REDUCTIONS OF POINTS ON ALGEBRAIC GROUPS, II

PETER BRUIN AND ANTONELLA PERUCCA

ABSTRACT. Let $A$ be the product of an abelian variety and a torus over a number field $K$, and let $m \geq 2$ be a square-free integer. If $\alpha \in A(K)$ is a point of infinite order, we consider the set of primes $p$ of $K$ such that the reduction $(\alpha \mod p)$ is well defined and has order coprime to $m$. This set admits a natural density, which we are able to express as a finite sum of products of $\ell$-adic integrals, where $\ell$ varies in the set of prime divisors of $m$. We deduce that the density is a rational number, whose denominator is bounded (up to powers of $m$) in a very strong sense. This extends the results of the paper Reductions of points on algebraic groups by Davide Lombardo and the second author, where the case $m$ prime is established.

1. INTRODUCTION

This article is the continuation of the paper Reductions of points on algebraic groups by Davide Lombardo and the second author [4]. We refer to this other work for the history of the problem, which started in the 1960s with work of Hasse on the multiplicative orders of rational numbers modulo primes.

Let $A$ be the product of an abelian variety and a torus over a number field $K$, and let $m \geq 2$ be a square-free integer. If $\alpha \in A(K)$ is a point of infinite order, we consider the set of primes $p$ of $K$ such that the reduction $(\alpha \mod p)$ is well defined and has order coprime to $m$. This set admits a natural density (see Theorem 7), which we denote by $\text{Dens}_m(\alpha)$.

The main question is whether we can write

\[ \text{Dens}_m(\alpha) = \prod_{\ell} \text{Dens}_\ell(\alpha) \]

where $\ell$ varies over the prime divisors of $m$. Let $K(A[m])$ be the $m$-torsion field of $A$. We prove that (1) holds if $K(A[m]) = K$ (i.e. if $A(K)$ contains all $m$-torsion points) or, more generally, if the degree $[K(A[\ell]) : K]$ is a power of $\ell$ for every prime divisor $\ell$ of $m$ (see Corollary 18). Indeed, (1) holds if the torsion fields/Kummer extensions of $\alpha$ related to different prime divisors of $m$ are linearly disjoint over $K$. In general, (1) does not hold: see Section 7.2 for an explicit example.

We are able to express $\text{Dens}_m(\alpha)$ as an integral over the image of the $m$-adic representation (see Theorem 16), and also as a finite sum of products of $\ell$-adic integrals (see Theorem 19). The latter decomposition allows us to prove that $\text{Dens}_m(\alpha)$ is a rational number whose denominator is uniformly bounded in a very strong sense (see Corollary 20).

Finally, we study Serre curves in detail in Section 6. With the partition given in Section 6.3, one can very easily compute $\text{Dens}_m(\alpha)$ if the $m^n$-Kummer extensions of $\alpha$ (defined in Section 3) have maximal degree for all $n$ or, more generally, if the degrees of these extensions are known and are the same with respect to the base fields $K$ and $K(A[m])$.

In general, to compute the density $\text{Dens}_m(\alpha)$ for the product of an abelian variety and a torus, we only need information on the Galois group of the $m^n$-torsion fields/Kummer extensions of $\alpha$ for some sufficiently large $n$. Thus a theoretical algorithm to compute the density exists, because the growth
in $n$ of the $m^n$-torsion fields/Kummer extensions of $\alpha$ is eventually maximal (see Proposition 5 and Remark 6 in view of [4, Lemma 11]).

Finally we point out that, since the category of algebraic groups that we consider is stable under products, our results allow us to replace $\alpha$ by a finitely generated subgroup of $A(K)$; see Remark 22.

2. INTEGRATION ON PROFINITE GROUPS

For every profinite group $G$, we write $\mu_G$ for the normalised Haar measure on $G$. More generally, if $X$ is a $G$-torsor, we write $\mu_X$ for the normalised Haar measure on $X$, defined by transporting $\mu_G$ along any isomorphism $G \cong X$ of $G$-torsors.

**Lemma 1.** Let $G$ be a profinite group, and let $H$ be an open subgroup of $G$. Suppose that we have $G = \prod_\ell G_\ell$, where $\ell$ varies in a finite set of prime numbers and each $G_\ell$ is a profinite group containing a pro-$\ell$-group $G'_\ell$ as an open subgroup. Let $G' = \prod_\ell G'_\ell$ and $H' = H \cap G'$. For each $x \in H/H'$, let $H(x)$ be the fibre over $x$ of the quotient map $H \to H/H'$.

1. The subgroup $H'$ is open in $H$, and for each $x \in H/H'$, the normalised Haar measure on the $H'$-torsor $H(x)$ is

$$\mu_H(x) = (H : H') \mu_{H|_{H(x)}}.$$

2. We can write

$$H' = \prod_\ell H'_\ell,$$

where each $H'_\ell$ is a pro-$\ell$-group, and the normalised Haar measures on $H'$ and the $H'_\ell$ are related by

$$\mu_{H'} = \prod_\ell \mu_{H'_\ell}.$$

3. We can write the $H'$-torsor $H(x)$ as

$$H(x) = \prod_\ell H_\ell(x),$$

where each $H_\ell(x)$ is a $H'_\ell$-torsor, and the normalised Haar measures on $H(x)$ and the $H_\ell(x)$ are related by

$$\mu_{H(x)} = \prod_\ell \mu_{H_\ell(x)}.$$

**Proof.** The claim that $H'$ is open in $H$ holds because $G'$ is open in $G$. The measure $\mu_{H|_{H(x)}}$ is $H'$-invariant and satisfies $\int_{H(x)} \mu_{H} = \frac{1}{(H : H')} \sum_{x \in H/H'} \int_{H(x)} f \, d\mu_{H(x)}$; this proves (1). Because $G'$ is a product of pro-$\ell$-groups for pairwise different $\ell$, every closed subgroup of $G'$ is similarly a product of pro-$\ell$-groups. This shows the existence of the $H'_\ell$ as in (2); the claim about $\mu_{H'}$ follows because $\prod_\ell \mu_{H'_\ell}$ satisfies the properties of the normalised Haar measure on $H'$. Finally, (3) is proved in the same way as (2).

**Proposition 2.** With the notation of Lemma 1, let $f : H \to \mathbb{C}$ be an integrable function.

1. We have

$$\int_H f \, d\mu_H = \frac{1}{(H : H')} \sum_{x \in H/H'} \int_{H(x)} f \, d\mu_{H(x)}.$$
We call the field extension $K_{m,n}/K_{m,n-1}$ the $m^n$-Kummer extension defined by the point $\alpha$. We view the $m$-adic representation as a representation of $\text{Gal}(K_{m^{-\infty}\alpha}/K)$.

We fix an element $\beta \in m^{-\infty}\alpha$, and define the arboreal representation

$$\omega_{\alpha,m^\infty} : \text{Gal}(K_{m^{-\infty}\alpha}/K) \to T_m A \rtimes \text{Aut}(T_m A)$$

$$\sigma \mapsto (t, M),$$
where \( M \) is the image of \( \sigma \) under the \( m \)-adic representation and \( t = \sigma(\beta) - \beta \). Then \( \omega_{\alpha,m} \) is an injective homomorphism of profinite groups identifying \( \text{Gal}(K_{m^{-n}\alpha}/K) \) with a subgroup of

\[
T_m A \rtimes \text{Aut}(T_m A) \cong \prod_{\ell \mid m} \mathbb{Z}_\ell^{b_A} \rtimes \prod_{\ell \mid m} \text{GL}_{b_A}(\mathbb{Z}_\ell) \cong \prod_{\ell \mid m} (\mathbb{Z}_\ell^{b_A} \rtimes \text{GL}_{b_A}(\mathbb{Z}_\ell)).
\]

Likewise, for each \( n \geq 1 \), the choice of \( \beta \) defines a homomorphism

\[
\omega_{\alpha,m^n} : \text{Gal}(K_{m^{-n}\alpha}/K) \longrightarrow A[m^n] \rtimes \text{Aut}(A[m^n])
\]

\[
\sigma \mapsto (t, M),
\]

where \( t \) and \( M \) are defined in a similar way as above. This identifies \( \text{Gal}(K_{m^{-n}\alpha}/K) \) with a subgroup of

\[
A[m^n] \rtimes \text{Aut}(A[m^n]) \cong \prod_{\ell \mid m} ((\mathbb{Z}/\ell^n\mathbb{Z})^{b_A} \rtimes \text{GL}_{b_A}(\mathbb{Z}/\ell^n\mathbb{Z})).
\]

We denote by \( G(\ell^n) \) the image of the \( \ell \)-adic representation in \( \text{Aut}(T_\ell A) \cong \text{GL}_{b_A}(\mathbb{Z}_\ell) \) and by \( G(\ell^\infty) \) the image of the mod \( \ell^\infty \) representation in \( \text{Aut}(A[\ell^\infty]) \cong \text{GL}_{b_A}(\mathbb{Z}/\ell^\infty\mathbb{Z}) \). Similarly, we denote by \( G(m^n) \) the image of the mod \( m^n \) representation in \( \text{Aut}(T_m A) \cong \prod_{\ell \mid m} \text{GL}_{b_A}(\mathbb{Z}_\ell) \) and by \( G(m^\infty) \) the image of the mod \( m^\infty \) representation in \( \text{Aut}(A[m^\infty]) \cong \text{GL}_{b_A}(\mathbb{Z}/m^\infty\mathbb{Z}) \).

