M' - I) = 2a + b'$ and hence $M' \in \mathcal{M}_{a,b'}$. □

6.3. Normalizers of Cartan subgroups. Recall the notation from Section 3.6.

Theorem 40. *Let G be open in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let n_0 be the level of G.*

(i) *If ℓ is odd or C is unramified, we have:*

$$\mu(\mathcal{M}^*_{a,b}) = \begin{cases} 0 & \text{if } a > 0 \\ \mu(\mathcal{M}^*_{0,b}(n_0)) & \text{if } a = 0, b < n_0 \\ \mu(\mathcal{M}^*_{0,n_0}(n_0)) \cdot (\ell - 1) \cdot \ell^{n_0 - b - 1} & \text{if } a = 0, b \geqslant n_0. \end{cases}$$

(ii) *If $\ell = 2$ and C is ramified, we have:*

$$\mu(\mathcal{M}^*_{a,b}) = \begin{cases} 0 & \text{if } a > 1 \\ \mu(\mathcal{M}^*_{a,b}(n_0)) & \text{if } a \leqslant 1 \text{ and } 2a + b \leqslant n_0 \\ \mu(\mathcal{M}^*_{a,n_0+1}(n_0)) \cdot 2^{n_0 - 2a - b} & \text{if } a \leqslant 1 \text{ and } 2a + b > n_0. \end{cases}$$

Proof. For (i), by Proposition 26 we have $\mu(\mathcal{M}^*_{a,b}) = 0$ for $a > 0$. For $b < n_0$ we clearly have $\mu(\mathcal{M}^*_{0,b}) = \mu(\mathcal{M}^*_{0,b}(n_0))$. If $b \geqslant n_0$, Theorem 31(ii) implies

$$\mathcal{M}^*_{0,b}(n_0) = \{M \in (G \setminus C)(n_0) : \det_\ell(M - I) \geqslant n_0\} = \mathcal{M}^*_{0,n_0}(n_0)$$

so in particular we have $\mu(\mathcal{M}^*_{0,b}(n_0)) = \mu(\mathcal{M}^*_{0,n_0}(n_0))$. We conclude by Theorem 27 and 31 respectively, by the same argument used to prove Proposition 33.

(ii) follows analogously from Proposition 26 and Theorem 31. Indeed, if $2a + b > n_0$ then $\mathcal{M}^*_{a,b}(n_0)$ is independent of b by Theorem 31(ii). □

Corollary 41. *Let G be open in the normalizer N of a Cartan subgroup C of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. For $a \in \{0, 1\}$ there exist (effectively computable) rational numbers $c_1(a), c_2(a), c_3(a)$ such that*

$$\mu(\mathcal{M}_{a,b}) = c_1(a)\ell^{-b},$$
$$\mu(\mathcal{M}_{a,b} \cap (N \setminus C)) = c_2(a)\ell^{-b},$$
$$\mu(\mathcal{M}_{a,b} \cap C) = c_3(a)\ell^{-b},$$

hold for all sufficiently large b (and the bound is effective). The rational constants $c_i(a)$ may depend on ℓ and G, as well as on a.

Proof. The assertion for $\mathcal{M}_{a,b}$ follows from the other two, and the assertion for $\mathcal{M}_{a,b} \cap (N \setminus C)$ holds by Theorem 40. Now consider $\mathcal{M}_{a,b} \cap C$. Because of Lemmas 37 and 38, we only need to consider the case when C is a split Cartan subgroup. We apply Proposition 32 (in view of Remark 36) to deduce that $\mu_{a,b}(n_0)$ is constant for $b \geqslant n_0$ and then apply Proposition 33. □

7. The results of the introduction

7.1. Proof of Theorem 1.

Definition 42. We call a subset of $\mathbb{N}^2$ *admissible* if it is the product of two subsets of $\mathbb{N}$, each of which is either finite or consists of all integers greater than some given one. The family of finite unions of admissible sets is closed w.r.t. intersection, union and complement.

