International Journal of Number Theory
Vol. 8, No. 7 (2012) 1687–1723

DOI: 10.1142/S1793042112500984

A PROBLEM OF FOMENKO'S RELATED TO ARTIN'S CONJECTURE

ADAM TYLER FELIX
Max Planck Institut für Mathematik
Vivatsgasse 7, 53111 Bonn, Germany
felix@mpim-bonn.mpg.de

M. RAM MURTY
Department of Mathematics and Statistics
Queen's University, 99 University Avenue
Kingston, ON, Canada, K7L 3N6
murty@mast.queensu.ca

Received 3 August 2011
Accepted 26 April 2012
Published 27 August 2012

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 Conjecture A of Hooley, Fomenko proved in 2004 that the average value of $i_a(p)$ is constant. We prove that the average value of $i_a(p)$ is constant without using Conjecture A of Hooley. More precisely, we show upon GRH that for any α with $0 \leq \alpha < 1$, there is a positive constant $c_\alpha > 0$ such that

$$\sum_{p \leq x} (\log i_a(p))^\alpha \sim c_\alpha \pi(x),$$

where $\pi(x)$ is the number of primes $p \leq x$. We also study related questions.

Keywords: Artin's conjecture; truncated divisor function; prime numbers.

Mathematics Subject Classification 2010: 11N37, 11N36, 11N25

1. Introduction

Let $p \in \mathbb{N}$ be a prime number. Let us consider $(\mathbb{Z}/p\mathbb{Z})^* := \{a \pmod p : p \nmid a\}$. Then $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. That is, there exists $a \in \mathbb{Z}$ such that $(\mathbb{Z}/p\mathbb{Z})^* = \langle a \pmod p \rangle$. In this case we say that a is a *primitive root modulo* p. In fact, it can also be shown that the number of generators of $(\mathbb{Z}/p\mathbb{Z})^*$ which have the form $a \pmod p$ in $(\mathbb{Z}/p\mathbb{Z})^*$ is $\varphi(p-1)$ where $\varphi(n) = \#\{1 \leq k \leq n : \gcd(k,n) = 1\}$. In [16, Article 57], Gauss used primitive roots to discuss the periodicity of the decimal expansion of $1/p$ for primes p not equal to 2 or 5. Both Euler and Jacobi used primitive roots before Gauss.

In 1927, Artin made the following conjecture (see [1, Introduction; 19]): let a be a fixed integer such that $a \neq 0, \pm 1$ or a perfect square. Let $a = b^h$ where b is an integer which is not a perfect power and $h \in \mathbb{N}$. Define $N_a(x) := \#\{p \leq x : (\mathbb{Z}/p\mathbb{Z})^* = \langle a \pmod p \rangle\}$. That is, $N_a(x)$ is the number of primes $p \leq x$ for which a is a primitive root modulo p. Then

$$N_a(x) \sim A_h \pi(x), \tag{1.1}$$

where $\pi(x) := \#\{p \leq x : p \text{ prime}\}$ and

$$A_h = \prod_{\substack{q|h \\ q \text{ prime}}} \left(1 - \frac{1}{q-1}\right) \prod_{\substack{q \nmid h \\ q \text{ prime}}} \left(1 - \frac{1}{q(q-1)}\right) > 0. \tag{1.2}$$

The heuristic behind this conjecture is based on the following idea: we have a is primitive root modulo p if and only if for all q which are prime the following conditions do not occur:

$$p \equiv 1 \pmod q, \tag{1.3}$$

$$a^{\frac{p-1}{q}} \equiv 1 \pmod q. \tag{1.4}$$

The first condition above occurs with a density of $1/\varphi(q) = 1/(q-1)$ of the primes by Dirichlet's theorem on primes in arithmetic progression. The second condition above 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 those.

Artin's conjecture is still unresolved. However, Hooley [19] provided the following conditional resolution.

Theorem 1.1 (Hooley). *Suppose $a \in \mathbb{Z}$ such that $a \neq 0, \pm 1$ or a perfect square. Suppose further that the generalized Riemann hypothesis holds for Dedekind zeta functions for the fields $\mathbb{Q}(\zeta_k, a^{1/k})$ with $k \in \mathbb{N}$ squarefree and where ζ_k is a primitive kth root of unity. Then,*

$$N_a(x) = A(a)\pi(x) + O\left(\frac{x \log\log x}{(\log x)^2}\right), \tag{1.5}$$

where the implied constant depends on a.

Hereafter, the generalized Riemann hypothesis will be denoted by GRH.

It should be noted that $A(a)$ in (1.5) is different from A_h in (1.2). It was discovered by Lehmer and Lehmer [26] that the constant deviated from the conjectural constant, and once informed, Artin made the corresponding correction (see [34]). 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

$$A(a) = A_h \left(1 - \mu(|a_1|) \prod_{\substack{q|\gcd(h,a_1) \\ q \text{ prime}}} \frac{1}{q-2} \prod_{\substack{q \nmid h \\ q|a_1 \\ q \text{ prime}}} \frac{1}{q^2-q-1}\right). \tag{1.6}$$

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

$$\#\{p \leq x : a \text{ is a primitive root modulo } p\} \geq \frac{cx}{(\log x)^2}, \tag{1.7}$$

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 [17] and Heath-Brown [18]. 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 $p \nmid a$. Then, define the *order of* a $(\text{mod } p)$, denoted $f_a(p)$, as

$$f_a(p) := \min\{k \in \mathbb{N} : a^k \equiv 1 \ (\text{mod } p)\} = |\langle a \ (\text{mod } p)\rangle|. \tag{1.8}$$

Since $p \nmid a$, $f_a(p)$ is well-defined by Fermat's little theorem. Define the *index of* a $(\text{mod } p)$, denoted $i_a(p)$, as

$$i_a(p) := [(\mathbb{Z}/p\mathbb{Z})^* : \langle a \ (\text{mod } p)\rangle] = \frac{p-1}{f_a(p)}. \tag{1.9}$$

We now reformulate Artin's conjecture in the following manner:

$$N_a(x) = \sum_{p \leq x} \chi_{\{1\}}(i_a(p)), \tag{1.10}$$

where, for $\mathcal{S} \subset \mathbb{N}$,

$$\chi_{\mathcal{S}}(n) = \begin{cases} 0 & \text{if } n \notin \mathcal{S}, \\ 1 & \text{if } n \in \mathcal{S}. \end{cases} \tag{1.11}$$

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

$$\sum_{p \leq x} f(i_a(p)) \sim c_{a,f}\pi(x), \tag{1.12}$$

where $c_{a,f}$ is a constant dependent on f and a? This question was first studied by Stephens [33], and then by Wagstaff [36], Murata [28], Elliott and Murata [8], Pappalardi [31], Bach *et al.* [2], and Fomenko [12] among others. It is investigated in detail in [11]. 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.

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 [12] proved it using GRH and Conjecture A of Hooley [20, p. 112]:

$$\sum_{p \leq x} \log(i_a(p)) \sim c_a \mathrm{li}(x) \tag{1.13}$$

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

Pappalardi [31] proved the following related theorem.

Theorem 1.2 (Pappalardi). *Let a be an integer different from 0 and ± 1. We have*

$$\frac{x}{\log x} \ll \sum_{p \leq x} \log(i_a(p)) \ll_a \frac{x \log\log x}{\log x}, \tag{1.14}$$

where the lower bound is unconditional, and we suppose the GRH holds for the Dedekind zeta functions for the fields $\mathbb{Q}(\zeta_k, a^{1/k})$ where ζ_k is a primitive kth root of unity as k ranges over prime powers for the upper bound.

Before we can state a result of Fomenko's we need to state the following conjecture of Hooley [20, p. 112].

Conjecture 1.3 (Conjecture A of Hooley). *Let $P_b(y; \ell, t)$ be the number of primes $p \leq y$ 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*

$$P_b(y; \ell, t) \ll \frac{y}{\varphi(\ell)(\log(2y/\ell))^2}, \tag{1.15}$$

where the implied constant is absolute.

For any integer a not equal to 0, ± 1, we have the following theorem of Fomenko [12].

Theorem 1.4 (Fomenko). *Suppose the GRH holds for Dedekind zeta functions for the fields $\mathbb{Q}(\zeta_k, a^{1/k})$ where ζ_k is a primitive kth root of unity and where k ranges over prime powers. Suppose further that Conjecture A of Hooley holds. Then*

$$\sum_{p \leq x} \log(i_a(p)) = c_a \mathrm{li}(x) + O\left(\frac{x \log\log x}{(\log x)^2}\right), \tag{1.16}$$

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

$$\mathrm{li}(x) = \int_2^x \frac{1}{\log t} dt. \tag{1.17}$$

In fact, letting $t = 0$ and restricting ℓ to the range $(\frac{\sqrt{y}}{(\log y)^4}, \sqrt{y}(\log y)^2]$ in Conjecture A of Hooley is all that is needed to prove the above theorem.

Our goal is to remove Conjecture A of Hooley from the work of Fomenko. We note that we will not be able to remove Conjecture A from the above case of $f(n) = \log n$. However, our technique narrowly misses this case. We will prove a similar result for $f(n) = (\log n)^\alpha$ where $\alpha \in (0, 1)$ is fixed upon GRH but not upon Conjecture A of Hooley.

We also note that in the above range it is sufficient to assume the Pair Correlation Conjecture instead of Conjecture A of Hooley. For a formulation of this conjecture see [29]. In fact, this conjecture allows us to obtain error terms which are significantly better than in Theorem 1.1 as well as in the above theorem.

1.2. *Conventions*

Throughout, a will denote an integer different from 0 and ± 1. The letters p and q will denote prime numbers with $p \nmid a$. We note that this will not affect the proofs as there are only finitely many primes which divide a. Also, d, k, m, n, and w will denote positive integers, and x, y, and z will denote positive real numbers.

By the notation $f(x) = O(g(x))$ or $f(x) \ll g(x)$, we mean that there exists a constant C such that for all x in the domain of f and g we have $|f(x)| \leq Cg(x)$. By $f(x) = O_a(g(x))$ or $f(x) \ll_a g(x)$ we mean that the above constant is dependent on a. This notation may be dropped in proofs for convenience. By $f(x) \sim g(x)$ we mean

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1, \tag{1.18}$$

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 "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 "quasi-Riemann hypothesis holds for a on $A \subset \mathbb{N}$ (at ε)" will hereafter signify "there exists $\varepsilon \in (0, 1/2]$ such that if $\Re(s) > 1 - \varepsilon$, then $\zeta_{K_n}(s) \neq 0$ for all $K_n = \mathbb{Q}(\zeta_n, a^{1/n})$ with n ranging over all values of $A \subset \mathbb{N}$."

For $b, k \in \mathbb{N}$ with $\gcd(b, k) = 1$, define $\pi(x; k, b) = \#\{p \leq x : p \equiv b \pmod{k}\}$. For $d \in \mathbb{N}$, define

$$\pi_d(x) := \#\{p \leq x : d \,|\, i_a(p)\}. \tag{1.19}$$

We also define the following arithmetic functions: for all $n \in \mathbb{N}$, we have

$$\begin{aligned}\Lambda(n) &:= \begin{cases}\log p & \text{if } n = p^\alpha \text{ for some } \alpha \in \mathbb{N},\\ 0 & \text{otherwise,}\end{cases}\\ \omega(n) &:= \#\{p|n\},\\ \Omega(n) &:= \#\{p^\alpha|n : \alpha \in \mathbb{N}\},\\ \tau(n) &:= \#\{d|n\},\end{aligned} \tag{1.20}$$

and, for $k \in \mathbb{N}$,

$$\tau_k(n) := \#\{(a_1, a_2, \ldots, a_k) \in \mathbb{N}^k : n = a_1 a_2 \cdots a_k\}. \tag{1.21}$$

The function Λ is known as the von Mangoldt function. Also, the index of $a \pmod p$ and order of $a \pmod p$ are defined as before and denoted by $i_a(p)$ and $f_a(p)$, respectively.