We write \( d_{A,\ell} \) for the dimension of the Zariski closure of \( G(\ell^\infty) \) in \( \text{GL}_{b_A}(\mathbb{Q}_\ell) \), and we put

\[
D_{A,m} = \prod_{\ell \mid m} \ell^{d_{A,\ell}}.
\]

We note that the \( d_{A,\ell} \) and \( D_{A,m} \) do not change when replacing \( K \) by a finite extension. Moreover, assuming the Mumford–Tate conjecture, all \( d_{A,\ell} \) are equal to \( d_A \), the dimension of the Mumford–Tate group, implying \( D_{A,m} = m^{d_A} \). This is known, for example, when \( A \) is an elliptic curve; in this case \( d_A \) equals 2 if \( A \) has complex multiplication, and 4 otherwise.

**Definition 3.** We say that \((A/K, m)\) satisfies eventual maximal growth of the torsion fields if there exists a positive integer \( n_0 \) such that for all \( N \geq n \geq n_0 \) we have

\[
[K_{m^{-N}} : K_{m^{-n}}] = D_{A,m}^{N-n}.
\]

We say that \((A/K, m, \alpha)\) satisfies eventual maximal growth of the Kummer extensions if there exists a positive integer \( n_0 \) such that for all \( N \geq n \geq n_0 \) we have

\[
[K_{m^{-N}\alpha} : K_{m^{-n}\alpha}] = (m^{b_A}D_{A,m})^{N-n}.
\]

**Remark 4.** Condition (2) means that there is eventual maximal growth of the torsion fields, that \( K_{m^{-n}\alpha} \) and \( K_{m^{-N}} \) are linearly disjoint over \( K_{m^{-n}} \), and that we have

\[
[K_{m^{-N}\alpha} : K_{m^{-n}\alpha}] = m^{b_A(N-n)}.
\]

If there is eventual maximal growth of the Kummer extensions, the rational number

\[
C_m := m^{b_A}/[K_{m^{-n}\alpha} : K_{m^{-n}}]
\]

is independent of \( n \) for \( n \geq n_0 \). In fact, \( C_m \) is an integer because \( \omega_{\alpha,m^n} \) maps \( \text{Gal}(K_{m^{-n}\alpha}/K_{m^{-n}}) \) injectively into \( A[m^n] \cong (\mathbb{Z}/m\mathbb{Z})^{b_A} \).

**Proposition 5.** If \( A \) is a semiabelian variety, then \((A/K, m)\) satisfies eventual maximal growth of the torsion fields. If \( A \) is the product of an abelian variety and a torus and \( \mathbb{Z}\alpha \) is Zariski dense in \( A \), then \((A/K, m, \alpha)\) satisfies eventual maximal growth of the Kummer extensions.
Proof. By [4, Lemma 12], if $A$ is a semiabelian variety and $\ell$ is a prime divisor of $m$, then $(A/K, \ell, \alpha)$ satisfies eventual maximal growth of the torsion fields. We also know that the degree $[K_{\ell^{-1}} : K_{\ell^{-n}}]$ is a power of $\ell$ for each $n$. Therefore the extensions $K_{m^{-1}}K_{\ell^{-n}}$ for $\ell \mid m$ are linearly disjoint over $K_{m^{-1}}$ and the first assertion follows. By [4, Remark 9], the second assertion holds for $(A/K, \ell, \alpha)$, where $\ell$ is any prime divisor of $m$. We conclude because the degrees of these Kummer extensions are powers of $\ell$. \qed

4. RELATING THE DENSITY AND THE ARBOREAL REPRESENTATION

Let $(A/K, m, \alpha)$ be as in Section 3.

4.1. The existence of the density. From now on, we assume that $(A/K, m, \alpha)$ satisfies eventual maximal growth of the Kummer extensions.

Remark 6. This is not a restriction if $A$ is the product of an abelian variety and a torus by Proposition 5. Indeed, consider the number of connected components of the Zariski closure of $Z\alpha$. If this number is not coprime to $m$, then the density $\text{Dens}_m(\alpha)$ is zero by [5, Main Theorem] while if it is coprime to $m$ we may replace $\alpha$ by a multiple to reduce to the case where the Zariski closure of $Z\alpha$ is connected. Finally, we may replace $A$ by the Zariski closure of $Z\alpha$ and reduce to the case where $Z\alpha$ is Zariski dense. Also notice that if $A$ is simple (i.e. has exactly two connected algebraic subgroups), then eventual maximal growth of the Kummer extensions is satisfied as soon as $\alpha$ has infinite order.

The $T_mA$-torsor $m^{-\infty}\alpha$ from Section 3 defines a Galois cohomology class

$$C_\alpha \in H^1(\text{Gal}(Km^{-\infty}\alpha/K), T_mA).$$

For any choice of $\beta \in m^{-\infty}\alpha$, this is the class of the cocycle

$$c_\beta : \quad \text{Gal}(Km^{-\infty}\alpha/K) \quad \longrightarrow \quad T_mA \quad \quad \sigma \quad \longmapsto \quad \sigma(\beta) - \beta.$$ 

We also consider the restriction map with respect to the cyclic subgroup generated by some element $\sigma \in \text{Gal}(Km^{-\infty}\alpha/K)$:

$$\text{Res}_\sigma : H^1(\text{Gal}(Km^{-\infty}\alpha/K), T_mA) \longrightarrow H^1(\langle \sigma \rangle, T_mA).$$

Theorem 7. If $(A/K, m, \alpha)$ satisfies eventual maximal growth of the Kummer extensions, then the density $\text{Dens}_m(\alpha)$ exists and equals the normalised Haar measure in $\text{Gal}(Km^{-\infty}\alpha/K)$ of the subset

$$S_\alpha := \{ \sigma \in \text{Gal}(Km^{-\infty}\alpha/K) \mid C_\alpha \in \ker(\text{Res}_\sigma) \} = \{ \sigma \in \text{Gal}(Km^{-\infty}\alpha/K) \mid \sigma(\beta) = \beta \text{ for some } \beta \in m^{-\infty}\alpha \}.$$

Proof. The generalisations of [2, Theorem 3.2] and [4, Theorem 7] to the composite case are straightforward. \qed

Similarly to [4, Remark 21], we may equivalently consider $S_\alpha$ as a subset of either $\text{Gal}(\bar{K}/K)$ or $\text{Gal}(Km^{-\infty}\alpha/K)$ with their respective normalised Haar measures.

Proposition 8. If $L/K$ is any Galois extension that is linearly disjoint from $Km^{-\infty}\alpha$ over $K$, then we have $\text{Dens}_L(\alpha) = \text{Dens}_K(\alpha)$.

Proof. The generalisation of [4, Proposition 22] to the composite case is straightforward. \qed
Lemma 10. For all $\im(\iota_n)$

Proof. This is proved as in [4, Lemma 25].

By Lemma 10, we can define

\begin{equation}
\omega_{x,\ell \alpha}(V) := \lim_{n \to \infty} w_{x,\ell \alpha}(V) \in \mathbb{Z}[1/\ell].
\end{equation}
From Proposition 9, we deduce that for all \( M \in \mathcal{G}(m^\infty) \), the value \( w_{m^n}(M) \) is also constant for \( n \) sufficiently large, so we can analogously define

\[
(9) \quad w_{m^\infty}(M) = \lim_{n \to \infty} w_{m^n}(M) \in \mathbb{Q}.
\]

**Proposition 11.** If \( M \in \mathcal{G}(m^\infty) \) is such that \( \pi_m M = x \), then we have

\[
(\ell) \quad w_{m^\infty}(M) = \prod_{\ell} w_{x,\ell^\infty}(\pi_{\ell^\infty} M).
\]

**Proof.** Taking the limit as \( n \to \infty \) in Proposition 9 yields the claim. \( \square \)

The following lemma gives sufficient conditions for the sets \( W_{m^n}(M) \) and the functions \( w_{m^n}(M) \) and \( w_{m^\infty}(M) \) to admit product decompositions without a dependence on the element \( x \in \mathcal{G}(m) \). It will not be used in the remainder of this article.

