Glasgow Math. J. **63** (2021) 484–502.
doi:10.1017/S0017089520000336.

REDUCTIONS OF POINTS ON ALGEBRAIC GROUPS, II

PETER BRUIN

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands
e-mail: *P.J.Bruin@math.leidenuniv.nl*

ANTONELLA PERUCCA

Department of Mathematics, University of Luxembourg, 6, Avenue de la Fonte,
4364 Esch-sur-Alzette, Luxembourg
e-mail: *antonella.perucca@uni.lu*

(Received 15 October 2019; revised 16 March 2020; accepted 26 June 2020; first published online 28 July 2020)

Abstract. Let A be the product of an abelian variety and a torus over a number field K, and let $m \geqslant 2$ be a square-free integer. If $\alpha \in A(K)$ is a point of infinite order, we consider the set of primes $\mathfrak{p}$ of K such that the reduction (α mod $\mathfrak{p}$) 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 ℓ-adic integrals, where ℓ 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.

2010 *Mathematics Subject Classification*. Primary: 11F80; Secondary: 14L10, 11G05, 11G10

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 $m \geqslant 2$ be a square-free integer. If $\alpha \in A(K)$ is a point of infinite order, we consider the set of primes $\mathfrak{p}$ of K such that the reduction (α mod $\mathfrak{p}$) is well defined and has order coprime to m. This set admits a natural density (see Theorem 7), which we denote by $\mathrm{Dens}_m(\alpha)$.

The main question is whether we can write

$$\mathrm{Dens}_m(\alpha) = \prod_{\ell} \mathrm{Dens}_\ell(\alpha), \tag{1.1}$$

where ℓ varies over the prime divisors of m. Let $K(A[m])$ be the m-torsion field of A. We prove that (1.1) 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 ℓ for every prime divisor ℓ of m (see Corollary 18). Indeed, (1.1) holds if the torsion fields/Kummer extensions of α related to different prime divisors of m are linearly disjoint over K. In general, (1.1) does not hold: see Section 7.2 for an explicit example.

We are able to express $\mathrm{Dens}_m(\alpha)$ as an integral over the image of the m-adic representation (see Theorem 16) and also as a finite sum of products of ℓ-adic integrals (see

Theorem 19). The latter decomposition allows us to prove that $\mathrm{Dens}_m(\alpha)$ 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 $\mathrm{Dens}_m(\alpha)$ if the m^n-Kummer extensions of α (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 $\mathrm{Dens}_m(\alpha)$ 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 α 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 α 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 α by a finitely generated subgroup of $A(K)$; see Remark 22.

2. Integration on profinite groups. For every profinite group G, we write μ_G for the normalised Haar measure on G. More generally, if X is a G-torsor, we write μ_X for the normalised Haar measure on X, defined by transporting μ_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 ℓ varies in a finite set of prime numbers, and each G_ℓ is a profinite group containing a pro-ℓ-group G'_ℓ 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'_ℓ is a pro-ℓ-group, and the normalised Haar measures on H' and the H'_ℓ 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'_ℓ-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 $\int_{H(x)} \mu_H = \frac{1}{(H:H')}$; this proves (1). Because G' is a

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

product of pro-ℓ-groups for pairwise different ℓ, every closed subgroup of G' is similarly a product of pro-ℓ-groups. This shows the existence of the H'_ℓ 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 $f\colon H \to \mathbb{C}$ be an integrable function.*

(1) We have

$$\int_H f\, d\mu_H = \frac{1}{(H:H')} \sum_{x \in H/H'} \int_{H(x)} f\, d\mu_{H(x)}.$$

(2) Suppose that for each $x \in H/H'$, the restriction of f to $H(x)$ admits a product decomposition

$$f|_{H(x)} = \prod_\ell f_{x,\ell},$$

where the $f_{x,\ell}\colon H_\ell(x) \to \mathbb{C}$ are integrable functions. Then we have

$$\int_H f\, d\mu_H = \frac{1}{(H:H')} \sum_{x \in H/H'} \prod_\ell \int_{H_\ell(x)} f_{x,\ell}\, d\mu_{H_\ell(x)}.$$

Proof. Part (1) follows by rewriting $\int_H f\, d\mu_H$ as $\sum_{x \in H/H'} \int_{H(x)} f\, d\mu_H$ and applying Lemma 1(1). Part (2) follows from part (1), Lemma 1(3) and the assumption on f. □

3. The arboreal representation.

Let K be a number field, and let $\overline{K}$ be an algebraic closure of K. Let A be a connected commutative algebraic group over K, and let b_A be the first Betti number of A. We fix a square-free integer $m \geqslant 2$. Below, we let ℓ vary in the set of prime divisors of m. We also fix a point $\alpha \in A(K)$.

We define $T_m A$ as the projective limit of the torsion groups $A[m^n]$ for $n \geqslant 1$; we can write $T_m A = \prod_\ell T_\ell A$, where the Tate module $T_\ell A$ is a free $\mathbb{Z}_\ell$-module of rank b_A.

We define the *torsion fields*

$$K_{m^{-n}} := K(A[m^n]) \quad \text{for } n \geqslant 1$$

and

$$K_{m^{-\infty}} := \bigcup_{n \geqslant 1} K_{m^{-n}}.$$

The Galois action on the m-power torsion points of A gives the *m-adic representation* of A, which maps $\mathrm{Gal}(\overline{K}/K)$ to the automorphism group of $T_m A$. We can also speak of the *mod m^n representation*, which describes the Galois action on $A[m^n]$. Choosing a $\mathbb{Z}_\ell$-basis for $T_\ell A$ for every prime divisor ℓ of m, we can identify the image of the m-adic representation with a subgroup of $\prod_\ell \mathrm{GL}_{b_A}(\mathbb{Z}_\ell)$ and the image of the mod m^n representation with a subgroup of $\prod_\ell \mathrm{GL}_{b_A}(\mathbb{Z}/\ell^n\mathbb{Z})$.

For $n \geqslant 1$, let $m^{-n}\alpha$ be the set of points in $A(\overline{K})$ whose m^nth multiple equals α. We also write

$$m^{-\infty}\alpha = \varprojlim_{n \geqslant 1} m^{-n}\alpha.$$

This is the set of sequences $\beta = \{\beta_n\}_{n \geqslant 1}$ such that $m\beta_1 = \alpha$ and $m\beta_{n+1} = \beta_n$ for every $n \geqslant 1$; it is a torsor under $T_m A$. We note that $m^{-n}0 = A[m^n]$ and $m^{-\infty}0 = T_m A$.

