COMPARING DENSITIES FOR POWERS IN ARTIN'S CONJECTURE ON PRIMITIVE ROOTS

ANTONELLA PERUCCA AND PIETRO SGOBBA

Abstract. We consider Artin's conjecture on primitive roots and related Artin-type problems, working over a number field K. Such problems deal with the reductions of algebraic numbers $\alpha \in K^\times$ modulo primes $\mathfrak{p}$ of K. The key property concerns the value of the index of $(\alpha \bmod \mathfrak{p})$, but it is also customary to require an additional Frobenius condition. The set of primes $\mathfrak{p}$ satisfying such properties admits a density, conditionally under the Extended Riemann Hypothesis. In this work we compare the density for α to the density for its powers, and also address some related questions.

1. Introduction

We investigate questions stemming from Artin's conjecture on primitive roots, and we refer the reader to Moree's survey [9] for an introduction to this research area.

Consider a rational number α which is not $0, 1, -1$ and it is not a square in $\mathbb{Q}^\times$, and exclude the finitely many primes p such that the reduction $(\alpha \bmod p)$ is not well-defined or it is zero. We may then ask whether α is a primitive root at p, which means that $(\alpha \bmod p)$ has index 1 in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. Conditionally under the Generalised Riemann Hypothesis (GRH), Hooley [1] proved that the set of prime numbers p for which α is a primitive root at p has a positive Dirichlet density, which we call $\mathrm{dens}(\alpha)$. He also gave explicit formulas for $\mathrm{dens}(\alpha)$ (which we recall in Section 2). Remark that some power of α is a primitive root at p only if α is a primitive root at p. Thus, for every positive integer m we have

$$\mathrm{dens}(\alpha^m) \leqslant \mathrm{dens}(\alpha)\,.$$

The difference between these two densities is explained by the contribution to $\mathrm{dens}(\alpha)$ given by the primes p such that $p \equiv 1 \bmod q$ holds for some prime divisor q of m.

In fact, it does happen that $\mathrm{dens}(\alpha^m) = \mathrm{dens}(\alpha)$. One first reason is the following: if α is an m-th power, then there is no contribution to $\mathrm{dens}(\alpha)$ from the primes considered above. However, the equality $\mathrm{dens}(\alpha^m) = \mathrm{dens}(\alpha)$ can hold even if for every $n > 1$ the rational number α is not an n-th power. For example, Hooley's formula imply that

$$\mathrm{dens}(-3^3) = \mathrm{dens}(-3)\,.$$

Indeed, there is no contribution to $\mathrm{dens}(-3)$ coming from the primes $p \equiv 1 \bmod 3$ because $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ and the index of $(-3 \bmod p)$ is even if $p \neq 3$ splits in $\mathbb{Q}(\sqrt{-3})$.

In Theorem 2.2 we provide a complete description for when we have $\mathrm{dens}(\alpha^m) = \mathrm{dens}(\alpha)$.

2010 *Mathematics Subject Classification.* 11A07, 11M26, 11R45.

Key words and phrases. primitive root, Artin's conjecture.

We also study the above question replacing $\mathbb{Q}$ by an arbitrary number field K, and assuming the Extended Riemann Hypothesis (ERH) which generalizes GRH. Remark that some of our results can be made unconditional by assuming that the involved densities do exist.

We also replace α by a finitely generated and torsion-free subgroup G of $K^\times$. Finally, we consider much more general conditions for the index of the reductions of G, see Theorem 4.1 and the results in Section 5. Our investigations naturally lead us to consider how the density for an algebraic number changes if we enlarge the number field that contains it, see for example Theorem 4.6.

There are several works in the literature addressing Artin's conjecture on primitive roots and its variants. For example, Lenstra [5] and Ziegler [14] provide formulas when the condition about the index being 1 is replaced by the index dividing t or the index being t for some positive integer t. Moreover, for $\alpha \in \mathbb{Q}$, restricting the classical Artin density $\mathrm{dens}(\alpha)$ by only considering the prime numbers in a given arithmetic progression was investigated by Lenstra, see [5, Theorem 8.3], by Moree [7, 8], and later by Lenstra et al. [6, Sect. 5]. Finally remark that to prove our results with a very general condition on the index we rely on the framework by Järviniemi and Perucca [3], later developed by these two authors and Sgobba in [4].

2. Comparing Artin densities for rational numbers

In this section we work over $\mathbb{Q}$, assuming GRH. We use the notation ℓ to denote prime numbers. For ℓ odd we set $\ell^* := (-1)^{(\ell-1)/2}\ell$, so $\mathbb{Q}(\sqrt{\ell^*})$ is the quadratic subextension of the cyclotomic field $\mathbb{Q}(\zeta_\ell)$. We write μ for the Moebius function.