**Lemma 12.** For all primes \( \ell \mid m \) and all \( n \geq 1 \), the following conditions are equivalent:

1. The intersection of the fields \( K_{m^{-1}} \) and \( K_{\ell^{-n} \alpha} \) is contained in \( K_{\ell^{-n}} \).
2. The intersection of the fields \( K_{m^{-1}} \) and \( K_{\ell^{-n} \alpha} \) equals \( K_{\ell^{-n}} \).
3. The fields \( K_{m^{-1}} K_{\ell^{-n}} \) and \( K_{\ell^{-n} \alpha} \) are linearly disjoint over \( K_{\ell^{-n}} \).
4. We have \( [K_{m^{-1}} K_{\ell^{-n} \alpha} : K_{m^{-1}} K_{\ell^{-n}}] = [K_{\ell^{-n} \alpha} : K_{\ell^{-n}}] \).
5. We have \( [K_{m^{-1}} K_{\ell^{-n} \alpha} : K_{m^{-1}}] = [K_{\ell^{-n} \alpha} : K_{\ell^{-n}}] \).

If these conditions are satisfied for all primes \( \ell \mid m \) and all \( n \geq 1 \), then the following statements hold:

6. We have \( C_m = \prod_{\ell} C_{\ell} \).
7. For all \( n \geq 1 \) and all \( M \in \mathcal{G}(m^n) \) we have \( W_{m^n}(M) = \prod_{\ell} W_{\ell^n}(\pi_{\ell^n} M) \).
8. For all \( n \geq 1 \) and all \( M \in \mathcal{G}(m^n) \) we have \( w_{m^n}(M) = \prod_{\ell} w_{\ell^n}(\pi_{\ell^n} M) \).
9. For all \( M \in \mathcal{G}(m^\infty) \) we have \( w_{m^\infty}(M) = \prod_{\ell} w_{\ell^\infty}(\pi_{\ell^\infty} M) \).

**Proof.** The equivalence of the conditions (1)–(4) follows from Galois theory, using the fact that all the fields involved are Galois extensions of \( K \). The conditions (4) and (5) are equivalent because \( [K_{m^{-1}} K_{\ell^{-n} \alpha} : K_{m^{-1}} K_{\ell^{-n}}] = [K_{\ell^{-n} \alpha} : K_{\ell^{-n}}] \) is a power of \( \ell \) and \( [K_{m^{-1}} : K_{m^{-1}} K_{\ell^{-n}}] \) is prime to \( \ell \). If condition (5) holds for a given \( n \geq 1 \) and all primes \( \ell \mid m \), then we have

\[
[K_{m^{-n} \alpha} : K_{m^{-n}}] = \prod_{\ell} [K_{m^{-n} \alpha} K_{\ell^{-n} \alpha} : K_{m^{-n}}]
= \prod_{\ell} [K_{\ell^{-n} \alpha} : K_{\ell^{-n}}].
\]

This implies that if (5) is true for all primes \( \ell \mid m \) and all \( n \geq 1 \), then (6) and (7) hold. Finally, it is clear that (7) implies (8) and (9). \( \square \)

### 4.3. Partitioning the image of the \( m \)-adic representation.

We view elements of \( \mathcal{G}(m^\infty) \) as automorphisms of \( A[m^\infty] = \bigcup_{n \geq 1} A[m^n] \). We then classify elements \( M \in \mathcal{G}(m^\infty) \) according to the group structure of \( \ker(M - I) \) and according to the projection \( \pi_m(M) \in \mathcal{G}(m) \). Note that if \( \ker(M - I) \) is finite, then it is a product over the primes \( \ell \mid m \) of finite abelian \( \ell \)-groups that have at most \( b_A \) cyclic components.

Let \( F \) be a group of the form \( \prod_{\ell \mid m} F_{\ell} \), where \( F_{\ell} \) is a finite abelian \( \ell \)-group with at most \( b_A \) cyclic components. We define the set

\[
(10) \quad \mathcal{M}_F := \{ M \in \mathcal{G}(m^\infty) \mid \ker(M - I : A[m^\infty] \to A[m^\infty]) \cong F \},
\]
and for every \( x \in G(m) \) we define the set
\[
M_{x,F} := \{ M \in G(m) \mid \ker (M - I : A[m] \to A[m]) \cong F, \pi_m(M) = x \}.
\]
We denote by \( M_F(*) \) and \( M_{x,F}(*) \), respectively, the images of these sets under the reduction map \( G(m) \to G(*) \). We also write
\[
M := \bigcup_F M_F = \bigcup_{x,F} M_{x,F},
\]
the union being taken over all \( x \in G(m) \) and over all groups \( F = \prod \ell F_\ell \) as above, up to isomorphism.

**Proposition 13.** The following holds:

1. The sets \( M_{x,F} \) are measurable in \( G(m) \), and the set \( M \) of \( \{11\} \) is measurable in \( G(m) \).
2. If \( n > v_\ell(\exp F) \) for all \( \ell | m \), then we have
   \[
   \mu_{G(m)}(M_{x,F}) = \mu_{G(m)}(M_{x,F}(m^n)).
   \]
3. We have \( \mu_{G(m)}(M_{x,F}) = 0 \) if and only if \( M_{x,F} = \emptyset \).
4. If \((A/K, m)\) satisfies eventual maximal growth of the torsion fields, then we have
   \[
   \mu_{G(m)}(M) = 1.
   \]

**Proof.** This is proved as in [\[4\] Lemma 23]. \( \square \)

5. THE DENSITY AS AN INTEGRAL

Suppose that \((A/K, m, \alpha)\) satisfies eventual maximal growth of the Kummer extensions. Recall from Remark 6 that this is not a restriction if \( A \) is the product of an abelian variety and a torus. By Theorem 7, computing \( \text{Dens}_{x,m}(\alpha) \) comes down to computing the Haar measure of \( S_\alpha \) in Gal\((K_{m^{\infty}\alpha}/K)\). The generalisation of [\[4\] Remark 19] to the composite case gives
\[
S_\alpha = \{(t, M) \in \text{Gal}(K_{m^{\infty}\alpha}/K) \mid M \in G(m) \text{ and } t \in \text{Im}(M - I)\}.
\]
In view of \( \{11\} \), we consider the sets
\[
S_{x,F} := \{(t, M) \in \text{Gal}(K_{m^{\infty}\alpha}/K) \mid M \in M_{x,F} \text{ and } t \in \text{Im}(M - I)\}.
\]
By assertion (4) of Proposition 13 and our assumption that \((A/K, m, \alpha)\) satisfies eventual maximal growth of the torsion fields, the set \( S_\alpha \) is the disjoint union of the sets \( S_{x,F} \) up to a set of measure 0. To see that the Haar measure of \( S_{x,F} \) is well defined and to compute it, we define for every \( n \geq 1 \) the set
\[
S_{x,F,m^n} = \{(t, M) \in \text{Gal}(K_{m^{\infty}\alpha}/K) \mid M \in M_{x,F}(m^n) \text{ and } t \in \text{Im}(M - I)\}.
\]

**Proposition 14.** Suppose \( n > n_0 \) and \( n > \max \{v_\ell(\exp F)\} \) for every \( \ell \), where \( n_0 \) is as in Definition 3. Then the set \( S_{x,F,m^n} \) is the image of \( S_{x,F} \) under the projection to \( \text{Gal}(K_{m^{\infty}\alpha}/K) \).

**Proof.** The set \( S_{x,F,m^n} \) clearly contains the reduction modulo \( m^n \) of \( S_{x,F} \). To prove the other inclusion, consider \((t_m, M_m) \in S_{x,F,m^n} \) and a lift \((t, M) \in \text{Gal}(K_{m^{\infty}\alpha}/K)\). Since \( n \) is sufficiently large with respect to \( F \), we have \( \ker(M - I) \cong F \). Clearly \( M_m^n \) and \( M \) have the same projection \( x \in G(m) \). To conclude, it suffices to ensure \( t \in \text{Im}(M - I) \). Take \( \tau_m^n \in A[m^n] \) satisfying \((M_m^n - I)(\tau_m^n) = t_m^n \), and some lift \( \tau \) of \( \tau_m^n \) to \( T_m(A) \): we may replace \( t \) by \((M - I)\tau\) because the difference is in \( m^n T_m(A) \) and since \( n > n_0 \) we know that \( \text{Gal}(K_{m^{\infty}\alpha}/K) \) contains \( m^n T_m(A) \times \{I\} \). \( \square \)
Theorem 15. We have
\[ \mu(S_{x,F}) = \frac{C_m}{\#F} \int_{M_{x,F}} w_{m^\infty}(M) \, d\mu_{G(m^\infty)}(M), \]
where \( C_m \) is the constant of (3) and \( w_m \) is as in (9).

