ON THE AVERAGE VALUE OF A FUNCTION OF THE RESIDUAL INDEX

AMIR AKBARY AND ADAM TYLER FELIX

ABSTRACT. For a prime p and a positive integer a relatively prime to p, we denote $i_a(p)$ as the index of the subgroup generated by a in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. Under certain conditions on the arithmetic function $f(n)$, we prove that the average value of $f(i_a(p))$, as a and p vary, is

$$\sum_{d=1}^{\infty} \frac{g(d)}{d\varphi(d)},$$

where $g(n) = \sum_{d|n} \mu(d)f(n/d)$ is the Möbius inverse of f and $\varphi(n)$ is the Euler function.

In honor of V. Kumar Murty on his sixtieth birthday

1. INTRODUCTION

For a prime p and a positive integer a relatively prime to p, we define the *residual index* of a mod p as the index of the subgroup $\langle a \rangle$ in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. We denote the residual index of a mod p by $i_a(p)$. There is vast literature on the distribution of the residual indices largely motivated by efforts on resolving the celebrated Artin's primitive root conjecture which deals with the distribution of primes p for which $i_a(p) = 1$ (see [12] for an extensive survey of results and generalizations related to this conjecture). More precisely, denoting the characteristic function of the set $\{1\}$ by $\chi_{\{1\}}$, Artin's conjecture predicts the average value of the function $\chi_{\{1\}}(i_a(p))$, for fixed a, as p varies. In [11], by heuristic reasoning, Laxton conjectured that, for a fixed integer $a > 1$, the density of the prime divisors of the recurrence $w_{n+2} = (a+1)w_{n+1} - aw_n$ is the same as the average value of $1/i_a(p)$ as p varies over primes (see [12, Section 9.4] for the latest developments on this conjecture).

In this note, we are partly inspired by a conjecture on the average value of $\log i_a(p)$ which is formulated in studying a concrete number-theoretic problem. An integer n is called an *x-pseudopower* of the base 2 if n is not a power of 2, but for all primes $p \leq x$ there is an integer $e_p \geq 0$ such that $n \equiv 2^{e_p} \bmod p$. In [1], Bach, Lukes, Shallit, and Williams studied the function $P_2(x)$, the smallest x-pseudopower of the base 2. The following conjecture is formulated in [1, p. 1740] following some probabilistic arguments.

Conjecture 1.1 (Bach-Lukes-Shallit-Williams). We have

$$\log P_2(x) \sim c_2 \frac{x}{\log x},$$

as $x \to \infty$, where c_2 is the constant in the asymptotic

$$\sum_{p \leq x} \log i_2(p) \sim c_2 \frac{x}{\log x},$$

as $x \to \infty$.

A similar conjecture and related results for a general base are stated in [1]. Conjecture 1.1 is a culmination of two conjectures (one regarding $P_2(x)$ and the other one related to $\log i_2(p)$). Fomenko [6] stated the second conjecture more explicitly. We state a version of the conjecture with an explicit constant.

Date: June 14, 2018.

Research of the first author is partially supported by NSERC. Research of the second author is partially supported by a PIMS postdoctoral fellowship.

Conjecture 1.2. For $a > 1$, as $x \to \infty$,

$$\sum_{p\le x} \log i_a(p) \sim c_a \mathrm{li}(x), \qquad \text{where} \qquad c_a := \sum_{d=1}^{\infty} \frac{\Lambda(d)}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]}. \tag{1.1}$$

Here, $\Lambda(d)$ is the von Mangoldt function, ζ_d is a primitive d-th root of unity, $a^{1/d}$ is the positive d-th root of a, and $\mathrm{li}(x) = \int_2^x dt/\log t$.

The exact values of $[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]$ are known (see Lemma 4.1). By employing these values we can show that $c_a > 0$. The best conditional upper bound and unconditional lower bounds on the above conjecture are due to Pappalardi [13, p. 386, Example 4]. Fomenko [6, Theorem 6(a)] gives a conditional resolution of this conjecture under the assumptions of the Generalized Riemann Hypothesis (GRH) and Conjecture A of Hooley. Another related result is [4, Theorem 1.5] that establishes, under the assumption of GRH, for $\alpha \in (0,1)$ the asymptotic

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

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

The conjectures discussed above can be considered as instances of a more general problem. In [13, p. 377] the following problem is proposed.

Generalized Artin Problem 1.3. For certain integers a and arithmetic functions $f(n)$, establish the asymptotic formula

$$\sum_{p\le x} f(i_a(p)) \sim c_{f,a}\mathrm{li}(x),$$

as $x \to \infty$, where

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

Here $g(n) = \sum_{d|n} \mu(d) f(n/d)$ is the Möbius inverse of $f(n)$.

Note that c_a given in (1.1) is the same as $c_{\log,a}$ as defined in Problem 1.3. The results on Problem 1.3 can be found in [13] and [4]. Most notably, under the assumption of GRH, Theorem 1.7 of [4] shows

$$\sum_{p\le x} f(i_a(p)) = c_{f,a}\mathrm{li}(x) + O_a\left(\frac{x}{(\log x)^{2-\epsilon-\alpha}}\right) \tag{1.2}$$

for arithmetic functions f and g satisfying

$$g(n) \ll \tau_k(n)^r (\log n)^{\alpha}, \tag{1.3}$$

with $k, r \in \mathbb{N}$ and $0 \le \alpha < 1$ all fixed. Here, $\tau_k(n)$ denotes the number of representations of n as product of k positive integers. Note that in the above asymptotic formula $c_{f,a}$ can be zero for certain a and f.

Our first result states that (1.2) is true when averaging over a for a larger class of functions f than those satisfying (1.3).