We define the fields

$$K_{m^{-n}\alpha} := K(m^{-n}\alpha) \quad \text{for } n \geqslant 1$$

and

$$K_{m^{-\infty}\alpha} := \bigcup_{n \geqslant 1} K_{m^{-n}\alpha}.$$

We call the field extension $K_{m^{-n}\alpha}/K_{m^{-n}}$ the m^n-*Kummer extension* defined by the point α. We view the m-adic representation as a representation of $\mathrm{Gal}(K_{m^{-\infty}\alpha}/K)$.

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

$$\begin{aligned} \omega_{\alpha,m^\infty} \colon \mathrm{Gal}(K_{m^{-\infty}\alpha}/K) &\longrightarrow T_m A \rtimes \mathrm{Aut}(T_m A) \\ \sigma &\longmapsto (t, M), \end{aligned}$$

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

$$T_m A \rtimes \mathrm{Aut}(T_m A) \cong \prod_\ell \mathbb{Z}_\ell^{b_A} \rtimes \prod_\ell \mathrm{GL}_{b_A}(\mathbb{Z}_\ell) \cong \prod_\ell (\mathbb{Z}_\ell^{b_A} \rtimes \mathrm{GL}_{b_A}(\mathbb{Z}_\ell)).$$

Likewise, for each $n \geqslant 1$, the choice of β defines a homomorphism

$$\begin{aligned} \omega_{\alpha,m^n} \colon \mathrm{Gal}(K_{m^{-n}\alpha}/K) &\longrightarrow A[m^n] \rtimes \mathrm{Aut}(A[m^n]) \\ \sigma &\longmapsto (t, M), \end{aligned}$$

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

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

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

We write $d_{A,\ell}$ for the dimension of the Zariski closure of $\mathcal{G}(\ell^\infty)$ in $\mathrm{GL}_{b_A,\mathbb{Q}_\ell}$, 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 $N \geqslant n \geqslant n_0$ we have

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

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

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 $N \geqslant n \geqslant n_0$ we have

$$[K_{m^{-N}\alpha} : K_{m^{-n}\alpha}] = (m^{b_A} D_{A,m})^{N-n}. \tag{3.1}$$

REMARK 4. Condition (3.1) 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

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

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

$$\mathrm{C}_m := m^{b_A n}/[K_{m^{-n}\alpha} : K_{m^{-n}}] \tag{3.2}$$

is independent of n for $n \geqslant n_0$. In fact, C_m is an integer because ω_{α,m^n} maps $\mathrm{Gal}(K_{m^{-n}\alpha}/K_{m^{-n}})$ 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 ℓ 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 $[K_{\ell^{-n}} : K_{\ell^{-1}}]$ is a power of ℓ 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 ℓ is any prime divisor of m. We conclude because the degrees of these Kummer extensions are powers of ℓ. □

4. Relating the density and the arboreal representation.

4.1. The existence of the density. Let $(A/K, m, \alpha)$ be as in Section 3. 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 $\mathbb{Z}\alpha$. If this number is not coprime to m, then the density $\mathrm{Dens}_m(\alpha)$ is zero by [5, Main Theorem] while if it is coprime to m we may replace α by a multiple to reduce to the case where the Zariski closure of $\mathbb{Z}\alpha$ is connected. Finally, we may replace A by the Zariski closure of $\mathbb{Z}\alpha$ and reduce to the case where $\mathbb{Z}\alpha$ 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 α has infinite order.

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

$$C_\alpha \in H^1(\mathrm{Gal}(K_{m^{-\infty}\alpha}/K), T_m A).$$

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

$$\begin{aligned} c_\beta :\ \mathrm{Gal}(K_{m^{-\infty}\alpha}/K) &\longrightarrow T_m A \\ \sigma &\longmapsto \sigma(\beta) - \beta. \end{aligned}$$

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

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

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

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

$$\begin{aligned} S_\alpha &:= \{\sigma \in \mathrm{Gal}(K_{m^{-\infty}\alpha}/K) \mid C_\alpha \in \ker(\mathrm{Res}_\sigma)\} \\ &= \{\sigma \in \mathrm{Gal}(K_{m^{-\infty}\alpha}/K) \mid \sigma(\beta) = \beta \textit{ for some } \beta \in m^{-\infty}\alpha\}. \end{aligned}$$

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

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

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

Proof. The generalisation of [4, Proposition 22] to the composite case is straightforward. □

4.2. Counting elements in the image of the arboreal representation. By Theorem 7, computing $\mathrm{Dens}_m(\alpha)$ comes down to computing the Haar measure of S_α in $\mathrm{Gal}(K_{m^{-\infty}\alpha}/K)$. This is why we now investigate the Galois groups $\mathrm{Gal}(K_{m^{-n}\alpha}/K)$ for positive integers n.

For $M \in \mathcal{G}(m^n)$ we define

$$\mathcal{W}_{m^n}(M) := \{t \in A[m^n] \mid (t, M) \in \mathrm{Gal}(K_{m^{-n}\alpha}/K)\} \tag{4.1}$$

and

$$\mathrm{w}_{m^n}(M) := \frac{\#\big(\mathrm{Im}(M-I) \cap \mathcal{W}_{m^n}(M)\big)}{\#\,\mathrm{Im}(M-I)} \in \mathbb{Q}. \tag{4.2}$$

We note that $\mathcal{W}_{m^n}(M)$ is a $\mathrm{Gal}(K_{m^{-n}\alpha}/K_{m^{-n}})$-torsor and in particular satisfies

$$\#\mathcal{W}_{m^n}(M) = [K_{m^{-n}\alpha} : K_{m^{-n}}].$$

For every prime divisor ℓ of m and every $n \geqslant 1$, we consider the Galois group of the compositum $K_{\ell^{-n}\alpha}K_{m^{-1}}$ over K and the inclusion

$$\iota_{\alpha,\ell^n} : \mathrm{Gal}(K_{\ell^{-n}\alpha}K_{m^{-1}}/K) \hookrightarrow \big(A[\ell^n] \rtimes \mathcal{G}(\ell^n)\big) \times \mathcal{G}(m).$$

For all $x \in \mathcal{G}(m)$ and $V \in \mathcal{G}(\ell^n)$, we define

$$\mathcal{W}_{x,\ell^n}(V) := \{\tau \in A[\ell^n] \mid (\tau, V, x) \in \mathrm{Im}\,\iota_{\alpha,\ell^n}\} \tag{4.3}$$

and

$$\mathrm{w}_{x,\ell^n}(V) := \frac{\#\big(\mathrm{Im}(V-I) \cap \mathcal{W}_{x,\ell^n}(V)\big)}{\#\,\mathrm{Im}(V-I)} \in \mathbb{Z}[1/\ell]. \tag{4.4}$$

We denote by π_* the projection onto $\mathcal{G}(*)$.