Proof. Choose \( n \) large enough so that \( n > n_0 \) and \( n > \max_\ell \{v_\ell(\exp F)\} \) for every \( \ell \), where \( n_0 \) is as in Definition 3. By definition (see (4)) we can write
\[ \#S_{x,F,m^n} = \sum_{M \in M_{x,F}(m^n)} \#(\text{Im}(M - I) \cap W_{m^n}(M)). \]

By definition (see (5)) we can express the summand as
\[ \# \text{Im}(M - I) \cdot w_{m^n}(M) = \frac{w_{m^n}(M) \cdot m^{bn}}{\#F}, \]
so from (3) we deduce
\[ \frac{\#S_{x,F,m^n}}{\#\text{Gal}(K_{m^{-n_\alpha}/K})} = \frac{1}{\#G(m^n)} \sum_{M \in M_{x,F}(m^n)} \frac{C_m}{\#F} \cdot w_{m^n}(M). \]

By (2) the left-hand side is a non-increasing function of \( n \), and therefore it admits a limit for \( n \to \infty \), which is \( \mu(S_{x,F}) \). The right-hand side is an integral over \( M_{x,F}(m^n) \) with respect to the normalised counting measure of \( G(m^n) \), and the matrices in \( M_{x,F} \) are exactly the matrices in \( G(m^n) \) whose reduction modulo \( m^n \) lies in \( M_{x,F}(m^n) \). Taking the limit in \( n \) we thus find the formula in the statement. \( \square \)

Theorem 16. We have
\[ \text{Dens}_m(\alpha) = C_m \left( \frac{1}{\#F} \int_{M_F} w_{m^\infty}(M) \, d\mu_{G(m^\infty)}(M) \right) \]
\[ = C_m \int_{G(m^\infty)} \frac{w_{m^\infty}(M)}{\# \ker(M - I)} \, d\mu_{G(m^\infty)}(M), \]
where the function \( w_{m^\infty} \) is as in (9), the constant \( C_m \) is as in (3), and \( F \) varies over the products over the primes \( \ell \mid m \) of finite abelian \( \ell \)-groups with at most \( b_A \) cyclic components.

Proof. To prove the first equality, note that \( M_F \) is the disjoint union of the \( M_{x,F} \) for \( x \in G(m) \). By Theorem 7 we may write \( \text{Dens}_m(\alpha) = \mu(S_\alpha) = \sum_{x,F} \mu(S_{x,F}) \) and then it suffices to apply Theorem 15. The second equality follows because the union of the sets \( M_F \) from (10) has measure 1 in \( G(m^\infty) \) by Proposition 13. \( \square \)

Corollary 17 ([4, Theorem 1 and Remark 27]). In the special case \( m = \ell \) we have
\[ \text{Dens}_\ell(\alpha) = C_\ell \sum_{F} \frac{1}{\#F} \int_{M_F} w_{\ell^\infty}(M) \, d\mu_{G(\ell^\infty)}(M) \]
\[ = C_\ell \int_{G(\ell^\infty)} \frac{w_{\ell^\infty}(M)}{\# \ker(M - I)} \, d\mu_{G(\ell^\infty)}(M), \]
where \( F \) varies among the finite abelian \( \ell \)-groups with at most \( b_A \) cyclic components.

Notice that we have \( \# \ker(M - I) = \ell^{v_\ell(\det(M - I))} \) for every \( M \in G(\ell^\infty) \); this shows the equivalence with [4, Theorem 1].
Corollary 18. Let \( \ell \) vary among the prime divisors of \( m \). If the fields \( K_{\ell^{-\infty}} \) are linearly disjoint over \( K \), then we have

\[
\text{Dens}_m(\alpha) = \prod_{\ell} \text{Dens}_\ell(\alpha).
\]

Proof. Note that we have \( C_m = \prod_{\ell} C_\ell \). By assumption, we also have \( \mathcal{G}(m^\infty) = \prod_{\ell} \mathcal{G}(\ell^\infty) \), which implies \( \mu(\mathcal{G}(m^\infty)) = \prod_{\ell} \mu(\mathcal{G}(\ell^\infty)) \), and \( w_{m^\infty}(M) = \prod_{\ell} w_{\ell^\infty}(\pi_{\ell^\infty} M) \). We conclude that (12) is the product of the expressions (13) for \( \ell \mid m \). \( \square \)

The conditions of Corollary 18 are satisfied for example if \( K_{\ell^{-1}} = K \), or more generally if the degree \( [K_{\ell^{-1}} : K] \) is a power of \( \ell \) for each \( \ell \). Under weaker conditions, \( \text{Dens}_m(\alpha) \) is not in general the product of the \( \text{Dens}_\ell(\alpha) \), but we can still express it as a sum of products of \( \ell \)-adic integrals, as the following result shows.

Theorem 19. Denote by \( H(x) = \prod_{\ell} H_\ell(x) \) the set of matrices in \( \mathcal{G}(m^\infty) \subseteq \prod_{\ell} \mathcal{G}(\ell^\infty) \) mapping to \( x \) in \( \mathcal{G}(m) \). We then have

\[
\text{Dens}_m(\alpha) = \frac{C_m}{\# \mathcal{G}(m)} \sum_{x \in \mathcal{G}(m)} \prod_{\ell} \int_{H_\ell(x)} \frac{w_{x,\ell^\infty}(M)}{\# \ker(M - I)} d\mu_{H_\ell(x)}(M),
\]

where \( w_{x,\ell^\infty} \) is as in (8).

Proof. Write \( S_x = \bigcup_F S_{x,F} \) and recall from Proposition 13 that the set of matrices \( M \) for which \( \ker(M - I) \) is infinite has measure zero in \( \mathcal{G}(m^\infty) \). By Theorem 15 we have

\[
\mu(S_x) = \sum_F \mu(S_{x,F}) = C_m \int_{H(x)} \frac{w_{m^\infty}(M)}{\# \ker(M - I)} d\mu_{\mathcal{G}(m^\infty)}(M).
\]

The assertion follows from Propositions 2 and 11. \( \square \)

Corollary 20. The density \( \text{Dens}_m(\alpha) \) is a rational number. Moreover, for every positive integer \( b \), there exists a non-zero polynomial \( p_b(t) \in \mathbb{Z}[t] \) with the following property: whenever \( K \) is a number field and \( A \) is the product of an abelian variety and a torus such that the first Betti number of \( A \) equals \( b \), then for all \( \alpha \in A(K) \) and all square-free integers \( m \geq 2 \) such that \( (A/K, m, \alpha) \) satisfies eventual maximal growth of the Kummer extensions, we have

\[
\text{Dens}_m(\alpha) \cdot \prod_{\ell} p_b(\ell) \in \mathbb{Z}[1/m],
\]

where \( \ell \) varies over the prime divisors of \( m \).

Proof. Recall that \( C_m \) is an integer. In view of Lemma 10, we can consider each \( \ell \)-adic integral in (14) and proceed as in the proof of [4, Theorem 36]. \( \square \)

Remark 21. For elliptic curves, it is also possible to bound the minimal denominator of \( \text{Dens}_m(\alpha) \). Indeed, let us consider (14), recalling that \( C_m \) is an integer. Each of the finitely many functions \( w_{x,\ell^\infty} \) takes only finitely many values: these are rational numbers whose minimal denominator divides \( \ell^{2n_0} \), where \( n_0 \) is large enough so that condition (2) holds for all \( N \geq n \geq n_0 \). If \( M \in \mathcal{M}_\ell(a,b) \) (see Section 6.2), then \( \# \ker(M - I) = \ell^{2a+b} \). The crucial fact is the independence of the number of lifts [3, Theorem 28]; the case distinction for the normaliser of a Cartan subgroup does not matter because we separately count the matrices in the Cartan subgroup and those in its complement. This means that the measure of \( \mathcal{M}_\ell(a,b) \cap H_\ell(x) \) is a fraction of that of \( \mathcal{M}_\ell(a,b) \): this ratio can take only finitely many values and can be understood by working modulo \( \ell^{n_0} \). We may then need to multiply the denominator in the measure of \( \mathcal{M}_\ell(a,b) \) by an integer which is at most \( \# \text{GL}_2(\ell^{n_0}) \). Essentially
we need to evaluate finitely many geometric series because of the eventual maximal growth of the torsion fields (the degrees \([K(E[ℓ^n]) : K]\) for \(n\) sufficiently large form a geometric progression) and we may reason as in \([4,\) Theorems 5 and 6].

