ON THE DISTRIBUTION OF THE DENSITY OF MAXIMAL ORDER ELEMENTS IN GENERAL LINEAR GROUPS

S. AIVAZIDIS AND E. SOFOS

ABSTRACT. In this paper we consider the density of maximal order elements in $GL_n(q)$. Fixing any of the rank $n$ of the group, the characteristic $p$ or the degree $r$ of the extension of the underlying field $F_q$ of size $q = p^r$, we compute the expected value of the said density and establish that it follows a distribution law.

1. Introduction

In a series of papers stretching from 1965 to 1972, and beginning with [ET65], Erdős and Turán examined in detail various questions of a statistical nature regarding the symmetric group. One might ask whether similar work can be done for other classes of groups; indeed, the most natural next candidate is the general linear group $GL_n(q)$ of $n \times n$ matrices over the finite field $F_q$. A notable difference between the two classes of groups is the dependence of the latter on more than one parameter. While Sym $(\Omega)$ is completely determined (up to isomorphism) by the cardinality of the set $\Omega$, the groups $GL_n(q)$ require 3 variables for their definition: the rank $n$ and the size $q$ of the underlying field, which, in turn, depends both on the characteristic of the field and on the degree of the extension. Stong [Sto93] considered the average order of a matrix in $GL_n(q)$ for fixed $q$ and varying $n$ and proved that

$$\log \nu_n = n \log q - \log n + o(\log n),$$

where

$$\nu_n = \frac{1}{|GL_n(q)|} \sum_{A \in GL_n(q)} \text{ord}(A).$$

Our purpose here is to address a question which is more limited in scope, but rather different in nature from Stong’s investigations. In particular, we shall consider elements of maximal order in $GL_n(q)$, also known as Singer cycles, and examine in detail the mean density of those elements in $GL_n(q)$. Fixing any two of the parameters $n, p, r$ and letting the remaining one vary accordingly, we show that the density of Singer cycles follows a distribution law and provide its expected value. It is straightforward to show that the maximal order of an element in $GL_n(q)$ is $q^n - 1$. In section 2 we shall do this after establishing existence of the said elements and obtain the formula

$$\frac{|GL_n(q)| \phi(q^n - 1)}{q^n - 1} \cdot \frac{1}{n},$$

for the number of Singer cycles, where $\phi$ is the usual Euler function. The core of the paper is concerned with their density function

$$p_n(q) := \frac{1}{n} \cdot \frac{\phi(q^n - 1)}{q^n - 1},$$

i.e., the probability that an element has maximal order in $GL_n(q)$.

2010 Mathematics Subject Classification. 11N45 (20G40, 20P05).

The first author acknowledges financial support from the N. D. Chrysovergis endowment under the auspices of the National Scholarships Foundation of Greece. The second author was supported by EPSRC grant EP/H005188/1.
We are interested in the distribution of $p_n(q)$ in the interval $(0, \frac{1}{n})$. If we fix $n$ and let $q \to \infty$ through prime powers, we see that $\lim_{q} p_n(q)$ does not exist. It thus makes sense to examine its average value instead. In Theorem 1.1 (i) we provide the answer to this question. However, the average is not greatly affected by the values that $p_n(q)$ assumes when $q$ varies through genuine powers of primes. We therefore investigate the average of $p_n(p^r)$ for fixed $n,p$ and for varying $r$. This is the content of Theorem 1.1 (ii). Lastly, by similar methods we provide the average value for the case that Strong deals with, that is when the field is fixed and the rank $n$ varies, and that is the content of Theorem 1.1 (iii). We notice here that similar questions have been considered previously in the case where one has the multiplicative group $\mathbb{Z}/m\mathbb{Z}$ instead of the general linear group. See for example [Li98] and the survey [LP02].

Before we state our first theorem, let us introduce some relevant terminology. For a prime $p$ and an integer $a$ coprime to $p$, we let $\ell_p(a)$ denote its multiplicative order (mod $p$), that is the least positive integer $k$ for which $p^k \equiv 1\pmod{a}$. Define for a prime $p$ and integer $r$ the following series

$$p(p, r) := \sum_{m \in \mathbb{N} \atop \gcd (\ell_p(m), r)} \frac{\mu(m) \gcd (\ell_p(m), r)}{\ell_p(m)}, \quad (1.2)$$

Here and throughout this paper $\sum_*$ denotes a summation over those positive integers $m$ that are coprime to $p$. We will show in Lemma 4.4 (iii) that this series is convergent. We also define for an integer $n$ the quantity

$$p_n := \frac{1}{n} \prod_{p} \left(1 - \frac{\gcd (p - 1, n)}{p(p - 1)}\right). \quad (1.3)$$

Notice that $p_1$ is the so–called Artin constant, arising in Artin’s primitive root conjecture. The infinite product in (1.3) converges since for fixed $n$ one has $\gcd (p - 1, n) \leq n$, hence

$$\sum_p \frac{\gcd (p - 1, n)}{p(p - 1)} \leq n \sum_p \frac{1}{p(p - 1)} < \infty.$$

Our first result is the following.

**Theorem 1.1.** Let $x \in \mathbb{R}_{>1}$ and denote the cardinality of the powers of primes below $x$ by $Q(x)$.

(i) For any fixed $n \in \mathbb{N}$ and any $A \in \mathbb{R}_{>1}$ one has

$$\frac{1}{Q(x)} \sum_{q \leq x} p_n(q) = p_n + O_{n,A} \left(\frac{1}{(\log x)^A}\right),$$

where the summation is taken over powers of primes.

(ii) For any fixed prime $p$ and $n \in \mathbb{N}$ one has

$$\frac{1}{x} \sum_{r \leq x} p_n(p^r) = \frac{1}{n} p(p, n) + O \left(\frac{\log (xn \log p)}{xn}\right),$$

where the implied constant is absolute.

(iii) For any fixed $q = p^r$ one has

$$\frac{1}{\log x} \sum_{n \leq x} p_n(q) = p(p, r) + O \left(\frac{\tau(r) \log (r \log p)}{\log x}\right),$$

where the implied constant is absolute and $\tau$ denotes the divisor function.
Remark 1.2. The above theorem reveals the noteworthy fact that the density of Singer cycles in \( \text{GL}_n(q) \) is approximated on average by a constant multiple of \( \frac{1}{n} \) when one allows any of the underlying parameters to vary.

The special case corresponding to \( n = 1 \) in Theorem 1.1 (i) has been dealt with previously by Stephens [Ste69, Lemma 1] and in an equivalent form by Pillai [Pil41, Theorem 1]. Following the proof of Theorem 1.1 (i), we show that the error of approximation can be substantially improved to

\[
O_n \left( \frac{(\log x)^{r(n)+2}}{\sqrt{x}} \right)
\]

under the assumption of the Generalised Riemann Hypothesis.

One should notice that the sequence \( p_n(q) \) oscillates wildly around its mean value in all cases of Theorem 1.1 and it would therefore be interesting to attain information regarding the nature of its distribution. It thus makes sense to examine how \( p_n(q) \) distributes over subintervals of \( (0, \frac{1}{n}) \). To that end let us recall some standard definitions from Probabilistic Number Theory (see [Ten95, Chapter III] for a detailed discussion). Let \( b_n \) be a sequence of real numbers and define for \( x, z \in \mathbb{R} \), the frequencies \( \nu_x \) as follows:

\[
\nu_x(n; b_n \leq z) := \left| \{ n \leq x : b_n \leq z \} \right| / x.
\]

Similarly denote

\[
\nu_x(q; b_q \leq z) := \left| \{ q \leq x : q \text{ is a prime power, } b_q \leq z \} \right| / Q(x).
\]

We say that the frequencies \( \nu_x \) converge to a limiting distribution as \( x \to \infty \), if for any \( z \) in a certain dense subset \( E \subset \mathbb{R} \), the following limit exists

\[
\lim_{x \to \infty} \nu_x(n; b_n \leq z),
\]

and furthermore, denoting its value by \( F(z) \), that one has

\[
\lim_{z \to \alpha} F(z) = \begin{cases} 
1, & \text{if } \alpha = +\infty \\
0, & \text{if } \alpha = -\infty 
\end{cases}.
\]

Thus the existence of a limiting distribution should be interpreted as an equidistribution of \( b_n \) with respect to some measure. We are now ready to state our second theorem.