Theorem 1.4. *Let $A > 1$ and $\beta < 1/2$. Suppose f and g are arithmetic functions such that, for all $n \in \mathbb{N}$,*

$$f(n) = \sum_{d|n} g(d) \qquad \text{and} \qquad g(n) \ll \exp\left((\log n)^{\beta}\right). \tag{1.4}$$

Then there exists a constant $c_1 > 0$ such that if $N > \exp(c_1(\log x)^{1/2})$, we have

$$\frac{1}{N}\sum_{a\le N}\sum_{p\le x} f(i_a(p)) = c_f\mathrm{li}(x) + O\left(\frac{x}{(\log x)^{A}}\right),$$

where

$$c_f := \sum_{d=1}^{\infty} \frac{g(d)}{d\varphi(d)}. \tag{1.5}$$

Note that (1.4) implies that $g(n) \ll n^\epsilon$ for all $\epsilon > 0$. Hence, the lower bound $d/\log\log d$ for $\varphi(d)$ (see [9, p. 267, Theorem 328]) yields

$$\sum_{d>y} \frac{g(d)}{d\varphi(d)} \ll \sum_{d>y} \frac{|g(d)|\log\log d}{d^2} \ll \sum_{d>y} \frac{1}{d^{2-\epsilon}} \ll \frac{1}{y^{1-\epsilon}}.$$

Thus, (1.5) is well-defined. Observe that c_f is well-defined as long as $g(n) \ll n^{1-\epsilon}$ for some $\epsilon > 0$.

For $f(n) = \chi_{\{1\}}(n)$ and $f(n) = 1/n$, Theorem 1.4 reproduces the results of Stephens [14] on the average Artin's conjecture and the average value of the counting function of prime divisors of a second-order linear recurrence. For $f(n) = \log n$ we have that $g(n) = \Lambda(n)$, the von Mangoldt function. Thus, we have the following direct corollary of Theorem 1.4.

Corollary 1.5. *Let $A > 1$ be fixed. Then there exists a constant $c_1 > 0$ such that if $N > \exp(c_1(\log x)^{1/2})$, we have*

$$\frac{1}{N}\sum_{a\le N}\sum_{p\le x} \log i_a(p) = \left(\sum_{d=1}^{\infty} \frac{\Lambda(d)}{d\varphi(d)}\right) \mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right).$$

The above corollary establishes that Conjecture 1.2 is true when averaging over a. It also provides a strengthening of [5, Theorem 3], which is an upper bound with the larger constant

$$\sum_{d=1}^{\infty} \frac{\log d}{d\varphi(d)}$$

instead of an asymptotic formula as in Corollary 1.5. We point out that the strategy of the proof of Theorem 3 of [5], and also our proof of Theorem 1.4, closely follow Stephens' proof of the average Artin conjecture in [14]. However a direct application of Stephens' method, as done in the proof of Theorem 3 of [5], will result in a complicated sum in the main term. The proof within [14] builds on the character sum $c_r(\chi)$ defined in (3.2). The novelty of our proof is use of a different character sum $C_d(\chi)$ defined in (3.1), which leads to an easier evaluation of the main term in Theorem 1.4.

We next note that

$$\sum_{d=1}^{\infty} \frac{\Lambda(d)}{d\varphi(d)} = \sum_{\substack{q\ge 2\\ \text{prime}}} \frac{q\log q}{(q-1)^2(q+1)}.$$

The sum on the right-hand side is the predicted expected value of $\log i_a(p)$ on [1, p. 1741], which is obtained following a probabilistic argument. A close examination of the heuristics in [1] reveals an explicit expression for the expected value of $f(i_a(p))$ for any additive arithmetic function $f(n)$ of suitable size. More precisely, if f is an additive function, we expect

$$c_f = \sum_{\substack{q\ge 2\\ \text{prime}}} \sum_{e\ge 1} \left(\frac{f(q^e)}{q^{2e}} + \frac{q-1}{q^{e+1}}\sum_{j=1}^{e-1}\frac{f(q^j)}{q^j}\right). \tag{1.6}$$

In fact we show that this is the case. If f is an additive function such that (1.6) converges absolutely, then

$$\sum_{d=1}^{\infty} \frac{g(d)}{d\varphi(d)} = \sum_{\substack{q\ge 2\\ \text{prime}}} \sum_{e\ge 1} \left(\frac{f(q^e)}{q^{2e}} + \frac{q-1}{q^{e+1}}\sum_{j=1}^{e-1}\frac{f(q^j)}{q^j}\right), \tag{1.7}$$

where

$$g(n) = \begin{cases} f(q^k) - f(q^{k-1}) & \text{if } n = q^k, \\ 0 & \text{otherwise.} \end{cases}$$

Here q denotes a prime and $g(n)$ is the Möbius inverse of the additive function $f(n)$. The proof of (1.7) is a straightforward computation of the coefficients of $f(q^i)$ on both sides of (1.7).

Recall that, for fixed a and certain functions f, the Generalized Artin Problem 1.3 predicts $c_{f,a}$ is the average value of $f(i_a(p))$, as p varies over primes. On the other hand Theorem 1.4 gives c_f as the average value of $f(i_a(p))$, as p varies over primes and a varies over positive integers. It is natural to ask whether or not the average value of $c_{f,a}$, as a varies, is c_f. For the Lang-Trotter conjecture for elliptic curves such questions have been asked by David and Pappalardi in [3]. In [10] Jones obtained results on such questions for several conjectures related to elliptic curves. We prove that under certain conditions the average of $c_{f,a}$, for $2 \le a \le N$, approaches c_f, as $N \to \infty$.