Let $\alpha \in \mathbb{Q}\backslash\{0, \pm 1\}$ be not a square in $\mathbb{Q}^\times$, and call δ the discriminant of the quadratic field $\mathbb{Q}(\sqrt{\alpha})$. Denote by τ the largest integer for which $\alpha \in \mathbb{Q}^{\times\tau}$ (remark that τ is odd). Artin's density [1] can then be written as

$$\mathrm{dens}(\alpha) = A(\tau) \begin{cases} 1 & \text{if } \delta \not\equiv 1 \pmod 4, \\ 1 - \mu(|\delta|) f_\tau(\delta) & \text{otherwise}, \end{cases} \tag{2.1}$$

where

$$A(\tau) := \prod_{\ell \mid \tau} \left(1 - \frac{1}{\ell - 1}\right) \prod_{\ell \nmid \tau} \left(1 - \frac{1}{\ell(\ell-1)}\right)$$

and

$$f_\tau(\delta) = \prod_{\ell \mid \delta,\ \ell \mid \tau} \frac{1}{\ell - 2} \prod_{\ell \mid \delta,\ \ell \nmid \tau} \frac{1}{\ell^2 - \ell - 1}.$$

The above formulas imply that $\mathrm{dens}(\alpha) > 0$. Indeed, it is well-known that the Artin constant $A(1)$ is non-zero (in fact, $A(1) \sim 0.37$) so its positive rational multiple $A(\tau)$ is non-zero.

Also remark that if t is the squarefree part of τ (namely, t is obtained from τ by removing repeated prime factors), then we have $A(t) = A(\tau)$.

Remark 2.1. *Let m be an odd positive integer. We then have*

$$\frac{\operatorname{dens}(\alpha^m)}{\operatorname{dens}(\alpha)} = \frac{A(\tau m)}{A(\tau)} \begin{cases} 1 & \text{if } \delta \not\equiv 1 \pmod 4, \\ \frac{1-\mu(|\delta|)f_{\tau m}(\delta)}{1-\mu(|\delta|)f_{\tau}(\delta)} & \text{otherwise}. \end{cases}$$

This ratio does not change if we replace m by its squarefree part, or if we remove from m prime factors that divide τ. In fact, we have

$$\frac{A(\tau m)}{A(\tau)} = \prod_{\ell \mid m,\, \ell \nmid \tau} \left(1 - \frac{1}{\ell - 1}\right)\left(1 - \frac{1}{\ell(\ell-1)}\right)^{-1} = \prod_{\ell \mid m,\, \ell \nmid \tau} \frac{\ell^2 - 2\ell}{\ell^2 - \ell - 1}. \tag{2.2}$$

In particular, if $\delta \not\equiv 1 \pmod 4$ or if the common prime factors of δ and m divide τ (in the latter case, we have $f_{\tau m} = f_\tau$), we have

$$\frac{\operatorname{dens}(\alpha^m)}{\operatorname{dens}(\alpha)} = \prod_{\ell \mid m,\, \ell \nmid \tau} \frac{\ell^2 - 2\ell}{\ell^2 - \ell - 1}.$$

In the following result we characterize when the ratio $\operatorname{dens}(\alpha^m)/\operatorname{dens}(\alpha)$ equals 1.

Theorem 2.2. *If m is a positive odd squarefree integer, then $\operatorname{dens}(\alpha) = \operatorname{dens}(\alpha^m)$ if and only if $\alpha \in \mathbb{Q}^{\times m}$ or there is $\ell \mid m$ such that $\alpha \in \mathbb{Q}^{\times m/\ell}$ and $\alpha/\ell^* \in \mathbb{Q}^{\times 2}$.*

Proof. Even in a more general setting $\operatorname{dens}(\alpha) = \operatorname{dens}(\alpha^m)$ means that $\operatorname{dens}(\alpha) = \operatorname{dens}(\alpha^q)$ holds for every prime $q \mid m$, and the condition for q holds if α is a q-th power, see Theorem 4.10 and Remark 4.3.

Sufficiency. We are left to prove that if α/ℓ^* is a square, then $\operatorname{dens}(\alpha) = \operatorname{dens}(\alpha^\ell)$. Our assumptions imply $\delta = \ell^* \equiv 1 \bmod 4$. Then the desired equality follows from Remark 2.1 because we have $\mu(|\delta|) = -1$ and

$$\frac{A(\ell)}{A(1)} = \frac{\ell(\ell-2)}{\ell^2 - \ell - 1} \qquad f_1(\delta) = \frac{1}{\ell^2 - \ell - 1} \qquad f_\ell(\delta) = \frac{1}{\ell - 2}.$$

Necessity. Suppose that α is not an m-th power and let $\ell \mid m$ be a prime such that $\alpha \notin \mathbb{Q}^{\times \ell}$. It suffices to prove that α/ℓ^* is a square (equivalently, $\delta = \ell^*$), because this implies that ℓ is unique. Remark that τ is coprime to 2ℓ. We know $\operatorname{dens}(\alpha^\ell) = \operatorname{dens}(\alpha)$ and we consider Remark 2.1. We exclude $\delta \not\equiv 1 \bmod 4$ because $A(\tau\ell) \neq A(\tau)$. We also get the identity

$$1 - \mu(|\delta|)f_\tau(\delta) = \frac{\ell(\ell-2)}{\ell^2 - \ell - 1}\big(1 - \mu(|\delta|)f_{\tau\ell}(\delta)\big). \tag{2.3}$$

