THE DISTRIBUTION OF THE NUMBER OF SUBGROUPS OF THE MULTIPLICATIVE GROUP

GREG MARTIN AND LEE TROUPE

Abstract. Let $I(n)$ denote the number of isomorphism classes of subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$, and let $G(n)$ denote the number of subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$ counted as sets (not up to isomorphism). We prove that both $\log G(n)$ and $\log I(n)$ satisfy Erdős–Kac laws, in that suitable normalizations of them are normally distributed in the limit. Of note is that $\log G(n)$ is not an additive function but is closely related to the sum of squares of additive functions. We also establish the orders of magnitude of the maximal orders of $\log G(n)$ and $\log I(n)$.

1. Introduction

The distribution of values of additive functions has long been of interest to number theorists. Perhaps the most famous result in this area is the celebrated Erdős–Kac theorem: if $\omega(n)$ and $\Omega(n)$ denote, respectively, the number of distinct prime factors of n and the number of prime factors of n counted with multiplicity, then the distributions of the values of both

$$\frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} \quad \text{and} \quad \frac{\Omega(n) - \log\log n}{\sqrt{\log\log n}}$$

tend to the standard normal distribution. In other words, both $\omega(n)$ and $\Omega(n)$ are, in the limit, "normally distributed with mean $\log\log n$ and variance $\log\log n$". Indeed, Erdős and Kac [4] established this property for a large class of additive functions, and many subsequent authors have widened even further the set of functions for which we know such Erdős–Kac laws. In this paper, we establish Erdős–Kac laws for two functions that count subgroups of a natural family of finite abelian groups, as we now describe.

Let $\mathbb{Z}_n^\times = (\mathbb{Z}/n\mathbb{Z})^\times$ denote the multiplicative group of units modulo n. Let $G(n)$ denote the number of subgroups of $\mathbb{Z}_n^\times$, counted as sets (rather than up to isomorphism), so that $G(8) = 5$, for example. The function $G(n)$ is not a multiplicative function of n, but it does have the property that $G(n) = \prod_{p\mid\phi(n)} G_p(n)$ (as we shall see below), where $G_p(n)$ denotes the number of p-subgroups of $\mathbb{Z}_n^\times$. One could perhaps say that $G(n)$ is "a multiplicative function of $\phi(n)$", or simply "ϕ-multiplicative," making

$$\log G(n) = \sum_{p\mid\phi(n)} \log G_p(n) \tag{1}$$

a "ϕ-additive" function. Our primary aim is to show that $\log G(n)$ possesses enough structure to satisfy a similar Erdős–Kac law:

2010 *Mathematics Subject Classification.* Primary 11N60, 11N45; secondary 11N37.

Theorem 1.1. *Define*

$$A_0 = \frac{1}{4}\sum_p \frac{p^2\log p}{(p-1)^3(p+1)} \quad \textit{and} \quad A = A_0 + \frac{\log 2}{2} \approx 0.72109$$

and

$$B = \frac{1}{4}\sum_p \frac{p^3(p^4-p^3-p^3-p-1)(\log p)^2}{(p-1)^6(p+1)^2(p^2+p+1)},$$

and set $C = \frac{(\log 2)^2}{3} + 2A_0\log 2 + 4A_0^2 + B \approx 3.924$. *(Both sums are taken over all primes* p*.) Then for every real number* u*,*

$$\lim_{x\to\infty}\frac{1}{x}\#\big\{n \le x\colon\ \log G(n) < A(\log\log n)^2 + u\cdot\sqrt{C}(\log\log n)^{3/2}\big\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\,dt.$$

In other words, the quantity $\log G(n)$ *is normally distributed, with mean* $A(\log\log n)^2$ *and variance* $C(\log\log n)^3$*.*

We briefly indicate the overall structure of the proof of Theorem 1.1. First, we understand the typical values of $\log G(n)$ by writing them as a linear combination of squares of well-understood additive functions, together with one anomalous "ϕ-additive" function.

Proposition 1.2. *Set* $X = (\log\log x)^{1/2}(\log\log\log x)^2$*. For any positive integer* n*, define*

$$P_n(x) = \log 2\cdot\omega(\phi(n)) + \frac{1}{4}\sum_{q\le X}\omega_q(n)^2\Lambda(q), \tag{2}$$

where $\Lambda(q)$ *denotes the usual von Mangoldt function, and where the* ω_q *are additive functions defined in Definition 2.7 below. Then for all but* $O(x/\log\log\log x)$ *integers* $n \le x$*,*

$$\log G(n) = P_n(x) + O\bigg(\frac{(\log\log x)^{3/2}}{\log\log\log x}\bigg). \tag{3}$$

For any function $f(n)$, define the "mean"

$$\mu(f) = \mu(f;x) = \sum_{p\le x}\frac{f(p)}{p}, \tag{4}$$

and set

$$D(x) = \log 2\cdot\mu(\omega\circ\phi) + \frac{1}{4}\sum_{q\le X}\mu(\omega_q)^2\Lambda(q) \tag{5}$$

(so that $D(x)$ is simply $P_n(x)$ with each function of n replaced by its mean). Our strategy is to show that the values of $P_n(x)$ for $n \le x$ are, asymptotically as x tends to ∞, normally distributed with mean $D(x)$ and variance $C(\log\log x)^3$, with C defined as in Theorem 1.1. We carry out this strategy via the "method of moments."

Proposition 1.3. *For any positive integer* h*, define the "*h*th moment"*

$$M_h(x) = \sum_{n\le x}\big(P_n(x) - D(x)\big)^h. \tag{6}$$

Then

$$\lim_{x\to\infty}\frac{M_h(x)}{C^{h/2}x(\log\log x)^{3h/2}} = \begin{cases}\frac{h!}{(h/2)!2^{h/2}}, & \textit{if } h \textit{ is even},\\ 0, & \textit{if } h \textit{ is odd}.\end{cases}$$

The quantity $\frac{h!}{(h/2)!2^{h/2}}$ for even h is precisely the hth moment of the standard normal distribution, and it is a famous lemma of Chebyshev that the normal distribution is determined by its moments (see Section 7 for more details).

Our proof is inspired by work of Granville and Soundararajan [8], who described a way to organize method-of-moments proofs in number theory to make the main terms more readily identifiable. The proof herein is tailored to the specific function $P_n(x)$ mentioned above, which can be viewed as a quadratic polynomial (in increasingly many variables) being evaluated at values of specific additive functions. For any fixed polynomial, one can apply the same techniques to its evaluation at values of additive functions from a much more general class, thereby obtaining Erdős–Kac laws for these polynomials of additive functions as well (including, for example, Erdős–Kac laws for products of additive functions). This generalization is the subject of forthcoming work by the authors.

Since $G(n)$ counts subgroups of $\mathbb{Z}_n^\times$ as sets, the reader might wonder about the equally natural function $I(n)$ that counts subgroups of $\mathbb{Z}_n^\times$ up to isomorphism. It turns out to be much easier to establish an Erdős–Kac law for $\log I(n)$, partially because $I(n)$ is a ϕ-multiplicative function of a much simpler type, but mostly because we can leverage existing work of Erdős and Pomerance [6] on the number of prime factors of $\phi(n)$ to greatly shorten our proof.