**Remark 22.** We may replace the point \(α\) by a finitely generated subgroup \(G\) of \(A(K)\). Indeed, let \(α_1, \ldots, α_r\) be generators for \(G\). We may then consider the point \(β = (α_1, \ldots, α_r)\) in the product \(A^r(K)\). Then the density \(\text{Dens}_m(β)\) for the single point \(β\) is exactly the density of primes \(p\) of \(K\) such that the order of \((G \mod p)\) is coprime to \(m\).

### 6. Serre Curves

**6.1. Definition of Serre curves.** Let \(E\) be an elliptic curve over a number field \(K\). We choose a Weierstrass equation for \(E\) of the form

\[
E: y^2 = (x - x_1)(x - x_2)(x - x_3),
\]

where \(x_1, x_2, x_3 \in K(E[2])\) are the \(x\)-coordinates of the points of order 2. The discriminant of the right-hand side of 15 is \(Δ = \sqrt{Δ^2}\), where

\[
\sqrt{Δ} = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1).
\]

We thus have \(K(\sqrt{Δ}) \subseteq K(E[2])\), and we define a character

\[
ψ_E: \text{Gal}(K(E[2]) / K) \longrightarrow \{±1\}
\]

\[
σ \mapsto σ(\sqrt{Δ})/\sqrt{Δ}.
\]

For any choice of basis of the 2-torsion of \(E\), we have the 2-torsion representation

\[
ρ_{E,2}: \text{Gal}(K(E[2]) / K) \longrightarrow \text{GL}_2(\mathbb{Z}/2\mathbb{Z}).
\]

Let \(ψ\) be the unique non-trivial character \(\text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow \{±1\}\); this corresponds to the sign character under any isomorphism of \(\text{GL}_2(\mathbb{Z}/2\mathbb{Z})\) with \(S_3\). The character \(ψ_E\) factors as

\[
ψ_E = ψ ∘ ρ_{E,2}.
\]

From now on, we take \(K = \mathbb{Q}\). All number fields that we will consider will be subfields of a fixed algebraic closure \(\overline{\mathbb{Q}}\) of \(\mathbb{Q}\).

Let \(d\) be an element of \(\mathbb{Q}^×\). Let \(m_d\) be the conductor of \(\mathbb{Q}(\sqrt{d})\); this is the smallest positive integer such that \(\sqrt{d}\) lies in the cyclotomic field \(\mathbb{Q}(\zeta_{m_d})\). Let \(d_{sf}\) be the square-free part of \(d\). We have

\[
m_d = \begin{cases} |d_{sf}| & \text{if } d_{sf} \equiv 1 \mod 4, \\ 4|d_{sf}| & \text{otherwise}. \end{cases}
\]

We define a character

\[
ε_d: \text{Gal}(\mathbb{Q}(\zeta_{m_d}) / \mathbb{Q}) \longrightarrow \{±1\}
\]

\[
σ \mapsto σ(\sqrt{d})/\sqrt{d}.
\]

If \(σ\) is the automorphism of \(\mathbb{Q}(\zeta_{m_d})\) defined by \(σ(\zeta_{m_d}) = \zeta_{m_d}^a\) with \(a \in (\mathbb{Z}/m_d\mathbb{Z})^×\), then \(ε_d(σ)\) equals the Jacobi symbol \((d/\alpha)\). We view \(ε_d\) as a character of \(\text{GL}_2(\mathbb{Z}/m_d\mathbb{Z})\) by composing with the determinant.

For all \(n \geq 1\), we have a canonical projection

\[
π_n: \text{GL}_2(\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z}).
\]
Fixing a \( \widehat{\mathbb{Z}} \)-basis for the projective limit of the torsion groups \( E[n](\overline{\mathbb{Q}}) \), we have a torsion representation

\[
\rho_E : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\widehat{\mathbb{Z}})
\]

The image of \( \rho_E \) is contained in the subgroup

\[
H_\Delta = \{ M \in \operatorname{GL}_2(\widehat{\mathbb{Z}}) \mid \psi(\pi_2(M)) = \varepsilon_\Delta(\pi_{m\Delta}(M)) \}
\]

of index 2 in \( \operatorname{GL}_2(\widehat{\mathbb{Z}}) \). This expresses the fact that \( \sqrt{\Delta} \) is contained in both \( \mathbb{Q}(E[2]) \) and \( \mathbb{Q}(E[m\Delta]) \).

An elliptic curve is said to be a Serre curve if the image of \( \rho_E \) is equal to \( H_\Delta \). As proven by N. Jones \cite{[1]}, almost all elliptic curves over \( \mathbb{Q} \) are Serre curves.

6.2. Counting matrices. Let \( \ell \) be a prime number. For all integers \( a, b \geq 0 \), we write \( \mathcal{M}_\ell(a, b) \) for the set of matrices \( M \in \operatorname{GL}_2(\mathbb{Z}_\ell) \) such that the kernel of \( M - I \) as an endomorphism of \((\mathbb{Q}_\ell/\mathbb{Z}_\ell)^2 \) is isomorphic to \( \mathbb{Z}/\ell^a \mathbb{Z} \times \mathbb{Z}/\ell^b \mathbb{Z} \).

If \( \mathcal{N} \) is a non-empty subset of \( \mathcal{M}_\ell(a, b) \) that is the preimage in \( \mathcal{M}_\ell(a, b) \) of its reduction modulo \( \ell^n \) (which means that \( \mathcal{N} \) contains the intersection of \( \mathcal{M}_\ell(a, b) \) with the set of preimages of \( (\mathcal{N} \mod \ell^n) \) in \( \operatorname{GL}_2(\mathbb{Z}_\ell) \)), then we have

\[
\frac{\mu_{\operatorname{GL}_2(\mathbb{Z}_\ell)}(\mathcal{N})}{\mu_{\operatorname{GL}_2(\mathbb{Z}_\ell)}(\mathcal{M}_\ell(a, b))} = \frac{\mu_{\operatorname{GL}_2(\mathbb{Z}/\ell^n \mathbb{Z})}(\mathcal{N} \mod \ell^n)}{\mu_{\operatorname{GL}_2(\mathbb{Z}/\ell^n \mathbb{Z})}(\mathcal{M}_\ell(a, b) \mod \ell^n)}
\]

by \cite{[3]} Theorem 27] (where the number of lifts is independent of the matrix). Notice that if \( a \geq n \), then \((\mathcal{N} \mod \ell^n)\) consists of the identity.

**Proposition 23.** If \( \mathcal{N} \) is a subset of \( \mathcal{M}_\ell(a, b) \) that is the preimage in \( \mathcal{M}_\ell(a, b) \) of its reduction modulo \( \ell \), then we have

\[
\mu_{\operatorname{GL}_2(\mathbb{Z}_\ell)}(\mathcal{N}) = \mu_{\operatorname{GL}_2(\mathbb{Z}/\ell \mathbb{Z})}(\mathcal{N} \mod \ell) \cdot \begin{cases} 
1 & \text{if } a = b = 0 \\
\ell^{-b}(\ell - 1) & \text{if } a = 0, b \geq 1 \\
\ell^{-4a} \cdot (\ell - 1)^2(\ell + 1) & \text{if } a \geq 1, b = 0 \\
\ell^{-4a-b} \cdot (\ell - 1)^2(\ell + 1)^2 & \text{if } a \geq 1, b \geq 1.
\end{cases}
\]

**Proof.** We are working with \( \operatorname{GL}_2(\mathbb{Z}_\ell) \), so we can apply \cite{[3]} Proposition 33] (see also \cite{[3]} Definition 19]). This gives the assertion for the set \( \mathcal{M}_\ell(a, b) \); we can conclude because of \cite{[16]}. \( \square \)

We now collect some results in the case \( \ell = 2 \). From \cite{[3]} Theorem 2] we know

\[
\mu_{\operatorname{GL}_2(\mathbb{Z}_2)}(\mathcal{M}_2(a, b)) = \begin{cases} 
1/3 & \text{if } a = b = 0 \\
1/2 \cdot 2^{-b} & \text{if } a = 0, b \geq 1 \\
2^{-4a} & \text{if } a \geq 1, b = 0 \\
3/2 \cdot 2^{-4a-b} & \text{if } a \geq 1, b \geq 1.
\end{cases}
\]

We consider the action of \( \operatorname{GL}_2(\mathbb{Z}/2^3 \mathbb{Z}) \) on \( \mathbb{Q}(\zeta_{2^3}) \) defined by \( M \zeta_{2^3} = \zeta_{2^3}^{\det M} \). The matrices \( M \in \operatorname{GL}_2(\mathbb{Z}/2^3 \mathbb{Z}) \) that fix \( \sqrt{-1} \) are those with \( \det(M) = 1, 5 \). The ones that fix \( \sqrt{2} \) are those with \( \det(M) = 1, 3 \). The ones that fix \( \sqrt{-2} \) are those with \( \det(M) = 1, 3 \).