Theorem 1.6. *Let f and g be arithmetic functions such that*

$$f(n) = \sum_{d|n} g(d) \qquad \textit{and} \qquad g(n) \ll n^{1-\epsilon} \tag{1.8}$$

for a fixed $\epsilon > 0$. Moreover, assume that $g(n)$ is supported on prime powers (i.e., $g(n) = 0$ for n not a prime power). We have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{2\le a\le N} c_{f,a} = c_f.$$

Corollary 1.7. *We have*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{2\le a\le N} \sum_{d=1}^{\infty} \frac{\Lambda(d)}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} = \sum_{d=1}^{\infty} \frac{\Lambda(d)}{d\varphi(d)}.$$

The proof of Theorem 1.6 uses an explicit formula for the values $[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]$ obtained by Wagstaff (see Lemma 4.1).

Remarks 1.8. (i) One can formulate results similar to Theorems 1.4 and 1.6 for the case $a < 0$.

(ii) Examining the proofs of Theorems 1.4 and 1.6 show that the assertions of these theorems remain true for functions $g(n)$ that are slightly larger than the written bounds in the theorems. For example the bound $\exp\left((\log n)^{\beta}\right)$ in Theorem 1.4 can be replaced by $\exp(h(n))$ where $h(n) = o\left((\log n)^{1/2}/\log\log n\right)$, as $n \to \infty$.

(iii) Note that the assertion of Theorem 1.6 is true for any additive function $f(n)$ with $g(n) \ll n^{1-\epsilon}$ for $\epsilon > 0$.

(iv) In Theorem 1.6, the condition that $g(n)$ is supported on prime powers is introduced in order to conveniently handle one of the error terms. We except that similar results to hold for arithmetic functions which have support outside the prime powers.

(v) It may be possible to prove results analogous to [14, Theorems 3 and 4] under suitable bounds on $f(n)$ and for all sufficiently large N. That is,

$$\sum_{p\le x} f(i_a(p)) \sim c_f \mathrm{li}(x),$$

as $x \to \infty$, holds for almost all positive integers $a \le N$.

The structure of the paper is as follows. In Section 2 we provide a heuristic argument that predicts the expression (1.6) for the average value c_f, where f is an additive arithmetic function. Section 3 is dedicated to a proof of Theorem 1.4. Finally in Section 4 we prove Theorem 1.6.

2. THE CASE OF ADDITIVE ARITHMETIC FUNCTIONS

Let f be an additive arithmetic function. Thus, $f(mn) = f(m) + f(n)$ for all coprime pairs (m,n). Note that for such function $f(1) = 0$. We follow closely the probabilistic argument given on [1, p. 1741] for the expected value of $\log i_a(p)$ to derive a formula for the expected value of $f(i_a(p))$ as p and a vary. We assume that f satisfies suitable growth conditions such that infinite sums occurring in the following argument are absolutely convergent. We denote the probability of an event A by $\Pr(A)$ and the expected value of a random variable X by $\mathrm{E}(X)$.

Writing $p-1 = q_1^{e_1}\dots q_r^{e_r}$ for a prime p yields

$$(\mathbb{Z}/p\mathbb{Z})^\times = C_1 \times \dots \times C_r,$$

where C_i is the q_i-Sylow subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. Note that each C_i is a cyclic subgroup of order $q_i^{e_i}$. Let $(a,p)=1$. Then a has the unique representation $a = a_1a_2\dots a_r$, where $a_i \in C_i$. Thus we have

$$i_a(p) = \prod_{i=1}^r [C_i : \langle a_i\rangle],$$

where $[C_i : \langle a_i\rangle]$ is the index of the subgroup $\langle a_i\rangle$ in the cyclic group C_i. Since f is additive, for fixed p, we have

$$f(i_a(p)) = f\left(\prod_{i=1}^r [C_i : \langle a_i\rangle]\right) = \sum_{i=1}^r f\left(\frac{q_i^{e_i}}{|\langle a_i\rangle|}\right).$$

Observe that for fixed $q_i^{e_i}$, we have, for $0 \le \alpha \le e_i$,

$$\Pr(|\langle a_i\rangle| = q_i^\alpha) = \frac{\varphi(q_i^\alpha)}{q_i^{e_i}}.$$

Therefore for a fixed $q_i^{e_i}\|(p-1)$ and varying a_i, we have

$$\mathrm{E}\left(f\left(\frac{q_i^{e_i}}{|\langle a_i\rangle|}\right)\right) = \frac{1}{q_i^{e_i}}f(q_i^{e_i}) + \frac{q_i-1}{q_i^{e_i}}f(q_i^{e_i-1}) + \dots + \frac{q_i-1}{q_i}f(1). \tag{2.1}$$

Let q be a fixed prime and e be a fixed non-negative integer. Heuristically,

$$\left(\frac{f(q^e)}{q^e} + \frac{q-1}{q}\sum_{j=1}^{e-1}\frac{f(q^j)}{q^j}\right)\frac{1}{q^e} \tag{2.2}$$

is the expected value of $f\left(\frac{q^e}{|\langle a_{p,q}\rangle|}\right)$, where $a_{p,q}$ is the image of a in q-Sylow subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$, as a varies over integers and p varies over all primes with $q^e\|(p-1)$. Note that (2.2) is the product of the expectation (2.1) and the density of primes p such that $q^e\|(p-1)$ (i.e., $\varphi(q)/\varphi(q^{e+1}) = 1/q^e$).