Theorem 1.3. The frequencies \( \nu_x \), with respect to any of the involved parametres, converge to a limiting distribution. More precisely:

(i) For fixed \( n \in \mathbb{N} \) the frequencies \( \nu_x(q; p_n(q) \leq z) \) converge to a continuous limiting distribution.

(ii) For fixed prime \( p \) and integer \( n \) the frequencies \( \nu_x(r; p_n(r^p) \leq z) \) converge to a limiting distribution.

(iii) For fixed prime power \( q = p^r \) the frequencies \( \nu_x(n; p_n(q) \leq \frac{z}{n}) \) converge to a limiting distribution.

Let us put Theorem 1.3 in context. The easier problem of determining the frequencies \( \nu_x(n; \phi(n)/n \leq z) \), where one ranges general integers \( n \), has received much attention. Shoenfeld [Sch28] proved that these frequencies converge to a limiting distribution, say \( F(z) \), and that \( F(z) \) is continuous. In a subsequent paper [Sch36] he showed that \( F(z) \) is strictly increasing. Erdős [Erd39] discovered the following asymptotic expression:

\[
F(1 - \epsilon) = 1 - \frac{e^{-\gamma}}{\log \frac{1}{\epsilon} + O \left( \frac{1}{(\log \frac{1}{\epsilon})^2} \right)}.
\]
uniformly for all $\epsilon \in (0,1)$, where $\gamma$ is the Euler constant. Toulmonde [Tou09] proved that we can in fact get a more precise expression in the right-hand-side of (1.4), involving an asymptotic expansion in negative powers of $\frac{1}{\log(1/\epsilon)}$ in place of the error term. The problem however becomes less easy when we range over powers of primes rather than general integers. The special case of part (i) of Theorem 1.3 corresponding to $n = 1$ has been handled by Kátai [Kát68], who showed that the limiting distribution exists and is continuous. Deshouillers and Hassani [DH12] proved that this limiting distribution possesses infinitely many points of non–differentiability. It would be desirable to have analogues of (1.4) for part (i) of Theorem 1.3, even in the case $n = 1$, a problem which is equivalent to obtaining an analogue of (1.4) regarding the limiting distribution of $\frac{\phi(p-1)}{p-1}$, as $p$ ranges in primes.

A few remarks about the proofs of the two theorems are in order. Part (i) of Theorem 1.1 is proved via splitting a certain sum over moduli into two ranges according to the size of the moduli. The contribution coming from the range corresponding to small moduli will give the main term after an application of the Bombieri–Vinogradov Theorem 3.1 and the range corresponding to large moduli will be shown to give a negligible contribution compared to the main term.

The proofs of Theorem 1.1 (ii) and Theorem 1.1 (iii) are rather similar; both are based on Lemma 5.4, which is similar to [Shp90, Theorem 3]. There, however, the dependence of the error term on the underlying parameters is not best possible and we will attempt to remedy this. The proof of Lemma 5.4 is based on Lemma 4.4, where all sums appearing in its statement resemble Romanoff’s series

$$\sum_{m \in \mathbb{N}} \frac{1}{m \ell_p(m)},$$

where $p$ is a fixed prime. We will bound such sums by introducing the auxiliary quantity $E_p(x, d)$, defined later in the proof of Lemma 4.4, which is a trick introduced by Erdős [Erd51].

The proof of Theorem 1.3 (i) is conducted via restricting attention to prime numbers below $x$ and then applying a theorem in [TF69] regarding distribution laws of $f(|g(p)|)$, for an additive function $f$ and a polynomial $g \in \mathbb{Z}[x]$. The proofs of parts (ii) and (iii) of Theorem 1.3 are again quite similar. Here, however, the sequence involved is not additive. Therefore we have to use a result for distribution laws of general arithmetic functions.

The rest of the paper is organised as follows. In section 2 some background on Singer cycles is given, resulting in the explicit estimation of $p_n(q)$. In section 3 we provide some analytic tools that will be used later in the proof of Theorem 1.1. In section 4 some auxiliary lemmata regarding upper bounds of sums of certain arithmetic functions are provided. Finally, in sections 5 and 6 we provide the proof of Theorems 1.1 and 1.3 respectively.

1.4. Notation. Throughout this paper $p$ will denote a prime and $q$ a (not necessarily proper) power of a prime.

(i) The notation $\sum_p$ is understood to be a sum taken over primes; similarly, $\sum_q$ should be read as a sum taken over powers of primes, and the same principle applies to products. As already mentioned, $\sum^*$ denotes a summation over positive integers that are coprime to $p$.

(ii) We shall write $p^\lambda \| n$ for a prime $p$ and positive integers $\lambda$, $n$ if $p^\lambda \mid n$ and $p^{\lambda+1} \nmid n$.

(iii) For the real functions $f(x)$, $g(x)$, defined for $x > 0$, the notation $f(x) = O(g(x))$ (or, equivalently, $f(x) \ll g(x)$) means that there exists an absolute constant $M > 0$ independent of $x$, such that $|f(x)| \leq M |g(x)|$ for $x > 0$. We shall write $f(x) =$
g(x) + O(h(x)) if (f − g)(x) = O(h(x)). When the implied constant depends on a set of parameters $S$, we shall write $f = O_S(g)$, or $f \ll_S g$. If no such subscript appears, then the implied constant is absolute.

(iv) As usual, we let $\mu(n)$ the Möbius function, $\sigma(n)$ the sum of divisors of $n$, and $\Lambda(n)$ the von Mangoldt function. This, we recall, is defined as

\[
\Lambda(n) = \begin{cases} 
\log p, & \text{if } n \text{ is a power of a prime } p, \\
0, & \text{otherwise}.
\end{cases}
\]

2. Singer cycles

An element of order $q^n - 1$ in $\text{GL}_n(q)$ is called a Singer cycle. That Singer cycles always exist can be seen as follows.

Let $\mathbb{F}_{q^n}$ be the $n$-degree field extension of $\mathbb{F}_q$, and let $\alpha$ be a primitive element of $\mathbb{F}_{q^n}^*$. The map

\[
s : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \quad x \mapsto \alpha x
\]

is $\mathbb{F}_q$-linear and invertible. Further, the order of $s$ is equal to that of $\alpha$ in $\mathbb{F}_{q^n}^*$, that is, $q^n - 1$.

In fact the integer $q^n - 1$ is maximal among possible element orders in $\text{GL}_n(q)$. To see why that must be the case, consider the algebra $\text{Mat}_n(q)$ of all $n \times n$ matrices over $\mathbb{F}_q$ and note that each element $A \in \text{GL}_n(q)$ generates a subalgebra $\mathbb{F}_q[A] \subseteq \text{Mat}_n(q)$. The Cayley-Hamilton theorem then ensures that $\dim \mathbb{F}_q[A] \leq n$, thus $o(A) \leq q^n - 1$ for all $A \in \text{GL}_n(q)$.

Our claim now is that $o(A) = q^n - 1$ if and only if the minimal polynomial $m_A(x)$ of $A$ is primitive of degree $n$ (recall that $f$ is a primitive polynomial if and only if any root of $f$ in the splitting field of $f$ generates the multiplicative group of that field). For this we shall need the following [LN94, Lemma 3.1].