1.3. *Problem setup*

Let $f : \mathbb{N} \to \mathbb{C}$. We now ask when does the following relation hold for $f : \mathbb{N} \to \mathbb{C}$:

$$\sum_{p \le x} f(i_a(p)) \sim c_{a,f}\pi(x), \tag{1.22}$$

where $c_{a,f}$ is a constant dependent on at most a and f?

We note that if we write

$$f(n) = \sum_{d|n} g(d), \tag{1.23}$$

where $g : \mathbb{N} \to \mathbb{C}$, then

$$\sum_{p \le x} f(i_a(p)) = \sum_{p \le x} \sum_{d|i_a(p)} g(d) = \sum_{d \le x} g(d) \sum_{\substack{p \le x\\ d|i_a(p)}} 1 = \sum_{d \le x} g(d)\pi_d(x). \tag{1.24}$$

We note that it is always possible to write

$$f(n) = \sum_{d|n} g(d) \tag{1.25}$$

by the Möbius inversion formula (see [6, Theorem 1.2.2]).

Assuming $g : \mathbb{N} \to \mathbb{C}$ is well-behaved, we have no difficulty applying standard techniques to obtain results of this nature. This is due to the fact that $d|i_a(p)$ if and only if p splits completely in $\mathbb{Q}(\zeta_d, a^{1/d})$ where ζ_d is a primitive dth root of unity (see Sec. 2.1). For example, $f(n) = \omega(n)$ and $f(n) = \Omega(n)$ easily fall into this category (see Sec. 7). However, more complicated functions cause difficulties if we try to use the standard techniques. For example, $f(n) = \log n$ or $f(n) = \tau(n)$ cause

difficulties when considering intermediate primes and large divisors, respectively. To see this, let us consider the following summation:

$$\begin{aligned}\sum_{p\le x}\log(i_a(p)) &= \sum_{p\le x}\sum_{d\mid i_a(p)}\Lambda(d)\\ &= \sum_{d\le\frac{\sqrt{x}}{(\log x)^B}}\Lambda(d)\pi_d(x) + \sum_{\frac{\sqrt{x}}{(\log x)^B}<d\le\sqrt{x}(\log x)^A}\Lambda(d)\pi_d(x)\\ &\quad + \sum_{\sqrt{x}(\log x)^A<d\le x}\Lambda(d)\pi_d(x), \end{aligned}\tag{1.26}$$

where $A, B > 0$ are fixed. Here we have used the fact that

$$\log n = \sum_{d\mid n}\Lambda(d)\tag{1.27}$$

for all $n \in \mathbb{N}$.

Now, the effective Chebotarev density theorem and GRH allow us to handle the first summation (see Sec. 3). Techniques of Hooley [19, Eq. (3)] allow us to handle the last summation. However, there is currently no method that allows us to bound the second summation adequately without assuming something beyond the reach of GRH and the Chebotarev density theorem. This is where Fomenko [12] assumed Conjecture A of Hooley. Similar difficulties exist for $f(n) = \tau(n)$, but they are more difficult because in the last summation Hooley's argument [19, Eq. (3)] no longer applies.

1.4. *Statement of theorems*

We will discuss a new technique that eliminates some of the aforementioned difficulties if we only assume GRH. The only aforementioned difficulty which we have discussed which this technique does not resolve is the case of the function $f(n) = \log n$.

We will prove the following theorem in Sec. 4.

Theorem 1.5. *Suppose GRH holds for a on $\mathbb{N}$. Let $\alpha \in (0,1)$ be fixed. Then, for any $\varepsilon > 0$, we have*

$$\sum_{p\le x}(\log i_a(p))^\alpha = c_{a,\alpha}\mathrm{li}(x) + O_a\left(\frac{x}{(\log x)^{2-\varepsilon-\alpha}}\right),\tag{1.28}$$

where $c_{a,\alpha}$ is a constant.

In Sec. 5, we will prove the following theorem.

Theorem 1.6. *Suppose GRH holds for a on $\mathbb{N}$. Then, for any $\varepsilon > 0$, we have*

$$\sum_{p\le x}\tau(i_a(p)) = c_{a,\tau}\mathrm{li}(x) + O_a\left(\frac{x}{(\log x)^{2-\varepsilon}}\right),\tag{1.29}$$

where

$$c_{a,\tau} = \sum_{d \geq 1} \frac{1}{[K_d : \mathbb{Q}]} \tag{1.30}$$

is a positive constant.

We will give an alternate proof of Theorem 1.6 in Sec. 6. This proof will generalize to the following theorem, which is also proven in Sec. 6.

Theorem 1.7. *Suppose GRH holds for a on $\mathbb{N}$. Let $f : \mathbb{N} \to \mathbb{C}$ and $g : \mathbb{N} \to \mathbb{C}$ be such that*

$$f(n) = \sum_{d|n} g(d) \tag{1.31}$$

for all $n \in \mathbb{N}$. Let $\alpha \in \mathbb{R}$ be fixed with $0 \leq \alpha < 1$, and let $k, r \in \mathbb{N}$ be fixed such that $|g(n)| \ll \tau_k(n)^r (\log n)^\alpha$ for all $n \in \mathbb{N}$ where the implied constant may depend on r, k and α. Then, there exists a constant $c_{a,f}$ such that

$$\sum_{p \leq x} f(i_a(p)) = c_{a,f} \mathrm{li}(x) + O_a\left(\frac{x}{(\log x)^{2-\varepsilon-\alpha}}\right) \tag{1.32}$$

for all $\varepsilon > 0$.

Note that this immediately implies the following corollary.

Corollary 1.8. *Suppose GRH holds for a on $\mathbb{N}$. Then, for any $\varepsilon > 0$, we have*

$$\sum_{p \leq x} \omega(i_a(p))^k = c_{a,\omega^k} \mathrm{li}(x) + O_a\left(\frac{x}{(\log x)^{2-\varepsilon}}\right), \tag{1.33}$$

$$\sum_{p \leq x} \Omega(i_a(p))^k = c_{a,\Omega^k} \mathrm{li}(x) + O_a\left(\frac{x}{(\log x)^{2-\varepsilon}}\right), \tag{1.34}$$

$$\sum_{p \leq x} 2^{k\omega(i_a(p))} = c_{a,\omega,k} \mathrm{li}(x) + O_a\left(\frac{x}{(\log x)^{2-\varepsilon}}\right), \tag{1.35}$$

and

$$\sum_{p \leq x} \tau_k(i_a(p))^r = c_{a,\tau_k^r} \mathrm{li}(x) + O_a\left(\frac{x}{(\log x)^{2-\varepsilon}}\right), \tag{1.36}$$

where $c_{a,\omega^k}, c_{a,\Omega^k}, c_{a,\omega,k}$, and c_{a,τ_k^r} are positive constants.

Proof. Let $f : \mathbb{N} \to \mathbb{C}$ be one of the functions $\omega(n)^k, \Omega(n)^k, 2^{k\omega(n)}$ or $\tau_k(n)^r$ with $k, r \in \mathbb{N}$ fixed. Then, by the Möbius inversion formula [6, Theorem 1.2.2], there exists $g : \mathbb{N} \to \mathbb{C}$ such that

$$f(n) = \sum_{d|n} g(d) \tag{1.37}$$

for all $n \in \mathbb{N}$. In fact, we have

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \tag{1.38}$$

for all $n \in \mathbb{N}$. Hence,

$$|g(n)| \leq \sum_{d|n} f\left(\frac{n}{d}\right) \leq \sum_{d|n} f(n) \leq \tau(n) f(n) \ll \tau_k(n)^{r+1} \tag{1.39}$$

since $\omega(n) \leq \Omega(n), 2^{\omega(n)} \leq \tau(n) \leq \tau_k(n)$ for all n and k, and since $f(d) \leq f(n)$ for all choices of f and $d|n$, and $2^{\omega(n)}$ is the number of squarefree divisors of n. □

These are new functions for which this relation holds. See [31] for more functions which can be developed from previous techniques.

In Sec. 7, we will prove the following theorems.

Theorem 1.9. *Suppose GRH holds for a on primes. Then*

$$\sum_{p \leq x} \omega(i_a(p)) = c_{a,\omega} \mathrm{li}(x) + O_a\left(\frac{x \log\log x}{(\log x)^2}\right), \tag{1.40}$$

where $c_{a,\omega} > 0$ is a constant dependent on a.

Theorem 1.10. *Suppose GRH holds for a on prime powers. Then*

$$\sum_{p \leq x} \Omega(i_a(p)) = c_{a,\Omega} \mathrm{li}(x) + O_a\left(\frac{x \log\log x}{(\log x)^2}\right), \tag{1.41}$$

where $c_{a,\Omega} > 0$ is a constant dependent on a.

2. Outline of Proofs

In order to evaluate the summations in question and $\pi_d(x) = \#\{p \leq x : d|i_a(p)\}$ in particular, we need the following classical result.

Lemma 2.1. *Let $d \in \mathbb{N}$ be fixed. Let p be a prime with $p \nmid a$. Then, $d|i_a(p)$ if and only if p splits completely in the field $\mathbb{Q}(\zeta_d, a^{1/d})$.*

Proof. We note that $d|i_a(p)$ if and only if $p \equiv 1 \pmod{d}$ and $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$. This second condition is equivalent to the $\nu^d \equiv a \pmod{p}$ having a solution modulo p. Thus, $d|i_a(p)$ if and only if $p \equiv 1 \pmod{d}$ and $\nu^d \equiv a \pmod{p}$ has a solution modulo p. These two conditions together imply that the polynomial $x^d - a$ splits into linear factors in $\mathbb{F}_p[x]$ by [10, Theorem 5.5.1]. Thus, if $d|i_a(p)$, then p splits completely in $\mathbb{Q}(a^{1/d})$. The condition $p \equiv 1 \pmod{d}$ gives us p splits completely in $\mathbb{Q}(\zeta_d)$. Thus, by algebraic number theory, p splits completely in $\mathbb{Q}(\zeta_d, a^{1/d})$. If $d \nmid i_a(p)$, then either $p \not\equiv 1 \pmod{d}$ or $a^{\frac{p-1}{d}} \not\equiv 1 \pmod{p}$. The first condition implies p does not split in $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\zeta_d, a^{1/d})$. The second condition implies that $x^d - a$ does not have a solution modulo p. Hence, $x^d - a$ cannot split into linear factors by

[10, Theorem 5.5.1]. Thus, p does not split completely in $\mathbb{Q}(a^{1/d})$, and hence, does not split in $\mathbb{Q}(\zeta_d, a^{1/d})$. Therefore, the result holds. □

This lemma will allow us to obtain an asymptotic formula for $\pi_d(x)$, which will then allow us to handle the behavior of our summations in question. To see this, let us first review Hooley's conditional proof of Artin's conjecture [19]: recall that

$$N_a(x) = \#\{p \leq x : i_a(p) = 1\}. \tag{2.1}$$

Hooley then introduced the following relation, which he called $R(q, p)$:

$$\begin{aligned} p &\equiv 1 \pmod{q}, \\ a^{\frac{p-1}{q}} &\equiv 1 \pmod{p}. \end{aligned} \tag{2.2}$$

Note that a is a primitive root modulo p if and only if $R(q, p)$ is false for all primes q. Define

$$N_a(x, \eta) := \#\{p \leq x : R(q, p) \text{ is false for all } q \leq \eta\} \tag{2.3}$$

and

$$M_a(x, \eta_1, \eta_2) := \#\{p \leq x : R(q, p) \text{ is true for some } \eta_1 < q \leq \eta_2\}. \tag{2.4}$$

Then, Hooley noted for any choice of ξ_1 with $\xi_1 \leq x - 1$, we have

$$N_a(x) = N_a(x, \xi_1) + O(M_a(x, \xi_1, x - 1)). \tag{2.5}$$

The error term $M_a(x, \xi_1, x - 1)$ can be handled using the Chebotarev density theorem assuming the GRH (which will be presented in Sec. 3), Mertens theorem [6, Theorem 1.4.3], and the Brun–Titchmarsh theorem [6, Theorem 7.3.1]. Hooley's bound is

$$M_a(x, \xi_1, x - 1) \ll \frac{x \log\log x}{(\log x)^2} \tag{2.6}$$

for an appropriate choice of ξ_1.

