# KUMMER THEORY FOR NUMBER FIELDS AND THE REDUCTIONS OF ALGEBRAIC NUMBERS II

ANTONELLA PERUCCA AND PIETRO SGOBBA

ABSTRACT. Let $K$ be a number field, and let $G$ be a finitely generated and torsion-free subgroup of $K^\times$. For almost all primes $\mathfrak{p}$ of $K$, we consider the order of the cyclic group $(G \bmod \mathfrak{p})$, and ask whether this number lies in a given arithmetic progression. We prove that the density of primes for which the condition holds is, under some general assumptions, a computable rational number which is strictly positive. We have also discovered the following equidistribution property if $\ell^e$ is a prime power and $a$ is a multiple of $\ell$ (and $a$ is a multiple of 4 if $\ell = 2$), then the density of primes $\mathfrak{p}$ of $K$ such that the order of $(G \bmod \mathfrak{p})$ is congruent to $a$ modulo $\ell^e$ only depends on $a$ through its $\ell$-adic valuation.

## 1. INTRODUCTION

If we reduce the number 2 modulo every odd prime number $p$, then we have the sequence of natural numbers given by the multiplicative order of $(2 \bmod p)$. This sequence is very mysterious, and for example it is not known unconditionally whether the order of $(2 \bmod p)$ equals $p-1$ for infinitely many primes $p$, see [3]. Now consider a non-zero integer $z$: the density of primes $p$ for which the multiplicative order of $(z \bmod p)$ lies in a given arithmetic progression has been studied in various papers by Chinen and Murata, and by Moree, see, e.g. [1, 4].

More generally, consider a number field $K$ and a multiplicative subgroup $G$ of $K^\times$ which is finitely generated. For positive integers $x, y$ with $y \mid x$ we denote by $K_x := K(\zeta_x)$ the $x$th cyclotomic extension of $K$, and by $K_{x,y} := K_x(\sqrt[y]{G})$ the $y$th Kummer extension of $G$ over $K_x$. If $\mathfrak{p}$ is a prime of $K$, then we write $\mathrm{ord}_{\mathfrak{p}}(G)$ for the multiplicative order of $(G \bmod \mathfrak{p})$, which we tacitly assume to be well-defined. As customary, given two integers $x, y$ we write $(x, y)$ for their greatest common divisor and $[x, y]$ for their least common multiple. Finally, if we assume (GRH) we mean the extended Riemann hypothesis for the Dedekind zeta function of number fields.

In [8] we have generalised results by Ziegler [10] to higher rank and have proven in particular the following statement.

**Theorem 1** ([8, Theorem 1.3])**.** *Let $K$ be a number field, and let $G$ be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank. Fix an integer $d \geqslant 2$, fix an integer $a$, and consider the following set of primes of $K$:*

$$\mathcal{P} := \{\mathfrak{p} : \mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d\}.$$

2010 *Mathematics Subject Classification.* Primary: 11R44; Secondary: 11R45, 11R18, 11R21.

*Key words and phrases.* Number field, reduction, multiplicative order, arithmetic progression, density.

*Let $\mathcal{P}(x)$ be the number of primes $\mathfrak{p}$ in $\mathcal{P}$ with norm up to $x$.*

*Assuming (GRH), for every $x \geqslant 1$ we have*

$$\mathcal{P}(x) = \frac{x}{\log x} \sum_{n,t \geqslant 1} \frac{\mu(n) c(n,a,d,t)}{[K_{[d,n]t,nt} : K]} + O\left(\frac{x}{\log^{3/2} x}\right), \tag{1}$$

*where $c(n,a,d,t) \in \{0,1\}$, and where $c(n,a,d,t) = 1$ if and only if the following conditions hold:*

*(i)* $(1+at, d) = 1$;
*(ii)* $(d,n) \mid a$;
*(iii) the element of* $\mathrm{Gal}(\mathbb{Q}(\zeta_{dt})/\mathbb{Q})$ *mapping* $\zeta_{dt}$ *to* $\zeta_{dt}^{1+at}$ *is the identity on* $\mathbb{Q}(\zeta_{dt}) \cap K_{nt,nt}$.

From this result it is not clear whether the natural density $\mathrm{dens}_K(G, a \bmod d)$ of the set $\mathcal{P}$ is a rational number, if it is strictly positive, or if it is possible to evaluate it. The main results of this paper are the following, where $K$, $G$, $a$, and $d$ are as in Theorem 1:

**Theorem 2.** *Assume (GRH). Let $d = \ell^e$ for some prime number $\ell$ and for some $e \geqslant 1$. Suppose that $K = K_\ell$ if $\ell$ is odd, or that $K = K_4$ if $\ell = 2$. Then the density $\mathrm{dens}_K(G, a \bmod \ell^e)$ depends on $a$ only through its $\ell$-adic valuation, and it is a computable strictly positive rational number. In particular, it is the same for all $a$ coprime to $\ell$.*

Although the previous result has an assumption on the base field, we do not need that assumption in the following corollary.

**Corollary 3** (Equidistribution property)**.** *Assume (GRH). Let $K$ be any number field, and let $d = \ell^e$ for a prime number $\ell$ and $e \geqslant 1$. Suppose that $\ell \mid a$ if $\ell$ is odd, or that $4 \mid a$ and $e \geqslant 2$ if $\ell = 2$. Then the density $\mathrm{dens}_K(G, a \bmod \ell^e)$ depends on $a$ only through its $\ell$-adic valuation, and it is a computable strictly positive rational number.*

The following result concerns the case of composite modulus.

**Theorem 4.** *Assume (GRH). Let $d \geqslant 2$ and set $r := \prod_{\ell \mid d} \ell$ to be its radical. Suppose that $K = K_r$ if $d$ is odd, or that $K = K_{2r}$ if $d$ is even. Then, for $a$ coprime to $d$, the density $\mathrm{dens}_K(G, a \bmod d)$ is a computable strictly positive rational number which does not depend on $a$.*

The following result generalises the positivity assertion of Corollary 3.

**Theorem 5.** *Assume (GRH). The density $\mathrm{dens}_K(G, a \bmod d)$ is strictly positive for any number field $K$ if $d$ is a prime power or if $a$ is coprime to $d$.*

Theorem 2 is proven in Section 3.1 for $\ell$ odd, and in Section 3.2 for $\ell = 2$, respectively. We prove Corollary 3 in Section 3.3. Theorem 4 is proven in Section 3.4, while Theorem 5 is proven in Section 3.5. Section 4 is devoted to removing from Theorem 1 the assumption that the group $G$ is torsion-free. Finally, Section 5 contains examples of applications of the above theorems and some numerical data.