Theorem 1.4. *For every real number u,*

$$\lim_{x\to\infty} \frac{1}{x}\#\left\{n \le x\colon\ \log I(n) < \frac{\log 2}{2}(\log\log n)^2 + u\cdot\sqrt{\frac{\log 2}{3}}(\log\log n)^{3/2}\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\,dt.$$

In other words, the quantity $\log I(n)$ is normally distributed, with mean $\frac{\log 2}{2}(\log\log n)^2$ and variance $\frac{\log 2}{3}(\log\log n)^3$.

The leading constant here, $\frac{\log 2}{2} \approx 0.34657$, for the typical size of $\log I(n)$ is a bit less than half the leading constant A for the typical size of $\log G(n)$ in Theorem 1.1; in other words, the total number $G(n)$ of subgroups of $\mathbb{Z}_n^\times$ is typically a bit more than the square of the number $I(n)$ of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$.

We begin by establishing Proposition 1.2 in Section 2, which will require a brief digression into counting subgroups of finite abelian p-groups using partitions and Gaussian binomial coefficients. Sections 3 through 7 comprise the proof of Theorem 1.1, with the verification of Proposition 1.3 taking place in Section 6; a more detailed roadmap is provided in Section 3, along with notation and conventions that will be used through the rest of the paper. Finally, Section 8 contains the proof of the aforementioned theorem about $I(n)$, along with proofs of the following maximal-order results for $\log G(n)$ and $\log I(n)$:

Theorem 1.5. *The order of magnitude of the maximal order of $\log G(n)$ is $(\log x)^2/\log\log x$. More precisely,*

$$\frac{1}{16}\frac{(\log x)^2}{\log\log x} + O\left(\frac{(\log x)^2\log\log\log x}{(\log\log x)^2}\right) \le \max_{n\le x}\big(\log I(n)\big) \le \frac{1}{4}\frac{(\log x)^2}{\log\log x} + O\left(\frac{(\log x)^2}{(\log\log x)^2}\right).$$

Theorem 1.6. *The order of magnitude of the maximal order of* $\log I(n)$ *is* $\log x/\log\log x$. *More precisely,*

$$\frac{\log 2}{5}\frac{\log x}{\log\log x}+O\biggl(\frac{\log x}{(\log\log x)^2}\biggr)\le \max_{n\le x}\bigl(\log I(n)\bigr)\le \pi\sqrt{\frac{2}{3}}\frac{\log x}{\log\log x}+O\biggl(\frac{\log x}{(\log\log x)^2}\biggr).$$

2. Expressing $\log G(n)$ as a polynomial of additive functions

In this section we prove Proposition 1.2. First, we import a classical identity for the number of subgroups of a finite abelian p-group, which we alter into an approximate form that is suitable for our application. Then we describe exactly the p-Sylow subgroup of the multiplicative group $\mathbb{Z}_n^\times$ and record its approximate number of subgroups. Finally we sum this contribution over all primes p, which mostly involves dealing with the complication of truncating this sum suitably to avoid being overwhelmed with error terms; we employ some "anatomy of integers" arguments to show that this truncation is valid for almost all integers n.

2.1. **Subgroups of p-groups.** Let us recall, from the classification of finitely generated abelian groups, that every finite abelian group of size p^m can be uniquely written in the form $\mathbb{Z}_{p^{\alpha_1}}\times\mathbb{Z}_{p^{\alpha_2}}\times\cdots$ for some nonincreasing sequence $(\alpha_1,\alpha_2,\dots)$ of nonnegative integers summing to m. (We avoid naming the length of such sequences by the convention that all but finitely many of the α_j equal 0.) In other words, isomorphism classes of finite abelian p-groups are in one-to-one correspondence with partitions $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\dots)$ of m.

A subpartition $\boldsymbol{\beta}$ of a partition $\boldsymbol{\alpha}$ is a nonincreasing sequence $(\beta_1,\beta_2,\dots)$ of positive integers such that $\beta_j\le\alpha_j$ for all $j\ge1$; we write $\boldsymbol{\beta}\preceq\boldsymbol{\alpha}$ when $\boldsymbol{\beta}$ is a subpartition of $\boldsymbol{\alpha}$. It is easy (though not quite trivial) to see that $\mathbb{Z}_{p^{\alpha_1}}\times\mathbb{Z}_{p^{\alpha_2}}\times\cdots$ contains an isomorphic copy of $\mathbb{Z}_{p^{\beta_1}}\times\mathbb{Z}_{p^{\beta_2}}\times\cdots$ if and only if $\boldsymbol{\beta}\preceq\boldsymbol{\alpha}$. We are interested in more precise information, however, about the number of subgroups of $\mathbb{Z}_{p^{\alpha_1}}\times\mathbb{Z}_{p^{\alpha_2}}\times\cdots$ that are isomorphic to $\mathbb{Z}_{p^{\beta_1}}\times\mathbb{Z}_{p^{\beta_2}}\times\cdots$.

Definition 2.1. Given partitions $\boldsymbol{\beta}\preceq\boldsymbol{\alpha}$ and a prime p, define $N_p(\boldsymbol{\alpha},\boldsymbol{\beta})$ to be the number of subgroups inside $\mathbb{Z}_{p^{\alpha_1}}\times\mathbb{Z}_{p^{\alpha_2}}\times\cdots$ that are isomorphic to $\mathbb{Z}_{p^{\beta_1}}\times\mathbb{Z}_{p^{\beta_2}}\times\cdots$. Define $N_p(\boldsymbol{\alpha})$ to be the number of subgroups inside $\mathbb{Z}_{p^{\alpha_1}}\times\mathbb{Z}_{p^{\alpha_2}}\times\cdots$ (as sets, not up to isomorphism), so that $N_p(\boldsymbol{\alpha})=\sum_{\boldsymbol{\beta}\preceq\boldsymbol{\alpha}}N_p(\boldsymbol{\alpha},\boldsymbol{\beta})$.

As it happens, there is a classical formula for $N_p(\boldsymbol{\alpha},\boldsymbol{\beta})$, most conveniently expressed in terms of conjugate partitions. Every partition $\boldsymbol{\alpha}$ has a conjugate partition $\boldsymbol{a}$, which is most easily obtained by transposing the Ferrers diagram corresponding to $\boldsymbol{\alpha}$. The number of parts (nonzero elements) of the conjugate partition $\boldsymbol{a}$ is exactly equal to α_1, and in general α_j equals the number of parts of $\boldsymbol{a}$ that are at least j in size; by the same token, the first part a_1 of $\boldsymbol{a}$ is equal to the number of parts of $\boldsymbol{\alpha}$, and so on.