By the inclusion–exclusion principle (also known as the Möbius inversion formula [6, Theorem 1.2.2]), we have

$$N_a(x, \xi_1) = \sum_d{}' \mu(d)\pi_d(x), \tag{2.7}$$

where the $'$ indicates that d is squarefree and has no prime factors exceeding ξ_1. Now, Lemma 2.1 along with GRH will give an asymptotic relation for this summation.

Our technique is similar to this last portion involving the inclusion–exclusion principle. For any function $f : \mathbb{N} \to \mathbb{C}$, we can find $g : \mathbb{N} \to \mathbb{C}$ such that

$$f(n) = \sum_{d|n} g(d) \tag{2.8}$$

for all $n \in \mathbb{N}$ by the Möbius inversion formula [6, Theorem 1.2.2]. By (1.24), we have

$$\sum_{p \leq x} f(i_a(p)) = \sum_{d \leq x} g(d)\pi_d(x). \tag{2.9}$$

Let y be a real number such that $1 \leq y \leq x$. Then, we have

$$\sum_{p \leq x} f(i_a(p)) = \sum_{d \leq y} g(d)\pi_d(x) + \sum_{y < d \leq x} g(d)\pi_d(x). \tag{2.10}$$

Using Lemma 2.1, GRH, and the Chebotarev density theorem, we will give an asymptotic relation for the first summation (after a suitable choice for y). The second summation will require a new idea. This new idea will be discussed in Sec. 3 and involves truncated divisor summations.

Note that Hooley's technique relied on $R(q, p)$ where q was prime. However, for many functions already discussed, we need q to be an arbitrary positive integer, and so, Hooley's technique will not work for these results.

3. Preliminaries

3.1. *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 $\mathcal{P}(K/\mathbb{Q})$ be the set of prime numbers p which ramify in K over $\mathbb{Q}$. Let $\pi_K(x)$ denote the prime numbers $p \leq x$ for which p splits completely in K over $\mathbb{Q}$. Then, the Chebotarev density theorem [4, 5] states

$$\pi_K(x) \sim \frac{\mathrm{li}(x)}{|G|} \tag{3.1}$$

as $x \to \infty$. The original statement of this 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 [23]. It has been improved by Serre [32], Murty *et al.* [30], and Murty and Murty [29]. The following version is Serre's [32] refinement of Lagarias and Odlyzko's result [23].

Theorem 3.1. *Let K be as above. Assuming GRH for the Dedekind zeta function of K, we have*

$$\pi_K(x) = \frac{\mathrm{li}(x)}{|G|} + O\left(\sqrt{x}\left(\frac{\log|d_K|}{n_K} + \log x\right)\right), \tag{3.2}$$

where the implied constant is absolute.

The following result known as Hensel's inequality is useful for bounding the error term in Theorem 3.1 (see [32, p. 130]).

Lemma 3.2. *Let K be a finite Galois extension with degree n_K and discriminant d_K. Then*

$$\log |d_K| \leq n_K \left(\log n_K + \sum_{p \in \mathcal{P}(K/\mathbb{Q})} \log p \right). \tag{3.3}$$

3.2. *Kummerian fields*

In order to compute Eq. (3.2), we will use (3.3). So we need to determine $n_K = |G|$, the size of the Galois group for K over $\mathbb{Q}$, and the discriminant d_K, or at least the primes which ramify in K over $\mathbb{Q}$ by (3.3) when $K = \mathbb{Q}(\zeta_n, a^{1/n})$.

Let us first consider $|G| = n_{\mathbb{Q}(\zeta_n, a^{1/n})} = [\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}]$ since $\mathbb{Q}(\zeta_n, a^{1/n})$ is the splitting field of $x^n - a$ over $\mathbb{Q}$ and hence, a Galois extension of $\mathbb{Q}$. One expects that the subfields $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(a^{1/n})$ of $\mathbb{Q}(\zeta_n, a^{1/n})$ have relatively small intersection. That is, we expect $[\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(a^{1/n}) : \mathbb{Q}]$ is bounded by some absolute constant. Hooley proved this for n squarefree (see [19, Eq. (12)]). This result is well-known if we assume $x^n - a$ is irreducible (see [7, Sec. 14.7, Exercises 4–6], and for cases of when $x^n - a$ is irreducible, see [25, Sec. VI.9]).

For the generic n, we have the following result of Wagstaff [36, Proposition 4.1]: let $a \in \mathbb{Z}$ be different from 0 and ± 1. Write $a = bc^2$ where b is a squarefree integer and $a > 0$ if and only if $b > 0$. Define

$$d(a) = \begin{cases} b & \text{if } b \equiv 1 \pmod 4, \\ 4b & \text{if } b \equiv 2, 3 \pmod 4. \end{cases} \tag{3.4}$$

Write $a = \pm a_0^h$ where $h = \max\{m \in \mathbb{N} : |a|^{1/m} \in \mathbb{Z}\}$ and $a_0 > 0$. That is, a_0 is not a perfect mth power of any positive integer unless $m = 1$. Let $n' = \frac{n}{\gcd(n,h)}$ for all $n \in \mathbb{N}$. Write $a_0 = a_1 a_2^2$ with $a_1, a_2 \in \mathbb{Z}$ and a_1 is squarefree.

Proposition 3.3. *Let $a \in \mathbb{Z}$ be different from 0 and ± 1. Let a_0, a_1, a_2, and h be as above. Let $n \in \mathbb{N}$ and let n' be as above. Write*

$$[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}] = \frac{n' \varphi(n)}{\varepsilon(n)} = \frac{n\varphi(n)}{\varepsilon(n) \gcd(n,h)}.$$

(a) *If $a > 0$, then we have*

$$\varepsilon(n) = \begin{cases} 2 & \text{if } 2|n', \text{ and } d(a_0)|n, \\ 1 & \text{otherwise.} \end{cases}$$

(b) *If $a < 0$, then we have $\varepsilon(n) = 1$ if n is odd. Suppose n is even. If n' is odd, then $\varepsilon(n) = 1/2$. If n' is even, then we have two cases $n' \equiv 2 \pmod 4$ or $4|n'$.*

Assume n is even and $n' \equiv 2 \pmod 4$. Then, we have

$$\varepsilon(m) = \begin{cases} 2 & \text{if } n \equiv 2 \pmod 4 \text{ and } d(-a_0)|n, \\ 2 & \text{if } n \equiv 4 \pmod 8 \text{ and } d(2a_0)|n, \\ 1 & \text{otherwise.} \end{cases}$$

If n is even and $4|n'$, then we have

$$\varepsilon(n) = \begin{cases} 2 & \text{if } d(a_0)|n, \\ 1 & \text{if } d(a_0) \nmid n. \end{cases}$$

Note that the function $\varepsilon(n)$ is absolutely bounded as it can only take the values $1/2, 1$, and 2. Also, $1 \leq \gcd(n, h) \leq h$ is absolutely bounded as h is fixed. Therefore, we have the following immediate corollary.

Corollary 3.4. *Let a be an integer different from 0 and ± 1. Let $n \in \mathbb{N}$. Then*

$$[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}] \asymp n\varphi(n). \tag{3.5}$$

This corollary is crucial for the both the main term and error term of the Theorem 3.1 as well as for determining when infinite summations of interest are convergent.

Let us now consider the discriminant of $\mathbb{Q}(\zeta_n, a^{1/n})$. By Lemma 3.2, we need only consider the primes which ramify in $\mathbb{Q}(\zeta_n, a^{1/n})$. By [22, Theorem 7.3], the primes which ramify in a number field K are exactly those primes which divide the discriminant of K over $\mathbb{Q}$. We have the following lemma.

Lemma 3.5. *If the prime p ramifies in $\mathbb{Q}(\zeta_n, a^{1/n})$, then p divides a or n.*

Proof. We note that by [3, Lemma 5, Sec. 2], we have that the discriminant of $\mathbb{Q}(\zeta_n, a^{1/n})$ over $\mathbb{Q}(\zeta_n)$ divides $n^n a^{n-1}$. By [10, Exercise 4.5.25], we have the discriminant $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is divisible by primes only dividing n. Thus, by [10, Exercise 5.6.25] and the standard properties of the relative norm, we have that a prime p divides $d_{\mathbb{Q}(\zeta_n, a^{1/n})}$ implies that p divides a or n. The result now follows from the remark in the preceding paragraph. □

Corollary 3.6. *Let $n \in \mathbb{N}$ be fixed. Suppose GRH holds for the Dedekind zeta function of $\mathbb{Q}(\zeta_n, a^{1/n})$. Then*

$$\pi_n(x) = \frac{\operatorname{li}(x)}{[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}]} + O_a(\sqrt{x}\log(nx)), \tag{3.6}$$

where the implied constant is dependent on a and can be explicitly computed.

Proof. By Lemma 3.2, we have

$$\frac{\log|d_K|}{n_K} \leq \log n_K + \log\left(\prod_{p \in \mathcal{P}(K/\mathbb{Q})} p\right) \tag{3.7}$$

for any number field K. For $K = \mathbb{Q}(\zeta_n, a^{1/n})$, we have

$$\frac{\log |d_{\mathbb{Q}(\zeta_n, a^{1/n})}|}{n_{\mathbb{Q}(\zeta_n, a^{1/n})}} \ll_a \log(n\varphi(n)) + \log an \ll_a \log an \ll_a \log n \tag{3.8}$$

by Proposition 3.3 and Lemma 3.5. The result now follows by Lemma 2.1 and the definition of $\pi_{\mathbb{Q}(\zeta_n, a^{1/n})}(x)$. □

We note that if we assume that the quasi-Riemann hypothesis is true for a at n, then we obtain the following corollary of the above discussion in the same manner.

Corollary 3.7. *Let $n \in \mathbb{N}$ be fixed. Suppose the quasi-Riemann hypothesis holds for the Dedekind zeta function of $\mathbb{Q}(\zeta_n, a^{1/n})$ (at ε). Then*

$$\pi_n(x) = \frac{\mathrm{li}(x)}{[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}]} + O_a(x^{1-\varepsilon} \log(nx)), \tag{3.9}$$

where the implied constant is dependent on a and can be explicitly computed.

3.3. *Truncated divisor summations*

The general idea of truncating the range of interest in summations involving divisor functions originates with van der Corput [35]. The following development was first initiated by Landreau [24] and continued by Iwaniec and Munshi [21] and Friedlander and Iwaniec [14].

We record the following result for completeness (see [15, Corollary 22.11]).

Lemma 3.8. *Let $k \geq 2$, $r \geq 1$, and $n \geq 1$. We have*

$$\tau_r(n) \leq \sum_{\substack{d|n \\ d \leq n^{1/k}}} (2\tau(d))^{(r-1)k(\log k)/\log 2}. \tag{3.10}$$

We also have the following lemma.

Lemma 3.9. *Let $r \geq 1$ and $k \geq 2$ be fixed integers. Suppose the quasi-Riemann hypothesis holds for a on $\mathbb{N}$. Then*

$$\sum_{p \leq x} \tau_k(i_a(p))^r \ll_{a,r,k} \pi(x). \tag{3.11}$$

Proof. Let $A = \frac{r(k-1)t \log t}{\log 2}$. We will see that our choice of t is bounded and thus A is bounded. This will be important in the sequel.