Notice that in this paper we rely on Theorem 1 and hence most of our results assume (GRH): if the density in Theorem 1 is known unconditionally, then our results would also be unconditional.

## 2. PRELIMINARIES

Let $K$ be a number field, and let $G$ be a finitely generated and torsion-free subgroup of $K^\times$. In the whole paper we tacitly assume that the primes $\mathfrak{p}$ of $K$ that we consider are such that the reduction of $G$ modulo $\mathfrak{p}$ is a well-defined subgroup of the multiplicative group of the residue field at $\mathfrak{p}$. Notice that the results of this section are unconditional.

### 2.1. **Prescribing valuations for the order.**

**Theorem 6.** *Let $\ell_1, \dots, \ell_n$ be distinct prime numbers and $x_1, \dots, x_n$ nonnegative integers. Then the density of primes $\mathfrak{p}$ of $K$ such that $v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G)) = x_i$ for all $i$ is a strictly positive computable rational number.*

*Proof.* The rationality of the density can be seen by neglecting the condition on the Frobenius in [5, Theorem 18]. For the positivity, apply [6, Proposition 12] to a basis $g_1, \dots, g_r$ of $G$ consisting of $\mathbb{Z}$-independent points of the multiplicative group $K^\times$. □

**Corollary 7.** *Given an integer $d \geqslant 2$ and a positive divisor $g$ of $d$, the sum of densities*

$$\sum_{\substack{0 \leqslant a < d \\ (a,d)=g}} \mathrm{dens}_K(G, a \bmod d) \tag{2}$$

*is a strictly positive computable rational number.*

*Proof.* We will express the sum (2) as a rational combination of densities as in Theorem 6. Write $g = \prod_{i=1}^n \ell_i^{f_i}$, and partition the index set as $\{1, \dots, n\} = I \sqcup J$ such that $f_i < v_{\ell_i}(d)$ for $i \in I$, and $f_i = v_{\ell_i}(d)$ for $i \in J$. Then it is easy to check that

$$\sum_{\substack{0 \leqslant a < d \\ (a,d)=g}} \mathrm{dens}_K(G, a \bmod d) = \mathrm{dens}_K\left(\left\{\mathfrak{p} : \begin{array}{l} v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G)) = f_i\,, \forall i \in I \\ v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G)) \geqslant f_i\,, \forall i \in J \end{array}\right\}\right). \tag{3}$$

From this expression and Theorem 6 we deduce that (2) is strictly positive. The density on the right-hand side of (3) is given by (applying the inclusion-exclusion principle for the primes up to $x$ and then taking the limit to make the densities)

$$\sum_{s=0}^{|J|} (-1)^s \sum_{\substack{S \subseteq J \\ |S|=s}} \mathrm{dens}_K\left(\left\{\mathfrak{p} : \begin{array}{l} v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G)) = f_i\,, \forall i \in I \\ v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G)) \leqslant f_i - 1\,, \forall i \in S \end{array}\right\}\right), \tag{4}$$

and each of the densities in (4) exists and equals

$$\mathrm{dens}_K\left(\left\{\mathfrak{p} : \begin{array}{l} v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G^h)) = f_i\,, \forall i \in I \\ v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G^h)) = 0\,, \forall i \in S \end{array}\right\}\right),$$

where $h = \prod_{i \in S} \ell_i^{f_i - 1}$. Such densities are computable rational numbers by Theorem 6. Hence the statement is proven. □

**Remark 8.** *Corollary 7 implies that the density $\mathrm{dens}_K(G, 0 \bmod d)$ is known unconditionally to be a strictly positive computable rational number.*

2.2. **Simplifications by changing the modulus.** We keep the notation of Theorem 1. By Remark 8 we may suppose that $0 < a < d$. The following lemma allows us to reduce to residue classes coprime to $d$ if $d$ is a prime power.

**Lemma 9.** *Let $d = \ell^e$, where $\ell$ is a prime number and $e \geqslant 1$. Suppose that $a = \ell^x \cdot w$, where $w$ is coprime to $\ell$ and $0 < x < e$. Set $w_j := w + j\ell^{e-x}$ for $0 \leqslant j < \ell$ (notice that $w_j$ is also coprime to $\ell$). Then the primes $\mathfrak{p}$ of $K$ such that $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d$ are exactly those such that*

$$\mathrm{ord}_{\mathfrak{p}}(G^{\ell^x}) \equiv w \bmod \ell^{e-x} \tag{5}$$

*minus those such that*

$$\mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}}) \equiv w_j \bmod \ell^{e-x+1} \tag{6}$$

*for some $0 \leqslant j < \ell$. In particular, we have*

$$\mathrm{dens}_K(G, a \bmod \ell^e) = \\ \mathrm{dens}_K(G^{\ell^x}, w \bmod \ell^{e-x}) - \sum_{j=0}^{\ell-1} \mathrm{dens}_K(G^{\ell^{x-1}}, w_j \bmod \ell^{e-x+1}) \,.$$

*Proof.* Notice that condition (6) for any $j$ implies condition (5) because $w_j$ is coprime to $\ell$ and hence we must have $\mathrm{ord}_{\mathfrak{p}}(G^{\ell^x}) = \mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}})$.

Let $\mathfrak{p}$ be a prime of $K$ such that $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d$. In particular, $\ell^x$ divides $\mathrm{ord}_{\mathfrak{p}}(G)$. Thus we have

$$\mathrm{ord}_{\mathfrak{p}}(G^{\ell^x}) = \frac{\mathrm{ord}_{\mathfrak{p}}(G)}{\ell^x} \qquad \text{and} \qquad \mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}}) = \frac{\mathrm{ord}_{\mathfrak{p}}(G)}{\ell^{x-1}} \,.$$

Dividing the congruence $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod \ell^e$ by $\ell^x$ and $\ell^{x-1}$, respectively, we obtain

$$\mathrm{ord}_{\mathfrak{p}}(G^{\ell^x}) \equiv w \bmod \ell^{e-x} \qquad \text{and} \qquad \mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}}) \equiv w\ell \bmod \ell^{e-x+1} \,.$$

We have proven one containment because $w\ell$ is not congruent to any of the $w_j$ modulo $\ell$.