**Lemma 2.1.** Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree $m \geq 1$ with $f(0) \neq 0$. Then there exists a positive integer $e \leq q^m - 1$ such that $f(x) \mid x^e - 1$.

The least such $e$ is called the order of $f$ and is denoted by $\text{ord}(f)$. Clearly $A^k = I_n$ if and only if $m_A(x) \mid x^k - 1$, $k \in \mathbb{N}$. Thus$^1$

\[
o(A) = \text{ord}(m_A).
\]

From Lidl and Niederreiter [LN94, Theorem 3.3] we know that the order of an irreducible polynomial of degree $n$ over $\mathbb{F}_q[x]$ is equal to the order of any of its roots in $\mathbb{F}_{q^n}^*$. Thus $\text{ord}(m_A) = q^n - 1$ if and only if $m_A$ is primitive and $\deg m_A = n$, as wanted. Note that the above argument shows that the minimal and the characteristic polynomial of a Singer cycle coincide.

We shall now give a proof for the number of Singer cycles as an application of a theorem of Reiner [Rei61, Theorem 2], but it ought to mentioned that the same formula can be obtained via the familiar Orbit–Stabiliser Theorem (a Singer cyclic subgroup has index exactly $n$ in its normaliser). Reiner computes the number of (not necessarily invertible) $n \times n$ matrices with entries in the finite field $\mathbb{F}_q$ having given characteristic polynomial. Let $R_n$ denote the ring of all $n \times n$ matrices with entries in $\mathbb{F}_q$, and define $F(u, r) = \prod_{i=1}^r (1 - u^{-i})$, where $F(u, 0) = 1$.

**Theorem 2.2** (Reiner [Rei61]). Let $g(x) \in \mathbb{F}_q[x]$ be a polynomial of degree $n$, and let

\[
g(x) = f_1^{n_1}(x) \cdots f_k^{n_k}(x)
\]

$^1$This yields yet another proof that the order of a matrix is at most $q^n - 1$.
be its factorisation in \( \mathbb{F}_q[x] \) into powers of distinct irreducible polynomials \( f_1(x), \ldots, f_k(x) \).
Set \( d_i := \deg(f_i(x)) \), \( 1 \leq i \leq k \). Then the number of matrices \( X \in \mathbb{R}_n \) with characteristic polynomial \( g(x) \) is

\[
q^{n^2 - n} \frac{F(q,n)}{\prod_{i=1}^k F(q^{d_i},n_i)}.
\]

Now take \( k = 1 \), \( n_1 = 1 \), and \( d_1 = n \) in the above formula and notice that a matrix whose characteristic polynomial is thus parameterised is necessarily invertible. In particular there are

\[
q^{n^2 - n} \frac{F(q,n)}{F(q^n,1)} = \frac{|\text{GL}_n(q)|}{q^n - 1}
\]
such matrices. Since there are precisely

\[
\frac{\phi(q^n - 1)}{n}
\]
primitive (thus also irreducible) polynomials of degree \( n \) in \( \mathbb{F}_q[x] \), the following has been proved.

**Lemma 2.3.** The number of Singer cycles in \( \text{GL}_n(q) \) is given by the formula

\[
|\text{GL}_n(q)| \frac{\phi(q^n - 1)}{q^n - 1}.
\]

### 3. Preliminaries

In this section we recall standard results regarding the distribution of primes in arithmetic progressions. Denote by \( \pi(x) = \sum_{p \leq x} 1 \), \( x \geq 3 \) the number of primes less than or equal to \( x \) and by \( \text{li}(x) \) the logarithmic integral

\[
\text{li}(x) := \int_2^x \frac{dt}{\log t}.
\]

The Prime Number Theorem states that for each \( A > 0 \) and for all \( x \geq 3 \) one has

\[
\pi(x) = \text{li}(x) + O_A \left( \frac{x}{(\log x)^A} \right).
\]

For coprime integers \( m, a \) and all \( x \geq 3 \), define

\[
\psi(x; m, a) := \sum_{n \leq x \atop n \equiv a (\text{mod } m)} \Lambda(n).
\] (3.1)

The Bombieri–Vinogradov theorem [Dav00, §28] then states that:

**Theorem 3.1.** For any fixed \( A > 0 \) and for all \( x \geq 3 \) one has

\[
\sum_{m \leq \sqrt{x}/(\log x)^A \atop a \equiv 1 (\text{mod } m)} \max_{(a,m) = 1} \left| \psi(x; m, a) - \frac{x}{\phi(m)} \right| \ll A \frac{x}{(\log x)^{A-5}}.
\]

We shall also make use of the following lemma.

**Lemma 3.2.** Let \( a, m \) be coprime integers. Then one has the following estimate

\[
\sum_{p \leq x \atop p \equiv a (\text{mod } m)} \frac{1}{p} = \frac{1}{\phi(m)} \log \log x + O_m(1),
\]

for \( x \geq 3 \).
Proof. Corollary 4.12(c) in Montgomery–Vaughan [MV07] yields
\[
\sum_{\substack{p \leq x \\
p \equiv a \pmod{m}}} \frac{1}{p} = \frac{1}{\phi(m)} \log \log x + O_m \left(1 + \sum_{\chi \neq \chi_0 \pmod{m}} \log |L(1, \chi)| \right),
\]
where the summation \(\sum_{\chi \neq \chi_0 \pmod{m}}\) is taken over non-trivial characters \((\pmod{m})\). Using the fact that there are finitely many such characters and that \(L(1, \chi) \neq 0\) for each such character proves the lemma. \(\square\)

4. Lemmata

In this section we introduce a certain arithmetical function \(\rho_n(m)\) and provide an explicit expression when \(m\) is square–free. We then obtain upper bounds for sums that involve this function. At the end of the section we give some auxiliary lemmata regarding sums that involve the multiplicative order function \(\ell_p(n)\).

Let \(n \in \mathbb{N}\) be a fixed positive integer, and define the function \(\rho_n : \mathbb{N} \rightarrow \mathbb{N}\) via the rule
\[
\rho_n(m) = \left| \left\{ a \pmod{m} : a^n \equiv 1 \pmod{m} \right\} \right|.
\]
(4.1)

It is a direct consequence of the Chinese Remainder Theorem that \(\rho_n\) is multiplicative. The verification of the following lemma is left to the reader.

**Lemma 4.1.** For all primes \(p\) and for all positive integers \(n\) one has
\[
\rho_n(p) = \gcd (p - 1, n).
\]

**Lemma 4.2.** One has the following bounds, valid for all \(n \in \mathbb{N}\) and for all \(x \geq 3\)
\[
\begin{align*}
(\text{i}) & \quad \sum_{m \leq x} \mu^2(m) \frac{\rho_n(m)}{m} \ll_n (\log x)^{\tau(n)}, \\
(\text{ii}) & \quad \sum_{m>x} \mu^2(m) \frac{\rho_n(m)}{m^2} \log m \ll_n \frac{1}{x} (\log x)^{\tau(n)+1}.
\end{align*}
\]

**Proof.** (i) We begin by noticing that if \(f : \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}\) is a multiplicative function then
\[
\sum_{m \leq x} \mu^2(m) f(m) \leq \prod_{p \leq x} \left(1 + f(p)\right).
\]
Setting \(f(m) = \frac{\rho_n(m)}{m}\) in the above relation yields
\[
\sum_{m \leq x} \mu^2(m) \frac{\rho_n(m)}{m} \leq \prod_{p \leq x} \left(1 + \frac{\gcd (p - 1, n)}{p}\right)
\]
for all \(x \geq 3\). The inequality \(1 + t \leq e^t\), valid for any \(t > 0\), shows that
\[
\prod_{p \leq x} \left(1 + \frac{\gcd (p - 1, n)}{p}\right) \leq \exp \left(\sum_{p \leq x} \frac{\gcd (p - 1, n)}{p}\right).
\]
Using the identity
\[
\gcd(a, b) = \sum_{d \mid a, d \mid b} \phi(d),
\]
valid for all \(a, b \in \mathbb{N}\), yields
\[
\sum_{p \leq x} \frac{\gcd (p - 1, n)}{p} = \sum_{d \mid n} \phi(d) \left(\sum_{\substack{p \leq x \\
p \equiv 1 \pmod{d}}} \frac{1}{p}\right).
\]