Let us recall some facts about $\tau(m)$:

$$\sum_{m \leq x} \frac{\tau(m)^A}{m} \ll (\log x)^{2^{[A]+1}} \tag{3.12}$$

and

$$\tau(m) \ll m^{\delta} \tag{3.13}$$

for any $\delta > 0$ (see [6, Exercises 10.5.3 and 1.5.3]). Thus, by Lemma 3.8, Corollaries 3.4, and 3.7, we have

$$\begin{aligned}\sum_{p\le x}\tau_k(i_a(p))^r &\le \sum_{p\le x}\sum_{\substack{m\mid i_a(p)\\ m\le x^{1/t}}}(2\tau(m))^A\\ &\ll \sum_{m\le x^{1/t}}\tau(m)^A\pi_m(x)\\ &\ll \mathrm{li}(x)\sum_{m\le x^{1/t}}\frac{\tau(m)^A}{m\varphi(m)}+O\left(x^{1-\varepsilon}\log x\sum_{m<x^{1/t}}\tau(m)^A\right)\\ &\ll \mathrm{li}(x)\sum_{m\ge 1}\frac{\tau(m)^A}{m\varphi(m)}+O(x^{1+\frac{1}{t}-\varepsilon}(\log x)^{2^{[A]+1}+1}).\end{aligned}\tag{3.14}$$

Choosing $t\in\mathbb{N}$ so that $\frac{1}{t}<\varepsilon\le\frac{1}{t-1}$, recalling that ε is a fixed number, and analyzing the O term give us

$$\sum_{p\le x}\tau_k(i_a(p))^r \ll \mathrm{li}(x)\sum_{m\ge 1}\frac{\tau(m)^A}{m\varphi(m)}+O(x^\theta)\tag{3.15}$$

for some $\theta<1$. Now,

$$\sum_{m\ge 1}\frac{\tau(m)^A}{m\varphi(m)}\ll\sum_{m\ge 1}\frac{1}{m^{1-\delta}\varphi(m)}\tag{3.16}$$

for any $\delta>0$ by (3.13), and this last term can be seen to be bounded for any $\delta<1$ by [6, Exercise 5.5.3]. Therefore, the result holds. □

We also have the following corollary of Theorem 1.2.

Corollary 3.10. *Suppose GRH holds for a on prime powers. Then, we have*

$$\#\{p\le x : i_a(p)>y\}\ll_a \frac{x\log\log x}{(\log x)(\log y)}.\tag{3.17}$$

Proof. By Theorem 1.2, we have

$$\log y\#\{p\le x : i_a(p)>y\}\le\sum_{p\le x}\log i_a(p)\ll_a\frac{x\log\log x}{\log x}.\tag{3.18}$$

Dividing both sides by $\log y$ gives the desired result. □

Note that the above results give the following lemma.

Lemma 3.11. *Suppose GRH holds for a on $\mathbb{N}$. Then, we have*

$$\sum_{\substack{p\le x\\ i_a(p)>\frac{\sqrt{x}}{(\log x)^B}}} \tau_k(i_a(p))^r \ll_a \frac{x}{(\log x)^{2-\varepsilon}} \tag{3.19}$$

for all $\varepsilon > 0$ and $B \in \mathbb{R}$ fixed.

Proof. To see this, let $s, t > 1$ be real numbers such that $\frac{1}{s} + \frac{1}{t} = 1$. Then, by Hölder's inequality, GRH, Lemma 3.9, and Corollary 3.10, we have

$$\begin{aligned}\sum_{\substack{p\le x\\ i_a(p)>\frac{\sqrt{x}}{(\log x)^B}}} \tau_k(i_a(p))^r &\le \left(\sum_{\substack{p\le x\\ i_a(p)>\frac{\sqrt{x}}{(\log x)^B}}} 1\right)^{\frac{1}{s}} \left(\sum_{\substack{p\le x\\ i_a(p)>\frac{\sqrt{x}}{(\log x)^B}}} \tau_k(i_a(p))^{rt}\right)^{\frac{1}{t}}\\ &\ll \left(\frac{\pi(x)\log\log x}{\log x}\right)^{\frac{1}{s}} (\pi(x))^{\frac{1}{t}}\\ &\ll \frac{\pi(x)(\log\log x)^{\frac{1}{s}}}{(\log x)^{\frac{1}{s}}}\\ &\ll \frac{x(\log\log x)^{\frac{1}{s}}}{(\log x)^{1+\frac{1}{s}}}. \end{aligned} \tag{3.20}$$

The result now follows upon noting that we may choose $s > 1$ arbitrarily close to 1 and that $\log\log x \ll (\log x)^{\delta}$ for every $\delta > 0$. □

4. The Function $(\log n)^{\alpha}$

In this section, we are going to prove Theorem 1.5.

Let $0 < \alpha < 1$ be a fixed real number. Write

$$(\log n)^{\alpha} = \sum_{d|n} g(d). \tag{4.1}$$

Then, by the Möbius inversion formula [6, Theorem 1.2.2], we have

$$g(n) = \sum_{d|n} \mu(d) \left(\log \frac{n}{d}\right)^{\alpha}, \tag{4.2}$$

and so,

$$|g(n)| \le (\log n)^{\alpha} \sum_{d|n} 1 = (\log n)^{\alpha} \tau(n). \tag{4.3}$$

By (1.24), we have

$$\sum_{p\le x}(\log i_a(p))^\alpha = \sum_{m\le x} g(m)\pi_m(x)$$
$$= \sum_{m\le y} g(m)\pi_m(x) + \sum_{y<m\le x} g(m)\pi_m(x), \tag{4.4}$$

where y with $y \le x$ will be chosen later.

By GRH and Corollary 3.6, we have

$$\sum_{m\le y} g(m)\pi_m(x) = \mathrm{li}(x)\sum_{m\le y}\frac{g(m)}{[\mathbb{Q}(\zeta_m, a^{1/m}):\mathbb{Q}]} + O\left(\sqrt{x}\log x\sum_{m\le y}|g(m)|\right)$$
$$= \mathrm{li}(x)\sum_{m\le y}\frac{g(m)}{[\mathbb{Q}(\zeta_m, a^{1/m}):\mathbb{Q}]} + O\left(\sqrt{x}\log x\sum_{m\le y}(\log m)^\alpha\tau(m)\right)$$
$$= \mathrm{li}(x)\sum_{m\le y}\frac{g(m)}{[\mathbb{Q}(\zeta_m, a^{1/m}):\mathbb{Q}]} + O(\sqrt{x}(\log x)^{1+\alpha}y\log y). \tag{4.5}$$

Choose $y = \frac{\sqrt{x}}{(\log x)^B}$ where B is a fixed real number. Thus, we have $\sqrt{x}(\log x)^{1+\alpha}y\log y \ll \frac{x}{(\log x)^{B-2-\alpha}}$. Also, by Corollary 3.4, (4.3), and (3.13), we have

$$\sum_{m\le y}\frac{g(m)}{[\mathbb{Q}(\zeta_m, a^{1/m}):\mathbb{Q}]} = \sum_{m\ge 1}\frac{g(m)}{[\mathbb{Q}(\zeta_m, a^{1/m}):\mathbb{Q}]} + O\left(\sum_{m>y}\frac{|g(m)|}{m\varphi(m)}\right)$$
$$= c_{a,\alpha} + O\left(\frac{\log y}{y^{1-\delta}}\right) \tag{4.6}$$

for any $\delta > 0$, and where

$$c_{a,\alpha} := \sum_{m\ge 1}\frac{g(m)}{[\mathbb{Q}(\zeta_m, a^{1/m}):\mathbb{Q}]} \tag{4.7}$$

is a constant. Thus,

$$\sum_{d\le\frac{\sqrt{x}}{(\log x)^B}} g(d)\pi_d(x) = c_{a,\alpha}\mathrm{li}(x) + O\left(\frac{x}{(\log x)^{B-2-\alpha}}\right). \tag{4.8}$$

Also, by Lemma 3.11, from the fact

$$\tau_{k+1}(n) = \sum_{d|n}\tau_k(d) \tag{4.9}$$

for all positive integers n and k, and since $y = \frac{\sqrt{x}}{(\log x)^B}$ for some fixed $B \in \mathbb{R}$, we have

$$\begin{aligned}\left|\sum_{y<m\leq x} g(m)\pi_m(x)\right| &= \left|\sum_{p\leq x}\sum_{\substack{y<m\leq x\\ m|i_a(p)}} g(m)\right| \\ &\leq (\log x)^\alpha \sum_{p\leq x}\sum_{\substack{m>y\\ m|i_a(p)}} \tau(m) \\ &\leq (\log x)^\alpha \sum_{\substack{p\leq x\\ i_a(p)>y}}\sum_{m|i_a(p)} \tau(m) \\ &\leq (\log x)^\alpha \sum_{\substack{p\leq x\\ i_a(p)>y}} \tau_3(i_a(p)) \\ &\ll \frac{x}{(\log x)^{2-\varepsilon-\alpha}}. \end{aligned} \tag{4.10}$$

Therefore, Theorem 1.5 holds by letting $B > 3+\alpha$ since ε can be chosen arbitrarily close to 0 and $\alpha < 1$.

We should note that this technique will not work for $\alpha = 1$ unless we can improve upon results of the following flavor

$$\#\{p \leq x : i_a(p) > y\} \ll \frac{\pi(x)\log\log x}{\log y}, \tag{4.11}$$

or prove related results about the number of primes with divisors in a specified range. The work of Erdős and Murty [9] and continuation by Ford [13] have shown that it is possible to obtain non-trivial upper bounds for

$$\#\left\{p \leq x : p-1 \text{ has a divisor in } \left(\frac{\sqrt{x}}{(\log x)^B}, \sqrt{x}(\log x)^B\right)\right\}. \tag{4.12}$$

However, these bounds do not resolve the problem for $\alpha = 1$ but also do not require the use of GRH for large divisors.

5. The Divisor Function

In this section, we will prove Theorem 1.6.

Recall the following theorem of Fomenko [12].

Theorem 5.1 (Fomenko). *Let $w \in \mathbb{N}$ be fixed. Suppose the GRH holds for a on $\mathbb{N}$. Define*

$$N_a(x;w) := \#\{p \leq x : i_a(p) = w\}. \tag{5.1}$$

Then

$$N_a(x;w) = A_a(w)\mathrm{li}(x) + O_A\left(\frac{x\log\log x}{\varphi(w)(\log x)^2}\right) + O_a\left(\frac{x}{(\log x)^A}\right), \tag{5.2}$$

where

$$A_a(w) = \sum_{k\geq 1} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{kw}, a^{1/kw}) : \mathbb{Q}]} \tag{5.3}$$

and A is any fixed real number.

We should note that if we are not interested in the dependence of w, then the above result is due to Wagstaff [36]. Also, if one is interested in the dependence on a, then the following result of Moree [27] is of interest:

$$N_a(x; w) = A_a(w)\mathrm{li}(x) + O\left(\frac{x \log\log x}{\varphi(w)(\log x)^2}\right) + O\left(\frac{x \log|a|}{(\log x)^2}\right). \tag{5.4}$$

We will also need the following fact:

$$\tau(n) = 2 \sum_{\substack{d|n \\ d\leq\sqrt{n}}} 1 - \delta(n), \tag{5.5}$$

where

$$\delta(n) := \begin{cases} 1 & \text{if } n \text{ is a square,} \\ 0 & \text{otherwise.} \end{cases} \tag{5.6}$$

Thus, we have

$$\begin{aligned} \sum_{p\leq x} \tau(i_a(p)) &= \sum_{p\leq x} \left(2 \sum_{\substack{d|i_a(p) \\ d\leq\sqrt{i_a(p)}}} 1 - \delta(i_a(p)) \right) \\ &= 2 \sum_{d\leq\sqrt{x}} \sum_{\substack{p\leq x \\ d|i_a(p)}} 1 - 2 \sum_{d\leq\sqrt{x}} \sum_{\substack{p\leq x \\ d|i_a(p) \\ i_a(p)<d^2}} 1 - \sum_{p\leq x} \delta(i_a(p)) \\ &= 2 \sum_{d\leq\sqrt{x}} \pi_d(x) - 2 \sum_{d\leq\sqrt{x}} \sum_{m=1}^{d-1} N_a(x; md) - \sum_{p\leq x} \delta(i_a(p)). \end{aligned} \tag{5.7}$$

We will evaluate each of these summations separately.