Let us write

$$f(\delta, \tau) := \prod_{\substack{q \mid \gcd(\delta,\tau) \\ q \neq \ell}} \frac{1}{q-2} \prod_{\substack{q \mid \delta \\ q \nmid \ell\tau}} \frac{1}{q^2 - q - 1}.$$

If $\ell \nmid \delta$, then (2.3) leads to a contradiction while, supposing $\ell \mid \delta$, (2.3) becomes

$$\ell^2 - \ell - 1 - f(\delta, h) = \ell(\ell-2) - \ell f(\delta, h).$$

We deduce $\mu(|\delta|)f(\delta,h)=-1$, namely $f(\delta,h)=1$ and $\mu(|\delta|)=-1$.

The second product in $f(\delta,h)$ must be empty, and in the first product we can at most have $q=3$. This gives $|\delta|=\ell$ (we exclude $|\delta|=3\ell$ because $\mu(3\ell)=1$). Recalling that $\delta\equiv 1 \bmod 4$ we obtain $\delta=\ell^*$. □

3. Preliminaries for the general case

3.1. **Setup.** We let K be a number field, and work within a fixed algebraic closure. We write ζ_n for a primitive n-th root of unity. Given a set $\mathcal{S}$ of primes of K, we denote by $\pi_{\mathcal{S}}(x)$ the number of primes $\mathfrak{p}\in\mathcal{S}$ with norm $\mathrm{N}\,\mathfrak{p}\leqslant x$.

We let $\alpha\in K^\times$ while G is a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. While considering the reductions of α or G modulo primes $\mathfrak{p}$ of K we tacitly exclude the finitely many $\mathfrak{p}$ such that the reduction modulo $\mathfrak{p}$ is not well-defined or it is not contained in the multiplicative group of the residue field $k_\mathfrak{p}$. We then denote by $\mathrm{ind}_\mathfrak{p}(\alpha)$ the index of $(\alpha \bmod \mathfrak{p})$ in $k_\mathfrak{p}^\times$, and similarly define $\mathrm{ind}_\mathfrak{p}(G)$.

By density we always mean Dirichlet density. If clear from the context, we don't specify the dependency of densities on the field K. We call $\mathrm{dens}(\alpha)$ the classical Artin density of the primes $\mathfrak{p}$ of K for which $\mathrm{ind}_\mathfrak{p}(\alpha)=1$, and if $t\geqslant 1$ we write $\mathrm{dens}(\alpha,t)$ if we require $\mathrm{ind}_\mathfrak{p}(\alpha)=t$. We write $\mathrm{dens}(\alpha, a \bmod d)$ if we require $\mathrm{ind}_\mathfrak{p}(\alpha)=1$ and restrict to the primes whose norm lies in the arithmetic progression $a \bmod d$. Notice that such densities are known to exist conditionally under the Extended Riemann Hypothesis, see [3, 4], because the condition on the norm is a Frobenius condition for the abelian field extension $K(\zeta_d)/K$, the Frobenius satisfying $\zeta_d\mapsto\zeta_d^a$.

Finally, we denote by $K(\zeta_n, G^{1/n})$ the cyclotomic-Kummer extension obtained by adding all n-th roots of the elements of G (equivalently, we may add the n-th roots of a set of generators for G).

3.2. **Dirichlet density in extensions.** Let Γ_K denote the set of primes of K of degree 1. The following result generalizes [11, Proposition 1] and it is unconditional:

Lemma 3.1. *Let L/K be an extension of number fields with Galois closure $\tilde{L}/K$, and let $\Gamma_{L,K}\subseteq\Gamma_K$ consist of the primes that split completely in L. Consider $S\subseteq\Gamma_{L,K}$ and let S_L be the primes of L lying over the primes of S. Then S has a Dirichlet density if and only if the same holds for S_L. In this case, we have*

$$\mathrm{dens}_L(S_L)=[\tilde{L}:K]\,\mathrm{dens}_K(S)\,.$$

Proof. Call $\mathcal{P}_K$ the set of primes of K. Since $\mathrm{dens}_L(\Gamma_L)=1$, by the definition of Dirichlet density we have

$$\mathrm{dens}_K(S):=\lim_{s\to 1^+}\frac{\sum_{\mathfrak{p}\in S}N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in\mathcal{P}_K}N(\mathfrak{p})^{-s}},\quad \mathrm{dens}_L(S_L):=\lim_{s\to 1^+}\frac{\sum_{\mathfrak{q}\in S_L}N(\mathfrak{q})^{-s}}{\sum_{\mathfrak{q}\in\Gamma_L}N(\mathfrak{q})^{-s}}\,.$$