We quote this classical formula, which can be found in [13, equation (1)] and the references cited therein:

Lemma 2.2. *Let p be prime, and let $\boldsymbol{\beta}\preceq\boldsymbol{\alpha}$ be partitions. Let $\boldsymbol{a}=(a_1,a_2,\dots,a_{\alpha_1},0,\dots)$ and $\boldsymbol{b}=(b_1,b_2,\dots,b_{\beta_1},0,\dots)$ be the conjugate partitions to $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, respectively. Then*

$$N_p(\boldsymbol{\alpha},\boldsymbol{\beta})=\prod_{j=1}^{\alpha_1}p^{(a_j-b_j)b_{j+1}}\begin{bmatrix}a_j-b_{j+1}\\ b_j-b_{j+1}\end{bmatrix}_p.$$

Here, $\begin{bmatrix} k \\ \ell \end{bmatrix}_p$ is the Gaussian binomial coefficient, defined to be 0 if $\ell < 0$ or $\ell > k$, and otherwise defined by

$$\begin{bmatrix} k \\ \ell \end{bmatrix}_p = \prod_{j=1}^{\ell} \frac{p^{k-\ell+j} - 1}{p^j - 1}. \tag{7}$$

The reader might gain some intuition from considering the case where $\boldsymbol{\alpha} = (1, \dots, 1, 0, \dots)$ and $\boldsymbol{\beta} = (1, \dots, 1, 0, \dots)$ are the finest possible partitions of k and ℓ, respectively, so that $N_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is the number of ℓ-dimensional subspaces of $\mathbb{F}_p^k$. In this case, $\boldsymbol{a} = (k, 0, \dots)$ and $\boldsymbol{b} = (\ell, 0, \dots)$ and so $N_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is simply $\begin{bmatrix} k \\ \ell \end{bmatrix}_p$. It can be seen that the numerator of the formula (7) is, up to a power of p, the number of $k \times \ell$ matrices over $\mathbb{F}_p$ with full rank ℓ (and the column space of each such matrix defines an ℓ-dimensional subspace of $\mathbb{F}_p^k$), while the denominator is, up to the same power of p, the number of invertible $\ell \times \ell$ matrices over $\mathbb{F}_p$ (which act by left multiplication on the set of $k \times \ell$ matrices while preserving their column spaces).

We will prefer an approximate version of the formula from Lemma 2.2, which the following pair of lemmas provides.

Lemma 2.3. *For any prime p and any integers $0 \le \ell \le k$, there exists a real number $0 \le \theta < 6$ such that*

$$\begin{bmatrix} k \\ \ell \end{bmatrix}_p = p^{\ell(k-\ell)}(1 + \theta p^{-1}).$$

Proof. For any integers $k \ge \ell \ge j \ge 1$, we have the inequalities

$$p^{k-\ell} \le \frac{p^{k-\ell+j} - 1}{p^j - 1} \le \frac{p^{k-\ell+j}}{p^j - 1} = \frac{p^{k-\ell}}{1 - p^{-j}}. \tag{8}$$

Note that

$$\prod_{j=2}^{\ell} (1 - p^{-j}) \ge 1 - \sum_{j=2}^{\ell} p^{-j} > 1 - \frac{1}{p(p-1)},$$

and so

$$\prod_{j=1}^{\ell} \frac{1}{1 - p^{-j}} < \frac{1}{1 - p^{-1}} \left(1 - \frac{1}{p(p-1)}\right)^{-1} \le 1 + 6p^{-1},$$

where the last inequality follows by a simple calculation. Therefore equation (8) implies that

$$p^{\ell(k-\ell)} \le \prod_{j=1}^{\ell} \frac{p^{k-\ell+j} - 1}{p^j - 1} \le p^{\ell(k-\ell)} \prod_{j=1}^{\ell} \frac{1}{1 - p^{-j}} < p^{\ell(k-\ell)}(1 + 6p^{-1}),$$

which establishes the lemma. □

Lemma 2.4. *Given partitions $\boldsymbol{\beta} \preceq \boldsymbol{\alpha}$, let $\boldsymbol{b}$ and $\boldsymbol{a}$ be the partitions conjugate to $\boldsymbol{\beta}$ and $\boldsymbol{\alpha}$ respectively. For any prime p,*

$$N_p(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \left(\prod_{j=1}^{\alpha_1} p^{(a_j - b_j) b_j} \right) \left(1 + \theta p^{-1}\right)^{\alpha_1}$$

for some real number $0 \le \theta < 6$.

Proof. By Lemmas 2.2 and 2.3, there exist real numbers $0 \le \theta_j < 6$ such that

$$\begin{aligned} N_p(\boldsymbol{\alpha}, \boldsymbol{\beta}) &= \prod_{j=1}^{\alpha_1} p^{(a_j - b_j)b_{j+1}} \begin{bmatrix} a_j - b_{j+1} \\ b_j - b_{j+1} \end{bmatrix}_p \\ &= \prod_{j=1}^{\alpha_1} p^{(a_j - b_j)b_{j+1}} \big(p^{(b_j - b_{j+1})(a_j - b_j)} (1 + \theta_j p^{-1}) \big) \\ &= \prod_{j=1}^{\alpha_1} p^{(a_j - b_j)b_j} (1 + \theta_j p^{-1}). \end{aligned}$$

The lemma now follows from the intermediate value property of the continuous function $f(\theta) = (1 + \theta p^{-1})^{\alpha_1}$ on the interval $0 \le \theta \le 6$, along with the observation that

$$f(0) \prod_{j=1}^{\alpha_1} p^{(a_j - b_j)b_j} \le \prod_{j=1}^{\alpha_1} p^{(a_j - b_j)b_j} (1 + \theta_j p^{-1}) \le f(6) \prod_{j=1}^{\alpha_1} p^{(a_j - b_j)b_j}.$$

$\square$

Finally, we want to sum $N_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ over all subpartitions $\boldsymbol{\beta}$ of $\boldsymbol{\alpha}$. It turns out that the dominant contribution to this sum comes from the subpartitions $\boldsymbol{\beta}$ nearest to $\frac{1}{2}\boldsymbol{\alpha}$.

Lemma 2.5. *For any integer $a \ge 0$ and any prime p, we have*

$$\sum_{b=0}^{a} p^{(a-b)b} = p^{a^2/4 + O(1)} \quad \textit{and} \quad p^{(a - \lfloor \frac{a}{2} \rfloor) \lfloor \frac{a}{2} \rfloor} = p^{a^2/4 + O(1)}.$$

Proof. Suppose first that $a = 2c$ is even. Using $(2c - b)b = c^2 - (c - b)^2 \le c^2 - (c - b)$ for $b \le c - 1$, we obtain

$$\sum_{b=0}^{a} p^{(a-b)b} = p^{c^2} + 2 \sum_{b=0}^{c-1} p^{(2c-b)b} = p^{c^2} + O\Bigg(\sum_{b=0}^{c-1} p^{c^2 - (c-b)} \Bigg) = p^{c^2} + O\big(p^{c^2 - 1}\big),$$

which is certainly of the form $p^{a^2/4 + O(1)}$. Even more simply, $p^{(a - \lfloor \frac{a}{2} \rfloor) \lfloor \frac{a}{2} \rfloor} = p^{(2c-c)c} = p^{a^2/4}$ exactly.