5.1. *The first summation*

We have

$$\sum_{d\leq\sqrt{x}} \pi_d(x) = \sum_{d\leq y} \pi_d(x) + \sum_{y<d\leq\sqrt{x}} \pi_d(x), \tag{5.8}$$

where y with $y \leq \sqrt{x}$ will be chosen later. By Corollary 3.4, GRH, and Corollary 3.6, we have

$$\begin{aligned}\sum_{d\leq y}\pi_d(x) &= \sum_{d\leq y}\frac{\mathrm{li}(x)}{[K_d:\mathbb{Q}]}+O(\sqrt{x}\log(dx))\\ &= \mathrm{li}(x)\sum_{d\geq 1}\frac{1}{[K_d:\mathbb{Q}]}+O\left(\mathrm{li}(x)\sum_{d>y}\frac{1}{d\varphi(d)}\right)\\ &\quad +O\left(\sqrt{x}\log x\sum_{d\leq y}1\right)\\ &= c_1\mathrm{li}(x)+O\left(\frac{x\log y}{y\log x}\right)+O(y\sqrt{x}\log x), \end{aligned} \tag{5.9}$$

where

$$c_1=\sum_{d\geq 1}\frac{1}{[K_d:\mathbb{Q}]} \tag{5.10}$$

is a constant by Corollary 3.4. Choosing $y=\frac{\sqrt{x}}{(\log x)^B}$ for any fixed real number B gives us

$$\sum_{d\leq \frac{\sqrt{x}}{(\log x)^B}}\pi_d(x)=c_1\mathrm{li}(x)+O\left(\frac{x}{(\log x)^{B-1}}\right). \tag{5.11}$$

Now,

$$\begin{aligned}\sum_{\frac{\sqrt{x}}{(\log x)^B}<d\leq\sqrt{x}}\pi_d(x) &= \sum_{\frac{\sqrt{x}}{(\log x)^B}<d\leq\sqrt{x}}\sum_{\substack{p\leq x\\ d\mid i_a(p)}}1=\sum_{p\leq x}\sum_{\substack{\frac{\sqrt{x}}{(\log x)^B}<d\leq\sqrt{x}\\ d\mid i_a(p)}}1\\ &\leq \sum_{\substack{p\leq x\\ i_a(p)>\frac{\sqrt{x}}{(\log x)^B}}}\sum_{d\mid i_a(p)}1=\sum_{\substack{p\leq x\\ i_a(p)>\frac{\sqrt{x}}{(\log x)^B}}}\tau(i_a(p))\\ &\ll \frac{x}{(\log x)^{2-\varepsilon}} \end{aligned} \tag{5.12}$$

for any $\varepsilon>0$ by Lemma 3.11. Thus,

$$\sum_{d\leq\sqrt{x}}\pi_d(x)=c_1\mathrm{li}(x)+O\left(\frac{x}{(\log x)^{2-\varepsilon}}\right). \tag{5.13}$$

5.2. *The second summation*

Let C be a fixed positive real number. For the second summation, we have

$$\sum_{d\le\sqrt{x}}\sum_{m=1}^{d-1} N_a(x;md) = \sum_{d\le(\log x)^C}\sum_{m=1}^{d-1} N_a(x;md) + \sum_{(\log x)^C<d\le\frac{\sqrt{x}}{(\log x)^C}}\sum_{m=1}^{d-1} N_a(x;md) + \sum_{\frac{\sqrt{x}}{(\log x)^C}<d\le\sqrt{x}}\sum_{m=1}^{d-1} N_a(x;md). \tag{5.14}$$

By Theorem 5.1, we have

$$\begin{aligned}&\sum_{d\le(\log x)^C}\sum_{m=1}^{d-1} N_a(x;md)\\ &= \sum_{d\le(\log x)^C}\sum_{m=1}^{d-1}\left(A_a(md)\mathrm{li}(x) + O\left(\frac{x\log\log x}{\varphi(md)(\log x)^2}\right) + O\left(\frac{x}{(\log x)^A}\right)\right)\\ &= \mathrm{li}(x)\sum_{d\le(\log x)^C}\sum_{m=1}^{d-1} A_a(md) + O\left(\frac{x\log\log x}{(\log x)^2}\sum_{d\le(\log x)^A}\sum_{m=1}^{d-1}\frac{1}{\varphi(md)}\right)\\ &\quad + O\left(\frac{x}{(\log x)^{A-2C}}\right).\end{aligned} \tag{5.15}$$

Now,

$$\begin{aligned}\sum_{d\le(\log x)^C}\sum_{m=1}^{d-1}\frac{1}{\varphi(md)} &\ll \sum_{d\le(\log x)^C}\frac{\log d}{\varphi(d)}\\ &\ll (\log\log x)^2.\end{aligned} \tag{5.16}$$

So, the first error term is $\ll \frac{x(\log\log x)^3}{(\log x)^2}$.

By Corollary 3.4, we have

$$\begin{aligned}A_a(w) := \sum_{k\ge1}\frac{\mu(k)}{[\mathbb{Q}(\zeta_{kw}, a^{1/kw}):\mathbb{Q}]} &\ll \sum_{k\ge1}\frac{1}{kw\varphi(kw)}\\ &\ll \frac{1}{w\varphi(w)}\sum_{k\ge1}\frac{1}{k\varphi(k)} \ll \frac{1}{w\varphi(w)}\end{aligned} \tag{5.17}$$

for all $w\in\mathbb{N}$. With this, it can be shown that

$$\sum_{d\le(\log x)^C}\sum_{m=1}^{d-1} A_a(md) = c_2 + O\left(\frac{(\log\log x)^2}{(\log x)^C}\right) \tag{5.18}$$

where

$$c_2 := \sum_{k\geq 1}\sum_{1\leq m<k} A_a(mk) = \sum_{k\geq 1}\sum_{m=1}^{k-1}\sum_{w\geq 1}\frac{\mu(w)}{[K_{kmw}:\mathbb{Q}]}. \tag{5.19}$$

Hence,

$$\sum_{d\leq(\log x)^C}\sum_{m=1}^{d-1} N_a(x;md) = c_2\mathrm{li}(x) + O\bigg(\frac{x(\log\log x)^3}{(\log x)^2}\bigg). \tag{5.20}$$

For the other summations, we have

$$\sum_{m=1}^{d-1} N_a(md) \leq \pi_d(x). \tag{5.21}$$

Thus, by GRH and Corollary 3.6, we have

$$\begin{aligned}\sum_{(\log x)^C<d\leq\frac{\sqrt{x}}{(\log x)^C}}\sum_{m=1}^{d-1} N_a(x;md) &\leq \sum_{(\log x)^C<d\leq\frac{\sqrt{x}}{(\log x)^C}} \pi_d(x)\\ &= \mathrm{li}(x)\sum_{(\log x)^C<d\leq\frac{\sqrt{x}}{(\log x)^C}}\frac{1}{[K_d:\mathbb{Q}]} + O\bigg(\frac{x}{(\log x)^{C-1}}\bigg)\\ &\ll \mathrm{li}(x)\sum_{(\log x)^C<d\leq\frac{\sqrt{x}}{(\log x)^C}}\frac{1}{d\varphi(d)} + O\bigg(\frac{x}{(\log x)^{C-1}}\bigg)\\ &\ll \frac{x\log\log x}{(\log x)^{C+1}} + \frac{x}{(\log x)^{C-1}}.\end{aligned} \tag{5.22}$$

Finally, by (5.12), we have

$$\sum_{\frac{\sqrt{x}}{(\log x)^C}<d\leq\sqrt{x}}\pi_d(x) \ll \frac{x}{(\log x)^{2-\varepsilon}} \tag{5.23}$$

for any $\varepsilon > 0$. Therefore,

$$\sum_{d\leq\sqrt{x}}\sum_{m=1}^{d-1} N_a(x;md) = c_2\mathrm{li}(x) + O\bigg(\frac{x}{(\log x)^{2-\varepsilon}}\bigg) \tag{5.24}$$

for any $\varepsilon > 0$.

5.3. *The third summation*

For the last summation, we have

$$\begin{aligned}\sum_{p\leq x}\delta(i_a(p)) &= \sum_{m\leq\sqrt{x}}\#\{p\leq x : i_a(p) = m^2\}\\ &= \sum_{m\leq\sqrt{x}} N_a(x;m^2).\end{aligned} \tag{5.25}$$

Now,

$$\sum_{m\le\sqrt{x}} N_a(x;m^2)=\sum_{m\le y} N_a(x;m^2)+\sum_{y<m\le\sqrt{x}} N_a(x;m^2), \tag{5.26}$$

where y with $y\le\sqrt{x}$ will be chosen later.

We will handle each of these summations separately.

By Theorem 5.1, for a fixed real number A, we have

$$\begin{aligned}\sum_{m\le y} N_a(x;m^2)&=\sum_{m\le y}\left(A_a(m^2)\mathrm{li}(x)+O\left(\frac{x\log\log x}{\varphi(m^2)(\log x)^2}\right)+O\left(\frac{x}{(\log x)^A}\right)\right)\\&=\mathrm{li}(x)\sum_{m\le y}A_a(m^2)+O\left(\frac{x\log\log x}{(\log x)^2}\right)+O\left(\frac{yx}{(\log x)^A}\right).\end{aligned} \tag{5.27}$$

Choose $y=(\log x)^C$ for some fixed real number C and $A=C+2$. Then, we have

$$\sum_{m\le(\log x)^C} N_a(x;m^2)=\mathrm{li}(x)\sum_{m\le(\log x)^C}A_a(m^2)+O\left(\frac{x\log\log x}{(\log x)^2}\right). \tag{5.28}$$

Now, by (5.17), we have

$$\sum_{m\le(\log x)^C}A_a(m^2)=c_3+O\left(\frac{\log\log x}{(\log x)^C}\right), \tag{5.29}$$

where

$$c_3:=\sum_{m\ge1}A_a(m^2)=\sum_{m\ge1}\sum_{w\ge1}\frac{\mu(w)}{[\mathbb{Q}(\zeta_{k^2w},a^{1/k^2w}):\mathbb{Q}]}. \tag{5.30}$$

Thus,

$$\sum_{m\le(\log x)^C} N_a(x;m^2)=c_3\mathrm{li}(x)+O\left(\frac{x\log\log x}{(\log x)^2}\right). \tag{5.31}$$

For the second summation, we have

$$\begin{aligned}\sum_{(\log x)^C<m\le\sqrt{x}} N_a(x;m^2)&\le\sum_{(\log x)^C<m\le\sqrt{x}}\pi(x;m^2,1)\\&=\sum_{(\log x)^C<m\le x^{\frac12-\delta}}\pi(x;m^2,1)+\sum_{x^{\frac12-\delta}<m\le\sqrt{x}}\pi(x;m^2,1)\end{aligned} \tag{5.32}$$

for any fixed $\delta \in (0, 1/2)$. Thus, by the Brun–Titchmarsh inequality (see [6, Theorem 7.3.1]) and the multiplicativity of the Euler totient function, we have

$$\begin{aligned}\sum_{(\log x)^C < m \le x^{\frac{1}{2}-\delta}} \pi(x; m^2, 1) &\ll \sum_{m > (\log x)^C} \frac{x}{\varphi(m^2)\log x} \\ &= \frac{x}{\log x} \sum_{m > (\log x)^C} \frac{1}{m\varphi(m)} \\ &\ll \frac{Cx \log\log x}{(\log x)^{1+C}} \end{aligned} \tag{5.33}$$

for any $\varepsilon > 0$. Thus, for $C > 1$, we have

$$\sum_{(\log x)^C < m \le x^{\frac{1}{2}-\delta}} \pi(x; m^2, 1) \ll \frac{x}{(\log x)^2}. \tag{5.34}$$

We also have, by the trivial bound $\pi(x, d, 1) \le x/d$, the following relation:

$$\sum_{x^{\frac{1}{2}-\delta} < m \le \sqrt{x}} \pi(x; m^2, 1) \ll \sum_{m > x^{\frac{1}{2}-\delta}} \frac{x}{m^2} \ll x^{\frac{1}{2}+\delta}. \tag{5.35}$$

Thus,

$$\sum_{p \le x} \delta(i_a(p)) = c_3 \mathrm{li}(x) + O\left(\frac{x \log\log x}{(\log x)^2}\right). \tag{5.36}$$

Therefore,

$$\sum_{p \le x} \tau(i_a(p)) = (2c_1 - 2c_2 - c_3)\mathrm{li}(x) + O\left(\frac{x}{(\log x)^{2-\varepsilon}}\right) \tag{5.37}$$

for any $\varepsilon > 0$.

