A RIGIDITY PHENOMENON FOR POWER MAPS

N. JONES

Abstract. Fix a number field K which is normal over $\mathbb{Q}$ and let $f : K \longrightarrow K$ be a function. We call f a global power map if there exists an integer exponent k so that $f(\alpha) = \alpha^k$ for every $\alpha \in K$. We call f a local power map at the prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ if f induces a well-defined group homomorphism on the multiplicative group $(\mathcal{O}_K/\mathfrak{p})^\times$. We conjecture that if f is a local power map at an infinite number of prime ideals $\mathfrak{p}$, then f must be a global power map. Our main theorem implies that if f is a local power map at every prime ideal $\mathfrak{p}$ in a set with positive upper density relative to the set of all prime ideals of K, then f must be a global power map. In particular, for $K = \mathbb{Q}$ this represents progress towards a conjecture of Fabrykowski and Subbarao.

1. Introduction

Broadly speaking, we refer to a collection of objects as *rigid* if every element in the collection is uniquely determined by less information than expected. In this paper, we consider the collection of power maps

$$\left\{ f : \mathbb{N} \longrightarrow \mathbb{N};\ f(n) = n^k,\ k \in \{0, 1, 2, \dots\} \right\},$$

which exhibits rigidity in various aspects. Indeed, a theorem of Erdős [2] implies that if $f : \mathbb{N} \longrightarrow \mathbb{N}$ is multiplicative and non-decreasing, then f is a power map. Fabrykowski and Subbarao [3, Theorem 2.1] proved that if $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is multiplicative and satisfies

$$\forall n \in \mathbb{N}, \quad f(n+p) \equiv f(n) \pmod{p} \tag{1}$$

for each prime number p, then either f is identically zero or f is a power map. They further conjectured the following stronger rigidity property for power maps.

Conjecture 1.1. *(Fabrykowski-Subbarao) Suppose $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is multiplicative and satisfies* (1) *for infinitely many primes p. Then either f is identically zero or there exists a non-negative integer k for which $f(n) = n^k$ for every $n \in \mathbb{N}$.*

This conjecture is open. The main result of the present paper represents progress towards its resolution. Our results are valid over more general number fields, and we formulate the problem in slightly different terms, as follows.

Let K be a number field which is Galois over $\mathbb{Q}$, let $\mathcal{O}_K$ denote its ring of integers, and let us set

$$\mathcal{P}_K := \{\text{prime ideals } \mathfrak{p} \subseteq \mathcal{O}_K\}.$$

For any $\mathfrak{p} \in \mathcal{P}_K$, let $\mathcal{O}_{K,(\mathfrak{p})} \subseteq K$ denote the localization of $\mathcal{O}_K$ at $\mathfrak{p}$ and $\mathcal{O}_{K,(\mathfrak{p})}^\times$ its unit group. Explicitly,

$$\mathcal{O}_{K,(\mathfrak{p})} := \{\alpha \in K :\ \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0\},$$
$$\mathcal{O}_{K,(\mathfrak{p})}^\times = \{\alpha \in K :\ \mathrm{ord}_{\mathfrak{p}}(\alpha) = 0\}.$$

As is well-known, $\mathcal{O}_{K,(\mathfrak{p})}$ is a local ring with maximal ideal $\mathfrak{p}\mathcal{O}_{K,(\mathfrak{p})}$, and one has an isomorphism

$$\frac{\mathcal{O}_{K,(\mathfrak{p})}}{\mathfrak{p}\mathcal{O}_{K,(\mathfrak{p})}} \simeq \frac{\mathcal{O}_K}{\mathfrak{p}} =: \mathbb{F}_{\mathfrak{p}}.$$

2010 *Mathematics Subject Classification.* 11N25, 11A07, 11R18.

Key words and phrases. Arithmetic functions, congruences, Chebotarev Density Theorem, Kummer theory.

This work was partially supported by a Ralphe E. Powe Junior Faculty Enhancement award and also by NSA grant H98230-12-1-0210. The author gratefully acknowledges Oak Ridge Associated Universities and the National Security Agency for this support.

For $\alpha, \beta \in K$, we write $\alpha \equiv \beta \pmod{\mathfrak{p}}$ exactly when $\alpha - \beta \in \mathfrak{p}\mathcal{O}_{K,(\mathfrak{p})}$. Here and throughout this paper, let A be a set satisfying

$$\mathbb{N} \subseteq A \subseteq K$$

and which is closed under multiplication, so that for any prime $\mathfrak{p}$, the subset

$$A_{(\mathfrak{p})}^{\times} := A \cap \mathcal{O}_{K,(\mathfrak{p})}^{\times}$$

is also closed under multiplication. Let us denote by $\mathcal{P}_{K,1} \subseteq \mathcal{P}_K$ the subset of prime ideals of inertial degree one:

$$\mathcal{P}_{K,1} := \{\mathfrak{p} \in \mathcal{P}_K : \ |\mathcal{O}_K/\mathfrak{p}| \text{ is prime}\}.$$

Given a function

$$f : A \longrightarrow K,$$

we consider the set $S_f \subseteq \mathcal{P}_{K,1}$ defined by

$$S_f := \{\mathfrak{p} \in \mathcal{P}_{K,1} : \ \exists k_{\mathfrak{p}} \in \mathbb{Z}/(N\mathfrak{p}-1)\mathbb{Z} \text{ such that } \forall \alpha \in A_{(\mathfrak{p})}^{\times}, \quad f(\alpha) \equiv \alpha^{k_{\mathfrak{p}}} \pmod{\mathfrak{p}}\}.$$

Equivalently, S_f is the set of prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ of inertial degree one for which

$$f(A_{(\mathfrak{p})}^{\times}) \subseteq \mathcal{O}_{K,(\mathfrak{p})}^{\times}$$

and for which there exists a multiplicative group homomorphism $f_{\mathfrak{p}} : \mathbb{F}_{\mathfrak{p}}^{\times} \longrightarrow \mathbb{F}_{\mathfrak{p}}^{\times}$ so that the diagram

$$\begin{array}{ccc} A_{(\mathfrak{p})}^{\times} & \xrightarrow{f} & \mathcal{O}_{K,(\mathfrak{p})}^{\times} \\ {\scriptstyle \mathrm{red}_p}\downarrow & & {\scriptstyle \mathrm{red}_p}\downarrow \\ \mathbb{F}_{\mathfrak{p}}^{\times} & \xrightarrow{f_p} & \mathbb{F}_{\mathfrak{p}}^{\times} \end{array} \tag{2}$$

commutes.

Definition 1.2. Let $\mathfrak{p} \in \mathcal{P}_{K,1}$. A function $f : A \longrightarrow K$ is a **local power map at** $\mathfrak{p}$ if $\mathfrak{p} \in S_f$.

Definition 1.3. A function $f : A \longrightarrow K$ is called a **global power map** if there is an exponent $k \in \mathbb{Z}$ such that, for each $\alpha \in A$ one has $f(\alpha) = \alpha^k$.

In these terms, we conjecture the following strong rigidity property for global power maps.

Conjecture 1.4. *Let A be a set which satisfies $\mathbb{N} \subseteq A \subseteq K$ and which is closed under multiplication. Suppose that $f : A \longrightarrow K$ is a local power map at an infinite set of primes (i.e. suppose that $|S_f| = \infty$). Then f must be a global power map.*

Remark 1.5. Conjecture 1.4 implies Conjecture 1.1. This connection will be discussed in more detail in Section 3.

Remark 1.6. It is essential that we consider primes of inertial degree one in the definition of S_f, for otherwise there are counterexamples to Conjecture 1.4. For instance, let $f : \mathbb{Q}(i) \longrightarrow \mathbb{Q}(i)$ be the restriction of complex conjugation. For each prime $p \equiv 3 \pmod 4$, the ideal $p\mathbb{Z}[i]$ is prime in $\mathbb{Q}(i)$, and f induces the Frobenius automorphism $x \mapsto x^p$ on $(\mathbb{Z}[i]/p\mathbb{Z}[i])^{\times}$. Thus, f is a local power map at an infinite set of primes (each of inertial degree two), but is not a global power map.

In the present paper, we will prove the following weakened version of Conjecture 1.4, in which "S_f is infinite" is replaced by "S_f has positive upper density in the primes." For any set S of prime ideals of K, define

$$S(x) := \{\mathfrak{p} \in S : \ N\mathfrak{p} \leq x\}$$

and the upper density

$$\overline{\delta}(S) := \limsup_{x \to \infty} \frac{|S(x)|}{\pi_K(x)}.$$

We will prove the following theorem.

Theorem 1.7. *Suppose K is a number field which is Galois over $\mathbb{Q}$ and A is a set which satisfies $\mathbb{N} \subseteq A \subseteq K$ and which is closed under multiplication. Let $f : A \longrightarrow K$ be any function which is not a global power map. Then there exist real constants $b_f, c_f > 0$ so that for $x \geq c_f$, the bound*

$$|S_f(x)| \ll \frac{\log\log\log x}{\log\log x} \cdot \mathrm{Li}(x) + b_f$$

holds, with an absolute implied constant. In particular, if $f : A \longrightarrow K$ is a function for which $\overline{\delta}(S_f) > 0$, then f is a global power map.