For \( a, b \in \{0, 1, 2, 3\} \) and \( z \in \{-1, 2, -2\} \), we write \( \mathcal{N}_2(a, b, z) \) for the set of matrices in \( \mathcal{M}_2(a, b) \) that fix \( \sqrt{z} \).

**Lemma 24.** We have

\[
\frac{\mu_{\operatorname{GL}_2(\mathbb{Z}_2)}(\mathcal{N}_2(a, b; -1))}{\mu_{\operatorname{GL}_2(\mathbb{Z}_2)}(\mathcal{M}_2(a, b))} = \begin{cases} 
1/2 & \text{for } a = 0, b \geq 0 \\
2/3 & \text{for } a = 1, b = 0 \\
1/3 & \text{for } a = 1, b \geq 1 \\
1 & \text{for } a \geq 2, b \geq 0
\end{cases}
\]
and

\[
\frac{\mu_{\text{GL}_2(\mathbb{Z}_2)}(N_2(a, b; \pm 2))}{\mu_{\text{GL}_2(\mathbb{Z}_2)}(M_2(a, b))} = \begin{cases} 
1/2 & \text{for } a \leq 1, b \geq 0 \\
2/3 & \text{for } a = 2, b = 0 \\
1/3 & \text{for } a = 2, b \geq 1 \\
1 & \text{for } a \geq 3, b \geq 0.
\end{cases}
\]

**Proof.** For \(a, b \in \{0, 1, 2, 3\}\) and \(d \in (\mathbb{Z}/2^3\mathbb{Z})^\times\), let \(h(a, b, d)\) be the number of matrices \(M \in \text{GL}_2(\mathbb{Z}/2^3\mathbb{Z})\) such that \(\det(M) = d\) and \(\ker(M - I) \cong \mathbb{Z}/2^a\mathbb{Z} \times \mathbb{Z}/2^a\mathbb{Z}\). Using [9] one can easily count these matrices:

- \(h(0, 0, d) = 128, h(0, 1, d) = 96\) and \(h(0, 2, d) = h(0, 3, d) = 48\) for all \(d\);
- \(h(1, 0, d) = 32\) for \(d = 1, 5\) and \(h(1, 0, d) = 16\) for \(d = 3, 7\);
- for \(b = 1, 2\) we have \(h(1, b, d) = 12\) for \(d = 1, 5\) and \(h(1, b, d) = 24\) for \(d = 3, 7\);
- \(h(2, 0, 1) = 4, h(2, 0, 5) = 2\) and \(h(2, 0, d) = 0\) for \(d = 3, 7\);
- \(h(2, 1, 1) = 3, h(2, 1, 5) = 6\) and \(h(2, 1, d) = 0\) for \(d = 3, 7\);
- \(h(3, 0, 1) = 1\) (the identity matrix) and \(h(3, 0, d) = 0\) for \(d = 3, 5, 7\).

This classification and [16] lead to the measures in the statement. \(\square\)

**Lemma 25.** For all \(a, b \geq 0\) and all \(M \in \mathcal{M}_2(a, b)\), we have

\[
\psi(M) = \begin{cases} 
-1 & \text{if } a = 0 \text{ and } b \geq 1, \\
1 & \text{otherwise}.
\end{cases}
\]

**Proof.** Consider matrices \(M \in \text{GL}_2(\mathbb{Z}/2\mathbb{Z})\). The matrices

\[
M \in \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}
\]

satisfy \(\psi(M) = 1\) and \(\dim_{\mathbb{F}_2} \ker(M - I) \in \{0, 2\}\). The matrices

\[
M \in \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}
\]

satisfy \(\psi(M) = -1\) and \(\dim_{\mathbb{F}_2} \ker(M - I) = 1\). This implies the claim. \(\square\)

Now let \(\ell\) be an odd prime number. We write

\[
\ell^* = (-1)^{(\ell-1)/2} \ell,
\]

so \(\varepsilon_{\ell^*}\) is a character of \((\mathbb{Z}/\ell\mathbb{Z})^\times\), and also of \(\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})\) via the determinant.

**Lemma 26.** Let \(M\) vary in \(\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \setminus \{I\}\), where \(\ell\) is an odd prime number.

1. There are \(\frac{1}{4}(\ell + 1)^2(\ell - 2)\) matrices \(M\) satisfying \(\varepsilon_{\ell^*}(M) = 1\) and \(\ell \mid \det(M - I)\).
2. There are \(\frac{1}{4}(\ell^3 - 2\ell^2 - \ell + 4)\) matrices \(M\) satisfying \(\varepsilon_{\ell^*}(M) = 1\) and \(\ell \nmid \det(M - I)\).
3. There are \(\frac{1}{4}(\ell(\ell^2 - 1)\) matrices \(M\) satisfying \(\varepsilon_{\ell^*}(M) = -1\) and \(\ell \mid \det(M - I)\).
4. There are \(\frac{1}{4}(\ell(\ell^2 - 1)(\ell - 2)\) matrices \(M\) satisfying \(\varepsilon_{\ell^*}(M) = -1\) and \(\ell \nmid \det(M - I)\).

**Proof.** (1) Write \(\chi(M)\) for the characteristic polynomial of \(M\). The condition \(\varepsilon_{\ell^*}(M) = 1\) is equivalent to \(\det(M) = \chi(0)\) being a square in \((\mathbb{Z}/\ell\mathbb{Z})^\times\), and the condition \(\ell \mid \det(M - I)\) is equivalent to \(\chi(1) = 0\) in \(\mathbb{Z}/\ell\mathbb{Z}\). Thus the matrices \(M\) satisfying both conditions are those for which there exists \(s \in (\mathbb{Z}/\ell\mathbb{Z})^\times\) with

\[
\chi(M) = (x - 1)(x - s^2).
\]
The matrices with $\chi(0) \neq 1$ (giving $\ell^{-1} - 1$ possibilities for $\chi$) are diagonalisable and we only have to choose the two distinct eigenspaces; this gives $(\ell + 1)/\ell$ matrices for every such $\chi$. The matrices with $\chi(0) = 1$ are the identity (which we are excluding) and the $\ell^2 - 1$ matrices conjugate to $\left( \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right)$. Note that (1) can also be obtained from [7, Table 1].

(2) There are $\frac{1}{\ell} \# \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ matrices satisfying $\varepsilon_{\ell^r} = 1$, and we only need to subtract the identity and the matrices from (1).

(3) There are $\ell^3 - 2\ell$ matrices in $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ having 1 as an eigenvalue (see for example [3, Proof of Theorem 2]), and we only need to subtract the identity and the matrices from (1).

(4) There are $\frac{1}{\ell} \# \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ matrices satisfying $\varepsilon_{\ell^r} = -1$, and we only need to subtract the matrices from (3). Alternatively, there are $\# \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) - (\ell^3 - 2\ell)$ matrices that do not have 1 as eigenvalue, and we only need to subtract the matrices from (2).

$\square$

6.3. Partitioning the image of the $m$-adic representation. Let $E$ be a Serre curve over $\mathbb{Q}$. Let $\Delta$ be the minimal discriminant of $E$, and let $\Delta_{sf}$ be its square-free part. We write $\Delta_{sf} = zu$, where $z \in \{1, -1, 2, -2\}$ and where $u$ is an odd fundamental discriminant. Then $|u|$ is the odd part of $m_\Delta$, and we have $\varepsilon_\Delta = \varepsilon_z \cdot \varepsilon_u$ as characters of $(\mathbb{Z}/m_\Delta \mathbb{Z})^\times$.