Using the identity
\[
\gcd(a, b) = \sum_{d \mid a, d \mid b} \phi(d),
\]
valid for all \(a, b \in \mathbb{N}\), yields
Using Lemma 3.2 for each inner sum gives
\[
\sum_{p \leq x} \frac{\gcd(p-1, n)}{p} = \tau(n) \log \log x + O_n(1),
\]
which proves that
\[
\sum_{m \leq x} \mu^2(m) \frac{\rho_n(m)}{m} \ll_n (\log x)^{\tau(n)}.
\]
(ii) Splitting the range of summation in disjoint intervals gives
\[
\sum_{m > x} \mu^2(m) \frac{\rho_n(m)}{m^2} \log m = \sum_{i=0}^{\infty} \sum_{xe^i < m \leq xe^{i+1}} \mu^2(m) \frac{\rho_n(m)}{m^2} \log m.
\]
Noticing that
\[
\sum_{xe^i < m \leq xe^{i+1}} \mu^2(m) \frac{\rho_n(m)}{m^2} \log m \leq \frac{(\log(xe^{i+1}))^{\tau(n)+1}}{xe^i} \sum_{m \leq xe^{i+1}} \mu^2(m) \frac{\rho_n(m)}{m},
\]
and applying part (i) yields
\[
\sum_{m > x} \mu^2(m) \frac{\rho_n(m)}{m^2} \log m \ll_n \frac{1}{x} \sum_{i=0}^{\infty} \frac{(\log(xe^{i+1}))^{\tau(n)+1}}{xe^i}.
\]
Using the inequality \(\log(ab) \leq (\log a)(\log b)\), valid for all \(a, b > e\) gives
\[
\sum_{m > x} \mu^2(m) \frac{\rho_n(m)}{m^2} \log m \ll_n \frac{(\log x)^{\tau(n)+1}}{x} \sum_{i=0}^{\infty} \frac{(i+1)^{\tau(n)+1}}{e^i}.
\]
This proves the assertion of the lemma since the series
\[
\sum_{i=0}^{\infty} \frac{(i+1)^{\tau(n)+1}}{e^i}
\]
is convergent.

We record here for future reference a familiar lemma which allows us to translate information about the asymptotic behaviour of weighted sums by \(\Lambda(k)\) into one regarding unweighted sums.

**Lemma 4.3.** Let \(b_k\) be a sequence of real numbers and define for any \(x \in \mathbb{R}_{>1}\),
\[
\beta(x) := \max \{|b_k| : 1 \leq k \leq x\}.
\]
Then one has the following estimates.

(i) For any \(x \in \mathbb{R}_{\geq 2}\), \(\sum_{q \leq x} b_q = \sum_{p \leq x} b_p + O \left( \sqrt{x} \beta(x) \log x \right)\).

(ii) Let \(c, A\) be positive constants such that \(\sum_{p \leq x} b_p \log p = cx + O \left( \frac{x}{(\log x)^A} \right)\), for all \(x \geq 3\). Then \(\sum_{p \leq x} b_p = c \text{li}(x) + O \left( \frac{x}{(\log x)^A} \right)\), for all \(x \geq 2\).

**Proof.** (i) Define \(k_0 := \left\lfloor \frac{\log x}{\log 2} \right\rfloor\). We partition the sum \(\sum_{q \leq x} b_q\) according to the values of prime powers that \(q\) assumes and this yields
\[
\sum_{q \leq x} b_q = \sum_{k=1}^{k_0} \sum_{p \leq x^{1/k}} b_{p^k}.
\]
Now notice that
\[ \sum_{k=2}^{k_0} \sum_{p \leq x^{1/3}} b_{p^k} \ll \beta(x) \left[ \pi \left( \sqrt{x} \right) + (k_0 - 2) \pi \left( x^{1/3} \right) \right], \]
and use the bound \( \pi(t) \ll \frac{t}{\log t} \), valid for all \( t \in \mathbb{R}_{>2} \), to get
\[ \sum_{k=2}^{k_0} \sum_{p \leq x^{1/3}} b_{p^k} \ll \sqrt{x} \beta(x) \log x. \]

The claim follows.

(ii) Applying partial summation yields
\[ \sum_{p \leq x} b_p = c \text{li}(x) + O \left( \frac{x}{\log x} + \int_2^x \frac{dt}{(\log t)^{A+1}} \right). \]

The use of the following inequalities
\[ \int_2^{\sqrt{x}} \frac{dt}{(\log t)^{A+2}} \leq \frac{\sqrt{x}}{(\log 2)^{A+2}}, \quad \int_{\sqrt{x}}^{x} \frac{dt}{(\log t)^{A+2}} \leq \frac{x - \sqrt{x}}{(\log (\sqrt{x}))^{A+2}}, \]
concludes the proof of the lemma. \( \square \)

In the following lemma we record auxiliary bounds that will be needed when we deal with cases (ii) and (iii) of Theorem 1.1.

**Lemma 4.4.** Let \( p \) be a fixed prime and \( d \in \mathbb{N} \). One has the following bounds, uniformly for all \( x \geq 1 \).

(i) \( \sum_{k \leq x} \sum_{\star} \frac{1}{m} \ll \log(xd \log p), \)

(ii) \( \sum_{k \geq x} \frac{1}{k} \sum_{\star} \frac{1}{m} \ll \frac{\log(xd \log p)}{x}, \)

(iii) the series \( p(p, r) \) defined in (1.2) converges for each prime \( p \) and each \( r \in \mathbb{N} \). Further, one has
\[ p(p, r) \ll \tau(r) \log(r \log p), \]
with an absolute implied constant.

**Proof.** (i) The integers \( m \) taken into account in the inner sum satisfy \( p^{kd} \equiv 1 (\text{mod } m) \) for some \( k \leq x \). Therefore each such \( m \) is a divisor of
\[ E_p(x, d) := \prod_{k \leq x} (p^{kd} - 1). \]

Hence the double sum is at most
\[ \sum_{m | E_p(x)} \frac{1}{m} = \frac{\sigma(E_p(x, d))}{E_p(x, d)}. \]

We now use the well–known bound
\[ \frac{\sigma(n)}{n} \ll \log \log n \]
to deduce that the double sum is
\[ \ll \log \log E_p(x, d). \]
One easily sees that
\[ E_p(x, d) \leq \prod_{k \leq x} p^{k_d} \leq p^{d x^2}, \]
which shows that the double sum is \( \ll \log \log (p^{d x^2}) \ll \log (x d \log p) \), as asserted.

(ii) The term corresponding to \( k = x \) makes a contribution only when \( x \) is an integer, in which case we get a contribution which is \( \ll \frac{1}{x} \log (x d \log p) \), as shown by the first part of this lemma. It remains to examine the contribution made by the terms corresponding to \( k > x \). Using partial summation along with part (i) we deduce that
\[ \sum_{k>x} \frac{1}{k} \sum_{\substack{m \in \mathbb{N} \\ell_p(m)=k \atop \ell_p(m)=kd}} \frac{1}{m} \ll \frac{\log (x d \log p)}{x} + \int_{x}^{\infty} \frac{\log (u d \log p)}{u^2} du. \]
Alluding to the estimate \( \int_{x}^{\infty} (\log u) u^{-2} du \ll \log (2x)x^{-1} \), valid for all \( x \geq 1 \), proves our claim.