Our proof of this theorem applies an effective version of the Chebotarev density theorem of Lagarias and Odlyzko to certain Kummer extensions attached to the function f. In Section 3, we deduce the following corollary, which details our progress towards Conjecture 1.1. For any function $f : \mathbb{N} \longrightarrow \mathbb{Z}$, we define

$$T_f := \{p \text{ prime} : \ \forall n \in \mathbb{N}, \quad f(n+p) \equiv f(n) \pmod{p}\}. \tag{3}$$

Thus, Conjecture 1.1 states that if $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is not identically zero or a global power map, then T_f is finite.

Corollary 1.8. *Let $f : \mathbb{N} \longrightarrow \mathbb{Z}$ be a multiplicative function and let T_f be defined by (3). Then either f is identically zero, or f is a global power map, or there exist real constants $b_f, c_f > 0$ so that, for $x \geq c_f$, the bound*

$$|T_f(x)| \ll \frac{\log\log\log x}{\log\log x} \cdot \pi(x) + b_f$$

holds, with an absolute implied constant. In particular, if $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is a multiplicative function for which $\overline{\delta}(T_f) > 0$, then either f is identically zero or f is a global power map.

Remark 1.9. In fact, Fabrykowski and Subbarao work with more general *quasi-multiplicative* functions (see Definition 3.1 below), but as we shall see, if f is quasi-multiplicative and $|T_f| = \infty$, then f is completely multiplicative. Thus, [3, Conjecture 3.1] is equivalent to Conjecture 1.1 and [3, Theorem 2.1] is equivalent to our formulation in the first paragraph of the present paper.

2. Notation

Throughout the paper, in addition to that already introduced, we will use the following notation. For a number field K, if $\gamma \in K^\times$ and $\mathfrak{p}$ is prime ideal of K, then there is a unique integer n for which $\gamma\mathcal{O}_K = \mathfrak{p}^n\mathfrak{a}$, where $\mathfrak{a}$ is a fractional ideal of K and $\mathfrak{p} \nmid \mathfrak{a}$. We then define $\mathrm{ord}_{\mathfrak{p}}(\gamma) := n$. Also, we define the ideal numerator $\mathfrak{num}(\gamma) \subseteq \mathcal{O}_K$ and denominator of $\mathfrak{den}(\gamma) \subseteq \mathcal{O}_K$ by

$$\mathfrak{num}(\gamma) := \prod_{\substack{\mathfrak{p} \in P_K \\ \mathrm{ord}_{\mathfrak{p}}(\gamma) > 0}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\gamma)}, \qquad \mathfrak{den}(\gamma) := \prod_{\substack{\mathfrak{p} \in P_K \\ \mathrm{ord}_{\mathfrak{p}}(\gamma) < 0}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\gamma)}.$$

Thus one has

$$\gamma\mathcal{O}_K = \mathfrak{num}(\gamma)\mathfrak{den}(\gamma)^{-1}.$$

We use the symbols $O(\cdot)$ and $\ll$ in the usual ways, namely if $f, g \colon [\gamma, \infty) \to \mathbb{C}$ are complex functions then we write

$$f = O(g), \quad \text{or equivalently} \quad f \ll g$$

if there is a positive constant C for which $|f(x)| \leq C|g(x)|$ for all $x \in [\gamma, \infty)$. In case there is an auxiliary parameter y upon which the implied constant C depends, we will indicate this with a subscript, so that

$$f = O_y(g) \quad \text{or equivalently} \quad f \ll_y g$$

is used to indicate that $|f(x)| \leq C(y)|g(x)|$, where the $C(y)$ may depend on y but not on x. We write $f(x) \sim g(x)$ as $x \to \infty$ to mean that $f(x)$ is asymptotic to $g(x)$ as $x \to \infty$, i.e. to mean that $\lim_{x\to\infty} f(x)/g(x) = 1$. When used as variables, the letters p and ℓ will denote prime numbers unless otherwise indicated, and

$$\pi(x) := \#\{p \leq x : \ p \text{ is prime}\}$$
$$\pi(x; a, q) := \#\{p \leq x : \ p \text{ is prime and } p \equiv a \mod q\},$$

for any $q \in \mathbb{N}$ and $a \in \mathbb{Z}$. We will often denote the reduction modulo $\mathfrak{p}$ map by

$$\begin{aligned} \mathcal{O}_{K,(\mathfrak{p})} &\to \mathbb{F}_{\mathfrak{p}} \\ n &\mapsto \overline{n}. \end{aligned}$$

3. Previous related results

In this section, we survey previous results in the literature towards Conjecture 1.1. We also clarify the connection between Conjectures 1.4 and 1.1. The following definition of quasi-multiplicative is used in [3]; we recall here two more common definitions for comparison.

Definition 3.1. A function $f : \mathbb{N} \longrightarrow \mathbb{C}$ is called **completely multiplicative** if for each $\alpha, \beta \in \mathbb{N}$,

$$f(\alpha\beta) = f(\alpha)f(\beta). \tag{4}$$

If (4) is satisfied whenever $\gcd(\alpha, \beta) = 1$ then f is called **multiplicative**. We call f **quasi-multiplicative** if, for any $n \in \mathbb{N}$ and any prime p not dividing n, one has

$$f(pn) = f(p)f(n).$$

Lemma 3.2. *Suppose that $f : A \longrightarrow K$ is a function for which S_f is infinite. Then*

$$f(A \cap K^\times) \subseteq K^\times, \tag{5}$$

and f is completely multiplicative, i.e. (4) holds for any $\alpha, \beta \in A$.

Proof. To prove (5), fix $\alpha \in A \cap K^\times$. If $f(\alpha) = 0$ then for each prime ideal $\mathfrak{p}$,

$$\mathrm{ord}_{\mathfrak{p}}(\alpha) = 0 \implies \mathfrak{p} \notin S_f, \tag{6}$$

implying that S_f is finite, a contradiction. Thus, (5) holds. To prove (4), fix $\alpha, \beta \in K^\times$ and note that

$$\forall \mathfrak{p} \in S_f,\ \mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta) = 0 \implies \mathfrak{p} \mid f(\alpha\beta) - f(\alpha)f(\beta).$$

Since S_f is infinite, there are infinitely many such primes $\mathfrak{p}$, and so $f(\alpha\beta) = f(\alpha)f(\beta)$. □

By the Lemma 3.2, one may as well add "f is completely multiplicative" to the hypothesis of Conjecture 1.4. The next lemma shows that Conjecture 1.1 is implied by Conjecture 1.4. Note that, for any $p \in T_f$, there is a well-defined function

$$f_p : \mathbb{F}_p \longrightarrow \mathbb{F}_p, \qquad f_p(\overline{n}) := f(n).$$

Lemma 3.3. *Suppose that $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is quasi-multiplicative and that T_f is infinite. Then either f is identically zero or S_f is infinite. (In either case, f is completely multiplicative.)*

Proof. Fix any prime $p \in T_f$ and note that $p \in S_f \cap T_f$ if and only if

$$f_p(\mathbb{F}_p^\times) \subseteq \mathbb{F}_p^\times \tag{7}$$

holds and f_p is a multiplicative homomorphism. Choose $g \in \mathbb{N}$ so that $\langle \overline{g} \rangle = \mathbb{F}_p^\times$. Suppose that (7) does not hold, i.e. that $f_p(\overline{g}^n) = \overline{0}$ for some positive integer n. By Dirichlet's theorem on primes in arithmetic progressions, one may find n prime numbers $q_1, q_2, \ldots, q_n$ for which

$$\forall i \in \{1, 2, \ldots, n\}, \quad q_i \equiv g \pmod{p}.$$

It follows from Definition 3.1 that

$$\overline{0} = f_p\left(\overline{g}^n\right) = f_p\left(\prod_{i=1}^{n} \overline{q}_i\right) = \prod_{i=1}^{n} f_p(\overline{q}_i) = \left(f_p(\overline{g})\right)^n, \tag{8}$$

and so we conclude that, for any prime $p \in T_f$,

$$\text{condition (7) fails} \implies f_p(\mathbb{F}_p) = \{\overline{0}\}.$$

Furthermore, if we set

$$T_0 := \{p \in T_f :\ f_p(\mathbb{F}_p) = \{\overline{0}\}\},$$

then for each $n \in \mathbb{N}$, $f(n)$ is divisible by every prime $p \in T_0$. Thus,

$$|T_0| = \infty \implies \forall n \in \mathbb{N},\ f(n) = 0.$$

Assuming f is not identically zero, we have that T_0 is finite, and putting $S := T_f - T_0$, we see that (7) holds for each $p \in S$. Furthermore, using Dirichlet's theorem on primes in arithmetic progressions and reasoning as in (8), one sees that the restriction of f_p to $\mathbb{F}_p^\times$ is a multiplicative homomorphism for each $p \in S$. In particular, $S = T_f \cap S_f$, which concludes the proof. □

The main result of [4] implies that, if the set $\{\text{all primes}\} - T_f$ is finite, then either f is identically zero or f is a global power map. A somewhat stronger result may be found in [8, Proposition 1, p. 329] (whose proof appeals to [1, Theorem 1]), which implies that if T_f has density one in the set of primes, then either f is identically zero or f is a global power map.