Now suppose that (5) holds, and that (6) does not hold for any $j$. In particular we must have $\mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}}) \neq \mathrm{ord}_{\mathfrak{p}}(G^{\ell^x})$. We deduce $\mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}}) = \ell \cdot \mathrm{ord}_{\mathfrak{p}}(G^{\ell^x})$, and therefore $\mathrm{ord}_{\mathfrak{p}}(G) = \ell^x \cdot \mathrm{ord}_{\mathfrak{p}}(G^{\ell^x})$. We may conclude because multiplying (5) by $\ell^x$ gives

$$\ell^x \cdot \mathrm{ord}_{\mathfrak{p}}(G^{\ell^x}) \equiv a \bmod d \,. \qquad \square$$

**Remark 10.** *Consider the condition $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d$. Decompose $(a, d) = sh$ where $s = \prod_{\ell \mid (a,d)} \ell$ is its radical, and write $a' = \frac{a}{h}$, $d' = \frac{d}{h}$. Notice that $(a', d') = s$ is squarefree. We claim that the following equivalence holds:*

$$\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d \qquad \Longleftrightarrow \qquad \mathrm{ord}_{\mathfrak{p}}(G^h) \equiv a' \bmod d' \,.$$

*If the first congruence is satisfied, then $(a, d)$ divides $\mathrm{ord}_{\mathfrak{p}}(G)$, so in particular we have*

$$\frac{\mathrm{ord}_{\mathfrak{p}}(G)}{h} \equiv a' \bmod d' \,.$$

*Since $h$ divides $\mathrm{ord}_{\mathfrak{p}}(G)$, we have $\frac{\mathrm{ord}_{\mathfrak{p}}(G)}{h} = \mathrm{ord}_{\mathfrak{p}}(G^h)$ and the second congruence holds. Conversely, if the second congruence is satisfied, then $s = (a', d')$ divides $\mathrm{ord}_{\mathfrak{p}}(G^h)$. Since $h$ introduces no new prime factors, we have*

$$\mathrm{ord}_{\mathfrak{p}}(G^h) \cdot h = \mathrm{ord}_{\mathfrak{p}}(G)$$

*and hence the congruence $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d$ holds.*

2.3. **A general result.** We keep the notation from Theorem 1, and we denote by $\mathrm{Dens}_K(G, d)$ the density of primes $\mathfrak{p}$ of $K$ such that $\mathrm{ord}_{\mathfrak{p}}(G)$ is coprime to $d$.

**Remark 11.** *From the results in* [2] *and* [7]*, under the assumptions of Theorems 2 and 4, the density $\mathrm{Dens}_K(G, d)$ depends on $G$ only through the $d$-parameters for the $\ell$-divisibility of $G$ for each $\ell \mid d$. As a consequence of the results of this paper, the same holds for the density $\mathrm{dens}_K(G, a \bmod d)$ considered in Theorems 2 and 4 and in Corollary 3.*

**Theorem 12.** *Let $\ell$ be a prime number. Suppose that for every $G$ and for every $e \geqslant 1$ we have*

$$\mathrm{dens}_K(G, w \bmod \ell^e) = \mathrm{dens}_K(G, w' \bmod \ell^e)$$

*as long as $w, w'$ are coprime to $\ell$. Then for every $G$ and for every $e \geqslant 1$ the density*

$$\mathrm{dens}_K(G, a \bmod \ell^e)$$

*depends on $a$ only through its $\ell$-adic valuation, and it is a computable rational number.*

*Proof.* We know from [2, Theorem 3] that the quantity

$$\mathrm{Dens}_K(G, \ell) = 1 - \mathrm{dens}_K(G, 0 \bmod \ell)$$

is a computable rational number. Then for every $a$ coprime to $\ell$, by the assumption on the equidistribution, we have

$$\mathrm{dens}_K(G, a \bmod \ell^e) = \frac{1}{\varphi(\ell^e)} \cdot \mathrm{Dens}_K(G, \ell)\,,$$

so that $\mathrm{dens}_K(G, a \bmod \ell^n)$ is a computable rational number which does not depend on $a$.

For $0 < a < \ell^e$ not coprime to $\ell$ we apply Lemma 9, which allows us to compute the density $\mathrm{dens}_K(G, a \bmod \ell^e)$ as the difference of densities which we know to be computable rational numbers. More precisely, by the equidistribution condition the formula given in Lemma 9 becomes

$$\begin{aligned}&\mathrm{dens}_K(G, a \bmod \ell^e) = \\ &\mathrm{dens}_K(G^{\ell^x}, w \bmod \ell^{e-x}) - \ell \cdot \mathrm{dens}_K(G^{\ell^{x-1}}, w \bmod \ell^{e-x+1})\,,\end{aligned}$$

where $a = w\ell^x$ and $x = v_\ell(a)$. In particular, this formula shows that what matters about $a$ is only its $\ell$-adic valuation.

Finally the density for $a = 0$ is given as the complementary density of all the considered cases, and hence it is also a computable rational number. □

**Remark 13.** *Notice that for $0 < a < \ell^e$ with some fixed valuation $v_\ell(a) = x$ where $0 \leqslant x < e$, the previous theorem says that we have the following density:*

$$\mathrm{dens}_K(G, a \bmod \ell^e) = \frac{1}{\varphi(\ell^{e-x})} \cdot \mathrm{dens}_K\left(\{\mathfrak{p} : v_\ell(\mathrm{ord}_\mathfrak{p}(G)) = x\}\right) . \tag{7}$$

**Proposition 14.** *With the assumptions of Theorem 12, we have that the density $\mathrm{dens}_K(G, a \bmod \ell^e)$ is strictly positive for every $a$.*

*Proof.* For $a = 0$ we know this unconditionally by Remark 8. For $0 < a < \ell^e$, by Theorem 6 the densities (7) in Remark 13 are strictly positive. □

We say that a prime $\mathfrak{p}$ of $K$ is of degree 1 if both its ramification index and its residue class degree over $\mathbb{Q}$ are equal to 1.