5.4. *Computation of the constant*

To finish the proof, we need to prove

$$\sum_{n \ge 1} \frac{1}{[K_n : \mathbb{Q}]} = 2c_1 - 2c_2 - c_3. \tag{5.38}$$

Note that

$$c_1 = \sum_{n \ge 1} \frac{1}{[K_n : \mathbb{Q}]}. \tag{5.39}$$

Therefore, we need to show $c_1 = 2c_2 + c_3$. That is,

$$\sum_{n \ge 1} \frac{1}{[K_n : \mathbb{Q}]} = 2 \sum_{k \ge 1} \sum_{1 \le m < k} A_a(mk) + \sum_{k \ge 1} A_a(k^2). \tag{5.40}$$

However, by Theorem 5.1, we have

$$\begin{aligned}
&2\sum_{k\geq 1}\sum_{1\leq m<k} A_a(mk)+\sum_{k\geq 1} A_a(k^2)\\
&\quad=2\sum_{k\geq 1}\sum_{m=1}^{k-1}\sum_{w\geq 1}\frac{\mu(w)}{[\mathbb{Q}(\zeta_{kmw},a^{1/kmw}):\mathbb{Q}]}+\sum_{k\geq 1}\sum_{w\geq 1}\frac{\mu(w)}{[\mathbb{Q}(\zeta_{k^2w},a^{1/k^2w}):\mathbb{Q}]}\\
&\quad=2\sum_{n\geq 1}\frac{1}{[\mathbb{Q}(\zeta_n,a^{1/n}):\mathbb{Q}]}\sum_{w|n}\mu(w)\sum_{\substack{\frac{n}{w}=mk\\ m<k}}1+\sum_{n\geq 1}\frac{1}{[\mathbb{Q}(\zeta_n,a^{1/n}):\mathbb{Q}]}\sum_{k^2|n}\mu\left(\frac{n}{k^2}\right).
\end{aligned}\tag{5.41}$$

Now, let

$$g(n)=\sum_{k^2|n}\mu\left(\frac{n}{k^2}\right).\tag{5.42}$$

We claim g is multiplicative. To see this, we note that if $\gcd(m,n)=1$, then $d^2|mn$ if and only if $d=d_1d_2$ with $\gcd(d_1,d_2)=1$ such that $d_1^2|m$ and $d_2^2|n$. Thus, g is multiplicative. Hence,

$$g(n)=\prod_{p^\alpha\|n}\left(\sum_{p^{2d}|p^\alpha}\mu(p^{\alpha-2d})\right)=\prod_{p^\alpha\|n}(-1)^\alpha=(-1)^{\Omega(n)}.\tag{5.43}$$

Let

$$f(n)=\sum_{\substack{n=mk\\ m<k}}1=\sum_{\substack{d|n\\ d<\sqrt{n}}}1.\tag{5.44}$$

This is true since $n=mk$ with $m<k$ if and only if $k|n$ and $\frac{n}{k}<k$. This last pair of conditions is equivalent to $k|n$ and $\sqrt{n}<k$. However,

$$\tau(n)=\sum_{d|n}1=2\sum_{\substack{d|n\\ d<\sqrt{n}}}1+\delta(n)\tag{5.45}$$

where

$$\delta(n)=\begin{cases}1 & \text{if } \sqrt{n}\in\mathbb{Z},\\ 0 & \text{otherwise.}\end{cases}\tag{5.46}$$

Therefore,

$$f(n)=\frac{\tau(n)-\delta(n)}{2}.\tag{5.47}$$

Hence, we will be finished if we can prove

$$1 = 2\sum_{w|n} \mu(w) \left(\frac{\tau(n/w) - \delta(n/w)}{2} \right) + (-1)^{\Omega(n)}, \tag{5.48}$$

or equivalently,

$$\sum_{w|n} \mu(w) \left(\frac{\tau(n/w) - \delta(n/w)}{2} \right) = \begin{cases} 0 & \text{if } \Omega(n) \text{ is even,} \\ 1 & \text{if } \Omega(n) \text{ is odd.} \end{cases} \tag{5.49}$$

By the Möbius inversion formula [6, Theorem 1.2.2], all we need to show is that

$$\frac{\tau(n) - \delta(n)}{2} = \#\{d|n : \Omega(d) \text{ is odd}\}. \tag{5.50}$$

In order to do this, we need the following lemma about generating functions.

Lemma 5.2. *Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be positive integers. For all $i \in \{1, 2, \ldots, r\}$, let*

$$f_i(x) = 1 + x + x^2 + \cdots + x^{\alpha_i}. \tag{5.51}$$

Let

$$f(x) = f_1(x) f_2(x) \cdots f_r(x) = \sum_{k \geq 0} a_k x^k, \tag{5.52}$$

where $a_k = 0$ for all $k > \alpha_1 + \alpha_2 + \cdots + \alpha_r$.

(a) *If there exists $i \in \{1, 2, \ldots, r\}$ such that α_i is odd, then*

$$\sum_{k \geq 0} a_{2k} = \sum_{k \geq 0} a_{2k+1}. \tag{5.53}$$

That is, the sum of the coefficients to an even power is equal to the sum of the coefficients to an odd power.

(b) *If all of $\alpha_1, \alpha_2, \ldots, \alpha_r$ are even, then*

$$\sum_{k \geq 0} a_{2k} = 1 + \sum_{k \geq 0} a_{2k+1}. \tag{5.54}$$

That is, the sum of the coefficients to an even power is equal to 1 *plus the sum of the coefficients to an odd power.*

Proof. (a) We will prove this by induction on r. The result holds for $r = 1$. Suppose it is true for $r - 1$ with $r \geq 2$. Let $f_1(x), f_2(x), \ldots, f_r(x)$ be as in (a). Without loss of generality, we may assume that α_1 is odd. Therefore, the result holds for $g(x) = f_1(x) f_2(x) \cdots f_{r-1}(x)$. Let $\{b_k\}_{k=0}^{\infty}$ be the coefficients of x^k for $g(x)$. Then, we have

$$\sum_{k \geq 0} b_{2k} = \sum_{k \geq 0} b_{2k+1}. \tag{5.55}$$

Now,

$$\begin{aligned} f(x) &= g(x)f_r(x) \\ &= \left(\sum_{k\geq 0} b_k x^k\right)(1 + x + x^2 + \cdots + x^{\alpha_r}) \\ &= \left(\sum_{k\geq 0} b_{2k}x^{2k} + \sum_{k\geq 0} b_{2k+1}x^{2k+1}\right)\left(\sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is even}}} x^m + \sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is odd}}} x^m\right) \\ &= \sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is even}}} \sum_{k\geq 0} b_{2k}x^{2k+m} + \sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is odd}}} \sum_{k\geq 0} b_{2k+1}x^{2k+1+m} \\ &\quad + \sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is odd}}} \sum_{k\geq 0} b_{2k}x^{2k+m} + \sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is even}}} \sum_{k\geq 0} b_{2k+1}x^{2k+1+m}. \end{aligned} \tag{5.56}$$

Therefore,

$$\begin{aligned} \sum_{k\geq 0} a_{2k} &= \sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is even}}} \sum_{k\geq 0} b_{2k} + \sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is odd}}} \sum_{k\geq 0} b_{2k+1} \\ &= \sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is even}}} \sum_{k\geq 0} b_{2k+1} + \sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is odd}}} \sum_{k\geq 0} b_{2k} \\ &= \sum_{k\geq 0} a_{2k+1}. \end{aligned} \tag{5.57}$$

Hence, part (a) holds.

(b) Again, we will prove this by induction on r. It is clear for $r = 1$. Suppose it is true for $r-1$ where $r \geq 2$. Let $f_1(x), f_2(x), \ldots, f_r(x)$ be as in (b). Let $g(x) = f_1(x)f_2(x)\cdots f_{r-1}(x)$. Let $\{b_k\}_{k=0}^{\infty}$ be the coefficients of x^k for $g(x)$. Then, we have

$$\sum_{k\geq 0} b_{2k} = 1 + \sum_{k\geq 0} b_{2k+1}. \tag{5.58}$$

Now,

$$\begin{aligned} f(x) &= g(x)f_r(x) \\ &= \left(\sum_{k\geq 0} b_k x^k\right)(1 + x + x^2 + \cdots + x^{\alpha_r}) \\ &= \left(\sum_{k\geq 0} b_{2k}x^{2k} + \sum_{k\geq 0} b_{2k+1}x^{2k+1}\right)\left(\sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is even}}} x^m + \sum_{\substack{0\leq m\leq \alpha_r \\ m \text{ is odd}}} x^m\right) \end{aligned}$$

$$= \sum_{\substack{0\le m\le \alpha_r \\ m \text{ is even}}} \sum_{k\ge 0} b_{2k} x^{2k+m} + \sum_{\substack{0\le m\le \alpha_r \\ m \text{ is odd}}} \sum_{k\ge 0} b_{2k+1} x^{2k+1+m}$$

$$+ \sum_{\substack{0\le m\le \alpha_r \\ m \text{ is odd}}} \sum_{k\ge 0} b_{2k} x^{2k+m} + \sum_{\substack{0\le m\le \alpha_r \\ m \text{ is even}}} \sum_{k\ge 0} b_{2k+1} x^{2k+1+m}. \tag{5.59}$$

Therefore,

$$\sum_{k\ge 0} a_{2k} = \sum_{\substack{0\le m\le \alpha_r \\ m \text{ is even}}} \sum_{k\ge 0} b_{2k} + \sum_{\substack{0\le m\le \alpha_r \\ m \text{ is odd}}} \sum_{k\ge 0} b_{2k+1}$$

$$= \sum_{\substack{0\le m\le \alpha_r \\ m \text{ is even}}} \left(1 + \sum_{k\ge 0} b_{2k+1}\right) + \sum_{\substack{0\le m\le \alpha_r \\ m \text{ is odd}}} \left(-1 + \sum_{k\ge 0} b_{2k}\right)$$

$$= \sum_{k\ge 0} a_{2k+1} + \sum_{\substack{0\le m\le \alpha_r \\ m \text{ is even}}} 1 - \sum_{\substack{0\le m\le \alpha_r \\ m \text{ is odd}}} 1$$

$$= 1 + \sum_{k\ge 0} a_{2k+1} \tag{5.60}$$

since α_r is even. Hence, part (b) holds. □

We claim that Lemma 5.2 implies

$$\frac{\tau(n) - \delta(n)}{2} = \#\{d|n : \Omega(d) \text{ is odd}\}. \tag{5.61}$$

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the unique prime power factorization of n. Then, we have

$$\sum_{d|n} d = \sum_{\substack{0\le \beta_i\le \alpha_i \\ \text{for all } i}} p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}. \tag{5.62}$$

Thus,

$$\#\{d|n : \Omega(d) \text{ is odd}\} = \sum_{\substack{0\le \beta_i\le \alpha_i \text{ for all } i \\ \beta_1+\beta_2+\cdots+\beta_r \text{ is odd}}} 1. \tag{5.63}$$

For $i \in \{1, 2, \ldots, r\}$, let $f_i(x) = 1 + x + x^2 + \cdots + x^{\alpha_i}$. Let

$$f(x) = f_1(x) f_2(x) \cdots f_r(x) = \sum_{k\ge 0} a_k x^k. \tag{5.64}$$

Also note that

$$f(x) = \sum_{\substack{0\le \beta_i\le \alpha_i \\ \text{for all } i}} x^{\beta_1+\beta_2+\cdots+\beta_r}. \tag{5.65}$$

Thus,

$$\sum_{k\geq 0} a_{2k+1} = \sum_{\substack{0\leq \beta_i \leq \alpha_i \text{ for all } i \\ \beta_1+\beta_2+\cdots+\beta_r \text{ is odd}}} 1. \tag{5.66}$$

Similarly, replacing "odd" with "even" gives us

$$\sum_{k\geq 0} a_{2k} = \sum_{\substack{0\leq \beta_i \leq \alpha_i \text{ for all } i \\ \beta_1+\beta_2+\cdots+\beta_r \text{ is even}}} 1. \tag{5.67}$$

Therefore, by Lemma 5.2, we have

$$\#\{d|n : \Omega(d) \text{ is odd}\} = \#\{d|n : \Omega(d) \text{ is even}\} \tag{5.68}$$

if some α_i is odd, and

$$\#\{d|n : \Omega(d) \text{ is odd}\} + 1 = \#\{d|n : \Omega(d) \text{ is even}\} \tag{5.69}$$

if all α_i are even. This last condition is equivalent to n being a square. Therefore, we have

$$\#\{d|n : \Omega(d) \text{ is odd}\} + \delta(n) = \#\{d|n : \Omega(d) \text{ is even}\}. \tag{5.70}$$

Hence,

$$\begin{aligned}\tau(n) &= \#\{d|n : \Omega(d) \text{ is odd}\} + \#\{d|n : \Omega(d) \text{ is even}\} \\ &= 2\#\{d|n : \Omega(d) \text{ is odd}\} + \delta(n).\end{aligned} \tag{5.71}$$

Thus,

$$\#\{d|n : \Omega(d) \text{ is odd}\} = \frac{\tau(n) - \delta(n)}{2}, \tag{5.72}$$

as required. Therefore, Theorem 1.6 holds.