Now since f is additive, a natural candidate for the expected value of $f(i_a(p))$ is

$$\sum_{\substack{q\ge 2\\ \text{prime}}}\sum_{e\ge 1}\left(\frac{f(q^e)}{q^{2e}} + \frac{q-1}{q^{e+1}}\sum_{j=1}^{e-1}\frac{f(q^j)}{q^j}\right). \tag{2.3}$$

If $f(n)$ is completely additive (i.e. $f(mn) = f(m) + f(n)$ for all m,n), then (2.3) can be simplified to

$$\sum_{\substack{q\ge 2\\ \text{prime}}}\sum_{e\ge 1} f(q)\left(\frac{e}{q^{2e}} + \frac{q-1}{q^{e+1}}\sum_{j=1}^{e-1}\frac{j}{q^j}\right) = \sum_{\substack{q\ge 2\\ \text{prime}}}\frac{qf(q)}{(q-1)^2(q+1)}. \tag{2.4}$$

Note that both (2.3) and (2.4) can be given as a unified formula

$$\sum_{d=1}^{\infty} \frac{g(d)}{d\varphi(d)},$$

where $g(d) = \sum_{\delta|d} \mu(\delta) f(d/\delta)$. In the next section we rigorously prove that this value is the average value of $f(i_a(p))$ for a large class of arithmetic functions f (not necessarily additive) that satisfy a suitable growth condition.

3. The case of general arithmetic functions

For $d \mid p-1$ and a Dirichlet character mod p, we set

$$C_d(\chi) = \frac{1}{p-1} \sideset{}{'}\sum_{b \bmod p} \bar{\chi}(b), \tag{3.1}$$

where the sum is taken over integers $1 \le b \le p$ with the property that $\mathrm{ord}_b(p) \mid (p-1)/d$. Here, $\mathrm{ord}_b(p)$ denotes the multiplicative order of b mod p. Letting

$$c_r(\chi) = \frac{1}{p-1} \sideset{}{''}\sum_{b \bmod p} \bar{\chi}(b), \tag{3.2}$$

where the sum is taken over integers $1 \le b \le p$ with the property that $\mathrm{ord}_b(p) = r$, we conclude that

$$C_d(\chi) = \sum_{r|\frac{p-1}{d}} c_r(\chi). \tag{3.3}$$

Let χ_0 denote the principal character mod p. From [14, Lemma 1] we know that if $\chi \ne \chi_0$, then

$$|c_r(\chi)| \le \frac{((p-1)/r, k)}{k(p-1)/r},$$

where k is the order of χ, and if $\chi = \chi_0$, then $|c_r(\chi_0)| = \varphi(r)/(p-1)$. By employing these values in (3.3) we deduce that if $\chi \ne \chi_0$, then

$$|C_d(\chi)| \le \frac{1}{k} \sum_{r|\frac{p-1}{d}} \frac{((p-1)/r, k)}{(p-1)/r},$$

where k is the order of χ. Note that this upper bound implies that

$$|C_d(\chi)| \le \frac{\tau(\frac{p-1}{d})}{k}, \tag{3.4}$$

where $\tau(n)$ is the divisor function. Also, $C_d(\chi_0) = 1/d$.

By the orthogonality of characters, we observe that

$$\sum_{\chi (\mathrm{mod}\ p)} \chi(a) C_d(\chi) = \begin{cases} 1 & \text{if } d|i_a(p), \\ 0 & \text{otherwise.} \end{cases} \tag{3.5}$$

In the proof we need the following version of the large sieve inequality for multiplicative characters given in [8, p. 16].

Lemma 3.1 (Gallagher). *Let M and N be positive integers and $(a_n)_{n=M+1}^{M+N}$ be a sequence of complex numbers. Then*

$$\sum_{q \le Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi(q)} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \ll (N+Q^2) \sum_{n=M+1}^{M+N} |a_n|^2,$$

where Q is any positive real number and $\sum_{\chi(q)}^*$ denotes a sum over all primitive Dirichlet characters χ modulo q.

We next introduce notation and results from [14]. Let

$$\tau_{k,N}(n) := \#\left\{(a_1, a_2, \ldots, a_k) \in [1,N]^k \cap \mathbb{N}^k;\ n = a_1 a_2 \cdots a_k\right\}.$$

We also set

$$\psi(X,Y) := \sum_{\substack{n \le X \\ p(n) \le Y}} 1,$$

where $p(n)$ is the largest prime factor of n. Note that we define $p(1) = \infty$. Parts (i) and (ii) of the following lemma are [14, Lemma 10] and [14, Lemma 8], respectively.

Lemma 3.2 (Stephens). (i) *For $k \in \mathbb{N}$, if $N^k \le x^8$, then*

$$\sum_{n \le N^k} \tau_{k,N}(n)^2 < N^k \left(\psi(N, 9\log x)\right)^k.$$

(ii) *For a sufficiently large constant $c_1 > 0$ there exists $c_2 > 0$ such that, if*

$$\exp\left(c_1 (\log x)^{1/2}\right) < N \le x^2,$$

then

$$x^{-1/2k} \left(\psi(N, 9\log x)\right)^{1/2} \ll \exp\left(-c_2 (\log x)^{1/2} / \log\log x\right),$$

where

$$k = [2\log x / \log N] + 1.$$

We are now ready to prove our first result.

Proof of Theorem 1.4. By (3.5), we have

$$\begin{aligned}\frac{1}{N}\sum_{a \le N}\sum_{p \le x} f(i_a(p)) &= \frac{1}{N}\sum_{a \le N}\sum_{p \le x}\sum_{d \mid i_a(p)} g(d) \\ &= \frac{1}{N}\sum_{a \le N}\sum_{p \le x}\sum_{d \mid p-1} g(d) \sum_{\chi (\mathrm{mod}\ p)} \chi(a) C_d(\chi). \qquad (3.6)\end{aligned}$$