We describe a general computational strategy to determine $\mu_{a,b}$ for all $a, b \geqslant 0$. Depending on the input data (i.e., a finite amount of information about the group G), we can choose which of the previous results must be applied, and we can compute the finitely many rational parameters that appear in the statements. After a case distinction, we have formulas for all measures $\mu_{a,b}$ that depend only on a, b, and finitely many known constants. As it can be seen from the explicit description below, the cases give a partition of $\mathbb{N}^2$ into finitely many admissible subsets and on each of them the formula for $\mu_{a,b}$ is as requested. We first need to express the relevant properties of G in terms of finitely many parameters:

(1) The group G is open in G', which is either $\mathrm{GL}_2(\mathbb{Z}_\ell)$, a Cartan subgroup, or the normalizer of a Cartan subgroup. We describe a Cartan subgroup with the integer parameters (c, d) of Section 2.3, which also determine whether this is split, nonsplit or ramified. The cardinality of the tangent space $\mathbb{T}$ and of its subset $\mathbb{T}^\times$ is known, see Section 2.6.
(2) We fix an integer $n_0 \geqslant 1$ such that G is the inverse image in G' of $G(n_0)$ for the reduction modulo ℓ^{n_0}. If $\ell = 2$ and G' is (the

normalizer of) a ramified Cartan subgroup, we take $n_0 \geqslant 2$ (n_0 is not necessarily the level of G, see Remark 20).

(3) We need to know the finite group $G(n_0)$ explicitly. From this we extract various data, including the order of $G(n_0)$, the index $[G'(n_0) : G(n_0)] = [G' : G]$, and the following information: for each of the finitely many pairs (a, b) such that $a < n_0$ and $b \leqslant n_0 - a$, we need to know the counting measure $\mu_{a,b}(n_0)$ and whether the set $G(n_0) \cap \mathcal{M}_{a,b}(G'; n_0)$ is empty or not. For (normalizers of) ramified Cartan subgroups we may also need finitely many other quantities which can all be read off $G(n_0)$, see the description below.

We make repeated use of the following remark: suppose that for (a, b) in some admissible set $S = A \times B$ with A finite we have $\mu_{a,b} = c(a)\ell^{-b}$, where $c(a)$ is a rational number depending on a. Then S is the finite union of the sets $S_a = \{a\} \times B$, and by choosing the constant $c'(a)$ appropriately we have $\mu_{a,b} = c'(a)\ell^{-a\dim(G)-b}$ for all $(a, b) \in S_a$.

If $G' = \mathrm{GL}_2(\mathbb{Z}_\ell)$: We can compute the values $\mu_{a,b}$ for all pairs (a, b) such that $\mathcal{M}_{a,b} \neq \emptyset$ by Propositions 32 and 33. Up to refining the partition, we can ensure that $\mu_{a,b}$ is a constant multiple of ℓ^{-4a-b} on every set of the partition.

We are left to determine the pairs (a, b) such that $\mathcal{M}_{a,b} = \emptyset$ (and hence $\mu_{a,b} = 0$) and show that they form an admissible subset of $\mathbb{N}^2$. By Remark 36 we know $\mathcal{M}_{a,b}(G') \neq \emptyset$, and by Remark 22 we just need to know whether $G(n_0) \cap \mathcal{M}_{a,b}(G'; n_0)$ is empty. By Proposition 32 (applied to G') there are only finitely many distinct sets of the form $\mathcal{M}_{a,b}(G'; n_0)$ to consider and it is a finite computation to determine those that intersect $G(n_0)$ trivially.

If G' is a nonsplit Cartan subgroup: By Lemma 35 and Remark 36 we reduce to the case $a \leqslant n_0$ and $b = 0$. Thus by Proposition 33 we only need to evaluate $\mu_{a,0}(n_0)$ for $a \leqslant n_0$. Since we only have finitely many values of a to consider, up to refining the partition we find that $\mu_{a,b}$ is a constant multiple of ℓ^{-2a-b} on every set of the partition.

If G' is a split Cartan subgroup: By Lemma 35 we reduce to the case $a \leqslant n_0$, so fix one of those finitely many values for a. By Proposition 33 it suffices to evaluate $\mu_{a,b}(n_0)$ for all $b \geqslant 0$. If $\mathcal{M}_{a,b} \neq \emptyset$, by Proposition 32 we only need to consider the finitely many cases for which $b \leqslant n_0$.

We are left to determine the pairs (a, b) such that $\mathcal{M}_{a,b} = \emptyset$ (and hence $\mu_{a,b} = 0$) and show that they form an admissible subset of $\mathbb{N}^2$. By Remark 36 the set $\mathcal{M}_{a,b}(G')$ is empty (and hence $\mathcal{M}_{a,b} = \emptyset$) if and only if $\ell = 2$ and $a = 0$. In the remaining cases we have $\mathcal{M}_{a,b}(G') \neq \emptyset$ and $a \leqslant n_0$, so we may reason as for $G' = \mathrm{GL}_2(\mathbb{Z}_\ell)$. Up to refining the partition, we find that $\mu_{a,b}$ is a constant multiple of ℓ^{-2a-b} on every set of the partition.

