Journal of Number Theory 133 (2013) 1738–1751

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Higher rank generalizations of Fomenko's conjecture

Adam Tyler Felix

University of Lethbridge, Department of Mathematics and Computer Science, 4401 University Drive West, Lethbridge, Alberta, T1K3M4, Canada

ARTICLE INFO

Article history:
Received 14 June 2011
Revised 8 August 2012
Accepted 1 September 2012
Available online 28 December 2012
Communicated by Greg Martin

MSC:
11N37
11N25
11N35

Keywords:
Artin's primitive root conjecture
Prime numbers
Fomenko's conjecture

ABSTRACT

Let a be a natural number greater than 1. For each prime p, let $i_a(p)$ denote the index of the group generated by a in $\mathbb{F}_p^*$. Assuming the generalized Riemann hypothesis and Hypothesis A of Hooley, Fomenko proved in 2004

$$\sum_{p\leqslant x}\log\bigl(i_a(p)\bigr)=c_a\,\mathrm{li}(x)+O\left(\frac{x\log\log x}{(\log x)^2}\right),$$

where c_a is a constant dependent on a, and where $\mathrm{li}(x)$ is the logarithmic integral. We prove a higher rank version of this result without using Hypothesis A of Hooley. More precisely, let $\{a_1,a_2,\ldots,a_r\}\subset\mathbb{Q}^*$ be a multiplicatively independent set of integers. Let $\Gamma=\langle a_1,a_2,\ldots,a_r\rangle$ be the group generated by $a_1,a_2,\ldots,a_r$ in $\mathbb{Q}^*$. For primes p, define $i_\Gamma(p)$ to be $[(\mathbb{Z}/p\mathbb{Z})^*:\Gamma \bmod p]$, where $\Gamma \bmod p$ is the group generated by $a_1,a_2,\ldots,a_r$ inside $\mathbb{F}_p^*$. We show that, for $r\geqslant 2$, there is a positive constant $c_\Gamma>0$ such that

$$\sum_{p\leqslant x}\log i_\Gamma(p)=c_\Gamma\,\mathrm{li}(x)+O\bigl(x^\theta\bigr),$$

where $\theta<1$.

E-mail address: adam.tyler.felix@gmail.com.

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2012.09.008

1. Introduction

In 1927, Emil Artin made the following conjecture (see [1, Introduction] and [14]): let a be a fixed integer such that $a \neq 0, \pm 1$ or a perfect square. Write $a = b^h$, where $b \in \mathbb{Z}$ is not a perfect power and $h \in \mathbb{N}$. For a group G with subset S, let $\langle S \rangle$ denote the subgroup of G generated by S. Define $N_a(x) := \#\{p \leqslant x\colon\ (\mathbb{Z}/p\mathbb{Z})^* = \langle a \bmod p \rangle\}$. Then,

$$N_a(x) \sim A_h \pi(x),$$

where $\pi(x) = \#\{p \leqslant x\colon\ p \text{ prime}\}$ and

$$A_h = \prod_{\substack{q|h \\ q \text{ prime}}} \left(1 - \frac{1}{q-1}\right) \prod_{\substack{q\nmid h \\ q \text{ prime}}} \left(1 - \frac{1}{q(q-1)}\right) > 0. \tag{1}$$

The heuristic behind this conjecture is based on the following idea. We have a is primitive root modulo p if, and only if, $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ for all primes $q|p-1$. Now $p \equiv 1 \bmod q$ occurs with a density of $1/\varphi(q) = 1/(q-1)$ of the primes p by Dirichlet's theorem on primes in arithmetic progression, and $a^{\frac{p-1}{q}} \equiv 1 \bmod p$ occurs with a density of $1/q$ of the primes since $a^{\frac{p-1}{q}}$ is a qth root of unity, and there are exactly q of such elements.

It should be noted the constant was later realized to be incorrect for certain a's (see the discussion after Theorem 1).

Artin's conjecture is still unresolved. However, Hooley [14] provided a conditional resolution. First, we will need to introduce the following notational conventions: let f, g be functions. By $f(x) = O(g(x))$, or equivalently, $f(x) \ll g(x)$, we mean that there exists a constant $C > 0$ such that, for all x in the domain of f/g, we have $|f(x)| \leqslant Cg(x)$. By $f(x) = O_T(g(x))$ or $f(x) \ll_T g(x)$, we mean that the above constant is dependent on T, where T is allowed to be a set. For example, $T = \Gamma$, or $T = \{r\} \cup \Gamma$. In this latter case, we will write $O_{r,\Gamma}$ instead of $O_{\{r\}\cup\Gamma}$. This notation may be dropped in proofs for convenience. By $f(x) \sim g(x)$, we mean

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

where x in the above limit is restricted to the domain of f and g.

The statement "GRH holds for a on $A \subset \mathbb{N}$" will hereafter signify the statement "GRH holds for all Dedekind zeta functions for the fields $\mathbb{Q}(\zeta_n, a^{1/n})$, where ζ_n is a primitive nth root of unity and n ranges over all values of $A \subset \mathbb{N}$".

The statement "GRH holds for Γ on $A \subset \mathbb{N}$" will hereafter signify the statement "GRH holds for all Dedekind zeta functions for the fields $\mathbb{Q}(\zeta_n, a_1^{1/n}, a_2^{1/n}, \ldots, a_r^{1/n})$, where ζ_n is a primitive nth root of unity and n ranges over all values of $A \subset \mathbb{N}$". For a number field K and a fixed $\delta \in [1/2, 1)$, the statement "δ-GRH holds for K" will hereafter signify the statement "$\zeta_K(s) \neq 0$ for all s with $\Re(s) > 1 - \delta$, where ζ_K is the Dedekind zeta function of K". For a fixed $\delta \in [1/2, 1)$, the statement "δ-GRH holds for Γ on $A \subset \mathbb{N}$" will hereafter signify the statement "δ-GRH holds for all Dedekind zeta functions for the fields $\mathbb{Q}(\zeta_n, a_1^{1/n}, a_2^{1/n}, \ldots, a_r^{1/n})$, where ζ_n is a primitive nth root of unity and n ranges over all values of $A \subset \mathbb{N}$".