We have

$$\sum_{\mathfrak{q}\in S_L}N(\mathfrak{q})^{-s}=[L:K]\sum_{\mathfrak{p}\in S}N(\mathfrak{p})^{-s}$$

and we may analogously relate the two sums over $\mathfrak{q} \in \Gamma_L$ and $\mathfrak{p} \in \Gamma_{L,K}$. We conclude because we have

$$\frac{1}{[\tilde{L} : K]} = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \Gamma_{L,K}} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{P}_K} N(\mathfrak{p})^{-s}}$$

by the Chebotarev Density Theorem applied to $\tilde{L}$ combined with the fact that the primes $\mathfrak{p}$ of K that split completely in L also split completely in $\tilde{L}$ (the reductions of all roots of the minimal polynomial of a primitive element of L belong to the residue field at $\mathfrak{p}$ because the polynomial splits into linear factors modulo $\mathfrak{p}$). □

4. Primes in arithmetic progression

In this section we assume ERH. We consider primes of K whose norm lies in a given arithmetic progression and such that the index of the reduction of G belongs to a given set of positive integers. We also require a Frobenius condition with respect to a given finite Galois extension of K.

Theorem 4.1. *Let F/K be a finite Galois extension of number fields, and let C be a conjugacy-stable subset of $\mathrm{Gal}(F/K)$. Let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. Let S be a non-empty set of positive integers, let $1 \leqslant a < d$ be coprime integers. Consider the set of primes of K given by*

$$\mathcal{P}_S(a,d) := \left\{ \mathfrak{p} : \mathrm{N}\,\mathfrak{p} \leqslant x,\ \mathrm{N}\,\mathfrak{p} \equiv a \bmod d,\ \mathrm{ind}_{\mathfrak{p}}(G) \in S,\ \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C \right\},$$

where $\mathfrak{p}$ varies through the primes of K unramified in F and such that $v_{\mathfrak{p}}(g) = 0$ for all $g \in G$. Then we have

$$\pi_{\mathcal{P}_S(a,d)}(x) = \frac{x}{\log x} \sum_{t \in S} \sum_{n=1}^{\infty} \frac{\mu(n) c(nt)}{[F(\zeta_{[d,nt]}, G^{1/nt}) : K]} + O\left(\frac{x}{(\log x)^{2 - \frac{1}{r+1}}} \right),$$

where

$$c(m) := |\{\sigma \in \mathrm{Gal}(F(\zeta_{[d,m]}, G^{1/m})/K) : \sigma|_{K(\zeta_m, G^{1/m})} = \mathrm{id},\ \sigma(\zeta_d) = \zeta_d^a,\ \sigma|_F \in C\}|.$$

For $S = \{t\}$ the double sum is just one sum and when $x \geqslant t^3$ we have the better error term

$$O\left(\frac{x}{\log^2 x} + \frac{x \log\log x}{\varphi(t) \log^2 x} \right).$$

Notice that for $F = K$ the coefficient $c(m)$ is 1 if the automorphism induced by $\zeta_d \mapsto \zeta_d^a$ is the identity on the intersection $K(\zeta_m, G^{1/m}) \cap \mathbb{Q}(\zeta_d)$, and it is 0 otherwise. Theorem 4.1 is a combination of two standard conditions which have been studied extensively, namely the index having prescribed value and the primes being in an arithmetic progression. For $K = \mathbb{Q}$ and G of rank 1 and $S = \{t\}$, Theorem 4.1 with $t = 1$ is stated in Moree's survey [9, Theorem 1], and for general t in [2, Theorem 3.1].

Proof of Theorem 4.1. We may suppose that the primes $\mathfrak{p}$ that are counted are of degree 1, as this restriction excludes only $O(\sqrt{x}/\log x)$ primes. The conditions $\mathrm{N}\,\mathfrak{p} \equiv a \bmod d$ and $(\mathfrak{p}, F/K) \subseteq C$ are equivalent to $(\mathfrak{p}, F(\zeta_d)/K) \subseteq C_{a,d}$, where

$$C_{a,d} := \{\sigma \in \mathrm{Gal}(F(\zeta_d)/K) : \sigma(\zeta_d) = \zeta_d^a, \sigma|_F \subseteq C\}.$$

Then for the second assertion it suffices to apply [12, Proposition 5.1] with $F' = F(\zeta_d)$ and $C' = C_{a,d}$. For the first assertion we apply [10, Theorem 1] in a similar way. □

Lemma 4.2. *If m is an odd positive integer, then we have*

$$\mathrm{dens}(G^m) = \mathrm{dens}(G) - \mathrm{dens}(G, S_1 \bmod m)$$

where S_1 is the set of integers that are congruent to 1 modulo some prime divisor of m. Consequently, we have $\mathrm{dens}(G^m) = \mathrm{dens}(G^{\mathrm{sqf}(m)})$, where $\mathrm{sqf}(m)$ denotes the squarefree part of m.