Now suppose that $a = 2c + 1$ is odd. Using $(2c + 1 - b)b = (c + \frac{1}{2})^2 - (c + \frac{1}{2} - b)^2 \le (c + \frac{1}{2})^2 - (c + \frac{1}{2} - b)$ for $b \le c - 1$, we obtain

$$\begin{aligned} \sum_{b=0}^{a} p^{(a-b)b} &= 2\Bigg(p^{c(c+1)} + \sum_{b=0}^{c-1} p^{(2c+1-b)b} \Bigg) \\ &= 2\Bigg(p^{c(c+1)} + O\Bigg(\sum_{b=0}^{c-1} p^{(c+\frac{1}{2})^2 - (c + \frac{1}{2} - b)} \Bigg) \Bigg) = 2p^{c(c+1)} + O\big(p^{(c+\frac{1}{2})^2 - \frac{1}{2}} \big). \end{aligned}$$

Since $(c + \frac{1}{2})^2 - \frac{1}{2} < c(c + 1)$, the right-hand side is $\asymp p^{c(c+1)} = p^{(c+\frac{1}{2})^2 - \frac{1}{4}}$, which is also of the form $p^{a^2/4 + O(1)}$. On the other hand, $p^{(a - \lfloor \frac{a}{2} \rfloor) \lfloor \frac{a}{2} \rfloor} = p^{(2c+1-c)c} = p^{a^2/4 + O(1)}$ as we have just seen. $\square$

Proposition 2.6. *For any prime p and any partition $\boldsymbol{\alpha}$,*

$$\log N_p(\boldsymbol{\alpha}) = \frac{\log p}{4}\sum_{j=1}^{\alpha_1} a_j^2 + O(\alpha_1 \log p).$$

Proof. We recall our notation $\boldsymbol{a} = (a_1, \dots, a_{\alpha_1}, 0, \dots)$ and $\boldsymbol{b} = (b_1, \dots, b_{\alpha_1}, 0, \dots)$ for the conjugate partitions of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, respectively. Since $N_p(\boldsymbol{\alpha}) = \sum_{\boldsymbol{\beta}\preceq\boldsymbol{\alpha}} N_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ by definition, Lemms 2.4 tells us that there exist constants $0 \le \theta_{\boldsymbol{\beta}} < 6$ and $0 \le \theta < 6$ such that

$$N_p(\boldsymbol{\alpha}) = \sum_{\boldsymbol{\beta}\preceq\boldsymbol{\alpha}} \Bigg(\prod_{j=1}^{\alpha_1} p^{(a_j-b_j)b_j}\Bigg)\big(1+\theta_{\boldsymbol{\beta}} p^{-1}\big)^{\alpha_1} = \big(1+\theta p^{-1}\big)^{\alpha_1} \sum_{\boldsymbol{\beta}\preceq\boldsymbol{\alpha}} \Bigg(\prod_{j=1}^{\alpha_1} p^{(a_j-b_j)b_j}\Bigg), \tag{9}$$

where the second equality again uses the intermediate value property of $f(\theta) = \big(1+\theta p^{-1}\big)^{\alpha_1}$ (and the positivity of each summand). On one hand, since every $\boldsymbol{\beta} \preceq \boldsymbol{\alpha}$ corresponds to certain choices $0 \le b_j \le a_j$, we have

$$\sum_{\boldsymbol{\beta}\preceq\boldsymbol{\alpha}} \Bigg(\prod_{j=1}^{\alpha_1} p^{(a_j-b_j)b_j}\Bigg) \le \sum_{b_1=0}^{a_1} \cdots \sum_{b_{\alpha_1}=0}^{a_{\alpha_1}} \prod_{j=1}^{\alpha_1} p^{(a_j-b_j)b_j} = \prod_{j=1}^{\alpha_1} \sum_{b_j=0}^{a_j} p^{(a_j-b_j)b_j} = \prod_{j=1}^{\alpha_1} p^{a_j^2/4+O(1)}$$

by Lemma 2.5. On the other hand, let $\boldsymbol{\beta}_1$ be the subpartition of $\boldsymbol{\alpha}$ whose conjugate partition is $\boldsymbol{b} = (\lfloor \frac{a_1}{2}\rfloor, \dots, \lfloor \frac{a_{\alpha_1}}{2}\rfloor, 0, \dots)$; considering only the summand on the right-hand side of equation (9) corresponding to $\boldsymbol{\beta} = \boldsymbol{\beta}_1$ yields

$$\sum_{\boldsymbol{\beta}\preceq\boldsymbol{\alpha}} \Bigg(\prod_{j=1}^{\alpha_1} p^{(a_j-b_j)b_j}\Bigg) \ge \prod_{j=1}^{\alpha_1} p^{(a_j-\lfloor \frac{a_j}{2}\rfloor)\lfloor \frac{a_j}{2}\rfloor} = \prod_{j=1}^{\alpha_1} p^{a_j^2/4+O(1)}$$

by Lemma 2.5 again. Combining these last two inequalities with equation (9), we conclude that

$$N_p(\boldsymbol{\alpha}) = \big(1+\theta p^{-1}\big)^{\alpha_1} \prod_{j=1}^{\alpha_1} p^{a_j^2/4+O(1)},$$

and therefore (since $\log(1+x)$ is bounded for $0 \le x < 3$)

$$\log N_p(\boldsymbol{\alpha}) = O(\alpha_1) + \sum_{j=1}^{\alpha_1}\bigg(\frac{a_j^2}{4} + O(1)\bigg)\log p = \frac{\log p}{4}\sum_{j=1}^{\alpha_1} a_j^2 + O(\alpha_1 \log p)$$

as claimed. □

2.2. **Counting p-subgroups of the multiplicative group.** We now begin the proof of Proposition 1.2 in earnest. As in the introduction, let $G(n)$ denote the number of subgroups of $\mathbb{Z}_n^\times$ and let $G_p(n)$ denotes the number of p-subgroups of $\mathbb{Z}_n^\times$. Since every finite abelian group is the direct product of its p-Sylow subgroups, it is easy to see that

$$G(n) = \prod_{p\mid\phi(n)} G_p(n) \quad \text{and thus} \quad \log G(n) = \sum_{p\mid\phi(n)} \log G_p(n).$$

Therefore, we first turn our attention to $\log G_p(n)$. It turns out that $\log G_p(n)$ can be expressed in terms of arithmetic functions $\overline{\omega}_{p^j}(n)$, defined in two stages as follows:

Definition 2.7. For any positive integer q, let $\omega_q(n)$ denote the number of distinct primes $p \mid n$ such that $p \equiv 1 \pmod{q}$. For example, $\omega_1(n) = \omega(n)$, while $\omega_2(n) = \omega(n) - 1$ when n is even and $\omega_2(n) = \omega(n)$ when n is odd.

These functions ω_q will play a prominent role in the remainder of this paper. Already we start forming our intuition: since $\omega(n)$ is typically about $\log\log n$, and since one in every $\phi(q)$ primes on average is congruent to 1 (mod q), the function $\omega_q(n)$ is typically about $\frac{1}{\phi(q)} \log\log n$ in size; and indeed, an Erdős–Kac law for $\omega_q(n)$ itself is straightforward to derive from the results in [4].

We must make a punctilious alteration to these functions ω_q in order for them to exactly describe the structure of $\mathbb{Z}_n^\times$. However, our intuition should also include the understanding that the difference between ω_q and its sibling $\overline{\omega}_q$ (defined momentarily) is negligible in the distributional sense; in particular, all we will really use is that $\overline{\omega}_q(n) = \omega_q(n) + O(1)$ uniformly in integers n and prime powers q. Recall that the notation $p^r \parallel m$ means that $p^r \mid m$ but $p^{r+1} \nmid m$.