If G' is a ramified Cartan subgroup: By Lemma 35 we reduce to the case $a \leqslant n_0$, so fix one of these finitely many values for a. By Propositions 10 and 11, the parameters for C are $(0, d)$ and we can apply Lemma 37. If we are in cases (i)–(ii) of this lemma, we only need to consider the finitely

many values $b \leqslant v_\ell(d) + 2$. The measure $\mu_{a,b}$ for a single pair (a, b) can be computed explicitly as $\mu_{a,b}(a+b+1)$. Notice that the group $G(a+b+1)$ and hence its subset $\mathcal{M}_{a,b}(a+b+1)$ can be determined from the knowledge of G' and $G(n_0)$. Now suppose that we are in case (iii) of Lemma 37. Recalling that $a \leqslant n_0$ is fixed, we may compute the finitely many measures $\mu_{a,b}$ where $b \leqslant v_\ell(d)$. For $b > v_\ell(d)$ we reduce to a similar problem for an unramified Cartan subgroup: if ℓ is odd, the Cartan subgroup with parameters $(0, 1)$ is unramified; if $\ell = 2$ we further apply Lemma 38. Once more, this gives a partition as requested.

The case when G' is the normalizer of a Cartan subgroup: As shown in Section 3.6, to reduce to the case when G' is a Cartan subgroup it suffices to compute the measures $\mu(\mathcal{M}^*_{a,b})$ for all $a, b \geqslant 0$. We achieve this by Theorem 40: it suffices to compute $\mu(\mathcal{M}^*_{a,b}(n_0))$ for finitely many pairs (a, b). The measures in the Cartan subgroup and those related to its complement in the normalizer add up to an expression of the desired form, because they can both be written as ℓ^{-2a-b} times a constant.

7.2. The special case where G has index 1.

Proof of Theorem 2. Consider Definition 19 and Proposition 33. The cases with $a > 0$ are clear because $n_0 = 1 \leqslant a$. If $a = b = 0$, we have $\mu_{0,0} = \mu_{0,0}(1) = \#\mathcal{M}_{0,0}(1)/\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ so it suffices to prove

$$\#\mathcal{M}_{0,0}(1) = \ell(\ell^3 - 2\ell^2 - \ell + 3).$$

Equivalently, we have to show that there are

$$\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) - \#\mathcal{M}_{0,0}(1) = \ell^3 - 2\ell$$

matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ that have 1 as an eigenvalue. This is done, e.g., in the course of [JR10, Proof of Theorem 5.5] (see also [Gek03, Section 4]), but for the convenience of the reader we sketch the computation. Matrices admitting 1 as an eigenvalue are the identity and those that are conjugate to one of the following:

$$J_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad J_\lambda = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \quad \lambda \neq 0, 1.$$

Since the centralizer of J_1 has size $\ell(\ell-1)$ while that of J_λ has size $(\ell-1)^2$, we may conclude by computing the size of the conjugacy classes as the index of the centralizer.

If $a = 0$ and $b > 0$, we have to evaluate $(\ell-1) \cdot \ell^{-b} \cdot \mu_{0,b}(1)$ for $b > 0$. By Proposition 32 and Remark 36 we have

$$\mu_{0,b}(1) = \mu_{0,1}(1) = \#\mathcal{M}_{0,1}(1)/\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

so it suffices to prove

$$\#\mathcal{M}_{0,1}(1) = (\ell^2 - \ell - 1)(\ell + 1).$$

We may conclude by noticing that $\mathcal{M}_{0,1}(1)$ consists of the $\ell^3-2\ell$ matrices in $\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ that have 1 as an eigenvalue, with the exception of the identity matrix. □