**Lemma 15.** *Let $K$ be a number field, and let $G$ be a finitely generated and torsion-free subgroup of $K^\times$. Let $a, d$ be integers with $d \geqslant 2$ and let $r := \prod_{\ell | d} \ell$ be the radical of $d$. Let $m = r$ if $d$ is odd, and $m = 2r$ otherwise. Consider the following set of primes $\mathfrak{p}$ of $K$:*

$$\mathcal{S} := \{\mathfrak{p} : \mathrm{ord}_\mathfrak{p}(G) \equiv a \bmod d,\ \mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m\} .$$

*Then the density of the set $\mathcal{S}$ exists and it is equal to*

$$\frac{1}{[K_m : K]} \cdot \mathrm{dens}_{K_m}(G, a \bmod d) . \tag{8}$$

**Remark 16.** *Notice that, assuming (GRH), a formula for the density of the set $\mathcal{S}$ is given in* [8, Corollary 5.2]. *By Theorems 2 and 4 it follows that the density* (8) *is a computable strictly positive rational number if $d$ is a prime power or if $a$ is coprime to $d$. Moreover, if $d = \ell^e$ for a prime $\ell$, then the density of $\mathcal{S}$ depends on $a$ only through its $\ell$-adic valuation, while if $d$ is composite and $(a, d) = 1$, then it does not depend on $a$.*

*Proof of Lemma 15.* We may assume that the primes $\mathfrak{p}$ of $\mathcal{S}$ are of degree 1 and unramified in $K_m$. Hence for a prime $\mathfrak{p}$ in $\mathcal{S}$ we have $\mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m$ if and only if $\mathfrak{p}$ splits completely in $K_m$. Therefore, the set of primes of $K_m$ lying above the primes of $\mathcal{S}$ is the set

$$\{\mathfrak{P} \subseteq K_m \text{ of degree } 1 : \mathrm{ord}_\mathfrak{P}(G) \equiv a \bmod d\} ,$$

which has density $\mathrm{dens}_{K_m}(G, a \bmod d)$. Thus we obtain that the density of the set $\mathcal{S}$ exists and it is equal to $1/[K_m : K]$ times $\mathrm{dens}_{K_m}(G, a \bmod d)$ (see for instance [7, Proposition 1]). □

## 3. Proof of the results in the Introduction

We keep the notation of Theorem 1.

### 3.1. **Proof of Theorem 2 for $\ell$ odd.**

**Lemma 17.** *Let $\ell$ be an odd prime number. Suppose that $K = K_\ell$. For every $G$ and for every $e \geqslant 1$ we have*

$$c(n, x, \ell^e, t) = c(n, x', \ell^e, t)$$

*as long as $x, x'$ are coprime to $\ell$.*

*Proof.* Let $d = \ell^e$. Let $a$ vary among the integers strictly between 0 and $d$ and coprime to $\ell$. Since $a$ is coprime to $\ell$ and $d = \ell^e$, the condition $(d, n) \mid a$ means $\ell \nmid n$ and it is independent of $a$. If $c(n, a, d, t)$ is non-zero, then the integer $t$ must be divisible by $\ell$ because $\zeta_\ell \in K$ and hence it must be fixed if raised to the power $1 + at$ (recall that $a$ is coprime to $\ell$). In particular, the condition $(1 + at, d) = 1$ holds independently of $a$.

We are left to check that Condition (iii) of Theorem 1 does not depend on $a$, provided that Conditions (i) and (ii) hold. Write $F := K_{nt,nt}$ and define $\tau := v_\ell(t)$. We thus have to show that the following is independent of $a$: the Galois group of $F_{\ell^{e+\tau}}/F$ contains the automorphism $\sigma_{1+ta}$ satisfying $\zeta_{\ell^{e+\tau}} \mapsto \zeta_{\ell^{e+\tau}}^{1+at}$. Since $K = K_\ell$, we have some largest integer $x \geqslant \tau \geqslant 1$ such that $F$ contains $\mathbb{Q}_{\ell^x}$, and this integer determines the Galois group of $F_{\ell^{e+\tau}}/F$, which is a finite cyclic $\ell$-group.

If $x \geqslant e + \tau$, then the field extension $F_{\ell^{e+\tau}}/F$ is trivial and the coefficient $c(n, a, \ell^e, t)$ is 0 independently of $a$. Now suppose that $\tau \leqslant x < e + \tau$. The exponents for the action on $\zeta_{\ell^{e+\tau}}$ are those corresponding to the automorphisms of order dividing $\ell^{e+\tau-x}$. Since $v_\ell(at)$ does not depend on $a$, we have that

$$v_\ell((1 + at)^{\ell^n} - 1) = \tau + n$$

independently of $a$ and we conclude. □

*Proof of Theorem 2 for $\ell$ odd.* Lemma 17 implies that the conditions of Theorem 12 are satisfied if $K = K_\ell$ (compare with formula (1)). Thus the density $\mathrm{dens}_K(G, a \bmod d)$ depends on $a$ only through its $\ell$-adic valuation, and it is a computable rational number. By Proposition 14 this rational number must be strictly positive. □

### 3.2. **Proof of Theorem 2 for $\ell = 2$.**

**Lemma 18.** *Suppose $K = K_4$. For every $G$ and for every $e \geqslant 1$ we have*

$$c(n, x, 2^e, t) = c(n, x', 2^e, t)$$

*as long as $x, x'$ are odd.*

*Proof.* Let $d = 2^e$. Notice that the claim is clear for $e = 1$, so suppose $e \geqslant 2$. Let $a$ vary in the odd integers strictly between 0 and $d$. Similarly to the proof of Lemma 17, the condition $(n, d) \mid a$ means that $2 \nmid n$ and is independent of $a$. Moreover, $t$ must be an even integer and hence the condition $(1+at, d) = 1$ is satisfied independently of $a$. Now suppose that the above conditions are satisfied, and let us focus on Condition (iii) of Theorem 1.

Set $\tau := v_2(t)$, and call $F$ the field $K_{nt,nt}$. Similarly to the proof of Lemma 17, we check that the following condition is independent of $a$: the Galois group of $F_{2^{e+\tau}}/F$ contains the automorphism $\sigma_{1+ta}$ satisfying $\zeta_{2^{e+\tau}} \mapsto \zeta_{2^{e+\tau}}^{1+at}$.

Recall that $K = K_4$, and call $x \geqslant 2$ the largest integer such that $F$ contains $\mathbb{Q}_{2^x}$ (we clearly have $x \geqslant \tau$). We then need to investigate the cyclic group $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_{2^x})$.

If $x \geqslant e+\tau$, then this field extension is trivial and we have $c(n, a, 2^e, t) = 0$ independently of $a$ (where $a$ is odd). If $x = \tau$ then $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_{2^x})$ contains $2^e$ automorphisms acting distinctly on $\zeta_{2^{e+\tau}}$ and fixing $\zeta_{2^\tau}$: we deduce that $c(n, a, 2^e, t) = 1$ independently of $a$ (where $a$ is odd).