PROPOSITION 9. *If $x \in \mathcal{G}(m)$ and $M \in \mathcal{G}(m^n)$ are such that $\pi_m M = x$, then we have*

$$\mathcal{W}_{m^n}(M) = \prod_\ell \mathcal{W}_{x,\ell^n}(\pi_{\ell^n} M)$$

and

$$\mathrm{w}_{m^n}(M) = \prod_\ell \mathrm{w}_{x,\ell^n}(\pi_{\ell^n} M).$$

Proof. Since the extensions $K_{\ell^{-n}\alpha} K_{m^{-1}}/K_{m^{-1}}$ have pairwise coprime degrees and hence are linearly disjoint, giving an element of $\mathrm{Gal}(K_{m^{-n}\alpha}/K)$ mapping to $x \in \mathcal{G}(m)$ is equivalent to giving, for each prime $\ell \mid n$, an element of $\mathrm{Gal}(K_{\ell^{-n}\alpha} K_{m^{-1}}/K)$ mapping to x. Hence, given an element $t = \sum_\ell t_\ell$ in $A[m^n] = \bigoplus_\ell A[\ell^n]$, we have $t \in \mathcal{W}_{m^n}(M)$ if and only if for every ℓ we have $t_\ell \in \mathcal{W}_{x,\ell^n}(\pi_{\ell^n} M)$. Therefore (t, M) is in $\mathrm{Gal}(K_{m^{-n}\alpha}/K)$ if and only if $(t_\ell, \pi_{\ell^n} M, x)$ is in the image of ι_{α,ℓ^n} for all ℓ. This implies the first claim. The second claim follows because we have $\mathrm{Im}(M - I) = \bigoplus_\ell \mathrm{Im}(\pi_{\ell^n} M - I)$. □

LEMMA 10. *For all $x \in \mathcal{G}(m)$ and $V \in \mathcal{G}(\ell^\infty)$, the value $\mathrm{w}_{x,\ell^n}(V)$ is constant for n sufficiently large.*

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

By Lemma 10, we can define

$$\mathrm{w}_{x,\ell^\infty}(V) = \lim_{n\to\infty} \mathrm{w}_{x,\ell^n}(V) \in \mathbb{Z}[1/\ell]. \tag{4.5}$$

From Proposition 9 we deduce that for all $M \in \mathcal{G}(m^\infty)$, the value $\mathrm{w}_{m^n}(M)$ is also constant for n sufficiently large, so we can analogously define

$$\mathrm{w}_{m^\infty}(M) = \lim_{n\to\infty} \mathrm{w}_{m^n}(M) \in \mathbb{Q}. \tag{4.6}$$

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

$$\mathrm{w}_{m^\infty}(M) = \prod_\ell \mathrm{w}_{x,\ell^\infty}(\pi_{\ell^\infty} M).$$

Proof. Taking the limit as $n \to \infty$ in Proposition 9 yields the claim. □

The following lemma gives sufficient conditions for the sets $\mathcal{W}_{m^n}(M)$ and the functions $\mathrm{w}_{m^n}(M)$ and $\mathrm{w}_{m^\infty}(M)$ 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 $n \geqslant 1$, 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 $K_{m^{-1}} K_{\ell^{-n}}$ 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 $[K_{m^{-n}} K_{\ell^{-n}\alpha} : K_{m^{-n}}] = [K_{\ell^{-n}\alpha} : K_{\ell^{-n}}]$.

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

(6) We have $\mathrm{C}_m = \prod_\ell \mathrm{C}_\ell$.
(7) For all $n \geqslant 1$ and all $M \in \mathcal{G}(m^n)$ we have $\mathcal{W}_{m^n}(M) = \prod_\ell \mathcal{W}_{\ell^n}(\pi_{\ell^n} M)$.

(8) *For all* $n \geqslant 1$ *and all* $M \in \mathcal{G}(m^n)$ *we have* $\mathrm{w}_{m^n}(M) = \prod_\ell \mathrm{w}_{\ell^n}(\pi_{\ell^n} M)$.
(9) *For all* $M \in \mathcal{G}(m^\infty)$ *we have* $\mathrm{w}_{m^\infty}(M) = \prod_\ell \mathrm{w}_{\ell^\infty}(\pi_{\ell^\infty} M)$.

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 $[K_{m^{-1}} K_{\ell^{-n}\alpha} : K_{m^{-1}} K_{\ell^{-n}}]$ is a power of ℓ and $[K_{m^{-n}} : K_{m^{-1}} K_{\ell^{-n}}]$ is prime to ℓ. If condition (5) holds for a given $n \geqslant 1$ and all primes $\ell \mid m$, then we have

$$\begin{aligned}[K_{m^{-n}\alpha} : K_{m^{-n}}] &= \prod_\ell [K_{m^{-n}} K_{\ell^{-n}\alpha} : K_{m^{-n}}] \\ &= \prod_\ell [K_{\ell^{-n}\alpha} : K_{\ell^{-n}}].\end{aligned}$$

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

4.3. Partitioning the image of the *m*-adic representation. We view elements of $\mathcal{G}(m^\infty)$ as automorphisms of $A[m^\infty] = \bigcup_{n \geqslant 1} A[m^n]$. 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 ℓ-groups that have at most b_A cyclic components.

Let F be a group of the form $\prod_{\ell \mid m} \mathrm{F}_\ell$, where F_ℓ is a finite abelian ℓ-group with at most b_A cyclic components. We define the set

$$\mathcal{M}_{\mathrm{F}} := \{M \in \mathcal{G}(m^\infty) \mid \ker\left(M - I : A[m^\infty] \to A[m^\infty]\right) \cong \mathrm{F}\}, \tag{4.7}$$

and for every $x \in \mathcal{G}(m)$ we define the set

$$\mathcal{M}_{x,\mathrm{F}} := \{M \in \mathcal{G}(m^\infty) \mid \ker\left(M - I : A[m^\infty] \to A[m^\infty]\right) \cong \mathrm{F},\ \pi_m(M) = x\}.$$

We denote by $\mathcal{M}_{\mathrm{F}}(*)$ and $\mathcal{M}_{x,\mathrm{F}}(*)$, respectively, the images of these sets under the reduction map $\mathcal{G}(m^\infty) \to \mathcal{G}(*)$. We also write

$$\mathcal{M} := \bigcup_{\mathrm{F}} \mathcal{M}_{\mathrm{F}} = \bigcup_{x,\mathrm{F}} \mathcal{M}_{x,\mathrm{F}}, \tag{4.8}$$

the union being taken over all $x \in \mathcal{G}(m)$ and over all groups $\mathrm{F} = \prod_\ell \mathrm{F}_\ell$ as above, up to isomorphism.