Hooley's theorem [14] is the following result:

Theorem 1 *(Hooley). Suppose $a \in \mathbb{Z}$ such that $a \neq 0, \pm 1$ or a perfect square. Suppose further that GRH holds for a on squarefree positive integers. Then,*

$$N_a(x) = A(a)\pi(x) + O_a\left(\frac{x \log\log x}{(\log x)^2}\right).$$

It should be noted that $A(a)$ in Theorem 1 is different from A_h in (1). It was discovered by Artin and the Lehmers [17] that Artin's original constant was off by a small factor for some $a \in \mathbb{Z}$ with $a \neq 0, \pm 1$ or a perfect square (see also Stevenhagen [26, §2]). In fact, let h be as above, and let $a = a_1 a_2^2$, where $a_1, a_2 \in \mathbb{Z}$ and a_1 is squarefree. If $a_1 \not\equiv 1 \pmod 4$, then $A(a) = A_h$, and if $a_1 \equiv 1 \pmod 4$, then

$$A(a) = A_h\left(1 - \mu\big(|a_1|\big) \prod_{\substack{q \mid \gcd(h, a_1) \\ q \text{ prime}}} \frac{1}{q-2} \prod_{\substack{q \nmid h \\ q \mid a_1 \\ q \text{ prime}}} \frac{1}{q^2 - q - 1}\right).$$

The best unconditional results are of the following flavor: one of 2, 3, or 5 is a primitive root modulo p for infinitely many primes p. In fact, we have

$$\#\{p \leqslant x\colon a \text{ is a primitive root modulo } p\} \geqslant \frac{cx}{(\log x)^2},$$

where $c > 0$ is a constant and a is one of 2, 3, or 5. This result originates in the work of Gupta and Murty [12] and Heath-Brown [13]. It should be noted that 2, 3, and 5 are not the only set of integers for which this result is applicable. In fact, we need three non-zero multiplicatively independent integers a, b, and c such that none of a, b, c, $-3ab$, $-3ac$, $-3bc$, or abc is a square for the result to be true for one of a, b, or c.

1.1. Generalizing Artin's conjecture

Let a be as before, and let p be a prime such that $p \nmid a$. We denote by $f_a(p)$ and $i_a(p)$ the order of a modulo p and the index of a modulo p, respectively.

We reformulate the quantity $N_a(x)$ in the following manner:

$$N_a(x) = \sum_{p \leqslant x} \chi_{\{1\}}\big(i_a(p)\big),$$

where χ_S is the characteristic function of the set S.

We would like to know what would occur if we change $\chi_{\{1\}}$ to a generic function $F : \mathbb{N} \to \mathbb{C}$. That is, can we obtain the following relation

$$\sum_{p \leqslant x} F\big(i_a(p)\big) \sim A_F(a)\pi(x)$$

where $A_F(a)$ is a constant dependent on F and a? This question was first studied by Stephens [25], then by Wagstaff [27], Murata [18], Elliott and Murata [7], Pappalardi [22], Bach, Lukes, Shallit, and Williams [2], and Fomenko [11] among others. It is investigated in detail in [9]. Of course, the functions F will have reasonable restrictions so as to not force an impossibility with the above relation. For example, $F(x) = x$ does not satisfy the above relation. To see this, we note that

$$\begin{aligned}\sum_{p \leqslant x} i_a(p) &= \sum_{p \leqslant x} \sum_{d \mid i_a(p)} \varphi(d) = \sum_{d \leqslant x} \varphi(d) \sum_{\substack{p \leqslant x \\ d \mid i_a(p)}} 1 \\ &\geqslant \sum_{d \leqslant (\log x)^{1/7}} \varphi(d) \#\big\{p \leqslant x\colon d \mid i_a(p)\big\}.\end{aligned}$$

By [10, Lemma 2.1], $d|i_a(p)$ if, and only if, p splits completely in $\mathbb{Q}(\zeta_d, a^{1/d})$ over $\mathbb{Q}$. So, for $d \leqslant (\log x)^{1/7}$, the unconditional Chebotarev density theorem (see [16, Theorem 1.4] or [22, p. 376]) gives us

$$\begin{aligned}\#\{p \leqslant x\colon d|i_a(p)\} &= \frac{\mathrm{li}(x)}{[\mathbb{Q}(\zeta_d : a^{1/d}) : \mathbb{Q}]} + O\big(x\exp\big(-A(\log x)^{5/14}\big)\big) \\ &= \frac{\mathrm{li}(x)}{[\mathbb{Q}(\zeta_d : a^{1/d}) : \mathbb{Q}]} + O\left(\frac{x}{(\log x)^B}\right),\end{aligned}$$

for any $B > 0$. We also have $[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}] \asymp d\varphi(d)$ by [27, Proposition 4.1]. Hence,

$$\begin{aligned}\sum_{p \leqslant x} i_a(p) &\geqslant \sum_{d \leqslant (\log x)^{1/7}} \varphi(d)\left(\frac{\mathrm{li}(x)}{[\mathbb{Q}(\zeta_d : a^{1/d}) : \mathbb{Q}]} + O\left(\frac{x}{(\log x)^B}\right)\right) \\ &\gg \mathrm{li}(x) \sum_{d \leqslant (\log x)^{1/7}} \frac{1}{d} + O\left(\frac{x}{(\log x)^B} \sum_{d \leqslant (\log x)^{1/7}} \varphi(d)\right) \\ &\gg \mathrm{li}(x)\log\log x + O\left(\frac{x}{(\log x)^{B-2/7}}\right) \\ &\gg \frac{x\log\log x}{\log x}\end{aligned}$$

for any $B \geqslant 1 + 2/7$.