Now let $m$ be a square-free positive integer. If $m = 2$, or if $m$ is odd, or if $u$ does not divide $m$, then we have

$$G(m^\infty) = \prod_\ell G(\ell^\infty).$$

If $m 
eq 2$ is even and $u$ divides $m$, then $G(m^\infty)$ has index 2 in $\prod_\ell G(\ell^\infty)$. The defining condition for the image of the $m$-adic representation is then $\psi = \varepsilon_\Delta$, or equivalently

$$\psi \cdot \varepsilon_z = \varepsilon_u.$$

We may then partition $G(m^\infty) \subseteq \prod_\ell G(\ell^\infty)$ into two sets that are products, namely

$$(G(2^\infty) \cap \{\psi \cdot \varepsilon_z = 1\}) \times (G(|u|^\infty) \cap \{\varepsilon_u = 1\}) \times G\left(\left| \frac{m}{2u} \right|^\infty\right)$$

and

$$(G(2^\infty) \cap \{\psi \cdot \varepsilon_z = -1\}) \times (G(|u|^\infty) \cap \{\varepsilon_u = -1\}) \times G\left(\left| \frac{m}{2u} \right|^\infty\right).$$

The set $G(|u|^\infty) \cap \{\varepsilon_u = 1\}$ is the disjoint union of sets of the form $\prod_\ell G(\ell^\infty) \cap \{\varepsilon_{\ell^r} = \pm 1\}$, choosing an even number of minus signs; for the set $G(|u|^\infty) \cap \{\varepsilon_u = -1\}$ we have to choose an odd number of minus signs. Since each $\ell \mid u$ is odd, the two sets $G(\ell^\infty) \cap \{\varepsilon_{\ell^r} = \pm 1\}$ can be investigated with the help of Lemma 26. Finally, the two sets $G(2^\infty) \cap \{\psi \cdot \varepsilon_z = \pm 1\}$ can be investigated using Lemmas 24 and 25.

7. Examples

7.1. Example (non-surjective mod 3 representation). Consider the non-CM elliptic curve

$$E: y^2 + y = x^3 + 6x + 27$$

of discriminant $-3^{19} \cdot 17$ and conductor $153 = 3^2 \cdot 17$ over $\mathbb{Q}$ [8, label 153.b2]. The group $E(\mathbb{Q})$ is infinite cyclic and is generated by the point

$$\alpha = (5, 13).$$

We will compute the following values (by testing the primes up to $10^6$, we have computed an approximation to $\text{Dens}_{E}(\alpha)$ using [9]):
The image of the 3-adic representation is the inverse image of its reduction modulo 3, the image of the mod 3 representation is isomorphic to the symmetric group of order 6, and the 3-adic Kummer map is surjective [4 Example 6.4]. The image of the mod 3 representation has a unique subgroup of index 2, so the field \( \mathbb{Q}(E[3]) \) contains as its only quadratic subextension the cyclotomic field \( \mathbb{Q}(\sqrt{-3}) \).

The image of the 2-adic representation is \( \text{GL}_2(\mathbb{Z}_2) \); see [8]. By [2] Theorem 5.2 the 2-adic Kummer map is surjective: the assumptions of that result are satisfied because the prime \( p = 941 \) splits completely in \( E[4] \) but the point \( \alpha \mod p \) is not 2-divisible over \( \mathbb{F}_p \). Since the image of the mod 2 representation has a unique subgroup of index 2, the field \( \mathbb{Q}(E[2]) \) contains as its only quadratic subextension the field \( \mathbb{Q}(\sqrt{-3}) \) (the square-free part of the discriminant of \( E \) is \(-51\)).

We have \( \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[9]) = \mathbb{Q} \) because the residual degree modulo 22699 of the extension \( \mathbb{Q}(E[2]), \mathbb{Q}(E[9]) / \mathbb{Q}(E[9]) \) is divisible by 3 and the degree of this extension is even because \( \mathbb{Q}(\sqrt{-51}) \) is not contained in \( \mathbb{Q}(E[3]) \). We deduce \( \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3]) = \mathbb{Q} \) by applying [4] Theorem 14 (i) (where \( K = \mathbb{Q}(E[2]) \)).

Moreover, we have \( \mathbb{Q}(E[3]) \cap \mathbb{Q}(E[4]) = \mathbb{Q} \) because \( \mathbb{Q}(\sqrt{-3}) \) is not contained in \( \mathbb{Q}(E[4]) \): the prime 941 is not congruent to 1 modulo 3 and splits completely in \( \mathbb{Q}(E[4]) \). By [4], Theorem 14 (i) we conclude that \( \mathbb{Q}(E[3]) \cap \mathbb{Q}(E[2]) = \mathbb{Q} \).

The 2-adic Kummer extensions of \( \alpha \) have maximal degree also over \( \mathbb{Q}(E[3]) \), in view of the maximality of the 2-Kummer extension, because the prime 4349 splits completely in \( \mathbb{Q}(2^{-2\alpha}) \) but not in \( \mathbb{Q}(\sqrt{-3}) \); see [4] Theorem 14 (ii) (where \( K = \mathbb{Q}(\sqrt{-3}) \)).

The 3-adic Kummer extensions of \( \alpha \) have maximal degree also over \( \mathbb{Q}(E[2]) \) because the prime 217981 splits completely in \( \mathbb{Q}(3^{-2\alpha}) \) but 3 divides the residual degree of \( \mathbb{Q}(E[2]) \); see [4] Theorem 14 (ii) (where \( K = \mathbb{Q}(E[2]) \)).

We thus have \( \mathcal{G}(6^\infty) = \mathcal{G}(2^\infty) \times \mathcal{G}(3^\infty) \), the \( 2^\infty \) Kummer extensions are independent from \( \mathbb{Q}(E[3]) \), and the \( 3^\infty \) Kummer extensions are independent from \( \mathbb{Q}(E[2]) \). We are thus in the situation that the fields \( \mathbb{Q}(2^{-\infty\alpha}) \) and \( \mathbb{Q}(3^{-\infty\alpha}) \) are linearly disjoint over \( \mathbb{Q} \). We deduce from Corollary 18 that the equality

\[
\text{Dens}_6(\alpha) = \text{Dens}_2(\alpha) \cdot \text{Dens}_3(\alpha)
\]

holds for \( \alpha \) and for its multiples. The 2-densities can be evaluated by [4] Theorem 35, for the 3-densities see [4] Example 6.4.

7.2. The Serre curve \( y^2 + y = x^3 + x^2 \). The elliptic curve

\[ E : y^2 + y = x^3 + x^2 \]

of discriminant \(-43\) and conductor 43 over \( \mathbb{Q} \) [8, label 43.a1] is a Serre curve [6, Example 5.5.7]. The group \( E(\mathbb{Q}) \) is infinite cyclic and is generated by the point \( \alpha = (0, 0) \).

The point \( \alpha \) satisfies

\[
\text{Dens}_2(\alpha) \cdot \text{Dens}_{43}(\alpha) \neq \text{Dens}_{2,43}(\alpha)
\]
because, as we will show below, we have
\[
\text{Dens}_2(\alpha) = \frac{11}{21}, \quad \text{Dens}_{43}(\alpha) = \frac{143510179}{146927088},
\]
\[
\text{Dens}_2(\alpha) \cdot \text{Dens}_{43}(\alpha) = \frac{143510179}{280497168} \approx 51.16279\%,
\]
\[
\text{Dens}_{2,43}(\alpha) = \frac{526206455}{1028489616} \approx 51.16303\%.
\]
We will also compute the following values (by testing the primes up to $10^6$), we have computed an approximation to $\text{Dens}_{2,43}(\alpha)$ using (9):

| Point  | $\alpha = (0, 0)$ | $\text{Dens}_{2,43}$ | primes $< 10^6$ |
|--------|-------------------|----------------------|-----------------|
| $2\alpha = (-1, -1)$ | 526206455/1028489616 = 51.163\% | 51.136\% |
| $4\alpha = (2, 3)$ | 42521603/57138312 = 74.418\% | 74.397\% |
|        | 176996107/2056979232 = 86.046\% | 86.072\% |

By looking at the reduction modulo 293, we see that $\alpha$ is not divisible by 2 over the 4-torsion field of $E$. Therefore, by [2, Theorem 5.2], for every prime number $\ell$ and for every $n \geq 1$ the degree of the $\ell^n$-Kummer extension is maximal, i.e.
\[
[Q_{\ell^{-n}\alpha} : Q_{\ell^{-n}}] = \ell^{2n}.
\]
The 43-adic Kummer extensions have maximal degree also over $Q(E[2])$, i.e.
\[
[Q_{43^{-n}\alpha}(E[2]) : Q_{43^{-n}}(E[2])] = 43^{2n},
\]
because the degree $[Q(E[2]) : Q] = 6$ is coprime to 43.

The extensions $Q(2^{-1}\alpha)$ and $Q(E[2 \cdot 43])$ are linearly disjoint over $Q(E[2])$, as can be seen by investigating the residual degree for the reduction modulo the prime 29327, which splits completely in $Q(E[2])$. Indeed, the residual degree of the extension $Q(2^{-1}\alpha)$ equals 4 while the residual degree of the extension $Q(E[2 \cdot 43])$ is odd because the prime is congruent to 1 modulo 43, and there are points of order 43 in the reductions (the subgroup of the upper unitriangular matrices in $GL_2(Z/43Z)$ has order 43).