Definition 2.8. For any prime power p^r, define

$$\overline{\omega}_{p^r}(n) = \begin{cases} \omega_{p^r}(n) + 1, & \text{if } p \text{ is odd and } p^{r+1} \mid n, \\ \omega_{p^r}(n), & \text{if } p \text{ is odd and } p^{r+1} \nmid n, \\ \omega_2(n) + 2, & \text{if } p^r = 2^1 \text{ and } 2^3 \mid n, \\ \omega_2(n) + 1, & \text{if } p^r = 2^1 \text{ and } 2^2 \parallel n, \\ \omega_2(n), & \text{if } p^r = 2^1 \text{ and } 2^2 \nmid n, \\ \omega_{2^r}(n) + 1, & \text{if } p = 2 \text{ and } r > 1 \text{ and } p^{r+2} \mid n, \\ \omega_{2^r}(n), & \text{if } p = 2 \text{ and } r > 1 \text{ and } p^{r+2} \nmid n. \end{cases}$$

Definition 2.9. For any prime p and any positive integer n, let $\lambda_p(n)$ denote the largest power of p that divides the Carmichael function $\lambda(n)$. In other words, $\lambda_p(n)$ is the exponent of the p-Sylow subgroup of $\mathbb{Z}_n^\times$.

Lemma 2.10. *Let n be a positive integer, and let p be a prime dividing $\phi(n)$. The p-Sylow subgroup of $\mathbb{Z}_n^\times$ is isomorphic to $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots$, where $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \dots)$ is the conjugate partition to*

$$\boldsymbol{a} = (a_1, a_2, \dots) = (\overline{\omega}_p(n), \overline{\omega}_{p^2}(n), \dots, \overline{\omega}_{p^{\lambda_p(n)}}(n), 0, \dots).$$

Proof. First let p be an odd prime. Write the p-Sylow subgroup of $\mathbb{Z}_n^\times$ as $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots$ for some partition $\boldsymbol{\alpha}$ which we want to determine. There are two possible sources of factors of p in $\phi(n)$: primes $q \mid n$ such that $q \equiv 1 \pmod{p}$ (including those congruent to 1 modulo higher powers of p), and p^2 itself (or a higher power of p) dividing n. Furthermore, by the Chinese remainder theorem and the existence of primitive roots modulo every odd prime power, we can say exactly how each of these sources affects the p-Sylow subgroup of $\mathbb{Z}_n^\times$.

Each prime $q \mid n$ such that $q \equiv 1 \pmod{p^j}$ contributes, to the the p-Sylow subgroup of $\mathbb{Z}_n^\times$, a factor of $\mathbb{Z}_{p^m}$ with $m \ge j$ (indeed, m is the exponent of p in the prime factorization of $q-1$). Moreover, if $p^{j+1} \mid n$, then this power of p contributes to the p-Sylow subgroup of $\mathbb{Z}_n^\times$ another factor of $\mathbb{Z}_{p^m}$ with $m \ge j$ (in this case, $m+1$ is the exponent of p in the prime factorization of n itself). All factors of the form $\mathbb{Z}_{p^m}$ in the primary decomposition of $\mathbb{Z}_n^\times$ arise in one of these two ways; therefore, the number of factors of order at least p^j in the

p-Sylow subgroup of $\mathbb{Z}_n^\times$ is exactly equal to $\overline{\omega}_{p^j}(n)$. But a_j, the jth entry in the conjugate partition to $\boldsymbol{\alpha}$, is precisely the number of factors of order at least p^j in $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots$. We conclude that $a_j = \overline{\omega}_{p^j}(n)$ as desired.

The case $p = 2$ follows by an similar analysis, complicated slightly by the fact that $\mathbb{Z}_2^\times \cong \mathbb{Z}_1$ and $\mathbb{Z}_4^\times \cong \mathbb{Z}_2$ while $\mathbb{Z}_{2^r}^\times \cong \mathbb{Z}_{2^{r-2}} \times \mathbb{Z}_2$ when $r \geq 3$. $\square$

It is worth remarking that in particular, Lemma 2.10 shows that the exponent of p in the prime factorization of $\phi(n)$ is exactly $\sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n)$ for every prime p. Consequently,

$$\sum_{p \mid \phi(n)} \sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n) \log p = \log \phi(n). \tag{10}$$

Furthermore, let $\nu_p(n)$ denote the power of p in the prime factorization of n. The proof of Lemma 2.10 also shows that for odd primes p,

$$\lambda_p(n) = \max\bigl\{\nu_p(n) - 1, \max\{j \colon \omega_{p^j}(n) \geq 1\}\bigr\};$$

when $p = 2$, we must replace $\nu_p(n) - 1$ with $\max\{0, \nu_2(n) - 2\}$. In either case,

$$\lambda_p(n) \leq \max\Bigl\{\nu_p(n), \sum_{j \geq 1} \omega_{p^j}(n)\Bigr\}. \tag{11}$$

With the following proposition, we may leave most of the details of abelian groups and partitions behind and operate within the realm of analytic number theory to complete the proof of Proposition 1.2.

Proposition 2.11. *For any positive integer n and any prime p dividing $\phi(n)$,*

$$\log G_p(n) = \frac{\log p}{4} \sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n)^2 + O(\lambda_p(n) \log p).$$

Moreover, if $p \parallel \phi(n)$, then $\log G_p(n) = \log 2$.

Proof. If $p \parallel \phi(n)$, then the p-part of $\mathbb{Z}_n^\times$ is precisely $\mathbb{Z}_p$, which trivially contains exactly two subgroups; hence $G_p(n) = 2$ in this case. In general, Proposition 2.6 tells us that

$$\log N_p(\boldsymbol{\alpha}) = \frac{\log p}{4} \sum_{j=1}^{\alpha_1} a_j^2 + O(\alpha_1 \log p),$$

while Lemma 2.10 gives us the exact evaluations $\alpha_1 = \lambda_p(n)$ and $a_j = \overline{\omega}_{p^j}(n)$. $\square$

2.3. **Counting all subgroups of the multiplicative group.** The main goal of this section is to establish Proposition 1.2, which says that $\log G(n)$ is approximately equal to a particular polynomial expression in additive functions of n, at least for most integers n.

Several times in the course of these proofs, we will make use of upper bounds (of the correct order of magnitude) that follow, via partial summation, from the prime number theorem, or indeed from Mertens's formulas or even Chebyshev's bounds for prime-counting functions. Such sums include sums over primes like $\sum_{p \leq y} 1/p$ or $\sum_{p > y} 1/p^2$, or sums over prime powers like $\sum_{p^j \leq y} \log^2(p^j)/p^j$ or $\sum_{q \leq y} \Lambda(q)/q$. Moreover, since $q/\phi(q) \leq 2$ for all prime powers q, such sums can also be modified to have denominators of $p-1$ instead of p, or $\phi(q)$ instead of q. In all such cases, we shall simply say "by partial summation" to indicate that the required upper bounds follows in a standard way from these prime-counting estimates.