From now on, suppose $\tau < x < e + \tau$. We see $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_{2^x})$ as a subgroup of the cyclic Galois group $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_4)$. That subgroup contains the elements of order dividing $2^{e+\tau-x}$. The Galois automorphisms are determined by the image of $\zeta_{2^{e+\tau}}$, and they are determined by the exponent to which they raise this element.

If $\tau = 1$, then we do not have the automorphism $\sigma_{1+ta}$ in $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_4)$ (independently of $a$) because $a$ is odd and hence $\zeta_4^{1+ta} \neq \zeta_4$. This means that in this case $c(n, a, 2^e, t) = 0$ independently of $a$ (for $a$ odd).

Finally suppose $1 < \tau < x < e + \tau$. Since $\tau > 1$, the automorphism $\sigma_{1+ta} \in \mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_4)$ is well-defined. We have to check whether $\sigma_{1+ta}$ also belongs to $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_{2^x})$ or not independently of $a$. It is then sufficient to show that the order of $\sigma_{1+ta}$ does not depend on $a$. This order is a power of 2, namely the smallest power $2^n$ such that $v((1 + at)^{2^n} - 1) \geqslant e + \tau$. Since $v_2(at) \geqslant 2$, then for every $n \geqslant 1$ we have $v_2((1 + at)^{2^n} - 1) = \tau + n$ independently of $a$ and hence the order of the automorphism $\sigma_{1+ta}$ does not depend on $a$. □

*Proof of Theorem 2 for $\ell = 2$.* Analogously to the proof for the odd case, it suffices to combine Lemma 18 with Theorem 12 and Proposition 14. □

### 3.3. **Proof of Corollary 3.**

*Proof of Corollary 3.* Let $m = \ell$ if $\ell$ is odd, and $m = 4$ if $\ell = 2$. Let $\mathfrak{p}$ be a prime of $K$ of degree 1, and which does not ramify in $K_m$. In view of our hypothesis on $a$, we have that if $\mathfrak{p}$ is such that $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod \ell^e$, then $\mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m$. We deduce from Lemma 15 that

$$\mathrm{dens}_K(G, a \bmod \ell^e) = \frac{1}{[K_m : K]} \cdot \mathrm{dens}_{K_m}(G, a \bmod \ell^e)\,.$$

By Theorem 2 we conclude that $\mathrm{dens}_K(G, a \bmod \ell^e)$ depends on $a$ only through its $\ell$-adic valuation and that it is a computable strictly positive rational number. □

### 3.4. **Proof of Theorem 4.**

**Lemma 19.** *Let $d \geqslant 2$ be an integer and write $d = \prod \ell^e$ for its prime decomposition. For the coefficients of Theorem 1, with respect to any fixed group $G$, we have*

$$c(n, a, d, t) = \prod_{\ell \mid d} c(n, a, \ell^e, t)\,.$$

*Proof.* We prove that $c(n, a, d, t) = 1$ if and only if $c(n, a, \ell^e, t) = 1$ for every prime divisor $\ell$ of $d$. It is clear that $(1 + at, d) = 1$ and $(d, n) \mid a$ if and only if $(1 + at, \ell^e) = 1$ and $(\ell^e, n) \mid a$ for every $\ell$. Now suppose that these conditions hold. Let $\sigma$ be the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_{dt})/\mathbb{Q})$ such that $\sigma(\zeta_{dt}) = \zeta_{dt}^{1+at}$, and let $\sigma_\ell$ be the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^e t})/\mathbb{Q})$ such

that $\sigma_\ell(\zeta_{\ell^e t}) = \zeta_{\ell^e t}^{1+at}$. We are left to show that $\sigma$ is the identity on $\mathbb{Q}(\zeta_{dt}) \cap K_{nt,nt}$ if and only if $\sigma_\ell$ is the identity on $\mathbb{Q}(\zeta_{\ell^e t}) \cap K_{nt,nt}$ for every $\ell$. This follows from the fact that $\mathbb{Q}(\zeta_{dt})$ is the compositum of the fields $\mathbb{Q}(\zeta_{\ell^e t})$, and $\sigma_\ell$ is the restriction of $\sigma$ to $\mathbb{Q}(\zeta_{\ell^e t})$ for each $\ell$. □

**Lemma 20.** *Let $d \geqslant 2$ be an integer and let $r := \prod_{\ell | d} \ell$ be its radical. Suppose that $K = K_r$ if $d$ is odd, or that $K = K_{2r}$ if $d$ is even. For the coefficients of Theorem 1, with respect to any fixed group $G$, we then have*

$$c(n, x, d, t) = c(n, x', d, t)$$

*as long as $x, x'$ are coprime to $d$.*

*Proof.* We have to show that, whenever $a$ is coprime to $d$, the coefficient $c(n, a, d, t)$ is independent of $a$. By Lemma 19 we may reduce to the case in which $d$ is a prime power, and then we may conclude by Lemma 17 if $d$ is odd, and Lemma 18 if $d$ is even. □

*Proof of Theorem 4.* By [7, Corollary 12] and [2, Theorem 3] the density $\mathrm{Dens}_K(G, d)$ of primes $\mathfrak{p}$ of $K$ such that $\mathrm{ord}_{\mathfrak{p}}(G)$ is coprime to $d$ is an explicitly computable rational number. This density can be decomposed as the sum over $a$, with $a$ coprime to $d$, of the densities $\mathrm{dens}_K(G, a \bmod d)$. Since $K_r = K$ if $d$ is odd, and $K_{2r} = K$ if $d$ is even, by Lemma 20 the above densities have equal value, so that for every $a$ coprime to $d$ we have

$$\mathrm{dens}_K(G, a \bmod d) = \frac{1}{\varphi(d)} \cdot \mathrm{Dens}_K(G, d)\,,$$

which is then a computable rational number. Moreover, this density is also strictly positive because by Theorem 6 the density $\mathrm{Dens}_K(G, d)$ is strictly positive. □

### 3.5. **Proof of Theorem 5.**

*Proof of Theorem 5.* Let $r$ be the radical of $d$, and let $m = r$ if $d$ is odd, and $m = 2r$ otherwise. Consider the following set of primes $\mathfrak{p}$ of $K$ of degree 1, and unramified in $K_m$:

$$\mathcal{S} := \{\mathfrak{p} : \mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d,\ \mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m\}\,.$$