We end by mentioning two other related rigidity results, each of which may be seen as generalizing our present context. I. Ruzsa [11] proved that, if $f : \mathbb{N} \longrightarrow \mathbb{Z}$ satisfies (1) for each $p \in \mathbb{N}$ together with an upper bound

$$|f(n)| \ll (e-1)^{\alpha n}$$

for some $\alpha < 1$, then f is a polynomial map. Ruzsa also conjectured that the same result should hold with $e-1$ replaced by e, and some progress on this conjecture has been made by Zannier [17]. On the other hand, for a higher-dimensional analogue, the main theorems in [8] articulate rigidity results for maps of abelian varieties.

4. Outline of the proof of Theorem 1.7

The rest of the paper is devoted to a proof of Theorem 1.7. We begin by reducing to the case $A = \mathbb{N}$.

Lemma 4.1. *Let $f : A \longrightarrow K$ and suppose that $|S_f| = \infty$. Then the following implication holds.*

$$f|_{\mathbb{N}} \text{ is a global power map} \implies f \text{ is a global power map.}$$

Proof. If $f(n) = n^k$ for all $n \in \mathbb{N}$, then $k_{\mathfrak{p}} = k$ for each $\mathfrak{p} \in S_f$ (this uses that $S_f \subseteq \mathcal{P}_{K,1}$). Thus, for each $\alpha \in A$, $\mathfrak{p} \mid f(\alpha) - \alpha^k$ for infinitely many prime ideals $\mathfrak{p}$, so f is a global power map. □

Since clearly $S_f \subseteq S_{f|_{\mathbb{N}}}$, we obtain the following corollary.

Corollary 4.2. *If Theorem 1.7 (resp. Conjecture 1.4) holds for $A = \mathbb{N}$, then it holds in general.*

We will now prove Theorem 1.7 for the case $A = \mathbb{N}$. First observe that, for any parameters $0 \leq Y < Z$, one may bound the quantity $|S_f(x)|$ by two sums:

$$|S_f(x)| \leq \sum_{\substack{\mathfrak{p} \in \mathcal{P}_{K,1}(x) \\ \forall \ell \in [Y,Z), \\ N\mathfrak{p} \not\equiv 1 \pmod{\ell}}} 1 \; + \sum_{Y \leq \ell < Z} \sum_{\substack{\mathfrak{p} \in S_f(x) \\ N\mathfrak{p} \equiv 1 \pmod{\ell}}} 1. \tag{9}$$

We will eventually choose $Y = Y(x)$ and $Z = Z(x)$ appropriately so as to optimally bound each of these quantities.

The first sum is dealt with quickly as an application of the Brun-Titchmarsh Theorem and Merten's Theorem. The former states that, for $q < x$, one has

$$\pi(x; a, q) \leq \frac{2x}{\varphi(q) \log(x/q)}, \tag{10}$$

while the latter states that

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \sim e^{-\gamma} \frac{1}{\log x} \tag{11}$$

as $x \longrightarrow \infty$.

Proposition 4.3. *Assume that*

$$2 \leq Y \leq Z \leq \frac{1}{3} \cdot \log x.$$

Then for Z sufficiently large, one has

$$\sum_{\substack{\mathfrak{p} \in \mathcal{P}_{K,1}(x) \\ \forall \ell \in [Y,Z), \\ N\mathfrak{p} \not\equiv 1 \pmod{\ell}}} 1 \; \ll \; \frac{\log Y}{\log Z} \cdot \frac{x}{\log x},$$

with an absolute implied constant.

Proof. We will apply (10) with

$$q := \prod_{Y \le \ell < Z} \ell,$$

which, by the prime number theorem, satisfies $q \le e^{(1+o(1))Z}$ as $Z \longrightarrow \infty$. In particular, since $Z \le \frac{1}{3}\log x$ we have

$$Z \gg 1 \Longrightarrow q \le x^{1/2}. \tag{12}$$

Consider the set $\mathcal{C} \subseteq \mathbb{Z}/q\mathbb{Z}$, defined by

$$\mathcal{C} := \{a \in \mathbb{Z}/q\mathbb{Z} : \gcd(a(a-1), q) = 1\}.$$

For $Z \le \frac{1}{3}\log x$, we have

$$\begin{aligned}
\sum_{\substack{\mathfrak{p} \in \mathcal{P}_{K,1}(x) \\ \forall \ell \in [Y,Z), \\ N\mathfrak{p} \not\equiv 1 \pmod{\ell}}} 1 \le \sum_{\substack{p \le x \\ \forall \ell \in [Y,Z), \\ p \not\equiv 1 \pmod{\ell}}} 1 &\le \sum_{a \in \mathcal{C}} \pi(x; a, q) + \pi(Z) \\
&\ll \frac{|\mathcal{C}|}{\varphi(q)} \cdot \frac{x}{\log x} + \frac{Z}{\log Z} \\
&= \prod_{Y \le \ell < Z} \left(1 - \frac{1}{\ell - 1}\right) \cdot \frac{x}{\log x} + \frac{Z}{\log Z} \\
&\ll \frac{\log Y}{\log Z} \cdot \frac{x}{\log x},
\end{aligned}$$

by (10), (11) and (12). This proves Proposition 4.3. □

It remains to bound the second sum in (9). Our key tool for doing so is an effective version of the Chebotarev density theorem, which was first proved by Lagarias and Odlyzko [9] and further refined by Serre [12]. We will now describe the theorem precisely in the form we will use it.

The Chebotarev density theorem gives an asymptotic formula for the number of prime ideals $\mathfrak{p}$ with $N\mathfrak{p} \le x$ for which the associated Frobenius automorphism has a prescribed action on a given fixed number field. More precisely, let L/K be a Galois extension of number fields and let us denote by $G := \mathrm{Gal}(L/K)$ the relative Galois group, $n_L := [L : \mathbb{Q}]$ the degree of L over $\mathbb{Q}$, and d_L the absolute discriminant of L. Furthermore, fix any subset $\mathcal{C} \subseteq G$ satisfying

$$\forall \sigma \in G, \quad \sigma \mathcal{C} \sigma^{-1} = \mathcal{C}. \tag{13}$$

For any prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ which doesn't ramify in L, let $\mathrm{Frob}_{\mathfrak{p}} \subseteq G$ denote the conjugacy class in G of the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{P}}$ attached to any prime ideal $\mathfrak{P} \subseteq \mathcal{O}_L$ lying over $\mathfrak{p} \subseteq \mathcal{O}_K$. By (13), either $\mathrm{Frob}_{\mathfrak{p}} \subseteq \mathcal{C}$ or $\mathrm{Frob}_{\mathfrak{p}} \cap \mathcal{C} = \emptyset$, and we consider the counting function

$$\pi(x; L/K, \mathcal{C}) := |\{\mathfrak{p} \in \mathcal{P}_K(x);\ \mathfrak{p} \text{ is unramified in } L \text{ and } \mathrm{Frob}_{\mathfrak{p}} \subseteq \mathcal{C}\}|.$$

The Chebotarev density theorem asserts that, as $x \longrightarrow \infty$, one has

$$\pi(x; L/K, \mathcal{C}) \sim \frac{|\mathcal{C}|}{|G|} \mathrm{Li}(x).$$

We will require the following effective version, which bounds the error term in this asymptotic in terms of data attached to the extension L/K. We will assume that

$$\begin{aligned}
&\exists \text{ a sequence of fields } \mathbb{Q} = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L \\
&\text{so that } \ \forall i \in \{1, 2, \ldots, m\}, \quad L_i \text{ is Galois over } L_{i-1}.
\end{aligned} \tag{14}$$

Theorem 4.4. *(Effective Chebotarev Theorem) Assume that* (14) *holds. Then there exist absolute, effectively computable positive constants c_1, c_2 and c_3 such that, if $x \ge 2$ and*

$$\sqrt{\frac{\log x}{n_L}} \ge c_3 \max\left\{\log |d_L|, |d_L|^{1/n_L}\right\}, \tag{15}$$

then

$$\left|\pi(x; L/K, \mathcal{C}) - \frac{|\mathcal{C}|}{|G|}\operatorname{Li}(x)\right| \leq c_1|\mathcal{C}| \cdot x \cdot \exp\left(-c_2\sqrt{\frac{\log x}{n_L}}\right).$$

Proof. The zeta function $\zeta_L(s)$ is known to have at most one real zero β satisfying

$$1 - \frac{1}{4\log|d_L|} \leq \beta;$$

such a zero β is called *exceptional*. Theorem 1.3 of [9] (see also Théorème 2 of [12]) it is proved that there exist absolute, effectively computable positive constants a_1, a_2 and a_3 such that, for each $x \geq 2$ satisfying $\log x \geq a_3 n_L(\log|d_L|)^2$, one has

$$\left|\pi(x; L/K, \mathcal{C}) - \frac{|\mathcal{C}|}{|G|}\operatorname{Li}(x)\right| \leq \frac{|\mathcal{C}|}{|G|}\operatorname{Li}(x^\beta) + a_1|\mathcal{C}| \cdot x \cdot \exp\left(-a_2\sqrt{\frac{\log x}{n_L}}\right),$$

where the term $\frac{|\mathcal{C}|}{|G|}\operatorname{Li}(x^\beta)$ may be suppressed if an exceptional zero β does not exist. In [13, p. 148], it is shown that, under the hypothesis (14), one has

$$1 - \frac{1}{4\log|d_L|} \leq \beta < \max\left\{1 - \frac{1}{16\log|d_L|}, 1 - \frac{a_4}{|d_L|^{1/n_L}}\right\},$$

for an appropriately chosen effectively computable positive constant a_4. Using this upper bound on β, one finds that, provided (15) holds, the term $\operatorname{Li}(x^\beta)$ is bounded above by a constant times $x\exp\left(-a_2\sqrt{\frac{\log x}{n_L}}\right)$, which gives Theorem 4.4. □

We will apply Theorem 4.4 in the context of certain Kummer extensions attached to f to deduce the following proposition.