6. Alternate Proof of Theorem 1.6 and its Generalization

6.1. *Proof of Theorem* 1.6

By (1.24) and since $\tau(n) = \sum_{d|n} 1$, we have

$$\sum_{p\leq x} \tau(i_a(p)) = \sum_{d\leq x} \pi_d(x) = \sum_{d\leq y} \pi_d(x) + \sum_{y<d\leq x} \pi_d(x), \tag{6.1}$$

where y with $y \leq x$ will be chosen later. Then, by GRH and Corollary 3.6, we have

$$\begin{aligned}\sum_{d\leq y} \pi_d(x) &= \sum_{d\leq y} \left(\frac{\mathrm{li}(x)}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} + O(\sqrt{x}\log(dx)) \right) \\ &= \mathrm{li}(x) \sum_{d\leq y} \frac{1}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} + O(y\sqrt{x}\log x) \\ &= \mathrm{li}(x) \sum_{d\geq 1} \frac{1}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} + O\left(\frac{x\log y}{y\log x}\right) + O(y\sqrt{x}\log x).\end{aligned} \tag{6.2}$$

Let $y = \frac{\sqrt{x}}{(\log x)^3}$. Then

$$\sum_{d\le y} \pi_d(x) = c_{a,\tau}\mathrm{li}(x) + O\bigg(\frac{x}{(\log x)^2}\bigg), \tag{6.3}$$

where

$$c_{a,\tau} = \sum_{d\ge 1} \frac{1}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} \tag{6.4}$$

is a constant by Corollary 3.4.

We also have

$$\begin{aligned}\sum_{\frac{\sqrt{x}}{(\log x)^2}<d\le x} \pi_d(x) &= \sum_{\frac{\sqrt{x}}{(\log x)^2}<d\le x} \sum_{\substack{p\le x\\ d\mid i_a(p)}} 1 = \sum_{p\le x} \sum_{\substack{\frac{\sqrt{x}}{(\log x)^2}<d\le x\\ d\mid i_a(p)}} 1\\ &\le \sum_{\substack{p\le x\\ i_a(p)>\frac{\sqrt{x}}{(\log x)^2}}} \sum_{d\mid i_a(p)} 1 = \sum_{\substack{p\le x\\ i_a(p)>\frac{\sqrt{x}}{(\log x)^2}}} \tau(i_a(p))\\ &\ll \frac{x}{(\log x)^{2-\varepsilon}}\end{aligned} \tag{6.5}$$

by Lemma 3.11. Therefore, Theorem 1.6 holds.

6.2. *Proof of Theorem* 1.7

By (1.24) and the hypothesis that $f(n) = \sum_{d\mid n} g(d)$, we have

$$\begin{aligned}\sum_{p\le x} f(i_a(p)) &= \sum_{d\le x} g(d)\pi_d(x)\\ &= \sum_{d\le y} g(d)\pi_d(x) + \sum_{y<d\le x} g(d)\pi_d(x),\end{aligned} \tag{6.6}$$

where y with $y \le x$ will be chosen later.

By GRH and Corollary 3.6, we have

$$\begin{aligned}\sum_{d\le y} g(d)\pi_d(x) &= \sum_{d\le y}\bigg(\frac{g(d)}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]}\mathrm{li}(x) + O(|g(d)|\sqrt{x}\log(dx))\bigg)\\ &= \mathrm{li}(x)\sum_{d\ge 1}\frac{g(d)}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} + O\bigg(\mathrm{li}(x)\sum_{d>y}\frac{|g(d)|}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]}\bigg)\\ &\quad + O\bigg(\sqrt{x}\log x\sum_{d\le y}|g(d)|\bigg).\end{aligned} \tag{6.7}$$

We claim $\tau_k(n) \ll n^\theta$ for all $\theta > 0$. To see this, note that it is true for $k = 1$ and $k = 2$ by (3.13). Assume it is true for k. Then,

$$\tau_{k+1}(n) = \sum_{d|n} \tau_k(d) \ll \sum_{d|n} d^\theta \ll n^\theta \tau(n) \ll n^{\theta'} \tag{6.8}$$

for all $\theta' > 0$. Hence, the claim holds by induction. By Corollary 3.4 and $|g(d)| \ll (\log d)^\alpha \tau_k(d)^r \ll d^\theta$ for all $\theta > 0$, we have

$$\left| \sum_{d\geq 1} \frac{g(d)}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} \right| \ll \sum_{d\geq 1} \frac{|g(d)|}{d\varphi(d)} \ll \sum_{d\geq 1} \frac{1}{d^{1-\theta}\varphi(d)} < \infty. \tag{6.9}$$

Therefore,

$$c_{a,f} := \sum_{d\geq 1} \frac{g(d)}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} \tag{6.10}$$

is a constant. Also,

$$\sum_{d>y} \frac{|g(d)|}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} \ll \frac{\log y}{y^{1-\theta}} \tag{6.11}$$

for all $\theta > 0$.

Let $B = 2r(k-1)$. By Lemma 3.8 (and an argument similar to that of Lemma 3.9), we have

$$\begin{aligned} \sum_{d\leq y} |g(d)| &\ll (\log y)^\alpha \sum_{d\leq y} \tau_k(d)^r \ll (\log y)^\alpha \sum_{d\leq y} \sum_{\substack{m|d \\ m\leq d^{1/2}}} (2\tau(m))^B \\ &\ll_{r,k} y(\log y)^\alpha \sum_{m\leq y^{1/2}} \frac{\tau(m)^B}{m} \\ &\ll_{r,k} y(\log y)^{\alpha+2^{B+1}} \end{aligned} \tag{6.12}$$

by (3.12). Thus, we obtain

$$\sum_{d\leq y} g(d)\pi_d(x) = c_{a,f}\mathrm{li}(x) + O\left(\frac{x\log y}{y^{1-\theta}\log x}\right) + O(y\sqrt{x}(\log y)^{\alpha+2^{B+1}}\log x) \tag{6.13}$$

for all $\theta > 0$. Let $y = \sqrt{x}/(\log x)^{\alpha+2^{B+1}+4}$. Then, the above relation becomes

$$\sum_{d\leq y} g(d)\pi_d(x) = c_{a,f}\mathrm{li}(x) + O(x^\Theta) + O\left(\frac{x}{(\log x)^3}\right) \tag{6.14}$$

for some $\Theta < 1$.

We also have

$$\begin{aligned}\left|\sum_{y<d\le x} g(d)\pi_d(x)\right| &= \left|\sum_{y<d\le x} g(d) \sum_{\substack{p\le x\\ d\mid i_a(p)}} 1\right| \\ &\le \sum_{y<d\le x} |g(d)| \sum_{\substack{p\le x\\ d\mid i_a(p)}} 1 \\ &\ll (\log x)^{\alpha} \sum_{\substack{p\le x\\ i_a(p)>y}} \sum_{d\mid i_a(p)} \tau_k(d)^r \\ &\le (\log x)^{\alpha} \sum_{\substack{p\le x\\ i_a(p)>y}} \left(\sum_{d\mid i_a(p)} \tau_k(d)\right)^r \\ &= (\log x)^{\alpha} \sum_{\substack{p\le x\\ i_a(p)>y}} \tau_{k+1}(i_a(p))^r \\ &\ll \frac{x}{(\log x)^{2-\varepsilon-\alpha}} \end{aligned} \tag{6.15}$$

for any $\varepsilon > 0$ by Lemma 3.11.

Therefore,

$$\sum_{p\le x} f(i_a(p)) = c_{a,f}\mathrm{li}(x) + O\left(\frac{x}{(\log x)^{2-\varepsilon-\alpha}}\right) \tag{6.16}$$

for any $\varepsilon > 0$.

7. The Functions $\omega(n)$ and $\Omega(n)$

7.1. *Proof of Theorem* 1.9

We have

$$\begin{aligned}\sum_{p\le x} \omega(i_a(p)) &= \sum_{p\le x} \sum_{q\mid i_a(p)} 1 = \sum_{q\le x} \sum_{\substack{p\le x\\ q\mid i_a(p)}} 1 = \sum_{q\le x} \pi_q(x) \\ &= \sum_{q\le y} \pi_q(x) + \sum_{y<q\le z} \pi_q(x) + \sum_{z<q\le x} \pi_q(x), \end{aligned} \tag{7.1}$$

where y and z with $y \le z \le x$ will be chosen later. By GRH and Corollary 3.6, we have

$$\begin{aligned}\sum_{q\le y} \pi_q(x) &= \sum_{q\le y} \left(\frac{\mathrm{li}(x)}{[\mathbb{Q}(\zeta_q, a^{1/q}) : \mathbb{Q}]} + O(\sqrt{x}\log(qx))\right) \\ &= \mathrm{li}(x) \sum_{q\le y} \frac{1}{[\mathbb{Q}(\zeta_q, a^{1/q}) : \mathbb{Q}]} + O\left(\frac{y\sqrt{x}\log x}{\log y}\right)\end{aligned}$$

$$= \mathrm{li}(x) \sum_{q \geq 2} \frac{1}{[\mathbb{Q}(\zeta_q, a^{1/q}) : \mathbb{Q}]} + O\left(\mathrm{li}(x) \sum_{q > y} \frac{1}{[\mathbb{Q}(\zeta_q, a^{1/q}) : \mathbb{Q}]} \right)$$

$$+ O\left(\frac{y\sqrt{x} \log x}{\log y} \right). \tag{7.2}$$

By Corollary 3.4, we have that

$$c_{a,\omega} := \sum_{q \geq 2} \frac{1}{[\mathbb{Q}(\zeta_q, a^{1/q}) : \mathbb{Q}]} \tag{7.3}$$

is a constant, and

$$\sum_{q > y} \frac{1}{q\varphi(q)} \ll \sum_{q > y} \frac{1}{q^2} \ll \frac{1}{y \log y}. \tag{7.4}$$

Thus,

$$\sum_{q \leq y} \pi_q(x) = c_{a,\omega} \mathrm{li}(x) + O\left(\frac{\mathrm{li}(x)}{y \log y} \right) + O\left(\frac{y\sqrt{x} \log x}{\log y} \right). \tag{7.5}$$

Suppose $z > \sqrt{x}$. Then, we have

$$\sum_{q > z} \pi_q(x) = \sum_{q > z} \#\{p \leq x : q | i_a(p)\}$$

$$= \# \bigcup_{q > z} \{p \leq x : q | i_a(p)\}. \tag{7.6}$$

To see this last equality, note that if p contributes to both $\pi_{q_1}(x)$ and $\pi_{q_2}(x)$, then q_1 and q_2 divide $i_a(p)$. However, if $q_1 \neq q_2$, then since they are primes, $q_1 q_2 | i_a(p)$, but $q_1 > z \geq \sqrt{x}$ and $q_2 > z \geq \sqrt{x}$. Thus, $x < q_1 q_2 \leq i_a(p) \leq p - 1 < x$, which is a contradiction. Therefore, $q_1 = q_2$ and the above inequality holds. Clearly,

$$\bigcup_{q > z} \{p \leq x : q | i_a(p)\} = \{p \leq x : q | i_a(p) \text{ for some } q > z\}$$

$$\subset \left\{ p \leq x : f_a(p) \leq \frac{x}{z} \right\}, \tag{7.7}$$

where we recall that $f_a(p)$ is the order of a modulo p. Therefore,

$$\sum_{q > z} \pi_q(x) \leq \# \left\{ p \leq x : f_a(p) \leq \frac{x}{z} \right\}$$

$$\leq \# \left\{ p : p \,\Big|\, \prod_{m \leq \frac{x}{z}} (a^m - 1) \right\}$$

$$\leq \sum_{m \leq \frac{x}{z}} \omega(a^m - 1) \ll \sum_{m \leq \frac{x}{z}} \frac{m}{\log m}$$

$$\ll \frac{x^2}{z^2 \log(x/z)}. \tag{7.8}$$

Let $y = \frac{\sqrt{x}}{(\log x)^4}$ and $z = \sqrt{x}(\log x)^2$. Then, we have

$$\sum_{q\le x}\pi_q(x) = c_{a,\omega}\mathrm{li}(x) + \sum_{y<q\le z}\pi_q(x) + O\bigg(\sqrt{x}\log x + \frac{x}{(\log x)^3} + \frac{x}{(\log x)^5}\bigg)$$

$$= c_{a,\omega}\mathrm{li}(x) + \sum_{y<q\le z}\pi_q(x) + O\bigg(\frac{x}{(\log x)^3}\bigg). \tag{7.9}$$