The case where the function $F(x) = \log x$ and $a = 2$ was first studied by Bach, Lukes, Shallit and Williams [2]. We refer to the following relation as Fomenko's conjecture since Fomenko [11] (see Theorem 3 below) proved it using GRH and Hypothesis A of Hooley [15, p. 112] (see the hypothesis below):

$$\sum_{p \leqslant x} \log\big(i_a(p)\big) \sim c_a \,\mathrm{li}(x),$$

for some constant $c_a > 0$. The authors of [2] mention heuristics that suggest the above relation is true for $a \geqslant 2$ and give computational evidence for $a = 2$, $a = 3$, and $a = 5$.

Pappalardi [22] showed the following theorem:

Theorem 2 *(Pappalardi). For $a \in \mathbb{Z}$ different from 0 and ± 1, we have*

$$\frac{x}{\log x} \ll \sum_{p \leqslant x} \log\big(i_a(p)\big) \ll \frac{x\log\log x}{\log x},$$

where the lower bound is unconditional, and for the upper bound, we suppose GRH holds for a on prime powers.

Recall the following hypothesis of Hooley [15, p. 112]:

Hypothesis *(Hypothesis A of Hooley).* Let $P_b(y; \ell, t)$ be the number of primes $p \leqslant y$ such that $2^t b$ is an ℓth-power residue modulo p and for which $\ell|p-1$. Then, for $y^{\frac{1}{4}} < \ell < y$, we have

$$P_b(y; \ell, t) \ll \frac{y}{\varphi(\ell)(\log(2y/\ell))^2},$$

where the implied constant is absolute.

For any a which is an integer not equal to 0 or ± 1, we have the following theorem of Fomenko [11]:

Theorem 3 *(Fomenko). Suppose GRH holds for a on prime powers. Suppose further Hypothesis* A *of Hooley holds. Then,*

$$\sum_{p \leqslant x} \log\bigl(i_a(p)\bigr) = c_a \operatorname{li}(x) + O\left(\frac{x \log\log x}{(\log x)^2}\right),$$

where c_a is an effectively computable constant dependent on a, and where

$$\operatorname{li}(x) = \int_2^x \frac{1}{\log t}\, dt.$$

In fact, letting $t = 0$ and restricting ℓ to be a prime in the range $(\sqrt{y}/(\log y)^4, \sqrt{y}(\log y)^2]$ in Hypothesis A of Hooley is all that is needed to prove the above theorem since this gives us

$$P_b(y; \ell, 0) \ll \frac{y}{\varphi(\ell)(\log y)^2}$$

in this range.

Hooley's Hypothesis A is difficult to prove or refute, even numerically. In fact, in order to refute it, one would need to show that

$$\limsup_{\substack{y \to \infty \\ y^{1/4} < \ell \leqslant y}} \frac{P_b(y; \ell, t)}{y/\varphi(\ell)(\log(2y/\ell))^2} = \infty.$$

That is, for every y, we need to find the $\ell_y \in (y^{1/4}, y)$ that corresponds to the maximum value for

$$\frac{P_b(y; \ell, t)}{y/\varphi(\ell)(\log(2y/\ell))^2}$$

with $\ell \in (y^{1/4}, y)$. Finding this ℓ_y will become more difficult as $y \to \infty$. Also, calculating $P_b(y; \ell, t)$ is highly non-trivial.

We also note that in the above range it is sufficient to assume the Pair Correlation Conjecture instead of Hypothesis A of Hooley. For a formulation of this conjecture, see Murty and Murty [20]. In fact, this conjecture allows us to obtain error terms which are significantly better than in Theorem 1 as well as in the above theorem. It also allows us to solve Hooley's Hypothesis A in the above range as long as t is still 0.

1.2. Higher rank versions

We let $\{a_1, a_2, \dots, a_r\}$ be a multiplicatively independent set of rational numbers. That is, $a_1^{n_1} a_2^{n_2} \cdots a_r^{n_r} = 1$ with $(n_1, n_2, \dots, n_r) \in \mathbb{Z}^r$ if, and only if, $(n_1, n_2, \dots, n_r) = (0, 0, \dots, 0)$. Throughout p and q will denote prime numbers, and x, y, and z will denote positive real numbers. Let $\nu_p(a)$ be the p-adic valuation of $a \in \mathbb{Q}^*$. That is, if $a = p^n(c/d)$ with $\gcd(c,d) = \gcd(p, cd) = 1$, then $\nu_p(a) = n$. Let $\Gamma = \langle a_1, a_2, \dots, a_r \rangle$ be the subgroup of $\mathbb{Q}^*$ generated by $a_1, a_2, \dots, a_r \in \mathbb{Q}^*$. For every prime number p with $\nu_p(a) = 0$ for all $a \in \Gamma$, we define

$$\Gamma_p := \Gamma \bmod p = \{a \bmod p \colon a \in \Gamma\}.$$

For each $i \in \{1, 2, \ldots, r\}$, write $a_i = A_i/B_i$ with $A_i, B_i \in \mathbb{Z}$, $\gcd(A_i, B_i) = 1$, and $B_i > 0$. There is a unique choice for these A_i's and B_i's. We note that

$$\left\{p\colon\ \nu_p(a) \neq 0 \text{ for some } a \in \Gamma\right\} = \left\{p\colon\ p|A_iB_i \text{ for some } i \in \{1, 2, \ldots, r\}\right\}.$$