In addition, we will make frequent use of the following Mertens-type estimate for arithmetic progressions, which can be found in [11] or [12]:

Lemma 2.12. *For $2 \le q \le x$, we have* $\displaystyle\sum_{\substack{p\le x \\ p\equiv 1 \pmod q}} \frac{1}{p} = \frac{\log\log x}{\phi(q)} + O\bigg(\frac{\log q}{\phi(q)}\bigg).$

For the rest of this section, we set

$$\begin{aligned} W &= \log\log\log x \\ X &= (\log\log x)^{1/2}(\log\log\log x)^2 \\ Y &= (\log\log x)^2. \end{aligned}$$

(Note that this definition of X is the same as in Proposition 1.2.)

Lemma 2.13. *For all but $O(x/W)$ integers $n \le x$,*

$$\max\bigg\{ \sum_{\substack{p\le Y \\ \lambda_p(n)\ge 1}} \log p, \sum_{p\le Y} \lambda_p(n)\log p, \sum_{p\le Y} \nu_p(n)\log p, \sum_{p^j\le Y} \omega_{p^j}(n)\log p \bigg\} \\ \ll \log\log x \cdot (\log\log\log x)^2. \quad (12)$$

Proof. The first sum on the left-hand side of equation (12) is clearly bounded above by the second sum; and this second sum, by equation (11), is bounded above by the maximum of third and fourth sums on the left-hand side. It therefore suffices to show that

$$\sum_{n\le x}\sum_{p\le Y} \nu_p(n)\log p + \sum_{n\le x}\sum_{p^j\le Y} \omega_{p^j}(n)\log p \ll x\log\log x \cdot \log Y, \quad (13)$$

for then there can be no more than $O(x/W)$ integers $n \le x$ for which either of the two summands exceeds $\log\log x \cdot \log Y \cdot W = \log\log x \cdot (\log\log\log x)^2$.

The first sum on the left-hand side of equation (13) can be bounded simply:

$$\begin{aligned} \sum_{n\le x}\sum_{p\le Y} \nu_p(n)\log p &= \sum_{n\le x}\sum_{p\le Y} \log p \sum_{\substack{j\ge 1 \\ p^j \mid n}} 1 = \sum_{p\le Y} \log p \sum_{j\ge 1} \sum_{\substack{n\le x \\ p^j\mid n}} 1 \\ &\le \sum_{p\le Y}\log p \sum_{j\ge 1} \frac{x}{p^j} = x\sum_{p\le Y} \frac{\log p}{p-1} \ll x\log Y \end{aligned}$$

by partial summation, which is more than sufficient. As for the second sum on the left-hand side of equation (13),

$$\begin{aligned} \sum_{n\le x}\sum_{p^j\le Y} \omega_{p^j}(n)\log p &= \sum_{n\le x}\sum_{p^j\le Y}\log p \sum_{\substack{q\mid n \\ q\equiv 1 \pmod{p^j}}} 1 = \sum_{p^j\le Y}\log p \sum_{\substack{q\le x \\ q\equiv 1 \pmod{p^j}}} \sum_{\substack{n\le x \\ q\mid n}} 1 \\ &\le \sum_{p^j\le Y}\log p \sum_{\substack{q\le x \\ q\equiv 1 \pmod{p^j}}} \frac{x}{q}. \end{aligned}$$

Since $Y < \log x$ when x is large enough, Lemma 2.12 yields

$$\begin{aligned}\sum_{n\le x}\sum_{p^j\le Y}\omega_{p^j}(n)\log p &\le x\sum_{p^j\le Y}\log p\bigg(\frac{\log\log x}{\phi(p^j)}+O\bigg(\frac{\log(p^j)}{\phi(p^j)}\bigg)\bigg)\\ &\ll x\log\log x\sum_{p^j\le Y}\frac{\log p}{\phi(p^j)}+x\sum_{p^j\le Y}\frac{\log^2(p^j)}{\phi(p^j)}\\ &\ll x\log\log x\cdot\log Y+x\log^2 Y\end{aligned}$$

by partial summation, completing the verification of the bound (13). □

The following lemma is very similar to known results (see [6] for example) on the scarcity of numbers n for which $\phi(n)$ is divisible by the square of a large prime.

Lemma 2.14. *All but $O(x/W)$ integers $n \le x$ have both $\lambda_p(n) \le 1$ for all $p > Y$ and $\omega_{p^j}(n) \le 1$ for all $p^j > Y$.*

Proof. First, fix a prime $p > Y$. If $\lambda_p(n) \ge 2$, then either $p^3 \mid n$ or there exists a prime $q \mid n$ with $q \equiv 1 \pmod{p^2}$; the number of integers $n \le x$ satisfying one of these two conditions is at most

$$\frac{x}{p^3}+\sum_{\substack{q\le x\\ q\equiv 1 \ (\mathrm{mod}\ p^2)}}\frac{x}{q}.$$

Therefore the total number of integers $n \le x$ for which $\lambda_p(n) \ge 2$ for even a single prime $p > Y$ is, by Lemma 2.12, at most

$$\begin{aligned}\sum_{Y<p\le x^{1/3}}\frac{x}{p^3}+\sum_{Y<p\le\sqrt{x}}\ \sum_{\substack{q\le x\\ q\equiv 1 \ (\mathrm{mod}\ p^2)}}\frac{x}{q}\\ <\sum_{p>Y}\frac{x}{p^3}+x\sum_{p>Y}\bigg(\frac{\log\log x}{\phi(p^2)}+O\bigg(\frac{\log p^2}{\phi(p^2)}\bigg)\bigg)\\ \ll\frac{x}{Y^2\log Y}+x\bigg(\frac{\log\log x}{Y\log Y}+\frac{1}{Y}\bigg)\end{aligned}$$

by partial summation; this is an acceptably small bound for the number of such $n \le x$, given our choices of Y and W.

Similarly, fix a prime power $p^j > Y$. If $\omega_{p^j}(n) \ge 2$, then there exist two distinct primes q and r dividing n such that $q \equiv r \equiv 1 \pmod{p^j}$. The number of integers $n \le x$ satisfying this condition is, by Lemma 2.12, at most

$$\begin{aligned}\sum_{\substack{q<r\le x\\ q\equiv r\equiv 1 \ (\mathrm{mod}\ p^j)}}\frac{x}{qr} &< \frac{x}{2}\bigg(\sum_{\substack{q\le x\\ q\equiv 1 \ (\mathrm{mod}\ p^j)}}\frac{1}{q}\bigg)^2\\ &\ll x\bigg(\frac{\log\log x}{\phi(p^j)}+\frac{\log p^j}{\phi(p^j)}\bigg)^2\ll x\bigg(\frac{(\log\log x)^2}{(p^j)^2}+\frac{(\log p^j)^2}{(p^j)^2}\bigg).\end{aligned}$$

Therefore the total number of integers $n \le x$ for which $\omega_{p^j}(n) \ge 2$ for even a single prime power $p^j > Y$ is

$$\ll \sum_{p^j > Y} x\left(\frac{(\log\log x)^2}{(p^j)^2} + \frac{(\log p^j)^2}{(p^j)^2}\right) \ll x\left(\frac{(\log\log x)^2}{Y\log Y} + \frac{\log Y}{Y}\right) \ll \frac{x}{W}$$

again by partial summation. $\square$

We now have collected enough results to obtain a not-quite-final version of Proposition 1.2 where, for the moment, the range of summation ($p^j \le Y$ rather than $p^j \le X$) is longer than we would like.