Proof. Let $\mathfrak{p}$ be a prime of K. The reduction $(G^m \bmod \mathfrak{p})$ has index 1 if and only if $(G \bmod \mathfrak{p})$ has index 1 and for every prime $q \mid m$ we have $\mathrm{N}\,\mathfrak{p} \not\equiv 1 \bmod q$. □

Remark 4.3. *By Lemma 4.2 we have $\mathrm{dens}(G) = \mathrm{dens}(G^m)$ if and only if $\mathrm{dens}(G) = \mathrm{dens}(G^{\mathrm{sqf}(m)})$. Consequently, the condition $\mathrm{dens}(G) = \mathrm{dens}(G^m)$ implies that $\mathrm{dens}(G) = \mathrm{dens}(G^{m^n})$ holds for every $n \geqslant 1$.*

Example 4.4. *We have $\mathrm{dens}(G^3) = \mathrm{dens}(G) - \mathrm{dens}(G, 1 \bmod 3) = \mathrm{dens}(G, 2 \bmod 3)$.*

Proposition 4.5. *If m is a squarefree integer, then we have*

$$\mathrm{dens}(G, 1 \bmod m) = \sum_{n \mid m} \mu(n)\,\mathrm{dens}(G^n).$$

Proof. Let $\mathfrak{p}$ be a prime of K such that $(G \bmod \mathfrak{p})$ has index 1. The condition $\mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m$ means that for all primes $q \mid m$ the index of $(G^q \bmod \mathfrak{p})$ is not 1. Given two distinct prime numbers q, q', we have that both $(G^q \bmod \mathfrak{p})$ and $(G^{q'} \bmod \mathfrak{p})$ have index 1 if and only if $(G^{qq'} \bmod \mathfrak{p})$ has index 1, and the same holds for finitely many prime numbers. Hence, applying the inclusion-exclusion principle over the prime factors of m yields the formula in the statement. □

Let L/K be a Galois extension of number fields. Consider a prime $\mathfrak{p}$ of K such that the index of $(G \bmod \mathfrak{p})$ is well-defined. If $\mathfrak{P}$ is a prime of L over $\mathfrak{p}$, then the index of $(G \bmod \mathfrak{P})$ is well-defined and it is a multiple of the index of $(G \bmod \mathfrak{p})$. The two indices are the same if and only if $\mathfrak{p}$ splits completely in L.

Theorem 4.6. *For every set S of positive integers and for every positive integer m the following holds:*

(4.1)
$$\mathrm{dens}_K(\mathfrak{p} : \mathrm{ind}_{\mathfrak{p}}(G) \in S, \mathrm{Frob}_{L/K}(\mathfrak{p}) = \mathrm{id}) = \frac{1}{[L:K]} \cdot \mathrm{dens}_L(\mathfrak{P} : \mathrm{ind}_{\mathfrak{P}}(G) \in S)$$

(4.2)
$$\mathrm{dens}_K(\mathfrak{p} : \mathrm{ind}_{\mathfrak{p}}(G) \in S, \mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m) = \frac{1}{[K(\zeta_m):K]} \mathrm{dens}_{K(\zeta_m)}(\mathfrak{P} : \mathrm{ind}_{\mathfrak{P}}(G) \in S)$$

(4.3)
$$\mathrm{dens}_K(\mathfrak{p} : \mathrm{ind}_{\mathfrak{p}}(G) = 1, \mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m) = \frac{1}{[K(\zeta_m):K]} \cdot \mathrm{dens}_{K(\zeta_m)}(G)\,.$$

Proof. The first equality is a consequence of Lemma 3.1, the second equality is a special case of the first (taking $L = K(\zeta_m)$), the third equality is a special case of the second (taking $S = \{1\}$). □

Remark 4.7. *For every positive even integer m we have $\mathrm{dens}(G^m) = 0$ because G consists of squares. If m is an odd positive integer, then we always have*

$$\mathrm{dens}(G^m) \leqslant \mathrm{dens}(G)$$

because G^m is a subgroup of G.

The two densities $\mathrm{dens}(G^m)$ and $\mathrm{dens}(G)$ may be the same though, even if m is prime and $G \neq W^m$ holds for any subgroup W of $K^\times$:

Example 4.8. *For $K = \mathbb{Q}$ and $\alpha = -3$ we have $\mathrm{dens}(\alpha) = \mathrm{dens}(\alpha^3)$. Indeed, α is a square in K_3 hence $\mathrm{dens}_{K_3}(\alpha) = 0$. By Theorem 4.6 we deduce that $(\mathrm{dens}\,\alpha, 1 \bmod 3) = 0$, and we may conclude by Lemma 4.2.*

Lemma 4.9. *For all positive integers t, m, M with $m \mid M$ the following holds:*

- *(i) We have $\mathrm{dens}(G^M) = \mathrm{dens}(G^m)$ if and only if for every prime $\ell \mid M$ we have $\mathrm{dens}(G^m, 1 \bmod \ell) = 0$ (this clearly holds if $\ell \mid m$).*
- *(ii) We have $\mathrm{dens}(G^M, t) = \mathrm{dens}(G^m, t)$ if and only if for every prime $\ell \mid \frac{M}{m}$ we have $\mathrm{dens}(G^m, t, 1 \bmod t\ell) = 0$.*

Proof. We may restrict to the primes $\mathfrak{p}$ of K of degree 1 (as the remaining primes have density 0) and we write $p = \mathrm{N}(\mathfrak{p})$ for the underlying rational prime.