(iii) The identity (4.2) and
\[ p(p, r) = \sum_{k=1}^{\infty} \frac{\gcd(k, r)}{k} \sum_{\substack{m \in \mathbb{N} \\ell_p(m)=k}} \frac{\mu(m)}{m} \]
show that one has
\[ p(p, r) = \sum_{d|r} \frac{\phi(d)}{d} \sum_{k=1}^{\infty} \frac{1}{k} \sum_{\substack{m \in \mathbb{N} \\ell_p(m)=kd}} \frac{\mu(m)}{m}, \]
which is bounded in absolute value by
\[ \sum_{d|r} \sum_{k=1}^{\infty} \frac{1}{k} \sum_{\substack{m \in \mathbb{N} \\ell_p(m)=kd}} \frac{1}{m}. \]
Using \( x = 1 \) in part (ii) concludes the proof of part (iii).

5. Proof of Theorem 1.1

In this section we prove Theorem 1.1. We begin by proving the auxiliary Lemmata 5.1, 5.2, and 5.3 and use them in succession to provide the proof of Theorem 1.1 (i). We then prove Lemma 5.4 from which we deduce the validity of Theorem 1.1 (ii) and Theorem 1.1 (iii).

For fixed \( n, m \in \mathbb{N} \) and \( x \in \mathbb{R}_{>1} \), define the following functions
\[ \Psi_n(x) := \sum_{k \leq x} \Lambda(k) \frac{\phi(k^n - 1)}{k^n - 1}, \]
and
\[ \Psi_n(x; m) := \sum_{\substack{a \pmod{m} \atop a^n \equiv 1 \pmod{m}}} \psi(x; m, a), \]
where \( \psi \) was defined in (3.1).

**Lemma 5.1.** For all naturals \( n \geq 1 \), and for all \( x \in \mathbb{R}_{>1} \) one has
\[ \Psi_n(x) = \sum_{m \leq x^n} \frac{\mu(m)}{m} \Psi_n(x; m). \]
Proof. The proof follows readily by noticing that
\[
\frac{\phi(k)}{k} = \sum_{m|k} \frac{\mu(m)}{m},
\]
and inverting the order of summation. \qed

**Lemma 5.2.** For any fixed constant \(A > 0\) and any fixed \(n \in \mathbb{N}\), one has uniformly for all \(x \geq 3\)
\[
\sum_{\sqrt{x}/(\log x)^A < m \leq x^n} \frac{\mu(m)}{m} \Psi_n(x; m) \ll_{n,A} x \sqrt{(\log x)^{2+\tau(n)+A}}.
\]

Proof. We break the summation over \(m\) into the two disjoint intervals \(\left[\sqrt{x}/(\log x)^A, x\right]\) and \((x, x^n]\). We first deal with the contribution afforded by the latter interval. We claim that for \(m > x\) one has \(\psi(x; m, a) \leq \log x\). To see why, note that there exists at most one \(k\) in \([1, x]\) such that \(k \equiv a\) \((\text{mod } m)\), and notice that \(\Lambda(k) \leq \log k\), for all \(k \in \mathbb{N}\), with equality if and only if \(k\) is prime. Thus \(\psi(x; m, a) \leq \log x\), as wanted. Recalling the definition of \(\rho_n(m)\), given in equation (4.1), we get for \(m > x\),
\[
\Psi_n(x; m) = \sum_{\substack{a \equiv 1 \pmod{m} \, \text{and } \psi(x; m, a) = \rho_n(m) \log x.}}
\]
Therefore
\[
\left| \sum_{x < m \leq x^n} \frac{\mu(m)}{m} \Psi_n(x; m) \right| \leq \log x \sum_{m \leq x^n} \mu^2(m) \frac{\rho_n(m)}{m}.
\]
We use the first part of Lemma 4.2 to conclude that
\[
\left| \sum_{x < m \leq x^n} \frac{\mu(m)}{m} \Psi_n(x; m) \right| \ll (\log x)^{1+\tau(n)}.
\]
We proceed by estimating the contribution inherited from \(m\) in the range \(\left(\sqrt{x}/(\log x)^A, x\right]\). Since
\[
\sum_{k \leq x \atop k \equiv a \pmod{m}} 1 \leq \left[\frac{x}{m}\right] + 1 \leq 2 \frac{x}{m},
\]
for \(m \leq x\), we see that
\[
\psi(x; m, a) = \sum_{k \leq x \atop k \equiv a \pmod{m}} \Lambda(k) \leq \log x \sum_{k \leq x \atop k \equiv a \pmod{m}} 1 \leq 2 \frac{x}{m} \log x.
\]
Therefore
\[
\left| \sum_{\sqrt{x}/(\log x)^A < m \leq x} \frac{\mu(m)}{m} \Psi_n(x; m) \right| \leq \sum_{\sqrt{x}/(\log x)^A < m \leq x} \frac{\mu^2(m)}{m} \sum_{a \equiv 1 \pmod{m}} \rho_n(m) \frac{\rho_n(m)}{m^2}.
\]
Using the second part of Lemma 4.2 we get
\[
x \log x \sum_{m > \sqrt{x}/(\log x)^A} \frac{\mu^2(m) \rho_n(m)}{m^2} \ll_{n,A} x \sqrt{(\log x)^{\tau(n)+A+2}},
\]
thus completing the proof. \qed
Lemma 5.3. For any fixed constant $A > 0$ one has uniformly for all $x \geq 3$

$$
\sum_{m \leq \sqrt{x} / (\log x)^A} \frac{\mu(m)}{m} \Psi_n(x;m) = n p_n x + O_n(A \left( \frac{x}{\log x} \right)^{A-5}).
$$

Proof. By the definition of $\Psi_n(x;m)$ we have

$$
\sum_{m \leq \sqrt{x} / (\log x)^A} \frac{\mu(m)}{m} \Psi_n(x;m) = \sum_{m \leq \sqrt{x} / (\log x)^A} \frac{\mu(m)}{m} \sum_{a \equiv 1 (\mod m)} \psi(x; a),
$$

which equals

$$
\sum_{m \leq \sqrt{x} / (\log x)^A} \frac{\mu(m)}{m} \sum_{a \equiv 1 (\mod m)} \left( \psi(x; a) - \frac{x}{\phi(m)} \right)
$$

$$
+ x \sum_{m \leq \sqrt{x} / (\log x)^A} \frac{\mu(m)}{m} \sum_{a \equiv 1 (\mod m)} \frac{1}{\phi(m)}
$$

$$
= \mathcal{E} + x \mathcal{M}, \text{ say.}
$$

Recalling the definition of $\rho_n(m)$ (equation (4.1)), one has

$$
|\mathcal{E}| \leq \sum_{m \leq \sqrt{x} / (\log x)^A} \frac{\rho_n(m)}{m} \max_{a \equiv 1 (\mod m)} \left| \psi(x; a) - \frac{x}{\phi(m)} \right| \psi(x; a),
$$

(5.2)

Now notice that by the definition of $\rho_n(m)$ one trivially has $\rho_n(m) \leq m$. Thus inequality (5.2) becomes

$$
|\mathcal{E}| \leq \sum_{m \leq \sqrt{x} / (\log x)^A} \frac{\rho_n(m)}{m} \max_{a \equiv 1 (\mod m)} \left| \psi(x; a) - \frac{x}{\phi(m)} \right| \psi(x; a) \ll A \left( \frac{x}{\log x} \right)^{A-5},
$$

where a use of Theorem 3.1 has been made. For the other term we get

$$
\mathcal{M} = \sum_{m \leq \sqrt{x} / (\log x)^A} \frac{\mu(m)}{m} \rho_n(m) \phi(m).
$$