Thus, $\#\{p\colon\ \nu_p(a) \neq 0 \text{ for all } a \in \Gamma\} < \infty$, and so, we will ignore this set throughout since it only contributes $O(1)$ to any summation of interest. Notice that Γ_p is a subgroup of $\mathbb{F}_p^*$. So, we define the index of Γ modulo p as the index of Γ_p over $\mathbb{F}_p^*$ and denote it by $i_\Gamma(p)$. That is,

$$i_\Gamma(p) := \left[\mathbb{F}_p^* : \Gamma_p\right] = \frac{p-1}{|\Gamma_p|}.$$

We also define the order of Γ modulo p and denote it by $f_\Gamma(p) := |\Gamma_p|$.

We are interested in computing

$$\sum_{p \leqslant x} \log\bigl(i_\Gamma(p)\bigr).$$

In Section 2, we will prove a similar result to that of Theorem 3 for $r \geqslant 2$. However, we will not need a higher rank version of Hypothesis A of Hooley to do this. We first define the following constants:

$$\theta := \theta(r) := \begin{cases} 9/10 & \text{if } r = 2, \\ 6/7 & \text{if } r = 3, \\ 5/6 & \text{if } r \geqslant 4 \end{cases}$$

and

$$\alpha := \alpha(r) := \begin{cases} 8/5 & \text{if } r = 2, \\ 11/7 & \text{if } r = 3, \\ 14/9 & \text{if } r = 4, \\ 4/3 & \text{if } r \geqslant 5. \end{cases}$$

Theorem 4. *Let $r \geqslant 2$. Suppose GRH holds for Γ on prime powers. Then, there exists a constant c_Γ such that*

$$\sum_{p \leqslant x} \log\bigl(i_\Gamma(p)\bigr) = c_\Gamma \operatorname{li}(x) + O_\Gamma\bigl(x^\theta (\log x)^\alpha\bigr),$$

where the implied constant is dependent on r and $a_1, a_2, \ldots, a_r$.

In fact, we will be able to show that in Theorem 4, only δ-GRH is necessary, where $\delta \in [1/2, 1)$ for r sufficiently large. To do this, we first extend the definitions of θ and α as follows:

$$\theta := \theta(\delta, r) := \begin{cases} \frac{(1+\delta)(r+1)}{2r+1} & \text{if } \frac{\delta}{1-\delta} < r < \frac{1+2\delta}{1-\delta}, \\ \frac{2+\delta}{3} & \text{if } r \geqslant \frac{1+2\delta}{1-\delta} \end{cases}$$

and

$$\alpha := \alpha(\delta, r) := \begin{cases} \frac{3r+2}{2r+1} & \text{if } \frac{\delta}{1-\delta} < r \leqslant \frac{1+2\delta}{1-\delta}, \\ \frac{4}{3} & \text{if } r > \frac{1+2\delta}{1-\delta}. \end{cases}$$

We note that $\theta(1/2, r) = \theta(r)$ and $\alpha(1/2, r) = \alpha(r)$.

In Section 3, we will prove the following theorem:

Theorem 5. *Let $\delta \in [1/2, 1)$ be fixed. Suppose δ-GRH holds for Γ for some $\delta \in [1/2, 1)$ fixed. For $r > \delta/(1-\delta)$, we have*

$$\sum_{p \leqslant x} \log\bigl(i_\Gamma(p)\bigr) = \mathrm{li}(x) \sum_{d=1}^{\infty} \frac{\Lambda(d)}{n_d} + O_\Gamma\bigl(x^\theta (\log x)^\alpha\bigr),$$

where $n_d = [\mathbb{Q}(\zeta_d, a_1^{1/d}, a_2^{1/d}, \ldots, a_r^{1/d}) : \mathbb{Q}]$ and the implied constant is dependent only on r and $a_1, a_2, \ldots, a_r$.

In Theorems 4 and 5, we obtain power-saving results. That is, all of our error terms are $O(x^\theta (\log x)^\alpha)$ with $\theta < 1$ and $\alpha \in \mathbb{R}$ fixed. This is in stark contrast to Theorems 1 and 3 where error terms are of the form

$$\frac{x \log\log x}{(\log x)^2}.$$

The study of these types of questions first began with Gupta and Murty [12] (it is what originally led to the unconditional results about Artin's conjecture) and continued with Pappalardi [23] and Cangelmi and Pappalardi [3], who studied how often $\Gamma_p = (\mathbb{Z}/p\mathbb{Z})^*$, the r-rank analogue of Artin's conjecture.

We note that these results can be used to prove that the smallest prime p_Γ for which $i_\Gamma(p) \neq 1$ satisfies $p_\Gamma \ll (\log a_1 a_2 \cdots a_r)^{6+\varepsilon}$. However, by looking at the primes which split in $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_r})$ the same can be done.

In Section 4, we will prove a corollary of Theorems 4 and 5.

2. Proof of Theorem 4

2.1. The Chebotarev density theorem

The Chebotarev density theorem is one of the main tools we will need in order to prove the results stated within.

Let K be a finite Galois extension of $\mathbb{Q}$ with Galois group G, degree n_K, and discriminant d_K. Let $\pi_K(x)$ denote the number of primes $p \leqslant x$ for which p splits completely in K over $\mathbb{Q}$. Then, the following corollary of the Chebotarev density theorem [4,5] states

$$\pi_K(x) \sim \frac{\mathrm{li}(x)}{|G|} \tag{2}$$

as $x \to \infty$. The original statement of the Chebotarev density theorem is a more general statement about how frequent the conjugacy class of the Frobenius automorphism associated to p is equal to a fixed conjugacy class of G. In order to use this result, we need error terms. Such a result is due to Lagarias and Odlyzko [16]. It has been improved by Serre [24], Murty, Murty, and Saradha [21], and Murty and Murty [20]. The following version is Serre's [24] refinement of Lagarias and Odlyzko's result [16].