Proposition 4.5. *Suppose that $f : \mathbb{N} \longrightarrow K^\times$ is not a global power map. There exists constants $a_f, b_f > 0$ so that, provided*

$$a_f \leq Y \leq Z \leq \left(\frac{\log x}{(6c_3\log\log x)^2}\right)^{1/15},$$

(where c_3 is the constant appearing in (15)) then one has

$$\sum_{Y \leq \ell < Z} \sum_{\substack{\mathfrak{p} \in S_f(x) \\ N\mathfrak{p} \equiv 1 \pmod{\ell}}} 1 \ll \frac{1}{Y\log Y} \cdot \operatorname{Li}(x) + b_f,$$

with an absolute implied constant.

Inserting the results of Propositions 4.3 and 4.5 into (9) and putting

$$Y = \frac{\log\log x}{(\log\log\log x)^2}, \qquad Z = \left(\frac{\log x}{(6c_2\log\log x)^2}\right)^{1/15},$$

we see that Theorem 1.7 follows.

5. Preliminaries on Kummer extensions

The rest of the paper is devoted to proving Proposition 4.5. Our proof uses Theorem 4.4 with L equal to a field extension of the form

$$L = K\left(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell}\right),$$

for appropriately chosen $n_1, n_2 \in \mathbb{N}$. If f is a global power map, then $L = K(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell})$, and one cannot deduce the result of Proposition 4.5. In case f is not a global power map but nevertheless $|S_f| = \infty$, then it is still not immediately clear that one may find $n_1, n_2 \in \mathbb{N}$ for which $[L : K(\zeta_\ell)] = \ell^4$ for all primes ℓ which are large enough, but we show that one may achieve $[L : K(\zeta_\ell)] \geq \ell^3$ for $\ell \gg_f 1$, which suffices for our purposes (see Corollary 5.5 below).

We begin by reviewing some fundamental facts about Kummer extensions in general. For any integers $m \geq 0$ and $n \geq 1$ and vector $\mathbf{c} = (c_1, c_2, \ldots, c_m) \in (K^\times)^m$, we will call a number field of the form

$$L = K(\zeta_n, \mathbf{c}^{1/n}) := K(\zeta_n, c_1^{1/n}, c_2^{1/n}, \ldots, c_m^{1/n})$$

a *Kummer extension* (in case $m = 0$, we interpret this as $K(\zeta_n, \mathbf{c}^{1/n}) := K(\zeta_n)$). In our application, we will deal exclusively with the case where $n = \ell$ is an odd prime number.

5.1. **The discriminant of a Kummer extension.** Because of (15), in order to apply Theorem 4.4 with L of the form $K(\zeta_\ell, \mathbf{c}^{1/\ell})$, we will need a bound on the absolute discriminant of L. Such a bound may be obtained from the following classical formula for relative discriminants.

Lemma 5.1. *Let $K \subseteq F \subseteq L$ be a tower of number fields, let $\Delta_{L/F} \subseteq \mathcal{O}_F$, $\Delta_{L/K} \subseteq \mathcal{O}_K$, and $\Delta_{F/K} \subseteq \mathcal{O}_K$ be the relative discriminants and let $N_{F/K} : F^\times \longrightarrow K^\times$ the usual norm map. Then one has*

$$\Delta_{L/K} = N_{F/K}(\Delta_{L/F})\Delta_{F/K}^{[L:F]}. \tag{16}$$

Proof. See for instance [5, p. 126]. □

The next lemma follows from the previous one by induction on m.

Lemma 5.2. *Let $L = K(\zeta_\ell, c_1^{1/\ell}, \ldots, c_m^{1/\ell})$, and let $\Delta_{L/K} \subseteq \mathcal{O}_K$ denote the relative discriminant and $d_L \in \mathbb{Z}$ the absolute discriminant. Then*

$$\Delta_{L/K} \;\; \textit{divides} \;\; \left(\prod_{i=1}^{m} \mathfrak{num}(c_i)\mathfrak{den}(c_i)\right)^{n_L/n_K} \ell^{(m+1)n_L/n_K}\mathcal{O}_K,$$

$$d_L \;\; \textit{divides} \;\; \left(d_K \cdot N_{K/\mathbb{Q}}\left(\prod_{i=1}^{m} \mathfrak{num}(c_i)\mathfrak{den}(c_i)\right)\right)^{n_L/n_K} \ell^{(m+1)n_L}.$$

In particular, we obtain the following corollary. Note that, for some bound a_K, one has that

$$\ell \geq a_K \implies [K(\mu_\ell) : K] = \ell - 1.$$

Let us put

$$b_{K,f,\mathbf{n}} := \max\left\{a_K, \left|d_K \cdot N_{K/\mathbb{Q}}\left(\prod_{i=1}^{2} n_i \mathfrak{num}(f(n_i))\mathfrak{den}(f(n_i))\right)\right|\right\}. \tag{17}$$

Corollary 5.3. *Suppose $f : K^\times \longrightarrow K^\times$ is any function and let $L = K\left(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell}\right)$. Then for any prime ℓ satisfying $\log \ell \geq b_{K,f,\mathbf{n}}$, one has*

$$\max\left\{\log|d_L|, |d_L|^{1/n_L}\right\} \;\leq\; (6n_K + 1)\ell^5 \log \ell.$$

5.2. **The Galois group of a Kummer extension.** We now describe the structure of $\mathrm{Gal}(K(\zeta_\ell, \mathbf{c}^{1/\ell})/K)$. Consider the group

$$(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m,$$

where the semi-direct product is defined via the multiplicative action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ on $(\mathbb{Z}/\ell\mathbb{Z})^m$, or explicitly

$$(a_1, \mathbf{b}_1) \cdot (a_2, \mathbf{b}_2) = (a_1 a_2, \mathbf{b}_2 + a_2\mathbf{b}_1),$$

where $\mathbf{b}_i \in (\mathbb{Z}/\ell\mathbb{Z})^m$. (Equivalently, the embedding

$$(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m \hookrightarrow GL_{m+1}(\mathbb{Z}/\ell\mathbb{Z})$$

$$(a, \mathbf{b}) \mapsto \begin{pmatrix} a & 0 \\ \mathbf{b} & I \end{pmatrix},$$

where I denotes the $m \times m$ identity matrix, allows one to regard $(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m$ as a subgroup of $GL_{m+1}(\mathbb{Z}/\ell\mathbb{Z})$.) There is an embedding of groups[1]

$$\begin{aligned} \mathrm{Gal}(K(\zeta_\ell, \mathbf{c}^{1/\ell})/K) &\hookrightarrow (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m \\ \begin{pmatrix} \zeta_\ell & \mapsto & \zeta_\ell^a \\ c_i^{1/\ell} & \mapsto & c_i^{1/\ell} \cdot \zeta_\ell^{b_i} \end{pmatrix} &\mapsto (a, \mathbf{b}), \end{aligned} \tag{18}$$

where $\mathbf{b} = (b_1, b_2, \ldots b_m)$. What is the image of this embedding? In general, the image depends on whether (and to what extent) there exist multiplicative relations

$$\mathbf{c}^{\mathbf{e}/\ell} := \prod_{i=1}^m (c_i^{1/\ell})^{e_i} \in K(\zeta_\ell)^\times, \tag{19}$$

where in the above, $\mathbf{e} = (e_1, e_2, \ldots, e_m) \in (\mathbb{Z}/\ell\mathbb{Z})^m$. In our application, we will need to understand the image of this embedding, even in the case where nontrivial relations such as (19) exist. Let $V_{\mathbf{c}}(\ell)$, respectively $V_{\mathbf{c}}^\perp(\ell)$ denote the $\mathbb{Z}/\ell\mathbb{Z}$-vector subspaces

$$\begin{aligned} V_{\mathbf{c}}(\ell) &:= \{\mathbf{e} \in (\mathbb{Z}/\ell\mathbb{Z})^m : \text{ the relation (19) holds}\} \\ V_{\mathbf{c}}^\perp(\ell) &:= \{\mathbf{b} \in (\mathbb{Z}/\ell\mathbb{Z})^m : \forall \mathbf{e} \in V_{\mathbf{c}}(\ell), \sum_{i=1}^m b_i e_i \equiv 0 \pmod{\ell}\}. \end{aligned} \tag{20}$$

Note that

$$\forall \sigma \in \mathrm{Gal}(\overline{K}/K), \quad \sigma(\mathbf{c}^{\mathbf{e}/\ell}) = \zeta_\ell^x \mathbf{c}^{\mathbf{e}/\ell}$$

for some $x \in \mathbb{Z}/\ell\mathbb{Z}$. Together with (19), this implies that, for each $\mathbf{e} \in V_{\mathbf{c}}(\ell)$, one has $\mathbf{c}^{\mathbf{e}/\ell} \in K^\times \cdot \mu_\ell$. It follows that, multiplying each $c_i^{1/\ell}$ by an appropriate ℓ-th root of unity, one may arrange that

$$\forall \mathbf{e} \in V_{\mathbf{c}}(\ell), \quad \mathbf{c}^{\mathbf{e}/\ell} \in K^\times. \tag{21}$$

It follows from (21) and (20) that the image of the embedding (18) is contained in the subgroup

$$(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes V_{\mathbf{c}}^\perp(\ell) \subseteq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^m.$$

In fact, the image of the embedding (18) is *equal* to $(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes V_{\mathbf{c}}^\perp(\ell)$, as stated in the following lemma.