PROPOSITION 13. *The following holds:*

(1) *The sets* $\mathcal{M}_{x,\mathrm{F}}$ *are measurable in* $\mathcal{G}(m^\infty)$*, and the set* $\mathcal{M}$ *of* (4.8) *is measurable in* $\mathcal{G}(m^\infty)$.
(2) *If* $n > v_\ell(\exp \mathrm{F})$ *for all* $\ell \mid m$*, then we have*

$$\mu_{\mathcal{G}(m^\infty)}(\mathcal{M}_{x,\mathrm{F}}) = \mu_{\mathcal{G}(m^n)}(\mathcal{M}_{x,\mathrm{F}}(m^n)).$$

(3) *We have* $\mu_{\mathcal{G}(m^\infty)}(\mathcal{M}_{x,\mathrm{F}}) = 0$ *if and only if* $\mathcal{M}_{x,\mathrm{F}} = \emptyset$.
(4) *If* $(A/K, m)$ *satisfies eventual maximal growth of the torsion fields, then we have*

$$\mu_{\mathcal{G}(m^\infty)}(\mathcal{M}) = 1.$$

Proof. This is proved as in [4, Lemma 23]. □

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

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 $\mathrm{Dens}_m(\alpha)$ comes down to computing the Haar measure of S_α in $\mathrm{Gal}(K_{m^{-\infty}\alpha}/K)$. The generalisation of [4, Remark 19] to the composite case gives

$$S_\alpha = \{(t, M) \in \mathrm{Gal}(K_{m^{-\infty}\alpha}/K) \mid M \in \mathcal{G}(m^\infty) \text{ and } t \in \mathrm{Im}(M - I)\}.$$

In view of (4.8), we consider the sets

$$S_{x,\mathrm{F}} := \{(t, M) \in \mathrm{Gal}(K_{m^{-\infty}\alpha}/K) \mid M \in \mathcal{M}_{x,\mathrm{F}} \text{ and } t \in \mathrm{Im}(M - I)\}.$$

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_α is the disjoint union of the sets $S_{x,\mathrm{F}}$ up to a set of measure 0. To see that the Haar measure of $S_{x,\mathrm{F}}$ is well defined and to compute it, we define for every $n \geqslant 1$ the set

$$S_{x,\mathrm{F},m^n} = \{(t, M) \in \mathrm{Gal}(K_{m^{-n}\alpha}/K) \mid M \in \mathcal{M}_{x,\mathrm{F}}(m^n) \text{ and } t \in \mathrm{Im}(M - I)\}.$$

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

Proof. The set S_{x,F,m^n} clearly contains the reduction modulo m^n of $S_{x,\mathrm{F}}$. To prove the other inclusion, consider $(t_{m^n}, M_{m^n}) \in S_{x,\mathrm{F},m^n}$ and a lift $(t, M) \in \mathrm{Gal}(K_{m^{-\infty}\alpha}/K)$. 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 $x \in \mathcal{G}(m)$. To conclude, it suffices to ensure $t \in \mathrm{Im}(M - I)$. Take $\tau_{m^n} \in A[m^n]$ satisfying $(M_{m^n} - I)(\tau_{m^n}) = t_{m^n}$, and some lift τ of τ_{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 $\mathrm{Gal}(K_{m^{-\infty}\alpha}/K)$ contains $m^n T_m(A) \times \{I\}$. □

THEOREM 15. *We have*

$$\mu(S_{x,\mathrm{F}}) = \frac{\mathrm{C}_m}{\#\mathrm{F}} \int_{\mathcal{M}_{x,\mathrm{F}}} \mathrm{w}_{m^\infty}(M)\, d\mu_{\mathcal{G}(m^\infty)}(M),$$

where C_m is the constant of (3.2) and w_{m^∞} is as in (4.6).

Proof. Choose n large enough so that $n > n_0$ and $n > \max_\ell\{v_\ell(\exp \mathrm{F})\}$ for every ℓ, where n_0 is as in Definition 3. By definition (see (4.1)) we can write

$$\#S_{x,\mathrm{F},m^n} = \sum_{M \in \mathcal{M}_{x,\mathrm{F}}(m^n)} \#\big(\mathrm{Im}(M - I) \cap \mathcal{W}_{m^n}(M)\big).$$

By definition (see (4.2)), we can express the summand as

$$\#\,\mathrm{Im}(M - I) \cdot \mathrm{w}_{m^n}(M) = \frac{\mathrm{w}_{m^n}(M) \cdot m^{bn}}{\#\mathrm{F}},$$

so from (3.2), we deduce

$$\frac{\#S_{x,\mathrm{F},m^n}}{\#\,\mathrm{Gal}(K_{m^{-n}\alpha}/K)} = \frac{1}{\#\mathcal{G}(m^n)} \sum_{M \in \mathcal{M}_{x,\mathrm{F}}(m^n)} \frac{\mathrm{C}_m}{\#\mathrm{F}} \cdot \mathrm{w}_{m^n}(M).$$

By (3.1), the left-hand side is a non-increasing function of n, and therefore, it admits a limit for $n \to \infty$, which is $\mu(S_{x,\mathrm{F}})$. The right-hand side is an integral over $\mathcal{M}_{x,\mathrm{F}}(m^n)$ with respect to the normalised counting measure of $\mathcal{G}(m^n)$, and the matrices in $\mathcal{M}_{x,\mathrm{F}}$ are exactly the matrices in $\mathcal{G}(m^\infty)$ whose reduction modulo m^n lies in $\mathcal{M}_{x,\mathrm{F}}(m^n)$. Taking the limit over n, we thus find the formula in the statement. □