Theorem 6. *Let K be as above. Assuming GRH for the Dedekind zeta function of K, we have*

$$\pi_K(x) = \frac{\mathrm{li}(x)}{|G|} + O\left(\sqrt{x}\left(\frac{\log|d_K|}{n_K} + \log x\right)\right), \tag{3}$$

where the implied constant is absolute.

The following result, known as Hensel's inequality, is useful for bounding the error term in Theorems 4 and 5 (see [24, p. 130]):

Lemma 1. *Let K be a finite Galois extension with degree n_K and discriminant d_K. Then,*

$$\log|d_K| \leqslant n_K\left(\log n_K + \sum_{p \in \mathcal{P}(K/\mathbb{Q})} \log p\right), \tag{4}$$

where $\mathcal{P}(K/\mathbb{Q})$ is the set of prime numbers p which ramify in K over $\mathbb{Q}$.

2.2. The proof of Theorem 4

For $d \in \mathbb{N}$, define

$$\pi_d(x) := \#\{p \leqslant x\colon d | i_\Gamma(p)\}.$$

Then, we have

$$\sum_{p \leqslant x} \log(i_\Gamma(p)) = \sum_{d \leqslant x} \Lambda(d)\pi_d(x).$$

Let $d \in \mathbb{N}$ be a fixed integer. We note that d divides $i_\Gamma(p) = \gcd(i_{a_1}(p), i_{a_2}(p), \ldots, i_{a_r}(p))$ if, and only if, $d | i_{a_j}(p)$ for all $j \in \{1, 2, \ldots, r\}$. This is true if, and only if, p splits completely in $\mathbb{Q}(\zeta_d, a_j^{1/d})$ for all $j \in \mathbb{Q}(\zeta_d, a_j^{1/d})$. So, $d | i_\Gamma(p)$ if, and only if, p splits completely in $\mathbb{Q}(\zeta_d, a_1^{1/d}, a_2^{1/d}, \ldots, a_r^{1/d})$. We note that if a prime ramifies in $\mathbb{Q}(\zeta_d, a_1^{1/d}, a_2^{1/d}, \ldots, a_r^{1/d})$, then it must divide dP, where P is the product of all primes p with $\nu_p(a) \neq 0$ for some $a \in \Gamma$ by an argument similar to the case when Γ is generated by a single element. By Theorem 6 and Lemma 1, we have

$$\pi_d(x) = \frac{\mathrm{li}(x)}{[K_d : \mathbb{Q}]} + O\left(\sqrt{x}\log\left(xd^{r+2}P\right)\right),$$

where P is the product of primes p with $\nu_p(a) \neq 0$ for some $a \in \Gamma$, $K_d = \mathbb{Q}(\zeta_d, \Gamma^{1/d})$, and $\Gamma^{1/d} := \{a^{1/d}\colon a \in \Gamma\}$. Let $n_d = [K_d : \mathbb{Q}]$. Thus, for some y to be chosen later, we have

$$\begin{aligned}
\sum_{d \leqslant y} \Lambda(d)\pi_d(x) &= \sum_{d \leqslant y} \Lambda(d)\left(\frac{\mathrm{li}(x)}{n_d} + O\left(\sqrt{x}\log\left(xd^{(r+2)}P\right)\right)\right) \\
&= \mathrm{li}(x)\sum_{d \leqslant y} \frac{\Lambda(d)}{n_d} + O\left(\sum_{q^\alpha \leqslant y} \log q\sqrt{x}\left(\log x + \alpha(r+2)\log q + \log P\right)\right).
\end{aligned}$$

Now,

$$\sum_{d\leqslant y}\frac{\Lambda(d)}{n_d}=\sum_{d=1}^{\infty}\frac{\Lambda(d)}{n_d}-\sum_{d>y}\frac{\Lambda(d)}{n_d}.$$

We note that the first summation above is a constant since $n_d \geqslant [\mathbb{Q}(\zeta_d, a_1^{1/d}):\mathbb{Q}] \asymp d\varphi(d)$ by [27, Proposition 4.1]. We have

$$\sum_{d>y}\frac{\Lambda(d)}{n_d}\ll\sum_{d>y}\frac{\Lambda(d)}{\varphi(d)d^r}\ll\frac{1}{y}$$

by partial summation and [6, Exercise 5.5.3]. Thus,

$$\sum_{d\leqslant y}\Lambda(d)\pi_d(x)=\operatorname{li}(x)\sum_{d=1}^{\infty}\frac{\Lambda(d)}{n_d}+O\left(\frac{\operatorname{li}(x)}{y}\right)$$
$$+O\left(\sum_{q^\alpha\leqslant y}\log q\sqrt{x}\big(\log x+\alpha(r+2)\log q+\log P\big)\right).$$

Now,

$$\sqrt{x}\log x\sum_{q^\alpha\leqslant y}\log q=\sqrt{x}\log x\sum_{n\leqslant y}\Lambda(n)\ll y\sqrt{x}\log x.$$

Also,

$$\sqrt{x}\sum_{q^\alpha\leqslant y}\alpha(r+2)(\log q)^2\ll(r+2)\sqrt{x}\log y\sum_{n\leqslant y}\log n\ll y\sqrt{x}(\log y)^2,$$

and

$$\log P\sum_{q^\alpha\leqslant y}\log q=\log P\sum_{n\leqslant y}\Lambda(n)\ll y\log P.$$