By Lemma 15 the set $\mathcal{S}$ has density equal to

$$\frac{1}{[K_m : K]} \cdot \mathrm{dens}_{K_m}(G, a \bmod d)\,.$$

By Theorems 2 and 4, the density $\mathrm{dens}_{K_m}(G, a \bmod d)$ is strictly positive if $d$ is a prime power or if $a$ is coprime to $d$, so the same holds for the density of $\mathcal{S}$. Consequently, the density $\mathrm{dens}_K(G, a \bmod d)$ is also strictly positive. □

## 4. Multiplicative groups with torsion

Stating Theorem 1 for a finite group is trivial (the given density is either 0 or 1). However it is not trivial to remove the assumption that the multiplicative group is torsion-free: this is what we achieve in this section. As a side remark, notice that our strategy also applies to the density considered in [8, Theorem 1.4], i.e. if we introduce a condition on the Frobenius conjugacy class with respect to a fixed finite Galois extension of the base field.

Let $K$ be a number field, and let $G'$ be a finitely generated (and not necessarily torsion-free) multiplicative subgroup of $K^\times$ of positive rank. Then we can write $G'$ as $G' = \langle\zeta\rangle \times G$, where $\zeta$ is a root of unity of $K$ generating the torsion part of $G'$ and $G$ is torsion-free. Let us exclude finitely many primes $\mathfrak{p}$ of $K$ so that the reduction of $G'$ is well-defined and we have $\mathrm{ord}_\mathfrak{p}(\zeta) = \mathrm{ord}(\zeta)$. The order of $G'$ modulo $\mathfrak{p}$ is then the least common multiple between the order of $G$ modulo $\mathfrak{p}$ and a fixed integer:

$$\mathrm{ord}_\mathfrak{p}(G') = [\mathrm{ord}_\mathfrak{p}(G), \mathrm{ord}(\zeta)]\,.$$

We may then reformulate the given problem.

**Remark 21.** *Let $G$ be a finitely generated and torsion-free subgroup of $K^\times$, and fix some integer $n \geqslant 2$. Given two integers $a$ and $d \geqslant 2$, we investigate the density of primes $\mathfrak{p}$ of $K$ for which*

$$[\mathrm{ord}_\mathfrak{p}(G), n] \equiv a \bmod d\,. \tag{9}$$

*Assuming (GRH), the case $n = 1$ is known, and our aim is reducing to this case. Notice that our method also shows that the considered density exists. We denote this density by $\mathrm{dens}'_K(G, n; a \bmod d)$.*

Let $\ell$ be a prime divisor of $n$. The aim is finding a way to replace $n$ with $\frac{n}{\ell}$ (or to conclude directly). We distinguish various cases.

*Case (i):* If $\ell \mid d$ and $\ell \nmid a$, then we have $\mathrm{dens}'_K(G, n; a \bmod d) = 0$ because $\ell$ divides $[\mathrm{ord}_\mathfrak{p}(G), n]$ and (9) cannot hold.

*Case (ii):* If $\ell \mid d$ and $\ell \mid a$, then the congruence $[\mathrm{ord}_\mathfrak{p}(G), n] \equiv a \bmod d$ is equivalent to

$$\big[\mathrm{ord}_\mathfrak{p}(G^\ell), \frac{n}{\ell}\big] \equiv \frac{a}{\ell} \bmod \frac{d}{\ell}\,,$$

so we have

$$\mathrm{dens}'_K(G, n; a \bmod d) = \mathrm{dens}'_K\left(G^\ell, \frac{n}{\ell}; \frac{a}{\ell} \bmod \frac{d}{\ell}\right).$$

*Case (iii):* Suppose that $\ell \nmid d$. Let $\tilde{\ell}$ be a multiplicative inverse for $\ell$ modulo $d$, and set $v := v_\ell(n)$. If $\ell^v \mid \mathrm{ord}_\mathfrak{p}(G)$, then we have

$$[\mathrm{ord}_\mathfrak{p}(G), n] \equiv a \bmod d \quad\iff\quad \big[\mathrm{ord}_\mathfrak{p}(G), \frac{n}{\ell}\big] \equiv a \bmod d\,. \tag{10}$$

If $\ell^v \nmid \mathrm{ord}_\mathfrak{p}(G)$, then we have

$$[\mathrm{ord}_\mathfrak{p}(G), n] \equiv a \bmod d \quad\iff\quad \big[\mathrm{ord}_\mathfrak{p}(G), \frac{n}{\ell}\big] \equiv a\tilde{\ell} \bmod d\,.$$

The condition $\ell^v \mid \mathrm{ord}_\mathfrak{p}(G)$ amounts to

$$\big[\mathrm{ord}_\mathfrak{p}(G), \frac{n}{\ell}\big] \equiv 0 \bmod \ell^v$$

and hence (recalling that $\ell$ and $d$ are coprime) we can easily combine this congruence and the congruence in (10) with the Chinese Remainder Theorem. The first subcase thus amounts to

$$\big[\mathrm{ord}_\mathfrak{p}(G), \frac{n}{\ell}\big] \equiv a\tilde{\ell}^v\ell^v \bmod d\ell^v\,.$$

Similarly, the second subcase amounts to letting $\left[\operatorname{ord}_{\mathfrak{p}}(G), \frac{n}{\ell}\right]$ be in the difference of congruence classes

$$(a\tilde{\ell} \bmod d) \setminus (a\tilde{\ell}^{v+1}\ell^v \bmod d\ell^v)\,.$$

Notice that the congruence classes for the first and second subcase are distinct. Thus if $\ell \nmid d$ we can explicitly write

$$\begin{aligned}\operatorname{dens}'_K(G, n; a \bmod d) = &\operatorname{dens}'_K\left(G, \frac{n}{\ell}; a_0 \bmod d\ell^v\right) + \operatorname{dens}'_K\left(G, \frac{n}{\ell}; a\tilde{\ell} \bmod d\right)\\ &- \operatorname{dens}'_K\left(G, \frac{n}{\ell}; a_0\tilde{\ell} \bmod d\ell^v\right),\end{aligned}$$

where we have set $a_0 := a\tilde{\ell}^v\ell^v \bmod d\ell^v$.

We have thus proven the following result.