(i): Suppose that $(G^m \bmod \mathfrak{p})$ has index 1. Then $(G^M \bmod \mathfrak{p})$ also has index 1 if and only if for every prime divisor ℓ of M/m the integer $\mathrm{N}(\mathfrak{p}) - 1$ is not a multiple of ℓ, which amounts to saying that $p \not\equiv 1 \bmod \ell$.

(ii): Suppose that $(G^m \bmod \mathfrak{p})$ has index t or, equivalently, order $(p-1)/t$. Then $(G^M \bmod \mathfrak{p})$ has index t or, equivalently, order $(p-1)/t$ if and only if each prime divisor ℓ of M/m does not divide $(p-1)/t$, which means $p \not\equiv 1 \bmod t\ell$. □

Theorem 4.10. *Let m, t be positive integers, with m odd and squarefree. Then the following are equivalent:*

- *(i) We have $\mathrm{dens}(G, t) = \mathrm{dens}(G^m, t)$.*
- *(ii) For every prime $\ell \mid m$, we have $\mathrm{dens}(G, t) = \mathrm{dens}(G^\ell, t)$.*

(iii) For every prime $\ell \mid m$, we have $\mathrm{dens}(G, t, 1 \bmod \ell) = 0$.

Proof. The equivalence of (ii) and (iii) can be obtained by fixing ℓ hence it is a consequence of Lemma 4.9(ii) applied to G and G^ℓ. Lemma 4.9(ii), applied to G and G^m, gives the equivalence of (i) and (iii). □

5. Comparing general Artin densities for powers

In this section we assume ERH. We write ℓ to denote prime numbers. We consider a set of positive integers H and study the condition $\mathrm{ind}_{\mathfrak{p}}(G) \in H$ using definitions and results from [4]. For a squarefree integer $Q > 1$ we consider the Q-adic valuation $\mathbb{Z}_{>0} \to \prod_{\ell \mid Q} \mathbb{Z}_{\geqslant 0}$ mapping m to the tuple $(v_\ell(m))_{\ell \mid Q}$, and we denote by H_Q the preimage under v_Q of $v_Q(H)$. We say that H is *cut by valuations* if $H = \bigcap_\ell H_\ell$, and we set $V_\ell := v_\ell(H)$. Then we define the following constants:

$$F_{v,r}(\ell) = \begin{cases} 1 - \frac{1}{\ell^r(\ell-1)} & \text{for } v = 0 \\ \frac{1}{\ell^{v(r+1)}} \cdot \frac{\ell}{(\ell-1)}\left(1 - \frac{1}{\ell^{r+1}}\right) & \text{for } v > 0\,, \end{cases}$$

and

$$A_{V_\ell,r}(\ell) := \sum_{v \in V_\ell} F_{v,r}(\ell), \quad A_{V,r} := \prod_\ell A_{V_\ell,r}(\ell)\,.$$

We denote by μ_{Haar} the normalized Haar measure. By [4, Theorem 23] there is a squarefree integer $B \geqslant 1$ which depends only on K and G such that

$$\mathrm{dens}(\mathfrak{p} : \mathrm{ind}_{\mathfrak{p}}(G) \in H) = A_{V,r} \cdot \mu_{\mathrm{Haar}}(C_{H,B}(G)) \prod_{\ell \mid B} A_{V_\ell,r}(\ell)^{-1}, \tag{5.1}$$

where

$$C_{H,B}(G) := \bigcup_{h \in H_B} C_h(G) = \bigsqcup_{\substack{h \in H_B \\ h \mid B^\infty}} C_h(G) \subseteq \mathrm{Gal}(K_{B^\infty,B^\infty}/K) \tag{5.2}$$

and $C_h(G)$ is the conjugacy-stable set of those K-automorphisms which fix $K(\zeta_h, G^{1/h})$, and for all $q \mid B$ prime do not fix the field $K(\zeta_{qh}, G^{1/qh})$. The extension K_{B^∞,B^∞} denotes the union of all extensions $K(\zeta_{B^e}, G^{1/B^e})$ with $e \geqslant 1$. Notice that this set up is unchanged if B is not squarefree.

We study how the above density changes if we replace G with G^m for some integer $m \geqslant 1$.