We have $\log P\ll_\Gamma 1$ as P is the product (of a finite number) of (fixed) primes p which satisfy $\nu_p(a)\neq 0$ for some $a\in\Gamma$. Therefore, we have

$$\sum_{d\leqslant y}\Lambda(d)\pi_d(x)=\operatorname{li}(x)\sum_{d=1}^{\infty}\frac{\Lambda(d)}{n_d}+O\left(\frac{\operatorname{li}(x)}{y}+y\sqrt{x}\log x+y\sqrt{x}(\log y)^2\right).$$

Now, we must deal with

$$\sum_{y<d\leqslant x}\Lambda(d)\pi_d(x).$$

We have

$$\sum_{y<d\leqslant x} \Lambda(d)\pi_d(x) \ll \log x \sum_{y<q^\alpha\leqslant x} \pi_{q^\alpha}(x)$$
$$= \log x \sum_{y<q^\alpha\leqslant x} \#\{p \leqslant x\colon q^\alpha | i_\Gamma(p)\}.$$

Let us consider

$$\sum_{y<q^\alpha\leqslant x} \#\{p \leqslant x\colon q^\alpha | i_\Gamma(p)\} = \sum_{y<q\leqslant x} \#\{p \leqslant x\colon q | i_\Gamma(p)\} + \sum_{\substack{y<q^\alpha\leqslant x\\ \alpha>1}} \#\{p \leqslant x\colon q^\alpha | i_\Gamma(p)\}.$$

Let

$$y = \frac{x^\Theta}{(\log x)^A},$$

where

$$\Theta = \begin{cases} 2/5 & \text{if } r = 2,\\ 5/14 & \text{if } r = 3,\\ 1/3 & \text{if } r \geqslant 4 \end{cases}$$

and

$$A = \begin{cases} 2/5 & \text{if } r = 2,\\ 3/7 & \text{if } r = 3,\\ 4/9 & \text{if } r = 4,\\ 2/3 & \text{if } r \geqslant 5. \end{cases}$$

We note $\Theta \geqslant 1/3$ for all $r \geqslant 2$.

We note that

$$\sum_{\substack{y<q^\alpha\leqslant x\\ \alpha>1}} \#\{p \leqslant x\colon q^\alpha | i_\Gamma(p)\} \ll \sum_{\substack{y<q^\alpha\leqslant x\\ \alpha>1}} \frac{x}{q^\alpha} \ll \frac{x}{\sqrt{y}}.$$

We also claim

$$\sum_{y<q\leqslant x} \#\{p \leqslant x\colon q | i_\Gamma(p)\} \ll \#\left\{p\colon |\Gamma_p| \leqslant \frac{x}{y}\right\}.$$

To see this, suppose the prime number p contributes to the left-hand side. That is, suppose there exist primes $q_1, q_2, \dots, q_n \in (y, x]$ such that $q_i | i_{\Gamma(p)}$. Since $q_1, q_2, \dots, q_n \in (y, x]$ are distinct,

$$\frac{x^{n\Theta}}{(\log x)^{An}} = y^n < q_1 q_2 \cdots q_n < i_\Gamma(p) < x.$$

Therefore, $n \leqslant \Theta^{-1} \leqslant 3$ for x sufficiently large. Thus,

$$\sum_{y<q\leqslant x} \#\{p \leqslant x\colon q|i_\Gamma(p)\} \ll \#\left\{p\colon |\Gamma_p| \leqslant \frac{x}{y}\right\}.$$

However, before we can bound this latter quantity, let us recall the following result of Gupta and Murty [12]:

Lemma 2 *(Gupta and Murty). Suppose $r \geqslant 2$. Then*

$$\#\{p\colon |\Gamma_p| \leqslant t\} \ll t^{1+\frac{1}{r}},$$

where the implied constant is dependent on at most r and $a_1, a_2, \ldots, a_r$.

Thus, we have

$$\sum_{y<q\leqslant x} \#\{p \leqslant x\colon q|i_\Gamma(p)\} \ll \left(\frac{x}{y}\right)^{\frac{r+1}{r}}.$$

Therefore,

$$\begin{aligned}\sum_{p\leqslant x} \log\bigl(i_\Gamma(p)\bigr) &= \mathrm{li}(x)\sum_{d=1}^{\infty}\frac{\Lambda(d)}{n_d} + O\left(\frac{\mathrm{li}(x)}{y}\right) + O\bigl(y\sqrt{x}\log x\bigr)\\ &\quad + O\bigl(y\sqrt{x}(\log y)^2\bigr) + O\left(\frac{x}{\sqrt{y}}\log x\right) + O\left(\left(\frac{x}{y}\right)^{\frac{r+1}{r}}\log x\right)\\ &= \mathrm{li}(x)\sum_{d=1}^{\infty}\frac{\Lambda(d)}{n_d} + O\bigl(x^{1-\Theta}(\log x)^A\bigr) + O\left(\frac{x^{\frac{1}{2}+\Theta}}{(\log x)^{A-2}}\right)\\ &\quad + O\bigl(x^{1-\frac{\Theta}{2}}(\log x)^{\frac{A}{2}+1}\bigr) + O\bigl(x^{\frac{(1-\Theta)(r+1)}{r}}(\log x)^{A+\frac{A}{r}+1}\bigr).\end{aligned}$$

Therefore, Theorem 4 holds.