THEOREM 16. *We have*

$$\begin{aligned}\mathrm{Dens}_m(\alpha) &= \mathrm{C}_m \sum_{\mathrm{F}} \frac{1}{\#\mathrm{F}} \int_{\mathcal{M}_\mathrm{F}} \mathrm{w}_{m^\infty}(M)\, d\mu_{\mathcal{G}(m^\infty)}(M) \\ &= \mathrm{C}_m \int_{\mathcal{G}(m^\infty)} \frac{\mathrm{w}_{m^\infty}(M)}{\#\ker(M-I)}\, d\mu_{\mathcal{G}(m^\infty)}(M), \qquad (5.1)\end{aligned}$$

where the function w_{m^∞} *is as in* (4.6)*, the constant* C_m *is as in* (3.2)*, and* F *varies over the products over the primes* $\ell \mid m$ *of finite abelian* ℓ*-groups with at most* b_A *cyclic components.*

Proof. To prove the first equality, note that $\mathcal{M}_\mathrm{F}$ is the disjoint union of the $\mathcal{M}_{x,\mathrm{F}}$ for $x \in \mathcal{G}(m)$. By Theorem 7, we may write $\mathrm{Dens}_m(\alpha) = \mu(S_\alpha) = \sum_{x,\mathrm{F}} \mu(S_{x,\mathrm{F}})$ and then it suffices to apply Theorem 15. The second equality follows because the union of the sets $\mathcal{M}_\mathrm{F}$ from (4.7) has measure 1 in $\mathcal{G}(m^\infty)$ by Proposition 13. □

COROLLARY 17 ([**4**, Theorem 1 and Remark 27]). *In the special case* $m = \ell$*, we have*

$$\begin{aligned}\mathrm{Dens}_\ell(\alpha) &= \mathrm{C}_\ell \sum_{\mathrm{F}} \frac{1}{\#\mathrm{F}} \int_{\mathcal{M}_\mathrm{F}} \mathrm{w}_{\ell^\infty}(M)\, d\mu_{\mathcal{G}(\ell^\infty)}(M) \\ &= \mathrm{C}_\ell \int_{\mathcal{G}(\ell^\infty)} \frac{\mathrm{w}_{\ell^\infty}(M)}{\#\ker(M-I)}\, d\mu_{\mathcal{G}(\ell^\infty)}(M), \qquad (5.2)\end{aligned}$$

where F *varies among the finite abelian* ℓ*-groups with at most* b_A *cyclic components.*

Notice that we have $\#\ker(M-I) = \ell^{v_\ell(\det(M-I))}$ for every $M \in \mathcal{G}(\ell^\infty)$; this shows the equivalence with [**4**, Theorem 1].

COROLLARY 18. *Let* ℓ *vary among the prime divisors of* m*. If the fields* $K_{\ell^{-\infty}\alpha}$ *are linearly disjoint over* K*, then we have*

$$\mathrm{Dens}_m(\alpha) = \prod_\ell \mathrm{Dens}_\ell(\alpha).$$

Proof. Note that we have $\mathrm{C}_m = \prod_\ell \mathrm{C}_\ell$. 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 $\mathrm{w}_{m^\infty}(M) = \prod_\ell \mathrm{w}_{\ell^\infty}(\pi_{\ell^\infty} M)$. We conclude that (5.1) is the product of the expressions (5.2) for $\ell \mid m$. □

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

$$\mathrm{Dens}_m(\alpha) = \frac{\mathrm{C}_m}{\#\mathcal{G}(m)} \sum_{x \in \mathcal{G}(m)} \prod_\ell \int_{H_\ell(x)} \frac{\mathrm{w}_{x,\ell^\infty}(M)}{\#\ker(M-I)}\, d\mu_{H_\ell(x)}(M), \qquad (5.3)$$

where $\mathrm{w}_{x,\ell^\infty}$ *is as in* (4.5).

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

Proof. Write $S_x = \bigcup_{\mathrm{F}} S_{x,\mathrm{F}}$ 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

$$\mu(S_x) = \sum_{\mathrm{F}} \mu(S_{x,\mathrm{F}}) = \mathrm{C}_m \int_{H(x)} \frac{\mathrm{w}_{m^\infty}(M)}{\#\ker(M-I)} d\mu_{\mathcal{G}(m^\infty)}(M).$$

The assertion follows from Propositions 2 and 11. □

COROLLARY 20. *The density* $\mathrm{Dens}_m(\alpha)$ *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* $m \geqslant 2$ *such that* $(A/K, m, \alpha)$ *satisfies eventual maximal growth of the Kummer extensions, we have*

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

where ℓ *varies over the prime divisors of m.*

Proof. Recall that C_m is an integer. In view of Lemma 10, we can consider each ℓ-adic integral in (5.3) and proceed as in the proof of [**4**, Theorem 36]. □

REMARK 21. For elliptic curves, it is also possible to bound the minimal denominator of $\mathrm{Dens}_m(\alpha)$. Indeed, let us consider (5.3), recalling that C_m is an integer. Each of the finitely many functions $\mathrm{w}_{x,\ell^\infty}$ takes only finitely many values: these are rational numbers whose minimal denominator divides ℓ^{2n_0}, where n_0 is large enough so that condition (3.1) holds for all $N \geqslant n \geqslant n_0$. 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 ℓ^{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 $\#\mathrm{GL}_2(\ell^{n_0})$. Essentially we need to evaluate finitely many geometric series because of the eventual maximal growth of the torsion fields (the degrees $[K(E[\ell^n]) : K]$ 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 $\alpha_1, \ldots, \alpha_r$ be generators for G. We may then consider the point $\beta = (\alpha_1, \ldots, \alpha_r)$ in the product $A^r(K)$. Then the density $\mathrm{Dens}_m(\beta)$ for the single point β is exactly the density of primes $\mathfrak{p}$ of K such that the order of $(G \bmod \mathfrak{p})$ 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

$$E\colon y^2 = (x - x_1)(x - x_2)(x - x_3), \tag{6.1}$$

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 (6.1) is $\Delta = \sqrt{\Delta}^2$, where

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

$$\sqrt{\Delta} = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1).$$

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

$$\psi_E\colon \operatorname{Gal}(K(E[2])/K) \longrightarrow \{\pm 1\}$$
$$\sigma \longmapsto \sigma(\sqrt{\Delta})/\sqrt{\Delta}.$$

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

$$\rho_{E,2}\colon \operatorname{Gal}(K(E[2])/K) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}).$$

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

$$\psi_E = \psi \circ \rho_{E,2}.$$

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 $\mathbb{Q}^\times$. 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

$$m_d = \begin{cases} |d_{\mathrm{sf}}| & \text{if } d_{\mathrm{sf}} \equiv 1 \bmod 4, \\ 4|d_{\mathrm{sf}}| & \text{otherwise.} \end{cases}$$