Interchanging the sums in (3.6), isolating the sum corresponding to the trivial character χ_0, and applying $C_d(\chi_0) = 1/d$ yield

$$\begin{aligned}\frac{1}{N}\sum_{a \le N}\sum_{p \le x} f(i_a(p)) &= \frac{1}{N}\sum_{p \le x}\sum_{d \mid p-1} g(d) \sum_{\chi \bmod p} C_d(\chi) \sum_{a \le N} \chi(a) \\ &= \frac{1}{N}\sum_{p \le x}\sum_{d \mid p-1} \frac{g(d)}{d}\left([N] - \left[\frac{N}{p}\right]\right) \\ &\quad + O\left(\frac{1}{N}\sum_{p \le x}\sum_{d \mid p-1} |g(d)| \sum_{\chi \ne \chi_0} |C_d(\chi)| \left|\sum_{a \le N} \chi(a)\right|\right). \qquad (3.7)\end{aligned}$$

3.1. **Evaluation of the main term of (3.7).** We have

$$\begin{aligned}\frac{1}{N}\sum_{p\le x}\sum_{d|p-1}\frac{g(d)}{d}\left([N]-\left[\frac{N}{p}\right]\right)&=\sum_{p\le x}\sum_{d|p-1}\frac{g(d)}{d}-\sum_{p\le x}\frac{1}{p}\sum_{d|p-1}\frac{g(d)}{d}+O\left(\frac{1}{N}\sum_{p\le x}\sum_{d|p-1}\frac{g(d)}{d}\right)\\&=\Sigma_1-\Sigma_2+O(\Sigma_3).\end{aligned}\tag{3.8}$$

Observe that

$$\sum_{p\le x}\sum_{d|p-1}\frac{g(d)}{d}=\sum_{d\le x}\frac{g(d)}{d}\pi(x;d,1),$$

where

$$\pi(x;d,1)=\#\{p\le x;\ p\equiv 1 \pmod d\}.$$

Thus, for $\alpha>1$, the sum Σ_1 in (3.8) is

$$\begin{aligned}\Sigma_1&=\sum_{d\le(\log x)^\alpha}\frac{g(d)}{d}\pi(x;d,1)+\sum_{(\log x)^\alpha<d\le x}\frac{g(d)}{d}\pi(x;d,1)\\&=\Sigma_{1,1}+\Sigma_{1,2}.\end{aligned}\tag{3.9}$$

The Siegel-Walfisz theorem (see [2, p. 125]) implies

$$\Sigma_{1,1}=\text{li}(x)\sum_{d\le(\log x)^\alpha}\frac{g(d)}{d\varphi(d)}+O\left(\frac{x}{(\log x)^B}\sum_{d\le(\log x)^\alpha}\frac{g(d)}{d}\right)$$

for any $B>1$. Thus, by (1.4) for $g(n)$, standard estimates yield

$$\begin{aligned}\Sigma_{1,1}&=\text{li}(x)\sum_{d\ge1}\frac{g(d)}{d\varphi(d)}+O\left(\text{li}(x)\sum_{d>(\log x)^\alpha}\frac{g(d)}{d\varphi(d)}\right)+O\left(\frac{x}{(\log x)^{B-1}}\right)\\&=c_f\text{li}(x)+O\left(\frac{x}{(\log x)^{1+\alpha(1-\epsilon)}}\right)+O\left(\frac{x}{(\log x)^{B-1}}\right)\\&=c_f\text{li}(x)+O\left(\frac{x}{(\log x)^{\min\{B-1,1+\alpha(1-\epsilon)\}}}\right)\end{aligned}\tag{3.10}$$

for arbitrary $\epsilon>0$.

Using the trivial bound for $\pi(x;d,1)$, we obtain

$$\Sigma_{1,2}\ll x\sum_{d>(\log x)^\alpha}\frac{g(d)}{d^2}\ll\frac{x}{(\log x)^{\alpha(1-\epsilon)}}.\tag{3.11}$$

Hence, applying (3.10) and (3.11) to (3.9) yields

$$\Sigma_1=c_f\text{li}(x)+O\left(\frac{x}{(\log x)^{\min\{B-1,\alpha(1-\epsilon)\}}}\right).$$

Note that, since B and α are arbitrary constants greater than 1, we have

$$\Sigma_1=c_f\text{li}(x)+O\left(\frac{x}{(\log x)^A}\right)\tag{3.12}$$

for any $A > 1$.

For Σ_2, we have

$$\Sigma_2 = \sum_{p \le x} \frac{1}{p} \sum_{d \mid p-1} \frac{g(d)}{d} = \sum_{d \le x} \frac{g(d)}{d} \sum_{\substack{p \le x \\ p \equiv 1 \bmod d}} \frac{1}{p}.$$

Thus, [2, p. 131, Exercise 9], [9, p. 267, Theorem 328], and (1.4) imply

$$\begin{aligned}\Sigma_2 &\ll \sum_{d \le x} \frac{g(d)(\log\log x + \log d)}{d\varphi(d)} \\ &\ll \exp\left((\log x)^{\beta}\right)(\log x + \log\log x).\end{aligned} \tag{3.13}$$

For Σ_3, note that

$$\Sigma_3 = \frac{1}{N}\Sigma_1 \ll \frac{\mathrm{li}(x)}{N}. \tag{3.14}$$

Now, (3.12), (3.13), and (3.14) applied to (3.8), imply the main term is equal to

$$c_f \mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right) + O\left(\frac{\mathrm{li}(x)}{N}\right) \tag{3.15}$$

for any $A > 1$.