We will show that this series converges. To that end, let us bound the tail of the series as follows. Using the inequality

$$
\phi(m) \gg \frac{m}{\log m},
$$

valid for all $m \geq 2$, we deduce that

$$
\left| \sum_{m \leq \sqrt{x} / (\log x)^A} \frac{\mu(m)}{m} \rho_n(m) \phi(m) \right| \ll \sum_{m \leq \sqrt{x} / (\log x)^A} \mu^2(m) \rho_n(m) \frac{m}{m^2} \log m.
$$

By part (ii) of Lemma 4.2

$$
\sum_{m \leq \sqrt{x} / (\log x)^A} \mu^2(m) \rho_n(m) \frac{m}{m^2} \log m \ll \left( \log \left( \frac{\sqrt{x}}{(\log x)^A} \right) \right)^{\tau(n)+1} \frac{\sqrt{x}}{(\log x)^A}.
$$

This in turn is bounded by

$$
\frac{(\log x)^{\tau(n)+A+1}}{\sqrt{x}},
$$
which tends to 0 as $x \to \infty$. We may therefore write

$$\mathcal{M} = \sum_{m=1}^{\infty} \frac{\mu(m) \rho_n(m)}{m} - \sum_{m > \sqrt{x}/(\log x)^A} \frac{\mu(m) \rho_n(m)}{m} \phi(m),$$

which, by the preceding bound, equals

$$\sum_{m=1}^{\infty} \frac{\mu(m) \rho_n(m)}{m} \phi(m) + O_n \left( \frac{(\log x)^{\tau(n)+A+1}}{\sqrt{x}} \right).$$

Notice that the function $\frac{\mu(m) \rho_n(m)}{m} \phi(m)$ is multiplicative, being the product of multiplicative functions. We may thus use Euler products to deduce that

$$\sum_{m=1}^{\infty} \frac{\mu(m) \rho_n(m)}{m} \phi(m) = \prod_p \left( 1 + \frac{\mu(p) \rho_n(p)}{p \phi(p)} \right).$$

Recall the definition of $p_n$ (equation (1.3)), as well as the fact that $\mu(p^k) = 0$ for $k \geq 2$. Hence

$$\sum_{m=1}^{\infty} \frac{\mu(m) \rho_n(m)}{m} \phi(m) = \prod_p \left( 1 - \frac{\gcd(p-1,n)}{p(p-1)} \right) = n p_n,$$

where the second equality follows from Lemma 4.1.

We may now combine Lemma 5.1, Lemma 5.2, and Lemma 5.3 to get that for any fixed $n \in \mathbb{N}$ and $A > 0$ one has

$$\Psi_n(x) = n p_n x + O_{n,A} \left( \frac{x}{(\log x)^{A-5}} \right), \quad (5.3)$$

for all $x \geq 2$.

**Proof of Theorem 1.1 (i).** Using (5.3) and the first part of Lemma 4.3 with

$$b_k = \Lambda(k) \frac{\phi(k^n-1)}{k^n-1},$$

we get

$$\sum_{p \leq x} \frac{\phi(p^n-1)}{p^n-1} \log p = n p_n x + O_{n,A} \left( \frac{x}{(\log x)^{A-5}} \right). \quad (5.4)$$

Inserting (5.4) into the second part of Lemma 4.3 with $b_k = \frac{\phi(k^n-1)}{k^n-1}$ gives

$$\sum_{p \leq x} \frac{\phi(p^n-1)}{p^n-1} = n p_n \text{li}(x) + O_{n,A} \left( \frac{x}{(\log x)^{A-5}} \right). \quad (5.5)$$

Using the first part of Lemma 4.3 with $b_k = n p_n(k)$ gives

$$\sum_{q \leq x} p_n(q) = \frac{1}{n} \sum_{p \leq x} \frac{\phi(p^n-1)}{p^n-1} + O_n \left( \frac{x}{\log x} \right),$$

which, when combined with (5.5), yields

$$\sum_{q \leq x} p_n(q) = p_n \text{li}(x) + O_{n,A} \left( \frac{x}{(\log x)^{A-5}} \right). \quad (5.6)$$
Recall that $Q(x)$ denotes the number of prime powers that are at most $x$. To finish the proof it suffices to notice that by the Prime Number Theorem in the form

$$
\pi(x) = \text{li}(x) + O_A \left( \frac{x}{(\log x)^A} \right)
$$

and the first part of Lemma 4.3 with $b_k = 1$, we have

$$
Q(x) = \pi(x) + O \left( \frac{\sqrt{x}}{\log x} \right),
$$

which implies that

$$
Q(x) = \text{li}(x) + O_A \left( \frac{x}{(\log x)^A} \right).
$$

Inserting this in (5.6) and using $\text{li}(x) \gg \frac{x}{\log x}$, valid for all $x \geq 3$, yields

$$
\frac{1}{Q(x)} \sum_{q \leq x} p_n(q) = p_n + O_{n,A} \left( \frac{1}{(\log x)^A} \right),
$$

for all $A > 0$ and $x \geq 3$. Since once is allowed to use any positive value for $A$, we can use $A + 6$ instead. This may increase the dependence of the implied constant on $A$ but doesn’t affect the validity of Theorem 1.1. We therefore conclude that for any positive $A$, the error term is $O_{n,A} \left( \frac{1}{(\log x)^A} \right)$, thus concluding the proof. \hfill \Box

The error term in (5.8) can be improved conditionally on the Generalised Riemann Hypothesis. Indeed, if one is to assume GRH for all $L$–functions of any modulus, then one can obtain

$$
\psi(x; m, a) = \frac{x}{\phi(m)} + O \left( \sqrt{x} (\log x)^2 \right),
$$

with an absolute implied constant, for all $m \geq 1$, $x \geq 3$, as shown in [MV07, Corollary 13.8]. Using this in place of Theorem 3.1 one can follow the steps in the proof of Theorem 1.1 to prove

$$
\frac{1}{Q(x)} \sum_{q \leq x} p_n(q) = p_n + O_n \left( \frac{(\log x)^{\tau(n)+2}}{\sqrt{x}} \right),
$$

for all $x \geq 3$.

The following lemma essentially contains the proof of both part (ii) and (iii) of Theorem 1.1. It is proved via introducing multiplicative indices in the sum and then applying Lemma 4.4.

**Lemma 5.4.** For all naturals $r \geq 1$ and for all $x \in \mathbb{R}_{> 1}$ one has

$$
\sum_{n \leq x} \frac{\phi(p^{rn} - 1)}{p^{rn} - 1} = p(p, r)x + O \left( \log (xr \log p) \right).
$$

**Proof.** In view of (5.1) we can write

$$
\sum_{n \leq x} \frac{\phi(p^{rn} - 1)}{p^{rn} - 1} = \sum_{m \leq p^x} \mu(m) \sum_{\substack{n \leq x \atop p^{rn} \equiv 1 (\text{mod } m)}} 1.
$$

The condition $p^{rn} \equiv 1 (\text{mod } m)$ is equivalent to

$$
\frac{\ell_p(m)}{\gcd(\ell_p(m), r)} | n.
$$
Grouping terms according to the value of the order, the double sum in the right-hand-side of the above equation is seen to equal

\[ \sum_{k \leq r x} \left\lfloor \frac{x}{k} \gcd(k, r) \right\rfloor \left( \sum_{m \in \mathbb{N}} \frac{\mu(m)}{m} \right). \]

Using \([t] = t + O(1)\), valid for all \(t \in \mathbb{R}_{\geq 0}\), we see that this is

\[ x \sum_{k \leq r x} \frac{\gcd(k, r)}{k} \left( \sum_{m \in \mathbb{N}} \frac{\mu(m)}{m} \right) + O \left( \sum_{k \leq r x} \sum_{m \in \mathbb{N}} \frac{1}{m} \right). \]

Part (i) of Lemma 4.4 implies that the error term is \(\ll \log(r x \log p)\). Recall the definition of \(p(p, r)\), stated in (1.2). The inequality \(\gcd(k, r) \leq r\) implies that the main term above equals

\[ x p(p, r) + O \left( x r \sum_{k > r x} \frac{1}{k} \sum_{m \in \mathbb{N}} \frac{1}{m} \right). \]

Using part (ii) of Lemma 4.4 to handle the above error term concludes our proof.