Lemma 2.15. *For all but $O(x/W)$ integers $n \le x$,*

$$\log G(n) = \omega(\phi(n))\log 2 + \tfrac{1}{4}\sum_{p^j \le Y} \omega_{p^j}(n)^2 \log p + O(\log\log x \cdot (\log\log\log x)^2).$$

Proof. By Proposition 2.11,

$$\begin{aligned}
\log G(n) &= \sum_{p \mid \phi(n)} \log G_p(n) \\
&= \sum_{\substack{p \mid \phi(n) \\ \lambda_p(n)\omega_p(n)=1}} \log 2 + \sum_{\substack{p \mid \phi(n) \\ \lambda_p(n)\omega_p(n)\ge 2}} \left(O(\lambda_p(n)\log p) + \frac{\log p}{4}\sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n)^2\right) \\
&= \sum_{\substack{p \mid \phi(n) \\ \lambda_p(n)\omega_p(n)=1}} \log 2 + O\Bigg(\sum_{\substack{p \mid \phi(n) \\ \lambda_p(n)\omega_p(n)\ge 2}} \lambda_p(n)\log p\Bigg) + \sum_{\substack{p \mid \phi(n) \\ \lambda_p(n)\omega_p(n)\ge 2 \\ j \le \lambda_p(n)}} \tfrac{1}{4}\overline{\omega}_{p^j}(n)^2\Lambda(p^j) \\
&= \sum_{p \mid \phi(n)} \log 2 + O\Bigg(\sum_{\substack{p \mid \phi(n) \\ \lambda_p(n)\omega_p(n)\ge 2}} (\log 2 + \lambda_p(n)\log p)\Bigg) + \sum_{\substack{p \mid \phi(n) \\ \lambda_p(n)\omega_p(n)\ge 2 \\ j \le \lambda_p(n)}} \tfrac{1}{4}\overline{\omega}_{p^j}(n)^2\Lambda(p^j).
\end{aligned}$$

Since $\lambda_p(n) \ge 1$ for all $p \mid \phi(n)$,

$$\sum_{\substack{p \mid \phi(n) \\ \lambda_p(n)\omega_p(n)\ge 2}} (\log 2 + \lambda_p(n)\log p) \ll \sum_{\substack{p \mid \phi(n) \\ \lambda_p(n)\omega_p(n)\ge 2}} \lambda_p(n)\log p.$$

Furthermore, by Lemma 2.14, for all but $O(x/W)$ integers $n \le x$ we never have $\lambda_p(n) \ge 2$ for any $p > Y$; for these non-exceptional integers, we can therefore incorporate the condition $p \le Y$ into the relevant sums, yielding

$$\log G(n) = \sum_{p \mid \phi(n)} \log 2 + O\Bigg(\sum_{p \le Y} \lambda_p(n)\log p\Bigg) + \sum_{\substack{p \le Y \\ p \mid \phi(n) \\ \lambda_p(n)\omega_p(n)\ge 2 \\ j \le \lambda_p(n)}} \tfrac{1}{4}\overline{\omega}_{p^j}(n)^2\Lambda(p^j).$$

In this last sum, for all but $O(x/W)$ integers $n \le x$, Lemma 2.14 also implies that $\omega_{p^j}(n) \le 1$ (and thus $\overline{\omega}_{p^j}(n) \ll 1$) for all $p^j > Y$, which implies

$$\sum_{\substack{p\le Y\\ p\mid\phi(n)\\ \lambda_p(n)\omega_p(n)\ge 2\\ j\le\lambda_p(n)\\ p^j>Y}} \overline{\omega}_{p^j}(n)^2\Lambda(p^j) \ll \sum_{\substack{p\le Y\\ p\mid\phi(n)\\ \lambda_p(n)\omega_p(n)\ge 2\\ j\le\lambda_p(n)\\ p^j>Y}} 1\cdot\Lambda(p^j) \le \sum_{\substack{p\le Y\\ j\le\lambda_p(n)}} 1\cdot\Lambda(p^j) = \sum_{p\le Y}\lambda_p(n)\log p;$$

therefore for these non-exceptional integers, we can strengthen the condition $p \le Y$ to $p^j \le Y$ in the last sum to obtain

$$\begin{aligned}\log G(n) &= \sum_{p\mid\phi(n)} \log 2 + O\biggl(\sum_{p\le Y}\lambda_p(n)\log p\biggr) + \sum_{\substack{p\mid\phi(n)\\ \lambda_p(n)\omega_p(n)\ge 2\\ j\le\lambda_p(n)\\ p^j\le Y}} \tfrac14\overline{\omega}_{p^j}(n)^2\Lambda(p^j)\\ &= \omega(\phi(n))\log 2 + \sum_{\substack{p\mid\phi(n)\\ \lambda_p(n)\omega_p(n)\ge 2\\ j\le\lambda_p(n)\\ p^j\le Y}} \tfrac14\overline{\omega}_{p^j}(n)^2\Lambda(p^j) + O\bigl((\log\log x)^2\log\log\log x\bigr), \qquad (14)\end{aligned}$$

where the second equality is valid for all but $O(x/W)$ integers $n \le x$ by Lemma 2.13. From the definition of $\overline{\omega}_{p^j}$, we know that $\overline{\omega}_{p^j}(n) = \omega_{p^j}(n) + O(1)$, and consequently $\overline{\omega}_{p^j}(n)^2 = \omega_{p^j}(n)^2 + O\bigl(\omega_{p^j}(n)+1\bigr)$. In particular,

$$\begin{aligned}\sum_{\substack{p\mid\phi(n)\\ \lambda_p(n)\omega_p(n)\ge 2\\ j\le\lambda_p(n)\\ p^j\le Y}} \tfrac14\overline{\omega}_{p^j}(n)^2\log p &= \sum_{\substack{p\mid\phi(n)\\ \lambda_p(n)\omega_p(n)\ge 2\\ j\le\lambda_p(n)\\ p^j\le Y}} \bigl(\tfrac14\omega_{p^j}(n)^2 + O(\omega_{p^j}(n)+1)\bigr)\log p\\ &= \sum_{\substack{p\mid\phi(n)\\ \lambda_p(n)\omega_p(n)\ge 2\\ j\le\lambda_p(n)\\ p^j\le Y}} \tfrac14\omega_{p^j}(n)^2\log p + O\biggl(\sum_{p^j\le Y}\omega_{p^j}(n)\log p + \sum_{p\le Y}\lambda_p(n)\log p\biggr),\end{aligned}$$

and by Lemma 2.13 this error term is also $\ll \log\log x\cdot(\log\log\log x)^2$ for all but $O(x/W)$ integers $n \le x$. Therefore we may modify equation (14) to

$$\log G(n) = \omega(\phi(n))\log 2 + \sum_{\substack{p\mid\phi(n)\\ \lambda_p(n)\omega_p(n)\ge 2\\ j\le\lambda_p(n)\\ p^j\le Y}} \tfrac14\omega_{p^j}(n)^2\log p + O(\log\log x\cdot(\log\log\log x)^2).$$

In this sum, we may remove the condition of summation $\lambda_p(n)\omega_p(n) \ge 2$ at a cost of at most $\sum_{p\le Y}\frac14\lambda_p(n)\log p$, which again is negligible for all but $O(x/W)$ integers $n \le x$ by Lemma 2.13. Since $\omega_{p^j}(n) = 0$ whenever $p \nmid \phi(n)$ or $j > \lambda_p(n)$, we may remove the conditions $p \mid \phi(n)$ and $j \le \lambda_p(n)$ as well. This establishes the lemma. $\square$

Finally, we show that we can truncate the range of summation in the above lemma from $p^j \le Y$ down to $p^j \le X$ at the cost of a larger error term, thereby obtaining Proposition 1.2.