3.2. **Evaluation of the Error Term of (3.7).**

We start by applying (1.4) and (3.4) to the error term in (3.7) to obtain

$$\begin{aligned}\frac{1}{N}\sum_{p \le x}\sum_{d \mid p-1} |g(d)| \sum_{\chi \ne \chi_0} |C_d(\chi)| \left|\sum_{n \le N} \chi(n)\right| &\ll \frac{\exp\left((\log x)^{\beta}\right)}{N} \sum_{p \le x}\sum_{\chi \ne \chi_0} \frac{1}{\mathrm{ord}\chi} \left|\sum_{n \le N} \chi(n)\right| \sum_{d \mid p-1} \tau\left(\frac{p-1}{d}\right) \\ &= \frac{\exp\left((\log x)^{\beta}\right)}{N} \sum_{p \le x} \tau_3(p-1) \sum_{\chi \ne \chi_0} \frac{1}{\mathrm{ord}\chi} \left|\sum_{n \le N} \chi(n)\right|,\end{aligned} \tag{3.16}$$

where $\tau_3(p-1) = \sum_{d \mid p-1} \tau(d)$ and $\mathrm{ord}\chi$ denotes the order of character χ. By Hölder's inequality, for any $k \in \mathbb{N}$, we have

$$\begin{aligned}\sum_{p \le x} \tau_3(p-1) \sum_{\chi \ne \chi_0} \frac{1}{\mathrm{ord}\chi} \left|\sum_{n \le N} \chi(n)\right| &\le \left(\sum_{p \le x}\sum_{\chi \ne \chi_0} \left(\frac{\tau_3(p-1)}{\mathrm{ord}\chi}\right)^{\frac{2k}{2k-1}}\right)^{1-\frac{1}{2k}} \left(\sum_{p \le x}\sum_{\chi \ne \chi_0} \left|\sum_{n \le N} \chi(n)\right|^{2k}\right)^{\frac{1}{2k}} \\ &= (\Sigma_4)^{1-\frac{1}{2k}} (\Sigma_5)^{\frac{1}{2k}}.\end{aligned} \tag{3.17}$$

For Σ_4, we have

$$\begin{aligned}\Sigma_4 &= \sum_{p \le x} \tau_3(p-1)^{\frac{2k}{2k-1}} \sum_{\chi \ne \chi_0} \frac{1}{(\mathrm{ord}\chi)^{\frac{2k}{2k-1}}} \\ &\ll \sum_{p \le x} \tau_3(p-1)^2 \sum_{\chi \ne \chi_0} \frac{1}{\mathrm{ord}\chi}.\end{aligned}$$

Note that

$$\sum_{\chi \ne \chi_0} \frac{1}{\mathrm{ord}\chi} = \sum_{d \mid p-1} \frac{1}{d} \sum_{\substack{\chi \ne \chi_0 \\ \mathrm{ord}\chi = d}} 1 \le \tau(p-1)$$

implies

$$\Sigma_4 \ll \sum_{p\le x} \tau_3(p-1)^3.$$

For the last summation, we can use truncated divisors from [7, Proposition 22.10] to get

$$\tau_3(p-1)^3 \le \sum_{\substack{d\mid p-1\\ d\le\sqrt{p}}} (2\tau(d))^{12}.$$

Thus,

$$\Sigma_4 \ll \sum_{p\le x}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}}} (2\tau(d))^{12}$$
$$\ll \sum_{d\le\sqrt{x}} \tau(d)^{12}\pi(x;d,1).$$

Now by applying the Brun-Titchmarsh inequality ([2, Theorem 7.3.1]), [9, p. 267, Theorem 328], and [2, Lemma 10.2.7] we conclude that

$$\Sigma_4 \ll \frac{x}{\log x}\sum_{d\le\sqrt{x}}\frac{\tau(d)^{12}}{\varphi(d)}$$
$$\ll x(\log x)^{4095}\log\log x. \tag{3.18}$$

By Lemma 3.1, we have

$$\Sigma_5 = \sum_{p\le x}\sum_{\chi\ne\chi_0}\left|\sum_{n\le N}\chi(n)\right|^{2k} \le \sum_{p\le x}\sum_{\chi\ne\chi_0}\left|\sum_{n\le N^k}\tau_{k,N}(n)\chi(n)\right|^{2}$$
$$\ll (x^2+N^k)\sum_{n\le N^k}\tau_{k,N}(n)^2.$$

Let $k=[2\log x/\log N]+1$. Now if $N>x^2$, then $k=1$, and thus

$$\Sigma_5 \ll N^2. \tag{3.19}$$

On the other hand if $\exp(c_1(\log x)^{1/2}) < N \le x^2$, where $c_1>0$ is the constant given in Lemma 3.2 (ii), we have that $k>1$ and $N^k\le x^4$. Therefore, by Lemma 3.2 (i), we have

$$\Sigma_5 \ll (x^2+N^k)N^k\left(\psi(N,9\log x)\right)^k. \tag{3.20}$$

Now applying (3.18), (3.19), (3.20) to (3.17) and using Lemma 3.2 (ii) yield

$$\sum_{p\le x}\tau_3(p-1)\sum_{\chi\ne\chi_0}\frac{1}{\mathrm{ord}\chi}\left|\sum_{n\le N}\chi(n)\right| \le Nx\exp\left(-c_2\frac{(\log x)^{1/2}}{\log\log x}\right)(\log x)^{4095}(\log\log x).$$

Finally by inserting the above bound to (3.16) and combining the error term with expression for the main term in (3.15), we have

$$\frac{1}{N}\sum_{p\le x}\sum_{a\le N} f(i_a(p)) = \left(\sum_{d=1}^{\infty}\frac{g(d)}{d\varphi(d)}\right)\mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right)$$

for $N>\exp(c_1(\log x)^{1/2})$ and all $A>1$. □

4. AVERAGE OF LOCAL AVERAGE VALUES

We need the following lemma which is Proposition 4.1 of [15] written for integers $a > 1$.