Proof of Theorem 1.1 (ii). Recall the definition of \(p_n(p^r)\) in equation (1.1). Using Lemma 5.4 yields

\[ \sum_{r \leq x p_n(p^r)} = \frac{1}{n} \sum_{r \leq x} \frac{\phi(p^rn - 1)}{p^rn - 1} \]

\[ = \frac{p(p, n)}{n} x + O \left( \frac{\log(xn \log p)}{n} \right), \]

which proves the assertion of Theorem 1.1 (ii).

Proof of Theorem 1.1 (iii). Define for \(x \geq 1\), \(r \in \mathbb{N}\), and \(p\) a prime

\[ E(x, p, r) := \sum_{n \leq x} \frac{\phi(p^rn - 1)}{p^rn - 1} - x p(p, r), \]

so that Lemma 5.4 is equivalent to

\[ E(x, p, r) \ll \log(xr \log p). \]

Using partial summation one sees that for any \(x \geq 1\),

\[ \sum_{n \leq x} p_n(p^r) = \frac{x p(p, r) + E(x, p, r)}{x} + \int_{1}^{x} \frac{u p(p, r) + E(u, p, r)}{u^2} du. \]

Part (iii) of Lemma 4.4 combined with (5.9) shows that this equals

\[ p(p, r) \log x + O(\tau(r) \log(r \log p)). \]

The proof is complete.
6. Proof of Theorem 1.3

We begin by stating two definitions that we will adhere to during the ensuing proofs.

Definition 6.1. A function \( f : \mathbb{N} \to \mathbb{R} \) is called strongly–additive if it satisfies
\[
f \left( \prod_{p \mid n} p^\lambda \right) = \sum_{p \mid n} f(p)
\]
for all \( n \in \mathbb{N} \).

Definition 6.2. Let \( b_n \) be a sequence of real numbers and \( x, z \in \mathbb{R} \). We define the frequencies
\[
\nu_x(p; b_p \leq z) := \frac{\left| \{ p \leq x : p \text{ is prime}, b_p \leq z \} \right|}{\pi(x)}
\]
where \( \pi(x) \) is the number of primes below \( x \).

Let \( f \) be a strongly–additive function and let \( g \in \mathbb{Z}[x] \). Define for each \( m \in \mathbb{N} \)
\[
\rho_g(m) := \left| \{ a \in [0, m) : g(a) \equiv 0 \pmod{m}, \gcd(a, m) = 1 \} \right|
\]
and notice that this is a generalisation of the function \( \rho_n \) defined at the beginning of section 4. The next theorem can be found in [TF69].

Theorem 6.3. Let \( f \) and \( g \) be as above. Assume that \( \rho_g(p)f(p) \to 0 \) as \( p \to \infty \) and that each of the following three series converges
\[
\sum_{|f(p)| > 1} \rho_g(p) \frac{p - 1}{|f(p)|}, \sum_{|f(p)| < 1} \rho_g(p)f(p) \frac{p - 1}{|f(p)|}, \sum_{|f(p)| < 1} \rho_g(p)f^2(p) \frac{p - 1}{|f(p)|}.
\]
Then the frequencies \( \nu_x(p; f(|g(p)|) \leq z) \) converge to a limiting distribution as \( x \to \infty \). Furthermore, the said limiting distribution is continuous if and only if the series
\[
\sum_{f(p) \neq 0} \rho_g(p) \frac{p - 1}{p}
\]
diverges.

Proof of Theorem 1.3 (i). We shall use Theorem 6.3 to prove that for fixed \( n \in \mathbb{N} \) the frequencies
\[
\nu_x\left(p; \frac{\phi(p^n - 1)}{p^n - 1} \leq z\right)
\]
converge to a limiting distribution as \( x \to \infty \). Define the strongly–additive function \( f(k) := \log \frac{\phi(k)}{k} \) and notice that the Taylor expansion of the logarithm implies that for any prime \( p \),
\[
f(p) = \log \left( 1 - \frac{1}{p} \right) = -\frac{1}{p} + O\left( \frac{1}{p^2} \right).
\]
Define the polynomial \( g_n(x) := x^n - 1 \) and notice that by Lemma 4.1
\[
\rho_{g_n}(p) = \gcd(p - 1, n) \leq n
\]
for all primes \( p \). Therefore
\[
\rho_{g_n}(p)f(p) \ll \frac{n}{p} \to 0
\]
as $p \to \infty$. We proceed to show that each of the three series in Theorem 6.3 converge. First, notice that $f(p) \in [-\log 2, 0)$ for all primes $p$, hence the first series contains no terms. Regarding the second series one has

$$
\sum_{|f(p)| \leq 1} \left| \frac{\rho_{g_n}(p)}{p-1} f(p) \right| = \sum_p \frac{\gcd(n, p-1)}{p-1} \left( \frac{1}{p} + O \left( \frac{1}{p^2} \right) \right) 
\ll n \sum_p \frac{1}{p^2} < \infty,
$$

thus the series is convergent. Similarly

$$
\sum_{|f(p)| \leq 1} \left| \frac{\rho_{g_n}(p)}{p-1} f^2(p) \right| \ll n \sum_p \frac{1}{p^2} < \infty,
$$

and the third series converges as well. To conclude the proof of the theorem we observe that the limiting distribution is continuous due to

$$
\sum_{|f(p)| \neq 0} \left| \frac{\rho_{g_n}(p)}{p-1} \right| \geq \sum_p \frac{1}{p-1} = \infty.
$$

Now notice that (5.7) implies that for each $x \geq 1, z \in \mathbb{R}$,

$$
\nu_x \left( p; \frac{\phi(p^n-1)}{p^n-1} \leq z \right) = \nu_x \left( q; \frac{\phi(q^n-1)}{q^n-1} \leq z \right) + O \left( \frac{1}{\sqrt{x}} \right).
$$

Thus letting $x \to \infty$ shows that the limiting distribution of

$$
\nu_x \left( p; \frac{\phi(p^n-1)}{p^n-1} \leq z \right)
$$

is equal to the limiting distribution of

$$
\nu_x \left( q; \frac{\phi(q^n-1)}{q^n-1} \leq z \right).
$$

The proof is now complete.

The following theorem, stated in [Ten95, Chapter III.2, Theorem 2], provides a general criterion that ensures the existence of a limiting distribution. Before presenting it we need the following definition.

**Definition 6.4.** Let $A \subseteq \mathbb{N}$. The density of $A$ is defined as

$$
d(A) := \lim_{x \to \infty} \frac{|\{n \leq x : n \in A\}|}{x},
$$

provided that the limit exists, and the upper density of $A$ as

$$
\overline{d}(A) := \limsup_{x \to \infty} \frac{|\{n \leq x : n \in A\}|}{x}.
$$

**Theorem 6.5.** Let $f : \mathbb{N} \to \mathbb{R}$ be a function and suppose that for any $\epsilon > 0$ there exists a function $\alpha_\epsilon(n) : \mathbb{N} \to \mathbb{N}$ having the following properties:
(i) \( \lim_{\epsilon \to 0} \lim_{T \to \infty} d \{ n : \alpha_\epsilon (n) > T \} = 0 \),

(ii) \( \lim_{\epsilon \to 0} d \{ n : |f(n) - f (\alpha_\epsilon (n))| > \epsilon \} = 0 \), and

(iii) for each \( \alpha \geq 1 \) the density \( d \{ n : \alpha_\epsilon (n) = \alpha \} \) exists.