Remark 5.1. *It follows from [4, 13] that B depends on G only through its parameters of ℓ-divisibility and its adelic failure (i.e. whether roots of its elements lie in a cyclotomic extension of K). Therefore, considering G^m instead of G only affects the former matter. More precisely, B is divisible by all primes ℓ for which the parameters of ℓ-divisibility are not all zero. Hence, for G^m it suffices to replace B with Bm. Thus, we have*

$$\frac{\mathrm{dens}(\mathfrak{p} : \mathrm{ind}_{\mathfrak{p}}(G) \in H)}{\mathrm{dens}(\mathfrak{p} : \mathrm{ind}_{\mathfrak{p}}(G^m) \in H)} = \frac{\mu_{\mathrm{Haar}}(C_{H,B}(G))}{\mu_{\mathrm{Haar}}(C_{H,Bm}(G^m))} \cdot \prod_{\ell \mid m, \ell \nmid B} A_{V_\ell,r}(\ell).$$

Theorem 5.2. *Suppose that m and B are coprime. We then have*

$$\operatorname{dens}(\mathfrak{p} : \operatorname{ind}_{\mathfrak{p}}(G^m) \in H) = A_{V,r} \cdot \mu_{\mathrm{Haar}}(C_{H,B}(G)) \cdot \prod_{\ell \mid m} A^{(m)}_{V_\ell,r}(\ell) \cdot \prod_{\ell \mid Bm} A_{V_\ell,r}(\ell)^{-1}, \tag{5.3}$$

where for $\ell \mid m$ we set

$$A^{(m)}_{V_\ell,r}(\ell) := \sum_{\substack{v \in V_\ell \\ v \geqslant v_\ell(m)}} F^{(m)}_{v,r}(\ell) \qquad \text{and} \qquad F^{(m)}_{v,r}(\ell) := \frac{1}{\ell^{v(r+1)}} \cdot \frac{\ell^{v_\ell(m)r+1}}{\ell - 1}\Big(1 - \frac{1}{\ell^r}\Big).$$

Proof. We start with the formula given in (5.1) with G and B replaced by G^m and Bm, respectively. By [3, Proposition 3.1(iii)] for every integer t and any prime $\ell \mid m$ coprime to t (by assumption ℓ is then coprime to B), we have

$$K(\zeta_{\ell^{v_\ell(m)}}, G^{m/\ell^{v_\ell(m)}}) \cap K(\zeta_t, G^{m/t}) = K,$$

as the former field on the left-hand side equals $K(\zeta_{\ell^{v_\ell(m)}})$ and the latter is contained in $K(\zeta_t, G^{1/t})$. We deduce that the conditions on the K-automorphisms defining $C_{H,B}(G^m)$ are independent from those defining $C_{H,\ell}(G^m)$ for $\ell \mid m$. Moreover, since $(B, m) = 1$, for every $v \geqslant 1$ we have $K(\zeta_{B^v}, G^{m/B^v}) = K(\zeta_{B^v}, G^{1/B^v})$. Hence, we obtain

$$C_{H,Bm}(G^m) = C_{H,B}(G) \times \bigoplus_{\ell \mid m} C_{H,\ell}(G^m).$$

This decomposition yields the second factor in (5.3), and we are left to justify the third factor in the formula. By definition, for $\ell \mid m$, the set $C_{H,\ell}(G^m)$ is the disjoint union of the conjugacy classes $C_{\ell^v}(G^m)$ for $v \geqslant 0$ with $\ell^v \in H_\ell$. This class is empty if $v < v_\ell(m)$, and otherwise it has Haar measure equal to $F^{(m)}_{v,r}(\ell)$. Taking the Haar measure of the direct sum of the sets $C_{H,\ell}(G^m)$ for $\ell \mid m$ completes the proof. □

Corollary 5.3. *For m coprime with B we have*

$$\frac{\operatorname{dens}(\mathfrak{p} : \operatorname{ind}_{\mathfrak{p}}(G) \in H)}{\operatorname{dens}(\mathfrak{p} : \operatorname{ind}_{\mathfrak{p}}(G^m) \in H)} = \prod_{\ell \mid m} A_{V_\ell,r}(\ell)/A^{(m)}_{V_\ell,r}(\ell).$$

Proof. This is an immediate consequence of Theorem 5.2. □

For the special case $\operatorname{ind}_{\mathfrak{p}}(G) = t$, we consider the r-rank Artin constant

$$A_r := \prod_{\ell} \Big(1 - \frac{1}{\ell^r(\ell - 1)}\Big).$$

Theorem 5.4. *The density* $\operatorname{dens}(G, t)$ *equals*

$$\frac{A_r}{t^{r+1}} \cdot \mu_{\mathrm{Haar}}(C_{(t,B^\infty)}(G)) \cdot \prod_{\ell \mid t} \frac{\ell^{r+1} - 1}{\ell^{r+1} - \ell^r - 1} \prod_{\ell \mid (t,B)} \frac{\ell^{(r+1)v_\ell(t)+r}(\ell - 1)}{\ell^{r+1} - 1} \prod_{\ell \mid B, \ell \nmid t} \frac{\ell^r(\ell - 1)}{\ell^{r+1} - \ell^r - 1}.$$