Lemma 4.1 (Wagstaff). *For an integer $a > 1$, write $a = a_0^{h_a}$, where a_0 is positive and not an exact power of an integer. Let $D(a)$ denote the discriminant of the field $\mathbb{Q}(\sqrt{a_0})$. Let $n_a = \operatorname{lcm}(2^{\nu_2(h_a)+1}, D(a))$, where $\nu_2(h_a)$ denotes the multiplicity of 2 in h_a. Then,*

$$[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}] = \frac{d\varphi(d)}{\varepsilon_a(d)\gcd(d, h_a)},$$

where

$$\varepsilon_a(d) = \begin{cases} 2 & \text{if } n_a \mid d, \\ 1 & \text{if } n_a \nmid d. \end{cases}$$

Proof of Theorem 1.6. In this proof a denotes an integer greater than 1. By Lemma 4.1 we have

$$\begin{aligned}\sum_{a\le N} c_{f,a} &= \sum_{a\le N}\sum_{d=1}^{\infty} \frac{g(d)}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} \\ &= \sum_{d=1}^{\infty} \frac{g(d)}{d\varphi(d)} \sum_{a\le N} \varepsilon_a(d)\gcd(d, h_a).\end{aligned}$$

Thus, our desired sum is

$$\sum_{a\le N} c_{f,a} = \sum_{d=1}^{\infty} \frac{g(d)}{d\varphi(d)} \left(\sum_{a\le N} \gcd(d, h_a) + \sum_{\substack{a\le N\\ n_a\mid d}} \gcd(d, h_a) \right).$$

Now by considering a parameter x we can write the above sum as

$$\begin{aligned}\sum_{a\le N} c_{f,a} &= \sum_{d\le x} \frac{g(d)}{d\varphi(d)} \left(\sum_{a\le N} \gcd(d, h_a) + \sum_{\substack{a\le N\\ n_a\mid d}} \gcd(d, h_a) \right) + \sum_{d> x} \frac{g(d)}{d\varphi(d)} \left(\sum_{a\le N} \gcd(d, h_a) + \sum_{\substack{a\le N\\ n_a\mid d}} \gcd(d, h_a) \right) \\ &= \Sigma_6 + \Sigma_7. \end{aligned} \tag{4.1}$$

We start by evaluating Σ_6. We have

$$\begin{aligned}\Sigma_6 &= \sum_{d\le x} \frac{g(d)}{d\varphi(d)} \sum_{a\le N} \gcd(d, h_a) + \sum_{d\le x} \frac{g(d)}{d\varphi(d)} \sum_{\substack{a\le N\\ n_a\mid d}} \gcd(d, h_a) \\ &= \Sigma_{6,1} + \Sigma_{6,2}.\end{aligned}$$

The inner summation in $\Sigma_{6,1}$ can be evaluated as follows.

$$\sum_{a\le N} \gcd(d, h_a) = \sum_{a\le N} \sum_{\substack{\delta\mid d\\ \delta\mid h_a}} \varphi(\delta) = \sum_{\delta\mid d} \varphi(\delta) \sum_{\substack{a\le N\\ \delta\mid h_a}} 1.$$

Note that, by the definition of h_a and since a is an integer greater than one, we have $\delta \mid h_a$ if and only if $a^{1/\delta} \in \mathbb{N} \setminus \{1\}$. Hence, the inner summation in the above sum becomes

$$\begin{aligned}\sum_{a\leq N} \gcd(d,h_a) &= \sum_{\delta\mid d}\varphi(\delta) \sum_{\substack{a\leq N\\ a^{1/\delta}\in\mathbb{N}\setminus\{1\}}} 1 = \sum_{\delta\mid d}\varphi(\delta)\left(N^{1/\delta}+O(1)\right)\\ &= N + O\left(dN^{1/2}\right).\end{aligned}$$

Therefore,

$$\begin{aligned}\Sigma_{6,1} &= \sum_{d\leq x}\frac{g(d)}{d\varphi(d)}\left(N+O\left(dN^{1/2}\right)\right)\\ &= N\sum_{d=1}^{\infty}\frac{g(d)}{d\varphi(d)} + O\left(N\sum_{d>x}\frac{g(d)}{d\varphi(d)}\right) + O\left(N^{1/2}\sum_{d\leq x}\frac{g(d)}{\varphi(d)}\right).\end{aligned}$$

We note that summation in the main term is c_f. The sum in the first error term is the tail of a convergent summation and can be bounded as follows. By (1.8) and the lower bound given in [9, p. 267, Theorem 328] for $\varphi(d)$, we have

$$\sum_{d>x}\frac{g(d)}{d\varphi(d)} \ll \sum_{d>x}\frac{\log\log d}{d^{1+\epsilon}} \ll \frac{1}{x^{\epsilon/2}}$$

for $\epsilon > 0$. Also, the sum in the second error term can be bounded by $x^{1-\epsilon}\log x$. Thus,

$$\Sigma_{6,1} = c_f N + O\left(\frac{N}{x^{\epsilon/2}}\right) + O\left(N^{1/2}x^{1-\epsilon}\log x\right). \tag{4.2}$$

For $\Sigma_{6,2}$, we recall that $n_a = \operatorname{lcm}(2^{\nu_2(h_a)+1}, D(a))$. Hence,

$$\begin{aligned}\Sigma_{6,2} &= \sum_{d\leq x}\frac{g(d)}{d\varphi(d)}\sum_{\substack{a\leq N\\ n_a\mid d}}\gcd(d,h_a)\\ &= \sum_{a\leq N}\sum_{\substack{d\leq x\\ 2^{\nu_2(h_a)+1}\mid d\\ D(a)\mid d}}\frac{g(d)\gcd(d,h_a)}{d\varphi(d)}.\end{aligned}$$