We define a character

$$\varepsilon_d\colon \operatorname{Gal}(\mathbb{Q}(\zeta_{m_d})/\mathbb{Q}) \longrightarrow \{\pm 1\}$$
$$\sigma \longmapsto \sigma(\sqrt{d})/\sqrt{d}.$$

If σ is the automorphism of $\mathbb{Q}(\zeta_{m_d})$ defined by $\sigma(\zeta_{m_d}) = \zeta_{m_d}^a$ with $a \in (\mathbb{Z}/m_d\mathbb{Z})^\times$, then $\varepsilon_d(\sigma)$ equals the Jacobi symbol $\left(\frac{d_{\mathrm{sf}}}{a}\right)$. We view ε_d as a character of $\mathrm{GL}_2(\mathbb{Z}/m_d\mathbb{Z})$ by composing with the determinant.

For all $n \geqslant 1$, we have a canonical projection

$$\pi_n\colon \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Fixing a $\widehat{\mathbb{Z}}$-basis for the projective limit of the torsion groups $E[n](\overline{\mathbb{Q}})$, we have a torsion representation

$$\rho_E\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

The image of ρ_E is contained in the subgroup

$$H_\Delta = \{M \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \mid \psi(\pi_2(M)) = \varepsilon_\Delta(\pi_{m_\Delta}(M))\}$$

of index 2 in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. 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 ρ_E is *equal* to H_Δ. As proven by N. Jones [1], almost all elliptic curves over $\mathbb{Q}$ are Serre curves.

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

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 ℓ^n (which means that $\mathcal{N}$ contains the intersection of $\mathcal{M}_\ell(a, b)$ with the set of preimages of ($\mathcal{N}$ mod ℓ^n) in $\mathrm{GL}_2(\mathbb{Z}_\ell)$), then we have

$$\frac{\mu_{\mathrm{GL}_2(\mathbb{Z}_\ell)}(\mathcal{N})}{\mu_{\mathrm{GL}_2(\mathbb{Z}_\ell)}(\mathcal{M}_\ell(a, b))} = \frac{\mu_{\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})}(\mathcal{N} \bmod \ell^n)}{\mu_{\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})}(\mathcal{M}_\ell(a, b) \bmod \ell^n)} \tag{6.2}$$

by [3, Theorem 27] (where the number of lifts is independent of the matrix). Notice that if $a \geqslant n$, then ($\mathcal{N}$ mod ℓ^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 ℓ, then we have*

$$\mu_{\mathrm{GL}_2(\mathbb{Z}_\ell)}(\mathcal{N}) = \mu_{\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}(\mathcal{N} \bmod \ell) \cdot \begin{cases} 1 & \text{if } a = b = 0 \\ \ell^{-b}(\ell-1) & \text{if } a = 0,\ b \geqslant 1 \\ \ell^{-4a} \cdot \ell(\ell-1)^2(\ell+1) & \text{if } a \geqslant 1,\ b = 0 \\ \ell^{-4a-b} \cdot (\ell-1)^2(\ell+1)^2 & \text{if } a \geqslant 1,\ b \geqslant 1. \end{cases}$$

Proof. We are working with $\mathrm{GL}_2(\mathbb{Z}_\ell)$, so we can apply [3, Proposition 33] (see also [3, Definition 19]). This gives the assertion for the set $\mathcal{M}_\ell(a, b)$; we can conclude because of (6.2). □

We now collect some results in the case $\ell = 2$. From [3, Theorem 2], we know

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

We consider the action of $\mathrm{GL}_2(\mathbb{Z}/2^3\mathbb{Z})$ on $\mathbb{Q}(\zeta_{2^3})$ defined by $M\zeta_{2^3} = \zeta_{2^3}^{\det M}$. The matrices $M \in \mathrm{GL}_2(\mathbb{Z}/2^3\mathbb{Z})$ that fix $\sqrt{-1}$ are those with $\det(M) = 1, 5$. The ones that fix $\sqrt{2}$ are those with $\det(M) = 1, 7$. 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*

$$\frac{\mu_{\mathrm{GL}_2(\mathbb{Z}_2)}(\mathcal{N}_2(a, b; -1))}{\mu_{\mathrm{GL}_2(\mathbb{Z}_2)}(\mathcal{M}_2(a, b))} = \begin{cases} 1/2 & \text{for } a = 0,\ b \geqslant 0 \\ 2/3 & \text{for } a = 1,\ b = 0 \\ 1/3 & \text{for } a = 1,\ b \geqslant 1 \\ 1 & \text{for } a \geqslant 2,\ b \geqslant 0 \end{cases}$$

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

and

$$\frac{\mu_{\mathrm{GL}_2(\mathbb{Z}_2)}(\mathcal{N}_2(a,b;\pm 2))}{\mu_{\mathrm{GL}_2(\mathbb{Z}_2)}(\mathcal{M}_2(a,b))} = \begin{cases} 1/2 & \text{for } a \leqslant 1,\ b \geqslant 0 \\ 2/3 & \text{for } a = 2,\ b = 0 \\ 1/3 & \text{for } a = 2,\ b \geqslant 1 \\ 1 & \text{for } a \geqslant 3,\ b \geqslant 0. \end{cases}$$

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 $M \in \mathrm{GL}_2(\mathbb{Z}/2^3\mathbb{Z})$ such that $\det(M) = d$ and $\ker(M - I) \cong \mathbb{Z}/2^a\mathbb{Z} \times \mathbb{Z}/2^{a+b}\mathbb{Z}$. 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 (6.2) lead to the measures in the statement. □

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

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

Proof. Consider matrices $M \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. 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. □

Now let ℓ be an odd prime number. We write

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

so ε_{ℓ^*} is a character of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ and also of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ via the determinant.

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

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

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

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 $\frac{\ell-1}{2}-1$ possibilities for χ) are diagonalisable, and we only have to choose the two distinct eigenspaces; this gives $(\ell+1)\ell$ matrices for every such χ. The matrices with $\chi(0)=1$ are the identity (which we are excluding) and the ℓ^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 $\frac{1}{2}\#\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ matrices satisfying $\varepsilon_{\ell^*}=1$, and we only need to subtract the identity and the matrices from (1).