Then the frequencies \( \nu_x (n; f(n) \leq z) \) converge to a limiting distribution as \( x \to \infty \).

We shall use this theorem to prove the following lemma.

**Lemma 6.6.** Fix \( c \in \mathbb{N} \) and a prime \( \eta \). Then the frequencies

\[
\nu_x \left( k; \frac{\phi(\eta^c k) - 1}{\eta^c k - 1} \leq \omega \right)
\]

converge to a limiting distribution as \( x \to \infty \).

**Proof.** Define for \( k \in \mathbb{N} \)

\[
f(k) := \log \frac{\phi(\eta^c k) - 1}{\eta^c k - 1} = \sum_{p | \eta^c k-1} \log \left( 1 - \frac{1}{p} \right)
\]

and for each fixed \( \epsilon > 0 \)

\[
\alpha_\epsilon (k) := \prod_{p^\lambda || k} p^\lambda
\]

where

\[
y := y(\epsilon) = \max \left\{ \eta, \exp \left( \frac{c \log \eta \epsilon^2}{\epsilon^2} \right) \right\}.
\]

It is not difficult to verify that with this choice of \( y \) the validity of \( y > \epsilon^{-2} \) is guaranteed, so that properties (i) and (iii) of Theorem 6.5 hold as in [Ten95, Ex. 1, p. 295]. In order to verify the validity of property (ii), let us begin by noticing that since \( \alpha_\epsilon (k) \) is a divisor of \( k \), we get by the inequality \( \log \left( 1 - \frac{1}{p} \right) \ll \frac{1}{p} \), valid for each prime \( p \), that

\[
|f(k) - f (\alpha_\epsilon (k))| \ll \sum_{p | \eta^c k-1} \frac{1}{p} \tag{6.1}
\]

Using (6.1) and the fact that \( \ell_\eta (p) | ck \) implies \( \ell_\eta (p) / \gcd (\ell_\eta (p), c) \leq k \), we deduce that

\[
\sum_{k \leq x} |f(k) - f (\alpha_\epsilon (k))| \ll \sum_{p | \eta^c k-1} \frac{1}{p} \left\{ k \leq x : \ell_\eta (p) \leq \ell_\eta (p) \right\}
\]

\[
\leq x \sum_{p > y} \frac{1}{p} \frac{\gcd (\ell_\eta (p), c)}{\ell_\eta (p)}.
\]

In light of the inequalities \( \gcd (\ell_\eta (p), c) \leq c \) and \( \log p < \ell_\eta (p) \log \eta \), the last expression is seen to be at most

\[
c x \log \eta \sum_{p > y} \frac{1}{p \log p}.
\]

Now Lemma 3.2 for \( a = m = 1 \) combined with partial summation implies that

\[
\sum_{p > y} \frac{1}{p \log p} = -\frac{\log \log y + O(1)}{\log y} + \int_y^\infty \frac{\log \log t + O(1)}{t \log^2 t} \, dt
\]

\[
\ll \frac{1}{\log y}.
\]
which shows that
\[ \sum_{k \leq x} |f(k) - f(\alpha \epsilon(k))| \ll \frac{cx \log \eta}{\log y}. \]

We may now use this inequality to deduce that
\[ \frac{1}{x} \left| \left\{ k \leq x : |f(k) - f(\alpha \epsilon(k))| > \epsilon \right\} \right| \leq \sum_{k \leq x} \frac{|f(k) - f(\alpha \epsilon(k))|}{cx} \ll \frac{c \log \eta}{\epsilon \log y} \leq \epsilon, \]
by the definition of \( y \). This establishes the validity of property (ii) and therefore Theorem 6.5 applies and shows that the frequencies
\[ \nu_x \left( k; \frac{\phi(\eta^{ck} - 1)}{\eta^{ck} - 1} \leq \omega \right) \]
converge to a limiting distribution as \( x \to \infty \). \( \square \)

Now the proof of part (ii) of Theorem 1.3 follows by setting \( \eta = p, c = n, k = r \) and \( \omega = zn \) in Lemma 6.6. The proof of part (iii) of Theorem 1.3 follows by setting \( \eta = p, c = r, k = n \) and \( \omega = z \) in the same Lemma.

Acknowledgements. We thank T. Browning and R. A. Wilson for helpful comments and I. E. Shparlinski for bringing his paper [Shp90] to our attention. Both the anonymous referees have contributed substantially to improving an earlier version of this manuscript by providing us with numerous comments and suggestions. For this we duly thank them.

References

[1] H. Davenport, *Multiplicative number theory*, third ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000.
[2] Jean-Marc Deshouillers and Mehdi Hassani, *A note on the distribution function of \( \phi(p-1)/(p-1) \),* J. Aust. Math. Soc. 93 (2012), no. 1-2, 77–83.
[3] Paul Erdős, *On the smoothness of the asymptotic distribution of additive arithmetical functions*, Amer. J. Math. 61 (1939), 722–725.
[4] P. Erdős, *On some problems of Bellman and a theorem of Romanoff*, J. Chinese Math. Soc. (N.S.) 1 (1951), 409–421.
[5] P. Erdős and P. Turán, *On some problems of a statistical group-theory. I*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete 4 (1965), 175–186 (1965).
[6] I. Kátai, *On distribution of arithmetical functions on the set prime plus one*, Compositio Math. 19 (1968), 278–289.
[7] S. Li, *On the number of elements with maximal order in the multiplicative group modulo \( n \),* Acta Arith. 86 (1998), no. 2, 113–132.
[8] R. Lidell and H. Niederreiter, *Introduction to finite fields and their applications*, first ed., Cambridge University Press, Cambridge, 1994.
[9] Shuguang Li and Carl Pomerance, *Primes roots: a survey*, Sûrikaisekikenkyûsho Kókyûroku (2002), no. 1274, 77–87.
[10] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.
[11] S. S. Pillai, *On the sum function connected with primitive roots*, Proc. Indian Acad. Sci., Sect. A. 134 (1941), 526–529.
[12] I. Reiner, *On the number of matrices with given characteristic polynomial*, Ill. J. Math. 5 (1961), 324–329.
[13] J. Schoenberg, *Über die asymptotische Verteilung reeller Zahlen mod 1*, Math. Z. 28 (1928), no. 1, 171–199.
[14] I. E. Shparlinski, *Some arithmetic properties of recurrence sequences*, Mathematical notes of the Academy of Sciences of the USSR 47 (1990), no. 6, 612–617 (English).
[Ste69] P. J. Stephens, *An average result for Artin’s conjecture*, Mathematika 16 (1969), 178–188.

[Sto93] R. Stong, *The average order of a matrix*, J. Combin. Theory Ser. A 64 (1993), no. 2, 337–343.

[Ten95] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.

[TF69] Ž. Toleuov and A. S. Faînleîb, *The distribution of values of arithmetic functions on certain subsets of a natural series*, Izv. Akad. Nauk UzSSR Ser. Fiz.-Mat. Nauk 13 (1969), no. 5, 23–27.

[Tou09] Vincent Toulmonde, *Comportement au voisinage de 1 de la fonction de répartition de φ(n)/n*, Int. J. Number Theory 5 (2009), no. 8, 1347–1384.

School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS

*E-mail address:* s.aivazidis@qmul.ac.uk

School of Mathematics, University of Bristol, Bristol BS8 1TW

*E-mail address:* efthymios.sofos@bristol.ac.uk