Now observe that d is a power of 2 since $g(n)$ is supported on prime powers and $2^{\nu_2(h_a)+1} \mid d$. On the other hand since $D(a) \mid d$, then $D(a)$ is a power of 2. Writing $a^{1/h_a} = a_0 = a_1^2 a_2$, for integer a_1 and square free integer a_2, we conclude that $D(a) = 4a_2$ or a_2. Since $D(a)$ is a power of 2, we have $a_2 = 2$ (in fact $D(a) = 8$). Thus, a^{1/h_a} is twice a perfect square. Writing $a = (2\square)^{h_a}$, we have

$$\Sigma_{6,2} \leq \sum_{\substack{a\leq N\\ a=(2\square)^{h_a}}}\sum_{m\leq \log x/\log 2}\frac{g(2^m)}{2^{m-1}} \ll N^{1/2}. \tag{4.3}$$

Here we used the facts that $\gcd(2^m, h_a) \leq 2^m$ and $\sum_{m=1}^{\infty} g(2^m)/2^m < \infty$ (by (1.8)). Hence, from (4.2) and (4.3) we deduce that

$$\Sigma_6 = c_f N + O\left(\frac{N}{x^{\epsilon/2}}\right) + O\left(N^{1/2}x^{1-\epsilon}\log x\right). \tag{4.4}$$

For Σ_7, by the aforementioned lower bound for $\varphi(d)$, we have

$$\begin{aligned}\Sigma_7 &= \sum_{d>x} \frac{g(d)}{d\varphi(d)} \left(\sum_{a\le N} \gcd(d, h_a) + \sum_{\substack{a\le N\\ n_a \mid d}} \gcd(d, h_a) \right) \\ &\ll \sum_{d>x} \frac{g(d)\log\log d}{d^2} \sum_{a\le N} h_a.\end{aligned}$$

Observing that $h_a \le \log N/\log 2$ and $g(n) \ll n^{1-\epsilon}$, the above inequality yields

$$\Sigma_7 \ll \frac{N \log N}{x^{\epsilon/2}}. \tag{4.5}$$

Now by applying (4.4) and (4.5) to (4.1) we have

$$\frac{1}{N}\sum_{a\le N} c_{f,a} = c_f + O\left(\frac{x^{1-\epsilon}\log x}{N^{1/2}}\right) + O\left(\frac{\log N}{x^{\epsilon/2}}\right).$$

We choose $x = N^{1/2}$ to obtain

$$\frac{1}{N}\sum_{a\le N} c_{a,f} = c_f + O\left(\frac{\log N}{N^{\epsilon/4}}\right).$$

□

References

[1] Eric Bach, Richard Lukes, Jeffrey Shallit, and H. C. Williams, *Results and estimates on pseudopowers*, Math. Comp. **65** (1996), no. 216, 1737--1747. MR1355005

[2] Alina Carmen Cojocaru and M. Ram Murty, *An introduction to sieve methods and their applications*, London Mathematical Society Student Texts, vol. 66, Cambridge University Press, Cambridge, 2006. MR2200366

[3] Chantal David and Francesco Pappalardi, *Average Frobenius distributions of elliptic curves*, Internat. Math. Res. Notices **4** (1999), 165--183. MR1677267

[4] Adam Tyler Felix and M. Ram Murty, *A problem of Fomenko's related to Artin's conjecture*, Int. J. Number Theory **8** (2012), no. 7, 1687--1723. MR2968946

[5] O. M. Fomenko, *Class numbers of indefinite binary quadratic forms*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **276** (2001), no. Anal. Teor. Chisel i Teor. Funkts. 17, 312--333, 354--355 (Russian, with Russian summary); English transl., J. Math. Sci. (N. Y.) **118** (2003), no. 1, 4918--4932. MR1850375

[6] ______, *On the class numbers of indefinite binary quadratic forms and the residual indices of integers modulo a prime p*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **286** (2002), no. Anal. Teor. Chisel i Teor. Funkts. 18, 179--199, 231--232 (Russian, with Russian summary); English transl., J. Math. Sci. (N. Y.) **122** (2004), no. 6, 3685--3698. MR1937377

[7] John Friedlander and Henryk Iwaniec, *Opera de cribro*, American Mathematical Society Colloquium Publications, vol. 57, American Mathematical Society, Providence, RI, 2010. MR2647984

[8] P. X. Gallagher, *The large sieve*, Mathematika **14** (1967), 14--20. MR0214562

[9] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., The Clarendon Press, Oxford University Press, New York, 1979. MR568909

[10] Nathan Jones, *Averages of elliptic curve constants*, Math. Ann. **345** (2009), no. 3, 685--710. MR2534114

[11] R. R. Laxton, *On groups of linear recurrences. I*, Duke Math. J. **36** (1969), 721--736. MR0258781

[12] Pieter Moree, *Artin's primitive root conjecture---a survey*, Integers **12** (2012), no. 6, 1305--1416. MR3011564

[13] F. Pappalardi, *On Hooley's theorem with weights*, Rend. Sem. Mat. Univ. Politec. Torino **53** (1995), no. 4, 375--388. Number theory, II (Rome, 1995). MR1452393

[14] P. J. Stephens, *Prime divisors of second order linear recurrences. II*, J. Number Theory **8** (1976), no. 3, 333--345. MR0417082

[15] Samuel S. Wagstaff Jr., *Pseudoprimes and a generalization of Artin's conjecture*, Acta Arith. **41** (1982), no. 2, 141--150. MR674829

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF LETHBRIDGE,
4401 UNIVERSITY DRIVE WEST, LETHBRIDGE, AB, T1K 3M4, CANADA
E-mail address: amir.akbary@uleth.ca

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF LETHBRIDGE,
4401 UNIVERSITY DRIVE WEST, LETHBRIDGE, AB, T1K 3M4, CANADA
E-mail address: adam.tyler.felix@gmail.com