Proof of Theorem 3. We can take $n_0 = 1$ so the cases with $a \geqslant 1$ follow immediately from Proposition 33 and (2.5). Now suppose $a = 0$. Consider a split Cartan subgroup with the diagonal model. For $b = 0$, in order to evaluate $\mu_{0,0}(1)$ we count those diagonal matrices $\mathrm{diag}(x, y)$ such that xy and $(x-1)(y-1)$ are in $(\mathbb{Z}/\ell\mathbb{Z})^\times$: this means $x, y \not\equiv 0, 1 \pmod{\ell}$, hence there are $(\ell-2)^2$ choices, out of $(\ell-1)^2$ total elements. For $b > 0$ we have $\mu_{0,b}(1) = \mu_{0,1}(1)$ by Proposition 32 and Remark 36. There are $2(\ell-2)$ diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that exactly one of the two diagonal entries is congruent to 1 modulo ℓ, so we get by Proposition 33:

$$\mu_{0,b} = \mu_{0,b}(1)\ell^{-b}(\ell-1) = \frac{2(\ell-2)}{(\ell-1)^2}(\ell-1)\ell^{-b}.$$

Now consider the nonsplit case. By Remark 36 we know $\mathcal{M}_{a,b} = \emptyset$ for $b > 0$. For $b = 0$ we need to evaluate $\mu_{0,0}$: by Lemma 25 and by the previous case $a \geqslant 1$ we have

$$1 = \sum_{a,b\geqslant 0} \mu_{a,b} = \sum_{a\geqslant 0} \mu_{a,0} = \mu_{0,0} + \sum_{a\geqslant 1} \ell^{-2a}. \qquad \square$$

Proof of Theorem 4. Let C be the Cartan subgroup and let C' be as in Lemma 14. Fixing some $n > a + b$ we get

$$\begin{aligned}\mu_{a,b} = \mu_{a,b}(n) &= \frac{\#\mathcal{M}_{a,b}(n)}{\#(C \cup C')(n)} \\ &= \frac{\#(\mathcal{M}_{a,b}(n) \cap C(n)) + \#(\mathcal{M}_{a,b}(n) \cap C'(n))}{2 \cdot \#C(n)}.\end{aligned}$$

By definition we have $\mu^C_{a,b} = \#(\mathcal{M}_{a,b}(n) \cap C(n))/\#C(n)$, so it suffices to show $\mu^*_{a,b} = \#(\mathcal{M}_{a,b}(n) \cap C'(n))/\#C(n)$. If $a > 0$ then no matrix in $C'(n)$ is in $\mathcal{M}_{a,b}(n)$ by Lemma 16. For $a = 0$ we are left to prove that for $n = b+1$ we have $\#\mathcal{M}_{0,b}(n) \cap C'(n) = \mu^*_{0,b} \cdot \#C(n)$. By Lemma 16 the elements of $C'(b+1)$ are those matrices of the form

$$M = \begin{pmatrix} \alpha & -d\beta + c\alpha \\ \beta & -\alpha \end{pmatrix} \quad \alpha, \beta \in \mathbb{Z}/\ell^{b+1}\mathbb{Z} \tag{7.1}$$

where c, d are here the reductions modulo ℓ^{b+1} of the parameters of C. Thus we need to count the pairs $(\alpha, \beta) \in (\mathbb{Z}/\ell^{b+1}\mathbb{Z})^2$ satisfying

$$\det_\ell(M - I) = v_\ell(1 - \alpha^2 + d\beta^2 - c\alpha\beta) = b. \tag{7.2}$$

We also need $\det_\ell(M) = v_\ell(-\alpha^2 + d\beta^2 - c\alpha\beta) = 0$, which for $b > 0$ follows from (7.2).

The count for the split case will give $(\ell-1)(\ell-2)$ for $b = 0$ and $(\ell-1)^2\ell^b$ for $b > 0$. The count for the nonsplit case will give $(\ell+1)(\ell-2)$ for $b = 0$ and

$(\ell^2-1)\ell^b$ for $b>0$. We then conclude by Lemma 13 because $\#C(b+1)$ equals $(\ell-1)^2\ell^{2b}$ and $(\ell^2-1)\ell^{2b}$ for the split and the nonsplit case respectively. One can easily check that the affine curve $\mathcal{D}: 1-x^2+y(dy-cx)=0$ (defined over $\mathbb{Z}_\ell$) is smooth over $\mathbb{Z}/\ell\mathbb{Z}$. We have $\#\mathcal{D}(\mathbb{Z}/\ell\mathbb{Z})=\ell\pm 1$, where the sign is $-$ (resp. $+$) if C is split (resp. nonsplit). Indeed, $\mathcal{D}$ can be identified over $\mathbb{Z}/\ell\mathbb{Z}$ with the open subscheme of $\{Z^2-X^2+Y(dY-cX)=0\}\cong\mathbb{P}^1$ given by $Z\neq 0$, and by Propositions 10 and 11 there are two (resp. zero) $\mathbb{Z}/\ell\mathbb{Z}$-points with $Z=0$ if C is split (resp. nonsplit).