Lemma 5.4. *Suppose that the roots $c_1^{1/\ell}, \ldots, c_m^{1/\ell}$ have been chosen so that* (21) *holds. Then the function* (18) *gives an isomorphism of groups*

$$\mathrm{Gal}(K(\zeta_\ell, \mathbf{c}^{1/\ell})/K) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes V_{\mathbf{c}}^\perp(\ell).$$

Proof. Let $B \subseteq K^\times$ be the multiplicative subgroup generated by $(K^\times)^\ell$ and $\{c_i : 1 \le i \le m\}$. In [10, Theorem 8.1, p. 294–295] it is shown that

$$\mathrm{Gal}(K(\zeta_\ell, \mathbf{c}^{1/\ell})/K(\zeta_\ell)) \simeq \frac{B}{(K^\times)^\ell}.$$

Noting that, under $\mathbf{c}^{\mathbf{n}} \overset{(\mathrm{mod}\ \ell)}{\mapsto} \mathbf{n} \pmod{\ell}$, one has

$$\frac{B}{(K^\times)^\ell} \simeq \frac{(\mathbb{Z}/\ell\mathbb{Z})^m}{V_{\mathbf{c}}(\ell)} \simeq V_{\mathbf{c}}^\perp(\ell),$$

one concludes that $\mathrm{Gal}(K(\zeta_\ell, \mathbf{c}^{1/\ell})/K(\zeta_\ell)) \simeq V_{\mathbf{c}}^\perp(\ell)$, and the conclusion of the lemma follows. □

Lemma 5.5. *Suppose that $f : \mathbb{N} \longrightarrow K^\times$ is a completely multiplicative function that is not a global power map. Then there exist positive integers n_1, n_2 and c_f for which*

$$\ell \nmid c_f \implies \begin{cases} \left[K\left(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}\right) : K(\zeta_\ell)\right] = \ell^2, & \text{and} \\ \left[K\left(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell}\right) : K(\zeta_\ell)\right] \ge \ell^3. \end{cases} \tag{22}$$

Proof. Note that f is a global power map if and only if the following two conditions hold.

[1]Here we are interpreting $\mathrm{Gal}(K(\zeta_\ell, \mathbf{c}^{1/\ell})/K)$ as operating on the *right*.

(1) For each rational prime p and prime ideal $\mathfrak{q} \in \mathcal{P}_K$, one has

$$\mathfrak{q} \mid f(p)\mathcal{O}_K \implies \mathfrak{q} \mid p\mathcal{O}_K.$$

(2) For any rational primes p and q and for any prime ideals $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}_K$ with $\mathfrak{p}$ lying above p and $\mathfrak{q}$ lying above q, one has

$$\frac{\mathrm{ord}_{\mathfrak{p}}(f(p))}{f_p} = \frac{\mathrm{ord}_{\mathfrak{q}}(f(q))}{f_q},$$

where f_p (resp. f_q) denotes the inertial degree of p (resp. q) in K.

Assume that f is not a global power map, so that at least one of these conditions fails. If (1) fails, then one can find a prime number p_1 and a prime ideal $\mathfrak{q} \in \mathcal{P}_K$ with

$$\mathfrak{q} \mid f(p_1) \text{ but } \mathfrak{q} \nmid p_1.$$

Let $\mathfrak{p}_1 \in \mathcal{P}_K$ be any prime ideal above p_1, let q be the rational prime below $\mathfrak{q}$, and pick any other rational prime $p_2 \notin \{p_1, q\}$ and any prime ideal $\mathfrak{p}_2$ lying over p_2. Setting $n_1 = p_1$ and $n_2 = p_2$ and considering the exponents of $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{q}$ in p_1, p_2 and $f(p_1)$, we see that

$$\begin{vmatrix} f_{p_1} & 0 & * \\ 0 & f_{p_2} & * \\ 0 & 0 & \mathrm{ord}_{\mathfrak{q}}(f(p_1)) \end{vmatrix} = f_{p_1} f_{p_2} \mathrm{ord}_{\mathfrak{q}}(f(p_1)) \not\equiv 0 \mod \ell \implies (22) \text{ holds},$$

so we may set $c_f := f_{p_1} f_{p_2} \mathrm{ord}_{\mathfrak{q}}(f(p_1))$ in this case.

On the other hand, if (1) holds but (2) fails, then let us write $\alpha_{\mathfrak{p}} := \mathrm{ord}_{\mathfrak{p}}(f(p))$, where p is the rational prime lying under p. One can find prime ideals $\mathfrak{p}_1 \neq \mathfrak{p}_2$ for which

$$\alpha_{\mathfrak{p}_1} f_{p_2} \neq \alpha_{\mathfrak{p}_2} \cdot f_{p_1},$$

where p_i denotes the prime lying under $\mathfrak{p}_i$. In case $p_1 \neq p_2$, then choose $\mathfrak{p}_3$ to be any other prime ideal lying over a prime $p_3 \notin \{p_1, p_2\}$ and set $n_1 := p_1 p_2 p_3$ and $n_2 := p_3$. Considering the subfield $K(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1 n_2)^{1/\ell})$, one sees that

$$\begin{vmatrix} f_{p_1} & 0 & \alpha_{\mathfrak{p}_1} \\ f_{p_2} & 0 & \alpha_{\mathfrak{p}_2} \\ f_{p_3} & f_{p_3} & 2\alpha_{\mathfrak{p}_3} \end{vmatrix} = f_{p_3}(f_{p_2}\alpha_{\mathfrak{p}_1} - f_{p_1}\alpha_{\mathfrak{p}_2}) \not\equiv 0 \mod \ell \implies (22) \text{ holds},$$

so we may set $c_f := |f_{p_3}(f_{p_1}\alpha_{\mathfrak{p}_2} - f_{p_2}\alpha_{\mathfrak{p}_1})|$ in this case. In case $p_1 = p_2 =: p$, we let p' be any other prime and $\mathfrak{p}'$ any prime of K over p'. Setting $n_1 := p$ and $n_2 := p'$ and considering the subfield $K(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell})$, we find that

$$\begin{vmatrix} f_p & 0 & \alpha_{\mathfrak{p}_1} \\ f_p & 0 & \alpha_{\mathfrak{p}_2} \\ 0 & f_{p'} & 0 \end{vmatrix} = f_{p'}(f_p\alpha_{\mathfrak{p}_1} - f_p\alpha_{\mathfrak{p}_2}) \not\equiv 0 \mod \ell \implies (22) \text{ holds},$$

and we may set $c_f := |f_{p'}(f_p\alpha_{\mathfrak{p}_1} - f_p\alpha_{\mathfrak{p}_2})|$ in this case, finishing the proof of Lemma 5.5. □

5.3. **The Frobenius automorphism in Kummer extensions.** We now turn our consideration to the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{P}}$ for a prime ideal $\mathfrak{P} \subseteq \mathcal{O}_L$ lying over $\mathfrak{p} \in \mathcal{P}_{K,1}$, where $L = K(\zeta_\ell, \mathbf{c}^{1/\ell})$ and $N\mathfrak{p} \equiv 1 \pmod{\ell}$. Note that for any $\mathfrak{p} \in \mathcal{P}_{K,1}$, $N\mathfrak{p}$ is prime.