3. Proof of Theorem 5

Recall that p splits completely in $\mathbb{Q}(\zeta_d, a_1^{1/d}, a_2^{1/d}, \ldots, a_r^{1/d})$ if, and only if, $d|i_\Gamma(p)$. Also, recall $\pi_d(x) := \#\{p \leqslant x\colon\ d|i_\Gamma(p)\}$. Therefore, by the δ-GRH and the Chebotarev density theorem (mimicking Lagarias and Odlyzko [16] and Serre [24]), we have

$$\pi_d(x) = \frac{\mathrm{li}(x)}{[K_d : \mathbb{Q}]} + O\bigl(x^\delta \log\bigl(xd^{r+2}P\bigr)\bigr),$$

where P is the product of all primes p satisfying $\nu_p(a) \neq 0$ for some $a \in \Gamma$.

Let

$$\Theta := \Theta(\delta, r) := \begin{cases} \frac{r(1-\delta)+1}{2r+1} & \text{if } \frac{\delta}{1-\delta} < r < \frac{1+2\delta}{1-\delta},\\ \frac{2(1-\delta)}{3} & \text{if } r \geqslant \frac{1+2\delta}{1-\delta}\end{cases}$$

and

$$A := A(\delta, r) := \begin{cases} \frac{r}{2r+1} & \text{if } \frac{\delta}{1-\delta} < r \leqslant \frac{1+2\delta}{1-\delta}, \\ \frac{2}{3} & \text{if } r > \frac{1+2\delta}{1-\delta}. \end{cases}$$

Note that Θ and A in the proof of Theorem 4 are equal to $\Theta(1/2, r)$ and $A(1/2, r)$, respectively.

Let $y = x^{\Theta}/(\log x)^{A}$. Since $\Theta > 0$, all the arguments from the previous section are still true, and we have

$$\sum_{p \leqslant x} \log\bigl(i_\Gamma(p)\bigr) = \operatorname{li}(x) \sum_{d=1}^{\infty} \frac{\Lambda(d)}{n_d} + O\left(\frac{x^{\delta+\Theta}}{(\log x)^{A-2}}\right) + O\bigl(x^{1-\frac{\Theta}{2}} (\log x)^{\frac{A}{2}+1}\bigr) + O\bigl(x^{\frac{(1-\Theta)(r+1)}{r}} (\log x)^{A+\frac{A}{r}+1}\bigr).$$

This completes the proof of Theorem 5 with

$$c_\Gamma = \sum_{d=1}^{\infty} \frac{\Lambda(d)}{n_d}.$$

It should be noted that $\Theta < 1$ for all $\delta \in [1/2, 1)$ and $r > \delta/(1-\delta)$. To see this we note that for case 1,

$$\frac{(1+\delta)(r+1)}{2r+1} < 1.$$

This is true if, and only if,

$$r > \frac{\delta}{1-\delta}.$$

For case 2, we have

$$\frac{2+\delta}{3} < 1.$$

Therefore, as when we assumed GRH, we have obtained power-saving error terms as long as $r > \delta/(1-\delta)$. We can use the above inequalities on r to determine corresponding inequalities for δ if so desired. Doing this yields the following theorem:

Theorem 7. *Let $r \geqslant 2$ and let $\delta < r/(r+1)$. Let θ and α be defined as in Theorem 5. Suppose δ-GRH holds for Γ on prime powers. Then, we have*

$$\sum_{p \leqslant x} \log\bigl(i_\Gamma(p)\bigr) = \operatorname{li}(x) \sum_{d=1}^{\infty} \frac{\Lambda(d)}{n_d} + O\bigl(x^{\theta} (\log x)^{\alpha}\bigr),$$

where $n_d := [\mathbb{Q}(\zeta_d, a_1^{1/d}, a_2^{1/d}, \ldots, a_r^{1/d}) : \mathbb{Q}]$ and the implied constant is dependent on r and $a_1, a_2, \ldots, a_r$.

4. An immediate corollary

We have the following corollary of Theorems 4 and 5:

Corollary 1. *Let $r \geqslant 2$ and $\delta \in [1/2, 1)$ with $\delta < r/(r+1)$. Suppose δ-GRH holds for Γ on prime powers.*

$$\sum_{p \leqslant x} \log\bigl(f_\Gamma(p)\bigr) = x - c_\Gamma \operatorname{li}(x) + O_{r,\Gamma}\bigl(x^\theta (\log x)^A\bigr),$$

where $\theta = \theta(\delta, r)$ and $\alpha = \alpha(\delta, r)$ in Theorem 5.

Proof. Note that

$$\begin{aligned}
\sum_{p \leqslant x} \log\bigl(f_\Gamma(p)\bigr) &= \sum_{p \leqslant x} \log(p-1) - \sum_{p \leqslant x} \log\bigl(i_\Gamma(p)\bigr) \\
&= \sum_{p \leqslant x} \log p + \sum_{p \leqslant x} \log\left(\frac{p-1}{p}\right) - \sum_{p \leqslant x} \log\bigl(i_\Gamma(p)\bigr) \\
&= \sum_{p \leqslant x} \log p - \sum_{p \leqslant x} \log\bigl(i_\Gamma(p)\bigr) + O(\log\log x).
\end{aligned}$$

Also, from Theorem 4 or 5, we have

$$\sum_{p \leqslant x} \log\bigl(i_\Gamma(p)\bigr) = c_\Gamma \operatorname{li}(x) + O\bigl(x^\theta (\log x)^\alpha\bigr).$$

So, we need to evaluate

$$\sum_{p \leqslant x} \log p.$$

We note that by the Aramata–Brauer theorem (see [8, §11.4] or [19, §2.3]), the δ-Riemann hypothesis (that is, the δ-GRH for $K = \mathbb{Q}$) is also true since our extension is Galois. That is, there are no zeros of the Riemann zeta function in the region $\Re(s) > \delta$ and $\delta \in [1/2, 1)$. Therefore, we may assume

$$\pi(x) = \operatorname{li}(x) + O\bigl(x^\delta \log x\bigr),$$

or equivalently,

$$\theta(x) := \sum_{p \leqslant x} \log p = x + O\bigl(x^\delta (\log x)^2\bigr).$$