**Theorem 22.** *Assume (GRH). Let $K$ be a number field, and let $G'$ be a finitely generated subgroup of $K^\times$ of positive rank. Let $n \geqslant 1$ be the order of the torsion of $G'$, and let $G$ be a torsion-free subgroup of $G'$ such that $G' = G \times \langle\zeta_n\rangle$. Let $a$ and $d \geqslant 2$ be fixed integers. The density of the set of primes $\mathfrak{p}$ of $K$*

$$\{\mathfrak{p} : \operatorname{ord}_{\mathfrak{p}}(G') \equiv a \bmod d\}$$

*exists and can be expressed as a finite sum of terms of the type*

$$(-1)^k \cdot \operatorname{dens}_K(G^m, a' \bmod d')$$

*where $k$, $m$, $a'$, $d'$ are integers and $m \mid n$.*

## 5. Examples

In this last section we work out some examples and collect some numerical data to illustrate our results.

**Example 23.** Let $K = \mathbb{Q}(\zeta_3)$ and consider the group $G = \langle 5, 7\rangle \leqslant \mathbb{Q}(\zeta_3)^\times$. We compute the density $\operatorname{dens}_K(G, a \bmod 9)$ for $0 \leqslant a < 9$. Since $\zeta_3 \in K$, we can use [2, Theorem 2] to compute the density of primes $\mathfrak{p}$ of $K$ for which the order of $G \bmod \mathfrak{p}$ is coprime to 3, and we have

$$\operatorname{Dens}_K(G, 3) = \frac{1}{13}\,.$$

Then by Theorem 2 we have:

$$\operatorname{dens}_K(G, a \bmod 9) = \frac{1}{78} \qquad \text{for } a \in \{1, 2, 4, 5, 7, 8\}\,.$$

For $a = 3$ or $a = 6$, by [2, Theorem 3] we have

$$\operatorname{Dens}_K(G^3, 3) = \frac{9}{13}$$

and applying Lemma 9 we obtain by the equidistribution property

$$\begin{aligned}\operatorname{dens}_K(G, a \bmod 9) &= \operatorname{dens}_K(G^3, 1 \bmod 3) - 3\operatorname{dens}_K(G, 1 \bmod 9)\\ &= \frac{9}{2 \cdot 13} - 3 \cdot \frac{1}{78} = \frac{4}{13}\,.\end{aligned}$$

For $a = 0$ we get the complementary density of $\mathrm{Dens}_K(G^3, 3)$ and hence

$$\mathrm{dens}_K(G, 0 \bmod 9) = \frac{4}{13}\,.$$

**Example 24.** Let $K = \mathbb{Q}(\zeta_4)$ and consider the group $G = \langle 3, 5\rangle \leqslant \mathbb{Q}(\zeta_4)^\times$. We compute the density of primes $\mathrm{dens}_K(G, a \bmod 8)$ for $0 \leqslant a < 8$. Since $\zeta_4 \in K$, by [2, Theorem 2] the density of primes $\mathfrak{p}$ of $K$ for which the order of $G \bmod \mathfrak{p}$ is odd is given by

$$\mathrm{Dens}_K(G, 2) = \frac{1}{28}\,.$$

Then by Theorem 2 we have:

$$\mathrm{dens}_K(G, a \bmod 8) = \frac{1}{112} \qquad \text{for } a \in \{1, 3, 5, 7\}\,.$$

For $a = 2$ or $a = 6$, by [2, Theorem 3] we have

$$\mathrm{Dens}_K(G^2, 2) = \frac{1}{7}\,,$$

and applying Lemma 9 we obtain by the equidistribution property

$$\begin{aligned}\mathrm{dens}_K(G, a \bmod 8) &= \mathrm{dens}_K(G^2, 1 \bmod 4) - 2\,\mathrm{dens}_K(G, 1 \bmod 8)\\ &= \frac{1}{14} - 2 \cdot \frac{1}{112} = \frac{3}{56}\,.\end{aligned}$$

For $a = 4$ we proceed similarly. By [2, Theorem 3] we have

$$\mathrm{Dens}_K(G^4, 2) = \frac{4}{7}\,,$$

and then, by Lemma 9, we obtain by the equidistribution property

$$\begin{aligned}\mathrm{dens}_K(G, 4 \bmod 8) &= \mathrm{dens}_K(G^4, 1 \bmod 2) - 2\,\mathrm{dens}_K(G^2, 1 \bmod 4)\\ &= \frac{4}{7} - \frac{1}{7} = \frac{3}{7}\,.\end{aligned}$$

Finally for $a = 0$ we obtain the complementary density

$$\mathrm{dens}_K(G, 0 \bmod 8) = \frac{3}{7}\,.$$

**Example 25.** Let $K = \mathbb{Q}(\zeta_{12})$ and consider the group $G = \langle 7, 11\rangle \leqslant \mathbb{Q}(\zeta_{12})^\times$. We compute the density of primes $\mathrm{dens}_K(G, a \bmod 12)$ for $a \in \{1, 5, 7, 11\}$, which are all equal by Theorem 4 as $\zeta_{12} \in K$. By [7, Corollary 12] the density of primes $\mathfrak{p}$ of $K$ for which the order of $G \bmod \mathfrak{p}$ is coprime to 12 can be computed as in the previous examples:

$$\mathrm{Dens}_K(G, 12) = \mathrm{Dens}_K(G, 4) \cdot \mathrm{Dens}_K(G, 3) = \frac{1}{364}\,.$$

Hence we obtain by the equidistribution

$$\mathrm{dens}_K(G, a \bmod 12) = \frac{1}{1456}\,.$$

In the following two examples we also compute with SageMath [9] approximated densities to support the validity of the equidistribution property of Corollary 3.