We begin by describing the situation when $m = 1$ and $c \notin (K^\times)^\ell$, i.e. (dropping subscripts) we have

$$L = L_c := K(\zeta_\ell, c^{1/\ell}) \neq K(\zeta_\ell) \qquad (c \in K^\times)$$

and

$$\begin{gathered} \mathrm{Gal}(L_c/K) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes \mathbb{Z}/\ell\mathbb{Z} \\ \begin{pmatrix} \zeta_\ell & \mapsto & \zeta_\ell^a \\ c^{1/\ell} & \mapsto & c^{1/\ell} \cdot \zeta_\ell^b \end{pmatrix} \mapsto (a, b), \end{gathered} \tag{23}$$

The minimal polynomials over K of ζ_ℓ and $c^{1/\ell}$, together with their factorizations over $\overline{K}$, are given respectively as follows:

$$\Phi_\ell(t) := \frac{t^\ell - 1}{t-1} = \prod_{i \in (\mathbb{Z}/\ell\mathbb{Z})^\times} (t - \zeta_\ell^i),$$
$$t^\ell - c = \prod_{i \in \mathbb{Z}/\ell\mathbb{Z}} (t - \zeta_\ell^i \cdot c^{1/\ell}).$$

In our present discussion, we will adopt the standing assumptions that

$$N\mathfrak{p} \equiv 1 \pmod{\ell} \quad \text{and} \quad \mathrm{ord}_{\mathfrak{p}}(c) = 0. \tag{24}$$

By Lemmas 5.2 and 5.4, these conditions imply that

$$\mathfrak{p} \text{ splits completely in } K(\zeta_\ell) \quad \text{and} \quad \mathfrak{p} \text{ is unramified in } L_c.$$

Consider the subgroup $\mu_\ell \subseteq \overline{\mathbb{F}}_{\mathfrak{p}}^\times$ of ℓ-th roots of unity. Since $N\mathfrak{p} \equiv 1 \pmod{\ell}$, one can find an element $z \in \mathbb{Z}$ whose reduction $\overline{z}$ modulo $\mathfrak{p}$ generates μ_ℓ, i.e. we have

$$\langle \overline{z} \rangle = \mu_\ell \subseteq \mathbb{F}_{\mathfrak{p}}^\times, \tag{25}$$

and the reductions modulo $\mathfrak{p}$ of the above minimal polynomials factorize over $\overline{\mathbb{F}}_{\mathfrak{p}}$ as

$$\Phi_\ell(t) \equiv \prod_{i \in (\mathbb{Z}/\ell\mathbb{Z})^\times} (t - \overline{z}^i) \pmod{\mathfrak{p}},$$
$$t^\ell - c \equiv \prod_{i \in \mathbb{Z}/\ell\mathbb{Z}} (t - \overline{z}^i \theta_c) \pmod{\mathfrak{p}},$$

for some $\theta_c \in \overline{\mathbb{F}}_{\mathfrak{p}}^\times / \mu_\ell$. Furthermore, one has the prime factorization

$$\mathfrak{p}\mathcal{O}_{K(\zeta_\ell)} = \prod_{i \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \mathfrak{p}_{z,i}, \qquad \left(\mathfrak{p}_{z,i} := \mathfrak{p}\mathcal{O}_{K(\zeta_\ell)} + (\zeta_\ell - z^{i^*})\mathcal{O}_{K(\zeta_\ell)}\right),$$

where i^* denotes an integer satisfying $i^* i \equiv 1 \pmod{\ell}$. Note that, by our choice of indexing, we have

$$\forall j \in (\mathbb{Z}/\ell\mathbb{Z})^\times, \qquad \mathfrak{p}_{z,i} = \mathfrak{p}_{z^j, ij}. \tag{26}$$

What about the splitting type of such a prime ideal $\mathfrak{p}_{z,i}$ in L_c? Since L_c has prime degree ℓ over $K(\zeta_\ell)$ and by (24), each $\mathfrak{p}_{z,i}$ either splits completely or remains inert in L_c. Furthermore, since L_c is Galois over K, the splitting type of each $\mathfrak{p}_{z,i}$ is the same. Under the assumptions (24), one has

$$\begin{aligned} \mathfrak{p}_{z,i} \text{ splits completely in } L_c &\iff c \pmod{\mathfrak{p}} \in (\mathbb{F}_{\mathfrak{p}}^\times)^\ell \\ &\iff \theta_c \in \mathbb{F}_{\mathfrak{p}}^\times / \mu_\ell \end{aligned} \tag{27}$$

If this is the case, we may allow z in (25) to be an arbitrary generator of $\mu_\ell \subset \mathbb{F}_{\mathfrak{p}}^\times$ and note also that, under the isomorphism (23),

$$\mathfrak{p}_{z,i} \text{ splits completely in } L_c \iff \mathrm{Frob}_{\mathfrak{P}} = (1,0),$$

for any prime ideal $\mathfrak{P} \subseteq \mathcal{O}_{L_c}$ lying over $\mathfrak{p}_{z,i}$.

In case $\mathfrak{p}_{z,i}$ does not split completely in L_c, the finite field $\mathbb{F}_{\mathfrak{p}}[\theta_c]$ has degree ℓ over $\mathbb{F}_{\mathfrak{p}}$, and we normalize our choice of $z = z_c \in \mathbb{Z}$ so that

$$\overline{z}_c := \frac{\theta_c^{N\mathfrak{p}}}{\theta_c} \in \mathbb{F}_{\mathfrak{p}}^\times \tag{28}$$

(Note that $\overline{z}_c \in \mathbb{F}_{\mathfrak{p}}^\times$ is independent of the choice of $\theta_c \in \overline{\mathbb{F}}_{\mathfrak{p}}^\times / \mu_\ell$). In this case, putting

$$\mathfrak{P}_{z_c,i} := \mathfrak{p}_{z_c,i}\mathcal{O}_{L_c} = \mathfrak{p}\mathcal{O}_{L_c} + (\zeta_\ell - z_c^{i^*})\mathcal{O}_{L_c}, \tag{29}$$

the ideal $\mathfrak{P}_{z_c,i}$ is prime and we have a prime factorization

$$\mathfrak{p}\mathcal{O}_{L_c} = \prod_{i \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \mathfrak{P}_{z_c,i}.$$

The following lemma characterizes the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{P}_{z_c,i}}$.

Lemma 5.6. *Suppose $c \in K^\times$ satisfies $L_c := K(\zeta_\ell, c^{1/\ell}) \neq K(\zeta_\ell)$. Furthermore, let $\mathfrak{p} \in \mathcal{P}_{K,1}$ be a prime ideal satisfying $N\mathfrak{p} \equiv 1 \pmod{\ell}$ and $\mathrm{ord}_{\mathfrak{p}}(c) = 0$. Then $\mathfrak{p}$ is unramified in L_c and, with notation as above, under the isomorphism $\mathrm{Gal}(L_c/K) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes \mathbb{Z}/\ell\mathbb{Z}$ given by (23), one has*

$$\mathrm{Frob}_{\mathfrak{P}_{z_c,i}} = \begin{cases} (1,0) & \text{if } \mathfrak{p} \text{ splits completely in } L_c \text{ and } \mathfrak{P}_{z_c,i} \text{ is any prime above } \mathfrak{p} \\ (1,i) & \text{if } p\mathcal{O}_{L_c} = \prod_{i \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \mathfrak{P}_{z_c,i}, \text{ where each } \mathfrak{P}_{z_c,i} \text{ is as in (29) and is prime.} \end{cases}$$

Proof. We need only concern ourselves with the case that $\mathfrak{p}$ does not split completely in L_c. In this case, consider the ring homomorphism $\pi_{z_c,i} : \mathcal{O}_{K(\zeta_\ell)} \longrightarrow \mathbb{F}_{\mathfrak{p}}$, induced by $\zeta_\ell \mapsto \overline{z}_c^{i^*}$. Note that

$$\ker \pi_{z_c,i} = \mathfrak{p}_{z_c,i} \quad \text{and} \quad \sigma_a(\mathfrak{p}_{z_c,i}) = \mathfrak{p}_{z_c,ai},$$

where $\sigma_a \mapsto a$ under $\mathrm{Gal}(K(\zeta_\ell)/K) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$. Since $\mathcal{O}_{L_c}/\mathfrak{P}_{z_c,i} \simeq \mathbb{F}_{\mathfrak{p}}(\theta_c)$ in this case, one may extend $\pi_{z_c,i}$ to a ring homomorphism $\varpi_{z_c,i} : \mathcal{O}_{L_c} \longrightarrow \mathbb{F}_{\mathfrak{p}}(\theta_c)$ for which $\varpi_{z_c,i}(c^{1/\ell}) = \theta_c$. Consider the induced isomorphism

$$\varpi_{z_c,i} : \mathcal{O}_{L_c}/\mathfrak{P}_{z_c,i} \longrightarrow \mathbb{F}_{\mathfrak{p}}(\theta_c).$$

By definition of $\mathrm{Frob}_{\mathfrak{P}_{z_c,i}}$, one has $\varpi_{z_c,i} \circ \mathrm{Frob}_{\mathfrak{P}_{z_c,i}} \circ \varpi_{z_c,i}^{-1}(\theta_c) = \theta_c^{\mathfrak{p}}$. On the other hand, if $\mathrm{Frob}_{\mathfrak{P}_{z_c,i}} \mapsto (1,b)$ under (23), then by (28), we have

$$\overline{z}_c\theta_c = \theta_c^{N\mathfrak{p}} = \varpi_{z_c,i}(\mathrm{Frob}_{\mathfrak{P}_{z_c,i}}(\varpi_{z_c,i}^{-1}(\theta_c))) = \varpi_{z_c,i}(\mathrm{Frob}_{\mathfrak{P}_{z_c,i}}(c^{1/\ell} \pmod{\mathfrak{P}_{z_c,i}})) = \varpi_{z_c,i}(\zeta_\ell^b c^{1/\ell}) = \overline{z}_c^{i^*b}\theta_c.$$

Thus, one finds that $b = i$, proving the lemma. □

The next Lemma follows from Lemma 5.6, and is essential in what follows. Our context is as before but with $m = 2k$ even, and we write $L = K(\zeta_\ell, \mathbf{c}^{1/\ell}, \mathbf{d}^{1/\ell}) := K(\zeta_\ell, c_1^{1/\ell}, \ldots, c_k^{1/\ell}, d_1^{1/\ell}, \ldots, d_k^{1/\ell})$. Thus,

$$\mathrm{Gal}(L/K) \hookrightarrow (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes \left((\mathbb{Z}/\ell\mathbb{Z})^k \times (\mathbb{Z}/\ell\mathbb{Z})^k\right), \tag{30}$$

and we regard elements of $\mathrm{Gal}(L/K)$ as triples $(a, \mathbf{b}, \mathbf{f})$ with $\mathbf{b}, \mathbf{f} \in (\mathbb{Z}/\ell\mathbb{Z})^k$. We denote by $\mathcal{C}_{2k} \subseteq \mathrm{Gal}(L/K)$ the subset

$$\mathcal{C}_{2k} := \{(1, \mathbf{b}, \mathbf{f}) \in \mathrm{Gal}(L/K) : \ \mathbf{f} = \lambda\mathbf{b} \text{ for some } \lambda \in \mathbb{Z}/\ell\mathbb{Z} \ \}, \tag{31}$$

which is stable by $\mathrm{Gal}(L/K)$-conjugation.