Putting all of this together we obtain

$$\begin{aligned}
\sum_{p \leqslant x} \log\bigl(f_\Gamma(p)\bigr) &= x + O\bigl(x^\delta (\log x)^2\bigr) - c_\Gamma \operatorname{li}(x) + O\bigl(x^\theta (\log x)^\alpha\bigr) \\
&= x - c_\Gamma \operatorname{li}(x) + O\bigl(x^\theta (\log x)^A\bigr)
\end{aligned}$$

since $\theta > \delta$. $\square$

Acknowledgments

Some portions of this work were part of the doctoral thesis of the author [9]. The author would like to thank M. Ram Murty, his supervisor, for comments on previous versions of this paper and guidance throughout the author's graduate school years at Queen's University. The author would also like to thank Amir Akbary and Pieter Moree for their comments on earlier versions of this work. Finally, the author would like to thank the referee for a careful reading of an earlier version of this work.

References

[1] Emil Artin, Collected Papers, Addison–Wesley, Reading, MA, 1965.
[2] Eric Bach, Richard Lukes, Jeffrey Shallit, Hugh Cowie Williams, Results and estimates on pseudoprimes, Math. Comp. 65 (1996) 1737–1747.
[3] Leonardo Cangelmi, Francesco Pappalardi, On the r-rank Artin conjecture, II, J. Number Theory 75 (1) (1999) 120–132.
[4] Nikolai Chebotarëv, Opredelenie plotnosti sovokupnosti prostykh chisel, prinadlezhashchikh zadannomu klassu podstanovok (Determination of the density of the set of prime numbers, belonging to a given substitution class), Izv. Ross. Akad. Nauk 17 (1923) 205–250.
[5] Nikolai Chebotarëv, Die Bestimmung der Dichtigkeit einer Menge Von Primzahlen, welche zu einer gegebeben Substitutionsklasse gehören, Math. Ann. 95 (1925) 191–228.
[6] Alina Carmen Cojocaru, M. Ram Murty, An Introduction to Sieve Methods and Their Applications, Cambridge University Press, New York, 2006.
[7] Peter D.T.A. Elliott, Leo Murata, On the average of the least primitive root modulo p, J. London Math. Soc. (2) 56 (1997) 435–454.
[8] Jody Esmonde, M. Ram Murty, Problems in Algebraic Number Theory, Springer-Verlag, New York, 2005.
[9] Adam Tyler Felix, Variations on Artin's primitive root conjecture, PhD thesis, Queen's University, 2011.
[10] Adam Tyler Felix, M. Ram Murty, A problem of Fomenko's related to Artin's conjecture, Int. J. Number Theory 8 (7) (2012) 1687–1723, http://dx.doi.org/10.1142/S1793042112500984.
[11] O.M. Fomenko, Class number of indefinite binary quadratic forms and the residual indices of integers modulo p, J. Math. Sci. 122 (6) (2004) 3685–3698.
[12] Rajiv Gupta, M. Ram Murty, A remark on Artin's conjecture, Invent. Math. 78 (1984) 127–130.
[13] D.R. Heath-Brown, Artin's conjecture for primitive roots, Quart. J. Math. Oxford 37 (1986) 27–38.
[14] Christopher Hooley, On Artin's conjecture, J. Reine Angew. Math. 225 (1967) 209–220.
[15] Christopher Hooley, Applications of Sieve Methods to the Theory of Numbers, Cambridge University Press, Cambridge, Great Britain, 1976.
[16] Jeffrey Lagarias, Andrew Odlyzko, Effective versions of the Chebotarev density theorem, in: Albrecht Fröhlich (Ed.), Algebraic Number Fields, Academic Press, Inc., New York, 1977, pp. 409–464.
[17] Derrick H. Lehmer, Emma Lehmer, Heuristics anyone?, in: G. Szego, et al. (Eds.), Studies in Mathematical Analysis and Related Topics, Stanford University Press, Stanford, CA, 1962.
[18] Leo Murata, A problem analogous to Artin's conjecture for primitive roots and its applications, Arch. Math. 57 (1991) 555–565.
[19] M. Ram Murty, V. Kumar Murty, Non-Vanishing of L-Functions and Applications, Birkhäuser Verlag, Basel, Switzerland, 1997.
[20] M. Ram Murty, V. Kumar Murty, The Chebotarev density theorem and pair correlation of zeros of Artin L-functions, preprint, 2004, pp. 1–19.
[21] M. Ram Murty, V. Kumar Murty, N. Saradha, Modular forms and the Chebotarev density theorem, Amer. J. Math. 110 (1988) 253–281.
[22] Francesco Pappalardi, On Hooley's theorem with weights, Rend. Semin. Mat. Univ. Politec. Torino 53 (1995) 375–388.
[23] Francesco Pappalardi, On the r-rank Artin conjecture, Math. Comp. 66 (1997) 853–868.
[24] Jean-Pierre Serre, Quelques applications du théorème de densité de Chebotarev, Publ. Math. Inst. Hautes Études Sci. 54 (1981) 323–401.
[25] P.J. Stephens, Prime divisors of second-order linear recurrences. I, J. Number Theory 8 (1976) 313–332.
[26] P. Stevenhagen, The correction factor in Artin's primitive root conjecture, J. Théor. Nombres Bordeaux 15 (1) (2003) 383–391.
[27] Samuel S. Wagstaff Jr., Pseudoprimes and a generalization of Artin's conjecture, Acta Arith. 41 (1982) 141–150.