**Example 26.** Consider the group $\langle 2\rangle \leqslant \mathbb{Q}^\times$. Focusing on the set of primes up to $10^6$, we find with SageMath the following approximated values for the density $\mathrm{dens}_{\mathbb{Q}}(2, a \bmod d)$:

| $a \bmod d$ | $\mathrm{dens}_{\mathbb{Q}}(2, a \bmod d)$ | primes up to $10^6$ |
|---|---|---|
| $4 \bmod 16$ | $1/6 \approx 0.1667$ | $0.1676$ |
| $12 \bmod 16$ | $1/6 \approx 0.1667$ | $0.1652$ |
| $3 \bmod 9$ | $1/8 = 0.125$ | $0.1236$ |
| $6 \bmod 9$ | $1/8 = 0.125$ | $0.1266$ |
| $9 \bmod 27$ | $1/24 \approx 0.0417$ | $0.0422$ |
| $18 \bmod 27$ | $1/24 \approx 0.0417$ | $0.0411$ |
| $3 \bmod 27$ | $1/24 \approx 0.0417$ | $0.0416$ |
| $6 \bmod 27$ | $1/24 \approx 0.0417$ | $0.0421$ |
| $15 \bmod 27$ | $1/24 \approx 0.0417$ | $0.0420$ |
| $21 \bmod 27$ | $1/24 \approx 0.0417$ | $0.0405$ |

For instance, by Corollary 3, for $3 \mid a$ and $d = 9$ or $d = 27$ we have

$$\mathrm{dens}_{\mathbb{Q}}(2, a \bmod d) = \frac{1}{[\mathbb{Q}(\zeta_3) : \mathbb{Q}]} \cdot \mathrm{dens}_{\mathbb{Q}(\zeta_3)}(2, a \bmod d)\,,$$

and similarly for $4 \mid a$ and $d = 16$. Thus we can compute these densities by following the same procedure as in the previous examples.

**Example 27.** We consider the group $G = \langle 2, 3\rangle \leqslant \mathbb{Q}^\times$ and we compute all the densities $\mathrm{dens}_{\mathbb{Q}}(G, a \bmod d)$ using the methods of the previous examples. Again we study the set of primes up to $10^6$ and find with SageMath the following approximated values for the considered densities:

| $a \bmod d$ | $\mathrm{dens}_{\mathbb{Q}}(G, a \bmod d)$ | primes up to $10^6$ |
|---|---|---|
| $4 \bmod 16$ | $17/112 \approx 0.1518$ | $0.1522$ |
| $12 \bmod 16$ | $17/112 \approx 0.1518$ | $0.1508$ |
| $3 \bmod 9$ | $2/13 \approx 0.1538$ | $0.1538$ |
| $6 \bmod 9$ | $2/13 \approx 0.1538$ | $0.1540$ |
| $9 \bmod 27$ | $2/39 \approx 0.0513$ | $0.0513$ |
| $18 \bmod 27$ | $2/39 \approx 0.0513$ | $0.0513$ |
| $3 \bmod 27$ | $2/39 \approx 0.0513$ | $0.0518$ |
| $6 \bmod 27$ | $2/39 \approx 0.0513$ | $0.0512$ |
| $15 \bmod 27$ | $2/39 \approx 0.0513$ | $0.0513$ |
| $21 \bmod 27$ | $2/39 \approx 0.0513$ | $0.0507$ |

**Example 28.** Let $K = \mathbb{Q}(\zeta_3)^\times$, and let $G$ be a finitely generated and torsion-free subgroup of $\mathbb{Q}(\zeta_3)^\times$. Consider the group $G' = G \times \langle \zeta_6\rangle$. We study the density of primes $\mathfrak{p}$ of $K$ such that $\mathrm{ord}_{\mathfrak{p}}(G') \equiv a \bmod 10$, as considered in Section 4. For $a = 1, 3, 5, 7, 9$, we have

$\mathrm{dens}'_K(G, 6; a \bmod 10) = 0$. For $a = 4$ we have

$$\begin{aligned}&\mathrm{dens}'_K(G, 6; 4 \bmod 10)\\ &= \mathrm{dens}'_K(G, 2; 24 \bmod 30) + \mathrm{dens}'_K(G, 2; 8 \bmod 10) - \mathrm{dens}'_K(G, 2; 18 \bmod 30)\\ &= \mathrm{dens}_K(G^2, 12 \bmod 15) + \mathrm{dens}_K(G^2, 4 \bmod 5) - \mathrm{dens}_K(G^2, 9 \bmod 15)\,,\end{aligned}$$

and also

$$\begin{aligned}&\mathrm{dens}'_K(G, 6; 4 \bmod 10) = \mathrm{dens}'_K(G^2, 3; 2 \bmod 5)\\ &= \mathrm{dens}_K(G^2, 12 \bmod 15) + \mathrm{dens}_K(G^2, 4 \bmod 5) - \mathrm{dens}_K(G^2, 9 \bmod 15)\,,\end{aligned}$$

where the difference in the two calculations consists only in whether we consider the prime 2 or the prime 3 first for the method described in Section 4. For $a = 2, 6, 8$ we can make a similar computation. Finally, for $a = 0$ we have

$$\mathrm{dens}'_K(G, 6; 0 \bmod 10) = \mathrm{dens}_K(G, 0 \bmod 5)\,,$$

as 2 always divides $\mathrm{ord}_{\mathfrak{p}}(G')$, and $\mathrm{ord}_{\mathfrak{p}}(G') \equiv 0 \bmod 5$ if and only if $\mathrm{ord}_{\mathfrak{p}}(G) \equiv 0 \bmod 5$.

## REFERENCES


[1] CHINEN, K. - MURATA, L., *On a distribution property of the residual order of $a \pmod p$ IV*. In: Papers from the 3rd China-Japan Seminar on Number Teory, Xi'an, China, February 12–16, 2004. (Zhang, Wenpeng, et al. eds), Number Theory. Tradition and Modernization. Developments in Math. Vol. 15, Springer, New York, 2006.

[2] DEBRY, C. - PERUCCA, A., *Reductions of algebraic integers*, J. Number Theory **167** (2016), 259–283.

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

[4] MOREE, P., *On the distribution of the order and index of $g \pmod p$ over residue classes III*. J. Number Theory **120** (2006), no. 1, 132–160.

[5] PERUCCA, A., *Multiplicative order and Frobenius symbol for the reductions of number fields*, J. S. Balakrishnan et al. (eds.), Research Directions in Number Theory, Association for Women in Mathematics, Series 19 (2019), 161–171.

[6] PERUCCA, A., *Prescribing valuations of the order of a point in the reductions of abelian varieties and tori*. J. Number Theory **129** (2009), no. 2, 469–476.

[7] PERUCCA, A., *Reductions of algebraic integers II*. I. I. Bouw et al. (eds.), Women in Numbers Europe II, Association for Women in Mathematics, Series 11 (2018), 10–33.

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

[9] SageMath, the Sage Mathematics Software System (Version 8.9), The Sage Developers, 2019, `https://www.sagemath.org`.

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



DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LUXEMBOURG, 6 AV. DE LA FONTE, 4364 ESCH-SUR-ALZETTE, LUXEMBOURG

*Email address*: `antonella.perucca@uni.lu; pietro.sgobba@uni.lu`