Lemma 5.7. *Let $L = K(\zeta_\ell, \mathbf{c}^{1/\ell}, \mathbf{d}^{1/\ell})$. Let $\mathfrak{p} \in \mathcal{P}_{K,1}$ be any prime ideal satisfying $N\mathfrak{p} \equiv 1 \pmod{\ell}$ and*

$$\mathrm{ord}_{\mathfrak{p}}\left(\prod_{i=1}^{k} c_i d_i\right) = 0.$$

Then $\mathfrak{p}$ is unramified in K and splits completely in the subfield $K(\zeta_\ell)$. Suppose further that, for some fixed $k_{\mathfrak{p}} \in \mathbb{Z}/(N\mathfrak{p} - 1)\mathbb{Z}$, one has

$$\forall i \in \{1, 2, \ldots, k\}, \quad d_i \equiv c_i^{k_{\mathfrak{p}}} \pmod{\mathfrak{p}}.$$

Then, under the embedding (30), the Frobenius class $\mathrm{Frob}_{\mathfrak{p}} \subseteq \mathrm{Gal}(L/K)$ satisfies

$$\mathrm{Frob}_{\mathfrak{p}} \subseteq \mathcal{C}_{2k}.$$

Proof. Note that, for any vector $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in K^m$, the diagram

$$\begin{array}{ccc} \mathrm{Gal}(K(\zeta_\ell, \mathbf{w}^{1/\ell})/K) & \longrightarrow & (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes V_{\mathbf{w}}^{\perp}(\ell) \\ {\scriptstyle \mathrm{res}}\downarrow & & \downarrow{\scriptstyle \pi_j} \\ \mathrm{Gal}(K(\zeta_\ell, w_j^{1/\ell})/K) & \longrightarrow & (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes V_{w_j}^{\perp}(\ell) \end{array} \tag{32}$$

commutes, where $\pi_j((a, \mathbf{b})) := (a, b_j)$. Taking any prime ideal $\mathfrak{p}$ as in the statement of the corollary, $\mathfrak{p}$ is unramified in $L = K(\zeta_\ell, \mathbf{c}^{1/\ell}, \mathbf{d}^{1/\ell})$, and we fix a prime $\mathfrak{P}$ of K lying over $\mathfrak{p}$. By the discussion preceding Lemma 5.6, for any multiplicative generator $z \in \mu_\ell \subseteq \mathbb{F}_{\mathfrak{p}}^\times$ we may find $i \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ for which

$$\mathfrak{P} \cap \mathcal{O}_{K(\zeta_\ell)} = \mathfrak{p}_{z,i}. \tag{33}$$

Let us fix an index $j \in \{1, 2, \ldots, k\}$ and put $c := c_j$ and $d := d_j$. Furthermore, denote by

$$\mathfrak{P}_c := \mathfrak{P} \cap \mathcal{O}_{L_c} \quad \text{and} \quad \mathfrak{P}_d := \mathfrak{P} \cap \mathcal{O}_{L_d}$$

the corresponding primes of $L_c := K(\zeta_\ell, c^{1/\ell})$ (resp. of $L_d := K(\zeta_\ell, d^{1/\ell})$) lying under $\mathfrak{P}$.

Case: $k_{\mathfrak{p}} \equiv 0 \pmod{\ell}$**.** Since $d \equiv c^{k_{\mathfrak{p}}} \pmod{\mathfrak{p}}$, we see in this case that $d \pmod{\mathfrak{p}} \in (\mathbb{F}_{\mathfrak{p}}^\times)^\ell$, so that by (27) and Lemma 5.6, one has $\mathrm{Frob}_{\mathfrak{P}_d} = (1, 0)$ in this case. Since this is independent of the index j, we see by (32) that the conclusion of the corollary holds, taking $\lambda = 0$ in (31).

Case: $k_{\mathfrak{p}} \not\equiv 0 \pmod{\ell}$**.** Now if $c \pmod{\mathfrak{p}} \in (\mathbb{F}_{\mathfrak{p}}^\times)^\ell$, then necessarily $d \equiv c^{k_{\mathfrak{p}}} \pmod{\mathfrak{p}} \in (\mathbb{F}_{\mathfrak{p}}^\times)^\ell$, and again by (27) and Lemma 5.6, we have that $\mathrm{Frob}_{\mathfrak{P}_c} = (1, 0)$ and $\mathrm{Frob}_{\mathfrak{P}_d} = (1, 0 \cdot k_{\mathfrak{p}})$, and (note that this covers the case $c \in (K^\times)^\ell$).

In case $c \pmod{\mathfrak{p}} \notin (\mathbb{F}_{\mathfrak{p}}^\times)^\ell$, we put $z = z_c$ in (33), possibly adjusting $i \pmod{\ell}$ appropriately. Noting that θ_d only depends on d modulo $\mathfrak{p}$, we may take $\theta_d = \theta_c^{k_{\mathfrak{p}}}$, and so $z_d \equiv z_c^{k_{\mathfrak{p}}} \pmod{\mathfrak{p}}$. Thus, by (29) and (26), we find that

$$\mathfrak{P}_c = \mathfrak{P}_{z_c, i} = \mathfrak{P}_{z_c^{k_{\mathfrak{p}}}, ik_{\mathfrak{p}}} = \mathfrak{P}_{z_d, ik_{\mathfrak{p}}}.$$

Applying Lemma 5.6, we conclude that $\mathrm{Frob}_{\mathfrak{P}_c} = (1, i)$ and $\mathrm{Frob}_{\mathfrak{P}_d} = (1, ik_{\mathfrak{p}})$, and since the factor $k_{\mathfrak{p}}$ is independent of the index j, we apply (32) to deduce the conclusion of Lemma 5.7 in this case. □

In particular, taking $\mathbf{c} = (n_1, n_2) \in \mathbb{N}^2$ and $\mathbf{d} = (f(n_1), f(n_2)) \in (K^\times)^2$, we obtain the following corollary. Recall that $b_{f,\mathbf{n}} := \left| \prod_{i=1}^{2} n_i \mathfrak{num}(f(n_i)) \mathfrak{den}(f(n_i)) \right|$.

Corollary 5.8. *Suppose that $f : \mathbb{N} \longrightarrow K^\times$ is any function, $n_1, n_2 \in \mathbb{N}$, and ℓ is an odd prime number. Put $L = K\left(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell}\right)$. Then, for each prime ideal $\mathfrak{p}$, one has*

$$\mathfrak{p} \in S_f \ \text{ and } \ N\mathfrak{p} \equiv 1 \pmod{\ell} \implies \mathrm{Frob}_{\mathfrak{p}} \subseteq \mathcal{C}_4 \ \text{ or } \ \mathfrak{p} \mid b_{f,\mathbf{n}},$$

where $\mathcal{C}_4$ is defined by taking $k = 2$ in (31).

Our final lemma shows that, if f is not a global power map, then the relevant Chebotarev factor $|\mathcal{C}_4|/|\operatorname{Gal}(L/K)|$ is bounded by a constant times $1/\ell^2$, which will allow us to deduce Proposition 4.5 from Theorem 4.4.

Lemma 5.9. *Suppose that $f : \mathbb{N} \longrightarrow K^\times$ is any function, let $n_1, n_2 \in \mathbb{N}$, let ℓ be an odd prime, and let $L := K\left(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1)^{1/\ell}, f(n_2)^{1/\ell}\right)$. Suppose that*

$$[K\left(\zeta_\ell, n_1^{1/\ell}, n_2^{1/\ell}, f(n_1 n_2)^{1/\ell}\right) : K(\zeta_\ell)] = \ell^3. \tag{34}$$

Then one has

$$\frac{|\mathcal{C}_4|}{|\operatorname{Gal}(L/K)|} \ \leq \ \frac{2}{\ell(\ell-1)},$$

where $\mathcal{C}_4$ is defined by taking $k = 2$ in (31).