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

6.3. Partitioning the image of the *m*-adic representation. Let E be a Serre curve over $\mathbb{Q}$. Let Δ be the minimal discriminant of E, and let Δ_{sf} be its square-free part. We write $\Delta_{\mathrm{sf}}=zu$, where $z\in\{1,-1,2,-2\}$ and where u is an odd fundamental discriminant. Then $|u|$ is the odd part of m_Δ, 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

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

If $m\neq 2$ is even and u divides m, then $\mathcal{G}(m^\infty)$ has index 2 in $\prod_\ell \mathcal{G}(\ell^\infty)$. 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 $\mathcal{G}(m^\infty)\subseteq\prod_{\ell\mid m}\mathcal{G}(\ell^\infty)$ into two sets that are products, namely

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

and

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

The set $\mathcal{G}(|u|^\infty)\cap\{\varepsilon_u=1\}$ is the disjoint union of sets of the form $\prod_{\ell\mid u}(\mathcal{G}(\ell^\infty)\cap\{\varepsilon_{\ell^*}=\pm1\})$, choosing an even number of minus signs; for the set $\mathcal{G}(|u|^\infty)\cap\{\varepsilon_u=-1\}$ we have to choose an odd number of minus signs. Since each $\ell\mid u$ is odd, the two sets $\mathcal{G}(\ell^\infty)\cap\{\varepsilon_{\ell^*}=\pm1\}$ can be investigated with the help of Lemma 26. Finally, the two sets $\mathcal{G}(2^\infty)\cap\{\psi\cdot\varepsilon_z=\pm1\}$ can be investigated using Lemmas 24 and 25.

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

7. Examples.

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

$$E\colon y^2+y=x^3+6x+27$$

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 $\mathrm{Dens}_6(\alpha)$ using [9]):

Point	Dens_2	Dens_3	Dens_6	primes $<10^6$
$\alpha=(5,\,13)$	$11/21$	$23/104$	$253/2184=11.584\ldots\%$	11.624%
$2\alpha=(-1,\,4)$	$16/21$	$23/104$	$46/273=16.849\ldots\%$	16.885%
$3\alpha=(-7/4,\,-31/8)$	$11/21$	$77/104$	$121/312=38.782\ldots\%$	38.730%
$6\alpha=(137/16,\,1669/64)$	$16/21$	$77/104$	$22/39=56.410\ldots\%$	56.373%
$4\alpha=(3,\,-9)$	$37/42$	$23/104$	$851/4368=19.482\ldots\%$	19.479%
$9\alpha=(\frac{19649}{12100},\,-\frac{9216643}{1331000})$	$11/21$	$95/104$	$1045/2184=47.847\ldots\%$	47.791%

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 $\mathrm{GL}_2(\mathbb{Z}_2)$; 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 (α 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 $\mathbb{Q}(\sqrt{-51})$ (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 $\mathbb{Q}(E[2],E[9])/\mathbb{Q}(E[9])$ 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 $\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3^\infty])=\mathbb{Q}$ 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 $\mathbb{Q}(E[3])\cap\mathbb{Q}(E[2^\infty])=\mathbb{Q}$.

The 2-adic Kummer extensions of α 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 α 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 $K=\mathbb{Q}(E[2])$).

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

We thus have $\mathcal{G}(6^\infty)=\mathcal{G}(2^\infty)\times\mathcal{G}(3^\infty)$, the 2^∞ Kummer extensions are independent from $\mathbb{Q}(E[3])$, and the 3^∞ 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

$$\mathrm{Dens}_6(\alpha)=\mathrm{Dens}_2(\alpha)\cdot\mathrm{Dens}_3(\alpha)$$

holds for α 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

$$E\colon y^2+y=x^3+x^2$$

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 α satisfies

$$\mathrm{Dens}_2(\alpha)\cdot\mathrm{Dens}_{43}(\alpha)\neq\mathrm{Dens}_{2\cdot 43}(\alpha)$$

because, as we will show below, we have

$$\mathrm{Dens}_2(\alpha)=\frac{11}{21},\qquad \mathrm{Dens}_{43}(\alpha)=\frac{143510179}{146927088},$$
$$\mathrm{Dens}_2(\alpha)\cdot\mathrm{Dens}_{43}(\alpha)=\frac{143510179}{280497168}\sim 51.16279\%,$$
$$\mathrm{Dens}_{2\cdot 43}(\alpha)=\frac{526206455}{1028489616}\sim 51.16303\%.$$

We will also compute the following values (by testing the primes up to 10^6, we have computed an approximation to $\mathrm{Dens}_{2\cdot 43}(\alpha)$ using [9]):

Point	$\mathrm{Dens}_{2\cdot 43}$	primes $<10^6$
$\alpha=(0,0)$	$526206455/1028489616=51.163\ldots\%$	51.136%
$2\alpha=(-1,-1)$	$42521603/57138312=74.418\ldots\%$	74.397%
$4\alpha=(2,3)$	$1769960107/2056979232=86.046\ldots\%$	86.072%

By looking at the reduction modulo 293, we see that α is not divisible by 2 over the 4-torsion field of E. Therefore, by [2, Theorem 5.2], for every prime number ℓ and for every $n\geqslant 1$, the degree of the ℓ^n-Kummer extension is maximal, i.e.

$$[\mathbb{Q}_{\ell^{-n}\alpha}:\mathbb{Q}_{\ell^{-n}}]=\ell^{2n}.$$

The 43-adic Kummer extensions have maximal degree also over $\mathbb{Q}(E[2])$, i.e.

$$[\mathbb{Q}_{43^{-n}\alpha}(E[2]):\mathbb{Q}_{43^{-n}}(E[2])]=43^{2n},$$

because the degree $[\mathbb{Q}(E[2]):\mathbb{Q}]=6$ is coprime to 43.

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

The extensions $\mathbb{Q}(2^{-1}\alpha)$ and $\mathbb{Q}(E[2\cdot 43])$ are linearly disjoint over $\mathbb{Q}(E[2])$, as can be seen by investigating the residual degree for the reduction modulo the prime 29327, which splits completely in $\mathbb{Q}(E[2])$. Indeed, the residual degree of the extension $\mathbb{Q}(2^{-1}\alpha)$ equals 4, while the residual degree of the extension $\mathbb{Q}(E[2\cdot 43])$ 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 $\mathrm{GL}_2(\mathbb{Z}/43\mathbb{Z})$ has order 43).