Proof. It suffices to notice that the set $H = \{t\}$ is trivially cut by valuations (by taking $H_\ell = \{v_\ell(t)\}$ for every ℓ) and to apply (5.1). In particular, we obtain

$$A_{V,r} = \frac{A_r}{t^{r+1}} \cdot \prod_{\ell \mid t} \frac{\ell^{r+1} - 1}{\ell^{r+1} - \ell^r - 1},$$

and $C_{H,B}(G) = C_{(t,B^\infty)}(G)$ by the definition in (5.2). □

Corollary 5.5. *For every odd positive integer m we have*

$$\frac{\operatorname{dens}(G^m, t)}{\operatorname{dens}(G, t)} = \frac{\mu_{\mathrm{Haar}}(C_{(t,(Bm)^\infty)}(G^m))}{\mu_{\mathrm{Haar}}(C_{(t,B^\infty)}(G))} \cdot \prod_{\ell \mid (t,m), \ell \nmid B} \frac{\ell^{(r+1)v_\ell(t)+r}(\ell - 1)}{\ell^{r+1} - 1} \prod_{\ell \mid m, \ell \nmid Bt} \frac{\ell^r(\ell - 1)}{\ell^{r+1} - \ell^r - 1}.$$

Proof. This is an immediate consequence of Theorem 5.4 and Remark 5.1. □

Corollary 5.6. *If $(B, t) = 1$, then we have*

$$\operatorname{dens}(G, t) = \frac{A_r}{t^{r+1}} \cdot \prod_{\ell \mid t} \frac{\ell^{r+1} - 1}{\ell^{r+1} - \ell^r - 1} \prod_{\ell \mid B} \frac{\ell^r(\ell - 1)}{\ell^{r+1} - \ell^r - 1}.$$

Proof. The formula of Theorem 5.4 simplifies straight-forwardly in the given special case. □

Remark 5.7. *Suppose that $(m, B) = 1$ and consider the ratio $\operatorname{dens}(G^m, t)/\operatorname{dens}(G, t)$. By Theorem 5.2, the ratio is zero if $v_\ell(t) < v_\ell(m)$ for some $\ell \mid (t, m)$, and otherwise it is*

$$\frac{\operatorname{dens}(G^m, t)}{\operatorname{dens}(G, t)} = \prod_{\ell \mid \gcd(t,m)} \frac{\ell^r - 1}{\ell^{r+1} - 1} \ell^{v_\ell(m)r+1} \prod_{\ell \mid m, \ell \nmid t} \frac{\ell^r(\ell - 1)}{\ell^{r+1} - \ell^r - 1}.$$

References

[1] C. Hooley, *Artin's conjecture for primitive roots*, J. Reine Angew. Math. **225** (1967), 209–220. 1, 2

[2] S. Hu, M.-S. Kim, P. Moree and M. Sha, *Irregular primes with respect to Genocchi numbers and Artin's primitive root conjecture*, J. Number Theory **205** (2019), 59–80. 5

[3] O. Järviniemi and A. Perucca, *Unified treatment of Artin-type problems*, Res. Number Theory **9** (2023), no. 10. 2, 4, 9

[4] O. Järviniemi, A. Perucca and P. Sgobba, *Unified treatment of Artin-type problems II*, submitted for publication (status: minor revisions), arXiv:2211.15614. 2, 4, 8

[5] H.W. Jr. Lenstra, *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 201–224. 2

[6] H.W. Jr. Lenstra, P. Moree and P. Stevenhagen, *Character sums for primitive root densities*, Math. Proc. Cambridge Philos. Soc. **157** (2014), no. 3, 489–511. 2

[7] P. Moree, *On primes in arithmetic progression having a prescribed primitive root*, J. Number Theory **78** (1999), 85–98. 2

[8] P. Moree, *On primes in arithmetic progression having a prescribed primitive root. II*, Funct. Approx. Comment. Math. **39** (2008), 133–144. 2

[9] P. Moree, *Artin's primitive root conjecture – a survey*, Integers **12** (2012), no. 6, 1305–1416. 1, 5

[10] P. Moree, A. Perucca and P. Sgobba. *The distribution of the multiplicative index of algebraic numbers over residue classes*, submitted for publication, arXiv:2302.05165. 6

[11] A. Perucca, *Reductions of algebraic integers II*, in Women in numbers Europe II, 19–33, Assoc. Women Math. Ser., 11, Springer, Cham, 2018. 4

[12] A. Perucca and P. Sgobba, *Kummer theory for number fields and the reductions of algebraic numbers*, Int. J. Number Theory, **15** (2019), no. 8, 1617–1633. 6

[13] A. Perucca, P. Sgobba and S. Tronto, *The degree of Kummer extensions of number fields*, Int. J. Number Theory, **15** (2021), no. 5, 1091–1110. 8

[14] V. Ziegler, *On the distribution of the order of number field elements modulo prime ideals*, Unif. Distrib. Theory **1** (2006), no. 1, 65–85. 2