Proof. By hypothesis, one has

$$\operatorname{Gal}(L/K) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z} \cdot \mathbf{d})^\perp,$$

for some $\mathbf{d} \in (\mathbb{Z}/\ell\mathbb{Z})^4$. If $\mathbf{d} = \mathbf{0}$, i.e. if $\operatorname{Gal}(L/K) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes (\mathbb{Z}/\ell\mathbb{Z})^4$, then directly from (31) one finds that

$$|\mathcal{C}_4| \leq \ell^3,$$

and the conclusion of the lemma follows. If $\mathbf{d} \neq \mathbf{0}$ then, writing $\mathbf{d} = (\mathbf{d}_1, \mathbf{d}_2)$ with $\mathbf{d}_i \in (\mathbb{Z}/\ell\mathbb{Z})^2$, we have that

$$\begin{aligned} \mathcal{C}_4 &= \{(1, \mathbf{b}, \lambda\mathbf{b}) : \ (\mathbf{b}, \lambda) \in (\mathbb{Z}/\ell\mathbb{Z})^3, \, \mathbf{b} \cdot \mathbf{d}_1 + \lambda\mathbf{b} \cdot \mathbf{d}_2 = 0\} \\ &= \{(1, \mathbf{b}, \lambda\mathbf{b}) : \ (\mathbf{b}, \lambda) \in (\mathbb{Z}/\ell\mathbb{Z})^3, \, \mathbf{b} \cdot (\mathbf{d}_1 + \lambda\mathbf{d}_2) = 0\}. \end{aligned}$$

Consider the equation

$$\mathbf{b} \cdot (\mathbf{d}_1 + \lambda\mathbf{d}_2) = 0. \tag{35}$$

By (34) we see that $\mathbf{d}_2 \neq \mathbf{0} \in (\mathbb{Z}/\ell\mathbb{Z})^2$, and so $\mathbf{d}_1 + \lambda\mathbf{d}_2 = \mathbf{0}$ for at most one $\lambda \in \mathbb{Z}/\ell\mathbb{Z}$. For such a λ, one counts ℓ^2 solutions $\mathbf{b} \in (\mathbb{Z}/\ell\mathbb{Z})^2$ to the equation (35), while for each of the other $\ell - 1$ values of λ one counts ℓ solutions. Thus, one has

$$|\mathcal{C}_4| \leq \ell(2\ell - 1),$$

and the conclusion of the lemma follows in this case as well. □

Remark 5.10. The hypothesis in Lemma 5.9 that f not be a global power map is critical. Indeed, if $f(\alpha) = \alpha^k$ for all $\alpha \in K$, then (e.g. provided n_2 is multiplicatively independent from n_1) under (30) one has

$$\mathrm{Gal}(L/K) = (\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes \{(\mathbf{b}, k\mathbf{b}) : \mathbf{b} \in (\mathbb{Z}/\ell\mathbb{Z})^2\}.$$

In particular, one finds that

$$\frac{|\mathcal{C}_4|}{|\mathrm{Gal}(L/K)|} = \frac{|\{(1, \mathbf{b}, k\mathbf{b}) : \mathbf{b} \in (\mathbb{Z}/\ell\mathbb{Z})^2\}|}{|(\mathbb{Z}/\ell\mathbb{Z})^\times \ltimes \{(\mathbf{b}, k\mathbf{b}) : \mathbf{b} \in (\mathbb{Z}/\ell\mathbb{Z})^2\}|} = \frac{1}{\ell - 1},$$

and our method of proof fails for this case (as it should).

6. Proof of Proposition 4.5

We now assume that f is not a global power map, and we may assume that $|S_f| = \infty$. Fix $\mathbf{n} = (n_1, n_2) \in \mathbb{N}^2$ as in Lemma 5.5, and define

$$a_f := \max\{c_f + 1, e^{b_{f,\mathbf{n}}}\},$$

where c_f is as in Lemma 5.5 and $b_{f,\mathbf{n}}$ is as in (17). Note that in particular, by Corollary 5.8, one has

$$\sum_{\substack{\mathfrak{p} \in S_f(x) \\ N\mathfrak{p} \equiv 1 \pmod{\ell}}} 1 \leq \pi(x; L/K, \mathcal{C}_4) + O(\omega(b_{f,\mathbf{n}})). \tag{36}$$

Our assumption that

$$Z \leq \left(\frac{\log x}{(6c_2 \log\log x)^2}\right)^{1/15} \tag{37}$$

implies that, for x large enough, one has $\sqrt{\log x/Z^5} \geq 6c_2 \cdot Z^5 \log Z$. By Corollary 5.3, $\ell \in [Y, Z)$ and $e^{b_{f,\mathbf{n}}} \leq a_f < Y$ guarantee that (15) holds in this case. Thus, for $Y > a_f$ and $\ell \in [Y, Z)$, Theorem 4.4 and Lemma 5.9 imply that

$$\begin{aligned} \pi(x; L/K, \mathcal{C}_4) &= \frac{|\mathcal{C}_4|}{|\mathrm{Gal}(L/K)|} \cdot \pi(x) + O\left(|\mathcal{C}_4| \cdot x \cdot \exp\left(-c_1\sqrt{\frac{\log x}{[L:K]}}\right)\right) \\ &\ll \frac{1}{\ell^2} \cdot \pi(x) + \ell^3 \cdot x \cdot \exp\left(-c_1\sqrt{\frac{\log x}{Z^5}}\right). \end{aligned} \tag{38}$$

Inserting this into of Lemma 5.9 into (36) and summing over primes $\ell \in [Y, Z)$, we obtain

$$\sum_{Y \leq \ell < Z} \sum_{\substack{\mathfrak{p} \in S_f(x) \\ N\mathfrak{p} \equiv 1 \pmod{\ell}}} 1 \ll \frac{1}{Y \log Y} \cdot \pi(x) + \frac{Z^4}{\log Z} \cdot x \cdot \exp\left(-c_1\sqrt{\frac{\log x}{Z^5}}\right) + \omega(b_{f,\mathbf{n}}).$$

By virtue of the bounds (37) and

$$\exp\left(-c_1(\log x)^{1/3}\right) \ll_A \frac{1}{(\log x)^A} \qquad (A > 0),$$

we see that the second remainder term satisfies

$$\frac{Z^4}{\log Z} \cdot x \cdot \exp\left(-c_1\sqrt{\frac{\log x}{Z^5}}\right) \ll_A \frac{x}{(\log x)^A}$$

for any $A > 0$, and since $Y < Z$, this observation finishes the proof of Proposition 4.5.

7. Acknowledgments

This paper was motivated by a question posed by C. Khare in connection with compatible systems of one-dimensional Galois representations. I thank Professor Khare for sharing this interesting question, and also Professor R. Khan, who originally communicated it to me. Some of the research leading to this paper was done during a research stay at the Universität Göttingen, and I would like to thank the university for providing a stimulating environment in which to work. I would also like to thank Professors S. Basarab and I. Rusza for stimulating discussions on this topic and for insightful comments. Finally, I would like to thank Professor R. Daileda for helpful feedback on an earlier version.

References

[1] C. Corrales and R. Schoof. The support problem and its elliptic analogue, *J. Number Theory* **64** (1997), 276–290.
[2] P. Erdős. On the distribution function of additive functions, *Ann. of Math.* **47** no. 2 (1946), 1–20.
[3] J. Fabrykowski and M. V. Subbarao. On a class of Arithmetic functions satisfying a congruence property, *J. Madras Univ.*, **51** no. 1 (1988), 48–56.
[4] J. Fehér and B. M. Phong. On a problem of Fabrykowski and Subbarao concerning quasi multiplicative functions satisfying a congruence property, *Acta. Math. Hungar.*, **89** (2000), 149–159.
[5] A. Frölich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics **27**, Cambridge Univ. Press (1991).
[6] R. Gupta and M. R. Murty. A remark on Artin's conjecture, *Invent. Math.* **78** no. 1 (1984), 127–130.
[7] D. R. Heath-Brown. Artin's conjecture for primitive roots, *Quart. J. Math. Oxford* **37** no. 1 (1986), 27–38.
[8] C. Khare and D. Prasad. Reduction of homomorphisms mod p and algebraicity, *J. Number Theory* **105** (2004), 322–332.
[9] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem, in A. Frohlich (ed.) *Algebraic Number Fields*, pp. 409–464, Academic Press, 1977.
[10] S. Lang, *Algebra*, Graduate Texts in Mathematics **211**, Springer (2002).
[11] I. Ruzsa. On congruence-preserving functions, *Mat. Lap.* **22** (1971), 125–134.
[12] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publ. Math. I. H. E. S.* **54** (1981), 123–201.
[13] H. M. Stark. Some effective cases of the Brauer-Siegel Theorem, *Invent. Math.* **23** (1974), 135–152.
[14] M. V. Subbarao. Arithmetic functions satisfying a congruence property, *Canad. Math. Bull.* **9** (1966), 143–146.
[15] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics **46**, Cambridge Univ. Press (1995).
[16] L. Washington. *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, **83**. Springer-Verlag, New York, 1982.
[17] U. Zannier. On periodic mod p sequences and G-functions, *Manuscripta mathematica* **90** no. 3 (1996), 391–402.

- Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 322 Science and Engineering Offices (M/C 249), 851 S. Morgan Street, Chicago, IL 60607-7045, USA.

E-mail address: ncjones@uic.edu