The 2-adic Kummer extensions have maximal degree also over $\mathbb{Q}(E[43])$, i.e.

$$[\mathbb{Q}_{2^{-n}\alpha}(E[43]) : \mathbb{Q}_{2^{-n}}(E[43])] = 2^{2n}.$$

To see this, we consider the intersection L of $\mathbb{Q}_{2^{-n}\alpha}$ and $\mathbb{Q}(E[43])$. This is a Galois extension of $\mathbb{Q}$, and the group $G = \mathrm{Gal}(L/\mathbb{Q})$ is a quotient of both $(\mathbb{Z}/2^n\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/43\mathbb{Z})$. Because $\mathrm{SL}_2(\mathbb{Z}/43\mathbb{Z})$ has no non-trivial quotient that can be embedded into a quotient of $(\mathbb{Z}/2^n\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$, the quotient map $\mathrm{GL}_2(\mathbb{Z}/43\mathbb{Z}) \to G$ factors as

$$\mathrm{GL}_2(\mathbb{Z}/43\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/43\mathbb{Z})^\times \longrightarrow G$$

This implies that L is a subfield of $\mathbb{Q}(\zeta_{43})$. Furthermore, L contains $\mathbb{Q}(\sqrt{-43})$. Because $(\mathbb{Z}/2^n\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$ does not have any quotient group of odd order, the maximal subfield of $\mathbb{Q}(\zeta_{43})$ that can be embedded into $\mathbb{Q}_{2^{-n}\alpha}$ is $\mathbb{Q}(\sqrt{-43})$, and we conclude that L equals $\mathbb{Q}(\sqrt{-43})$.

It follows that for $m = 2\cdot 43$, we have the maximal degree $[\mathbb{Q}_{m^{-n}\alpha} : \mathbb{Q}_{m^{-n}}] = m^{2n}$ and, more generally, that for every multiple P of α we have $[\mathbb{Q}_{m^{-n}P} : \mathbb{Q}_{m^{-n}}] = [\mathbb{Q}_{2^{-n}P} : \mathbb{Q}_{2^{-n}}]\cdot[\mathbb{Q}_{43^{-n}P} : \mathbb{Q}_{43^{-n}}]$. 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 α. 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 $\frac{1}{2\cdot 42}$ (respectively, $\frac{41}{2\cdot 42}$) is the counting measure in $\mathrm{GL}_2(\mathbb{Z}/43\mathbb{Z})$ of the matrices such that $\varepsilon_{-43} = -1$ and that are in $(\mathcal{M}_{43}(0, b) \bmod \ell)$ for some $b > 0$ (respectively, for $b = 0$). By multiplying this quantity by $43^{-b}\cdot 42$, we obtain by Proposition 23 that $\mu_{\mathrm{GL}_2(\mathbb{Z}_{43})}(\mathcal{M}_{43}(0, b)) = \frac{1}{2}43^{-b}$ for $b > 0$. By [4, Example 28], the contribution to Dens_{43} coming from the matrices in $\mathcal{G}(43^\infty)$ such that $\varepsilon_{-43} = -1$ is then

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

From [4, Theorem 35] we know that $\mathrm{Dens}_{43}(\alpha) = 143510179/146927088$, and hence the contribution to $\mathrm{Dens}_{43}(\alpha)$ coming from the matrices in $\mathcal{G}(43^\infty)$ such that $\varepsilon_{-43} = +1$ equals

$$\mathrm{Dens}_{43}(\varepsilon_{-43} = 1) = \frac{3261637}{6678504}.$$

Now we work with the 2-adic representation, which is surjective and restrict to counting the contribution to $\mathrm{Dens}_2(\alpha)$ coming from the matrices satisfying $\psi = -1$. In view of Lemma 25 and Proposition 23, we find $\mu_{\mathrm{GL}_2(\mathbb{Z}_2)}(\mathcal{M}_2(0, b)) = 1/2\cdot 2^{-b}$ for $b > 0$. By [4, Example 28], the contribution to $\mathrm{Dens}_2(\alpha)$ coming from the matrices in $\mathcal{G}(2^\infty)$ such that $\psi = -1$ is therefore

$$\mathrm{Dens}_2(\psi = -1) = \sum_{b>0} 1/2\cdot 2^{-2b} = 1/6. \tag{7.1}$$

https://doi.org/10.1017/S0017089520000336 Published online by Cambridge University Press

From [4, Theorem 35] we know that $\mathrm{Dens}_2(\alpha) = 11/21$, and hence the contribution to Dens_2 coming from the matrices in $\mathcal{G}(2^\infty)$ such that $\psi = 1$ is

$$\mathrm{Dens}_2(\psi = 1) = 5/14.$$

Finally, by the partition in Section 6.3, we can compute the requested density as the following combination of the above quantities:

$$\begin{aligned}\mathrm{Dens}_{2\cdot 43}(\alpha) = 2\big(&\mathrm{Dens}_2(\psi = 1)\cdot \mathrm{Dens}_{43}(\varepsilon_{-43} = 1)\\ &+ \mathrm{Dens}_2(\psi = -1)\cdot \mathrm{Dens}_{43}(\varepsilon_{-43} = -1)\big).\end{aligned} \tag{7.2}$$

Indeed, let us consider Theorem 19, recalling that $\mathrm{C}_m = 1$. 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 $\mathrm{Dens}_{2\cdot 43}(\alpha)$ coming from H_+ and H_-, gives

$$\mathrm{Dens}^+ = \frac{\#\mathcal{G}(2)\#\mathcal{G}(43)}{\#\mathcal{G}(2\cdot 43)} \int_{H_{2,+}} \frac{\mathrm{w}_{2^\infty}(M)}{\#\ker(M-I)}\, d\mu_{\mathcal{G}_{2^\infty}}(M) \cdot \int_{H_{43,+}} \frac{\mathrm{w}_{43^\infty}(M)}{\#\ker(M-I)}\, d\mu_{\mathcal{G}_{43^\infty}}(M),$$

and similarly for Dens^-. This yields formula (7.2).

For the point 2α, by [4, Example 28], we only need to scale (7.1) by a factor 2, giving $1/3$ and $3/7$ as the two contributions to $\mathrm{Dens}_2(2\alpha)$ by [4, Theorem 35]. For the point 4α, we adapt (7.1) 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 $\mathrm{Dens}_2(4\alpha)$.

ACKNOWLEDGMENTS. The authors 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) (2010), 1547–1570.

2. R. Jones and J. Rouse, Galois theory of iterated endomorphisms, *Proc. Lond. Math. Soc. (3)* **100**(3) (2010), 763–794. Appendix A by Jeffrey D. Achter.

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

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

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

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

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

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

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