Then, since $q|i_a(p)$ implies $q|p-1$, we have

$$\sum_{y<q\le z}\pi_q(x) \ll \sum_{y<q\le z}\pi(x;q,1) \ll \frac{x}{\log x}\sum_{y<q\le z}\frac{1}{q}$$

$$\ll \frac{x}{(\log x)^2}\sum_{y<q\le z}\frac{\log q}{q} \ll \frac{x\log\log x}{(\log x)^2} \tag{7.10}$$

by Mertens' theorem [6, Theorem 1.4.3] and the Brun–Titchmarsh inequality [6, Theorem 7.3.1]. Therefore, we have

$$\sum_{p\le x}\omega(i_a(p)) = \sum_{q\le x}\pi_q(x) = c_{a,\omega}\mathrm{li}(x) + O\bigg(\frac{x\log\log x}{(\log x)^2}\bigg). \tag{7.11}$$

7.2. *Proof of Theorem* 1.10

We have

$$\sum_{p\le x}\Omega(i_a(p)) = \sum_{p\le x}\sum_{q^k\|i_a(p)} k = \sum_{q\le x}\sum_{\substack{p\le x\\ q^k|i_a(p)}} 1 = \sum_{q^k\le x}\pi_{q^k}(x)$$

$$= \sum_{q^k\le y}\pi_{q^k}(x) + \sum_{q^k>y}\pi_{q^k}(x), \tag{7.12}$$

where y with $y\le x$ will be chosen later.

By GRH and Corollary 3.6, we have

$$\sum_{q^k\le y}\pi_{q^k}(x) = \sum_{q^k\le y}\bigg(\frac{\mathrm{li}(x)}{[\mathbb{Q}(\zeta_{q^k}, a^{1/q^k}):\mathbb{Q}]} + O(\sqrt{x}\log(q^k x))\bigg)$$

$$= \mathrm{li}(x)\sum_{q^k\le y}\frac{1}{[\mathbb{Q}(\zeta_{q^k}, a^{1/q^k}):\mathbb{Q}]} + O\bigg(\frac{y\sqrt{x}\log x}{\log y}\bigg)$$

$$= \mathrm{li}(x)\sum_{q^k\ge 2}\frac{1}{[\mathbb{Q}(\zeta_{q^k}, a^{1/q^k}):\mathbb{Q}]} + O\bigg(\mathrm{li}(x)\sum_{q^k>y}\frac{1}{[\mathbb{Q}(\zeta_{q^k}, a^{1/q^k}):\mathbb{Q}]}\bigg)$$

$$+ O\bigg(\frac{y\sqrt{x}\log x}{\log y}\bigg). \tag{7.13}$$

By Corollary 3.4,

$$c_{a,\Omega} := \sum_{q^k \geq 2} \frac{1}{[\mathbb{Q}(\zeta_{q^k}, a^{1/q^k}) : \mathbb{Q}]} \tag{7.14}$$

is a constant, and

$$\sum_{q^k > y} \frac{1}{q^k \varphi(q^k)} \ll \sum_{q^k > y} \frac{1}{q^{2k}} \ll \frac{1}{y \log y}. \tag{7.15}$$

Thus,

$$\sum_{q^k \leq y} \pi_{q^k}(x) = c_{a,\Omega} \mathrm{li}(x) + O\left(\frac{\mathrm{li}(x)}{y \log y}\right) + O\left(\frac{y\sqrt{x} \log x}{\log y}\right). \tag{7.16}$$

Let $y = \frac{\sqrt{x}}{(\log x)^4}$. Then,

$$\sum_{q^k \leq y} \pi_{q^k}(x) = c_{a,\Omega} \mathrm{li}(x) + O\left(\frac{x}{(\log x)^4}\right). \tag{7.17}$$

Now,

$$\sum_{q^k > y} \pi_{q^k}(x) = \sum_{q > y} \pi_q(x) + \sum_{\substack{q^k > y \\ k \geq 2}} \pi_{q^k}(x). \tag{7.18}$$

However, using the trivial bound $\pi_d(x) \leq x/d$, we have

$$\sum_{\substack{q^k > y \\ k \geq 2}} \pi_{q^k}(x) \ll \sum_{\substack{q^k > y \\ k \geq 2}} \frac{x}{q^k} \ll \frac{x}{\sqrt{y}} = x^{\frac{3}{4}} (\log x)^{\frac{3}{2}}. \tag{7.19}$$

Finally, we have

$$\sum_{q > y} \pi_q(x) = \sum_{y < q \leq z} \pi_q(x) + \sum_{q > z} \pi_q(x). \tag{7.20}$$

Let $z = \sqrt{x}(\log x)^2$. Then, as in the previous proof, we have

$$\sum_{q > z} \pi_q(x) \ll \frac{x}{(\log x)^5} \tag{7.21}$$

and

$$\sum_{y < q \leq z} \pi_q(x) \ll \frac{x \log\log x}{(\log x)^2}. \tag{7.22}$$

Therefore, we have

$$\sum_{p \leq x} \Omega(i_a(p)) = \sum_{q^\alpha \leq x} \pi_{q^\alpha}(x) = c_{a,\Omega} \mathrm{li}(x) + O\left(\frac{x \log\log x}{(\log x)^2}\right). \tag{7.23}$$

Comment. We note that the coefficients $c_{a,f}$ in Theorem 1.7 may tell us important information about the statistics of the sequence of numbers $i_a(p)$ as p ranges over primes. We relegate the determination of these statistics to a future paper.

Acknowledgments

The research of the first author was supported by an NSERC PGS-D scholarship. The research of the second author was supported by an NSERC Discovery grant. Some portions of this work were part of the doctoral thesis of the first author [11]. We thank Amir Akbary and Pieter Moree for their comments on an earlier version of this work. We also thank the referee for their comments.

References

[1] E. Artin, *Collected Papers* (Addison-Wesley, Reading, MA, 1965).
[2] E. Bach, R. Lukes, J. Shallit and H. C. Williams, Results and estimates on pseudoprimes, *Math. Comp.* **65** (1996) 1737–1747.
[3] B. J. Birch, Cyclotomic fields and Kummer extensions, in *Algebraic Number Theory*, eds. J. W. S Cassels and A. Fröhlich (London Mathematical Society, 2010), pp. 85–93.
[4] N. 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 (in Russian).
[5] ———, Die Bestimmung der Dichtigkeit einer Menge Von Primzahlen, welche zu einer gegebeben Substitutionsklasse gehören, *Math. Ann.* **95** (1925) 191–228 (in German).
[6] A. C. Cojocaru and M. R. Murty, *An Introduction to Sieve Methods and Their Applications* (Cambridge University Press, New York, 2006).
[7] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 2nd edn. (Wiley, Hoboken, NJ, 2004).
[8] P. D. T. A. Elliott and L. Murata, On the average of the least primitive root modulo p, *J. London Math. Soc.* (*2*) **56** (1997) 435–454.
[9] P. Erdös and M. R. Murty, The order of a (mod p), in *Number Theory*, CRM Proceedings Lecture Notes, Vol. 19 (American Mathematical Society, Providence, RI, 1999), pp. 87–97.
[10] J. Esmonde and M. R. Murty, *Problems in Algebraic Number Theory* (Springer-Verlag, New York, 2005).
[11] A. T. Felix, Variations on Artin's primitive root conjecture, Ph.D. thesis, Queen's University (2011).
[12] 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.
[13] K. Ford, The distribution of integers with a divisor in a given interval, *Ann. of Math.* (*2*) **168**(2) (2008) 367–433.
[14] J. B. Friedlander and H. Iwaniec, The illusory sieve, *Int. J. Number Theory* **1**(4) (2005) 459–494.
[15] ———, *Opera de Cribro*, American Mathematical Society Colloquium Publications, Vol. 57 (American Mathematical Society, Providence, RI, 2010).
[16] C. F. Gauss, *Disquisitiones Arithmetical*, English translation by Arthur A. Clarke (Yale University Press, 1965).
[17] R. Gupta and M. R. Murty, A remark on Artin's conjecture, *Invent. Math.* **78** (1984) 127–130.
[18] D. R. Heath-Brown, Artin's conjecture for primitive roots, *Q. J. Math.* **37** (1986) 27–38.

[19] C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967) 209–220.
[20] ———, *Applications of Sieve Methods to the Theory of Numbers* (Cambridge University Press, Cambridge, 1976).
[21] H. Iwaniec and R. Munshi, Cubic polynomials and quadratic forms, *J. London Math. Soc.* (*2*) **81**(1) (2010) 45–64.
[22] G. J. Janusz, *Algebraic Number Fields*, Graduate Studies in Mathematics, Vol. 7, 2nd edn. (American Mathematical Society, Providence, RI, 1996).
[23] J. Lagarias and A. Odlyzko, Effective versions of the Chebotarev density theorem, in *Algebraic Number Fields*, ed. A. Frohlich (Academic Press, 1977), pp. 409–464.
[24] B. Landreau, Majorations de fonctions arithmétiques en moyenne sur des ensembles de faible densité, in *Séminaire de Théorie des Nombres*, 1987–1988 (Talence, 1987–1988) (Univ. Bordeaux I, Talence, 1988), Exp. No. 13, 18 pp. (in French).
[25] S. Lang, *Elliptic Curves*: *Diophantine Analysis* (Springer-Verlag, Berlin, 1978).
[26] D. H. Lehmer and E. Lehmer, Heuristics anyone?, in *Studies in Mathematical Analysis and Related Topics*, eds. G. Szego *et al.* (Stanford University Press, 1962), pp. 202–210.
[27] P. Moree, On the distribution of the order and index of $g \pmod p$ over residue classes I, *J. Number Theory* **114**(2) (2005) 238–271.
[28] L. Murata, A problem analogous to Artin's conjecture for primitive roots and its applications, *Arch. Math.* **57** (1991) 555–565.
[29] M. R. Murty and V. K. Murty, The Chebotarev density theorem and pair correlation of zeros of Artin L-functions, preprint (2004) 19 pp.
[30] M. R. Murty, V. K. Murty and N. Saradha, Modular forms and the Chebotarev density theorem, *Amer. J. Math.* **110** (1988) 253–281.
[31] F. Pappalardi, On Hooley's theorem with weights, *Rend. Sem. Mat. Univ. Pol. Torino* **53** (1995) 375–388.
[32] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. Inst. Hautes Études Sci.* **54** (1981) 323–401 (in French).
[33] P. J. Stephens, Prime divisors of second-order linear recurrences. I, *J. Number Theory* **8** (1976) 313–332.
[34] P. Stevenhagen, The correction factor in Artin's primitive root conjecture, *J. Théor. Nombres Bordeaux* **15** (2003) 383–391.
[35] J. G. van der Corput, Une inégalité relative au nombre de diviseurs, *Kon. Nederl. Akad. Wetensch. Proc.* **42** (1939) 547–553 (in French).
[36] S. S. Wagstaff, Jr., Pseudoprimes and a generalization of Artin's conjecture, *Acta Arith.* **41** (1982) 141–150.