The case $b=0$. There are precisely $\ell^2-(\ell\pm 1)$ pairs $(\alpha,\beta)\in(\mathbb{Z}/\ell\mathbb{Z})^2$ that do not correspond to points in $\mathcal{D}(\mathbb{Z}/\ell\mathbb{Z})$. Since we only want invertible matrices, we need to exclude those pairs such that $-\alpha^2+d\beta^2-c\alpha\beta=0$. By Propositions 10 and 11 this equation has $2\ell-1$ solutions if C is split and has only the trivial solution $\alpha=\beta=0$ if C is nonsplit.

The case $b>0$. As $\mathcal{D}$ is smooth over $\mathbb{F}_\ell$, by (the higher-dimensional version of) Hensel's Lemma [Nek, Proposition 7.8] we have

$$\#\mathcal{D}(\mathbb{Z}/\ell^b\mathbb{Z})=\ell^{b-1}\cdot\#\mathcal{D}(\mathbb{Z}/\ell\mathbb{Z}).$$

A pair $(\alpha,\beta)\in(\mathbb{Z}/\ell^{b+1}\mathbb{Z})^2$ as in (7.2) reduces to a point in $\mathcal{D}(\mathbb{Z}/\ell^b\mathbb{Z})$, so it suffices to prove that there are precisely $\ell^2-\ell$ pairs (α,β) as in (7.2) that lie over some fixed $(\overline{\alpha},\overline{\beta})\in\mathcal{D}(\mathbb{Z}/\ell^b\mathbb{Z})$. There are ℓ^2 lifts of $(\overline{\alpha},\overline{\beta})$ to $(\mathbb{Z}/\ell^{b+1}\mathbb{Z})^2$ and we must avoid those in $\mathcal{D}(\mathbb{Z}/\ell^{b+1}\mathbb{Z})$, which are exactly ℓ again by Hensel's Lemma. □

Acknowledgements. We thank the referee for their useful suggestions.

References

[Bor91] Borel, Armand. Linear algebraic groups. Second edition. Graduate Texts in Mathematics, 126. *Springer-Verlag, New York*, 1991. MR1102012, Zbl 0726.20030.

[FJ08] Fried, Michael D.; Jarden, Moshe. Field arithmetic. Third edition. Revised by Jarden. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge., 11. *Springer-Verlag, Berlin*, 2008. MR2445111, Zbl 1145.12001.

[Gek03] Gekeler, Ernst-Ulrich. Frobenius distributions of elliptic curves over finite prime fields. *Int. Math. Res. Not.* (2003), no. 37, 1999–2018. MR1995144, Zbl 1104.11033, doi: 10.1155/S1073792803211272.

[JR10] Jones, Rafe; Rouse, Jeremy. Galois theory of iterated endomorphisms. Appendix A by Jeffrey D. Achter. *Proc. Lond. Math. Soc. (3)* **100** (2010), no. 3, 763–794. MR2640290, Zbl 1244.11057, doi: 10.1112/plms/pdp051.

[LP16] Lombardo, Davide; Perucca, Antonella. Reductions of points on algebraic groups. arXiv:1612.02847.

[Nek] Nekovář, Jan. Algebra 2 (version finale). Lecture notes E.N.S. 2015–2016, available as Polycopiés de cours via `https://www.math.ens.fr/enseignement/archives_pedagogiques.html`.

[Oes82] Oesterlé, Joseph. Réduction modulo p^n des sous-ensembles analytiques fermés de $\mathbf{Z}_p^N$. *Invent. Math.* **66** (1982), no. 2, 325–341. MR656627, Zbl 0473.12015, doi: 10.1007/BF01389398.

[Ser72] Serre, J.-P. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), no. 4, 259–331. MR0387283, Zbl 0235.14012, doi: 10.1007/BF01405086.

[The17] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu`, 2017.

(Davide Lombardo) Dipartimento di Matematica, Università di Pisa, Largo Pontecorvo 5, 56127 Pisa, Italy
`davide.lombardo@unipi.it`

(Antonella Perucca) Universität Regensburg, Universitätsstrasse 31, 93053 Regensburg, Germany
`mail@antonellaperucca.net`

This paper is available via `http://nyjm.albany.edu/j/2017/23-41.html`.