The 2-adic Kummer extensions have maximal degree also over $Q(E[43])$, i.e.
\[
[Q_{2^{-n}\alpha}(E[43]) : Q_{2^{-n}}(E[43])] = 2^{2n}.
\]
To see this, we consider the intersection $L$ of $Q_{2^{-n}\alpha}$ and $Q(E[43])$. This is a Galois extension of $Q$, and the group $G = \text{Gal}(L/Q)$ is a quotient of both $(Z/2^nZ)^2 \times GL_2(Z/2^nZ)$ and $GL_2(Z/43Z)$. Because $SL_2(Z/43Z)$ has no non-trivial quotient that can be embedded into a quotient of $(Z/2^nZ)^2 \times GL_2(Z/2^nZ)$, the quotient map $GL_2(Z/43Z) \rightarrow G$ factors as $GL_2(Z/43Z) \rightarrow (Z/43Z)^\times \rightarrow G$.

This implies that $L$ is a subfield of $Q(\zeta_{43})$. Furthermore, $L$ contains $Q(\sqrt{-43})$. Because $(Z/2^nZ)^2 \times GL_2(Z/2^nZ)$ does not have any quotient group of odd order, the maximal subfield of $Q(\zeta_{43})$ that can be embedded into $Q_{2^{-n}\alpha}$ is $Q(\sqrt{-43})$, and we conclude that $L$ equals $Q(\sqrt{-43})$.

It follows that for $m = 2 \cdot 43$ we have the maximal degree $[Q_{m^{-n}\alpha} : Q_{m^{-n}}] = m^{2n}$ and, more generally, that for every multiple $P$ of $\alpha$ we have $[Q_{m^{-n}\alpha} : Q_{m^{-n}}] = [Q_{2^{-n}P} : Q_{2^{-n}}] = [Q_{43^{-n}P} : Q_{43^{-n}}]$. We may then apply [4, Example 28] and various results in this paper to compute the exact densities in the above table, and we use [9] to numerically verify them for the primes up to $10^6$.

We conclude by sketching the computations for the point $\alpha$. The 43-adic representation is surjective and the 43-Kummer extensions have maximal degree. By parts (3) and (4) of Lemma [26] we find that
\( \frac{1}{2^{11}} \) (respectively, \( \frac{41}{2^{11}} \)) is the counting measure in \( \text{GL}_2(\mathbb{Z}/43\mathbb{Z}) \) of the matrices such that \( \varepsilon_{-43} = -1 \) and that are in \( (\mathcal{M}_{43}(0, b) \mod \ell) \) for some \( b > 0 \) (respectively, for \( b = 0 \)). By multiplying this quantity by \( 43^{-b} \cdot 42 \) we obtain by Proposition \([43] \) that \( \mu_{\text{GL}_2(\mathbb{Z}/43)}(\mathcal{M}_{43}(0, b)) = \frac{1}{2} \cdot 43^{-b} \) for \( b > 0 \). By \([43] \) Example 28] the contribution to \( \text{Dens}_{43} \) coming from the matrices in \( \mathcal{G}(43^\infty) \) such that \( \varepsilon_{-43} = -1 \) is then

\[
\text{Dens}_{43}(\varepsilon_{-43} = -1) = \frac{41}{2 \cdot 42} + \sum_{b > 0} \frac{1}{2} \cdot 43^{-2b} = \frac{1805}{2 \cdot 42 \cdot 44}.
\]

From \([43] \) Theorem 35 we know that \( \text{Dens}_{43}(\alpha) = 143510179/146927088 \), and hence the contribution to \( \text{Dens}_{43}(\alpha) \) coming from the matrices in \( \mathcal{G}(43^\infty) \) such that \( \varepsilon_{-43} = +1 \) equals

\[
\text{Dens}_{43}(\varepsilon_{-43} = +1) = \frac{3261637}{6678504}.
\]

Now we work with the 2-adic representation, which is surjective, and restrict to counting the contribution to \( \text{Dens}_{2}(\alpha) \) coming from the matrices satisfying \( \psi = -1 \). In view of Lemma \([23] \) and Proposition \([23] \) we find \( \mu_{\text{GL}_2(\mathbb{Z}/2)}(\mathcal{M}_{2}(0, b)) = 1/2 \cdot 2^{-b} \) for \( b > 0 \). By \([43] \) Example 28] the contribution to \( \text{Dens}_{2}(\alpha) \) coming from the matrices in \( \mathcal{G}(2^\infty) \) such that \( \psi = -1 \) is therefore

\[
\text{Dens}_{2}(\psi = -1) = \sum_{b > 0} 1/2 \cdot 2^{-2b} = 1/6.
\]

From \([43] \) Theorem 35 we know that \( \text{Dens}_{2}(\alpha) = 11/21 \), and hence the contribution to \( \text{Dens}_{2} \) coming from the matrices in \( \mathcal{G}(2^\infty) \) such that \( \psi = 1 \) is

\[
\text{Dens}_{2}(\psi = 1) = 5/14.
\]

Finally, by the partition in Section \( \textbf{6.3} \) we can compute the requested density as the following combination of the above quantities:

\[
\text{Dens}_{2,43}(\alpha) = 2 \left( \text{Dens}_{2}(\psi = 1) \cdot \text{Dens}_{43}(\varepsilon_{-43} = 1) + \text{Dens}_{2}(\psi = -1) \cdot \text{Dens}_{43}(\varepsilon_{-43} = -1) \right).
\]

Indeed, let us consider Theorem \([19] \) recalling that \( C_m = 1 \). Let us call \( H_+ \) the subset of \( \mathcal{G}(m^\infty) \) consisting of elements whose image in \( \mathcal{G}(2) \) satisfies \( \psi = 1 \) and whose image in \( \mathcal{G}(43) \) satisfies \( \varepsilon_{-43} = 1 \), and define analogously \( H_- \) with \( \psi = -1 \) and \( \varepsilon_{-43} = -1 \). Write \( H_+ = H_{2,+} \times H_{43,+} \), where \( H_{2,+} \subseteq \mathcal{G}(2^\infty) \) and \( H_{43,+} \subseteq \mathcal{G}(43^\infty) \). Similarly, write \( H_- = H_{2,-} \times H_{43,-} \). The formula of Theorem \([19] \) considering the two contributions for \( \text{Dens}_{2,43}(\alpha) \) coming from \( H_+ \) and \( H_- \), gives

\[
\text{Dens}^+ = \frac{\# \mathcal{G}(2) \# \mathcal{G}(43)}{\# \mathcal{G}(2 \cdot 43)} \int_{H_{2,+}} \frac{w_{2^\infty}(M)}{\# \ker(M - I)} \, d\mu_{\mathcal{G}_{2^\infty}}(M) \cdot \int_{H_{43,+}} \frac{w_{43^\infty}(M)}{\# \ker(M - I)} \, d\mu_{\mathcal{G}_{43^\infty}}(M),
\]

and similarly for \( \text{Dens}^- \). This yields formula \((18)\).

For the point \( 2\alpha \), by \([43] \) Example 28] we only need to scale \((17)\) by a factor 2, giving \( 1/3 \) and \( 3/7 \) as the two contributions to \( \text{Dens}_{2}(2\alpha) \) by \([43] \) Theorem 35. For the point \( 4\alpha \), we adapt \((17)\) as \( 2 \cdot 1/2 \cdot 2^{-2} + \sum_{b > 1} 4 \cdot 1/2 \cdot 2^{-2b} \) and obtain \( 5/12 \) and \( 13/28 \) as the two contributions to \( \text{Dens}_{2}(4\alpha) \).

\[\text{ACKNOWLEDGMENTS}\]

We would like to thank Davide Lombardo and the referee for their valuable comments on the paper.
REFERENCES

[1] N. Jones. Almost all elliptic curves are Serre curves. *Trans. Amer. Math. Soc.*, 362(3):1547–1570, 2010.

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

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

[4] D. Lombardo and A. Perucca. Reductions of points on algebraic groups. *J. Inst. Math. Jussieu*, doi:10.1017/S1474748019000598;1–33, 2020.

[5] A. Perucca. Prescribing valuations of the order of a point in the reductions of abelian varieties and tori. *J. Number Theory*, 129:469–476, 2009.

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

[7] A. V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, 4:e4, 79, 2016.

[8] The LMFDB Collaboration. The L-functions and modular forms database. [http://www.lmfdb.org](http://www.lmfdb.org) 2016.

[9] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.3)*. 2016. [http://www.sagemath.org](http://www.sagemath.org).


Email address: P.J.Bruin@math.leidenuniv.nl

University of Luxembourg, Department of Mathematics, 6, Avenue de la Fonte, 4364 Esch-sur-Alzette, Luxembourg

Email address: antonella.perucca@uni.lu