Proof of Proposition 1.2. In the notation of Proposition 1.2 and of this section, Lemma 2.15 states that for all but x/W integers $n \le x$,

$$\log G(n) = P_n(x) + \tfrac{1}{4} \sum_{X<q\le Y} \omega_q(n)^2 \Lambda(q) + O(\log\log x \cdot (\log\log\log x)^2).$$

Therefore it suffices to show that for all but x/W integers $n \le x$, the sum in the equation above is $\ll (\log\log x)^{3/2}/\log\log\log x$. In turn, this statement can be established by showing that

$$\sum_{n\le x} \sum_{X<q\le Y} \omega_q(n)^2 \Lambda(q) \ll \frac{x(\log\log x)^{3/2}}{(\log\log\log x)^2}. \tag{15}$$

We may write

$$\begin{aligned}
\sum_{n\le x} \sum_{X<q\le Y} \omega_q(n)^2 \Lambda(q) &= \sum_{n\le x} \sum_{X<q\le Y} \Lambda(q) \Bigg(\sum_{\substack{p\mid n \\ p\equiv 1 \ (\mathrm{mod}\ q)}} 1 \Bigg)^2 \\
&= \sum_{n\le x} \sum_{X<q\le Y} \Lambda(q) \sum_{\substack{p_1,p_2\mid n \\ p_1\equiv p_2\equiv 1 \ (\mathrm{mod}\ q)}} 1 \\
&= \sum_{X<q\le Y} \Lambda(q) \sum_{p_1\equiv p_2\equiv 1 \ (\mathrm{mod}\ q)} \sum_{\substack{n\le x \\ p_1,p_2\mid n}} 1 \\
&= \sum_{X<q\le Y} \Lambda(q) \sum_{p\equiv 1 \ (\mathrm{mod}\ q)} \sum_{\substack{n\le x \\ p\mid n}} 1 + \sum_{X<q\le Y} \Lambda(q) \sum_{\substack{p_1\equiv p_2\equiv 1 \ (\mathrm{mod}\ q) \\ p_1\ne p_2}} \sum_{\substack{n\le x \\ p_1p_2\mid n}} 1.
\end{aligned}$$

For the first sum, Lemma 2.12 gives

$$\begin{aligned}
\sum_{n\le x} \sum_{X<q\le Y} \Lambda(q) \sum_{\substack{p\mid n \\ p\equiv 1 \ (\mathrm{mod}\ q)}} 1 = \sum_{X<q\le Y} \Lambda(q) \sum_{\substack{p\le x \\ p\equiv 1 \ (\mathrm{mod}\ q)}} \sum_{\substack{n\le x \\ p\mid n}} 1
&\ll x \sum_{X<q\le Y} \Lambda(q) \sum_{\substack{p\le x \\ p\equiv 1 \ (\mathrm{mod}\ q)}} \frac{1}{p} \\
&\ll x\log\log x \sum_{X<q\le Y} \frac{\Lambda(q)}{\phi(q)} \ll x\log\log x \cdot \log Y
\end{aligned}$$

by partial summation. For the second sum, we argue similarly:

$$\begin{aligned}
\sum_{n\le x} \sum_{X<q\le Y} \Lambda(q) \sum_{\substack{p_1,p_2\le x \\ p_1p_2\mid n \\ p_1\equiv p_2\equiv 1 \ (\mathrm{mod}\ q)}} 1 &\ll \sum_{X<q\le Y} \Lambda(q) \sum_{\substack{p_1,p_2 \\ p_1\equiv p_2\equiv 1 \ (\mathrm{mod}\ q)}} \frac{x}{p_1p_2} \\
&\ll x(\log\log x)^2 \sum_{q>X} \frac{\Lambda(q)}{q^2} \ll x(\log\log x)^2/X = \frac{x(\log\log x)^{3/2}}{(\log\log\log x)^2}.
\end{aligned}$$

These last two upper bounds establish the estimate (15) and therefore the proposition. $\square$

3. Notation and setup

In this section, we prepare some notation we will need to prove Proposition 1.3. At the end of the section, we outline the main stages of the proof, which span the next several sections.

Definition 3.1. Define the function

$$\omega_0(n) = \omega(\phi(n)).$$

Comparing with Definition 2.7 shows that this notation ω_0 is mathematically dubious, but it will be typographically convenient. For example, we note that $\omega_q(p) \ll \log z$ for every $q \geq 0$ and every prime $p \leq z$: when $q \geq 2$ this is obvious from Definition 2.7, while for $q = 0$ we have $\omega_0(p) = \omega(p-1) \leq \log(p-1)/\log 2$.

In this notation, the definitions (2) and (5) become

$$\begin{aligned} P_n(x) &= \log 2 \cdot \omega_0(n) + \frac{1}{4} \sum_{2 \leq q \leq X} \omega_q(n)^2 \Lambda(q) \\ D(x) &= \log 2 \cdot \mu(\omega_0) + \frac{1}{4} \sum_{2 \leq q \leq X} \mu(\omega_q)^2 \Lambda(q), \end{aligned} \tag{16}$$

where (by equation (4)) we may simply write

$$\mu(\omega_q) = \sum_{p \leq x} \frac{\omega_q(p)}{p}$$

for every $q \geq 0$. We shall continue to write ranges of summation over q as either $2 \leq q$, when the sum excludes $q = 0$, or $0 \leq q$, when the sum includes $q = 0$.

By way of intuition, the typical size of $\omega_0(n)$ is $\frac{1}{2}(\log\log x)^2$; this is quite a bit larger than the typical size of any $\omega_q(n)$ with $q \geq 2$ but, on the other hand, these ω_q typically occur squared, while the function ω_0 typically occurs to the first power. Consequently, the contribution of the two types of function to the typical size of $P_n(x)$ is of the same order of magnitude. The typical size of $P_n(x)$, as n varies over integers up to x, is asymptotically $D(x)$ (due essentially to "linearity of expectation"), and consequently the distribution of the difference $P_n(x) - D(x)$ will be the main focus of our investigation.

Definition 3.2. For any prime p, define the function

$$f_p(a) = \begin{cases} 1 - 1/p, & \text{if } p \mid a, \\ -1/p, & \text{if } p \nmid a. \end{cases}$$

We extend this function completely multiplicatively in the subscript (not, as might be expected, in the argument): for any positive integer r, we set

$$f_r(a) = \prod_{p^\alpha \| r} f_p(a)^\alpha.$$

Finally, we set

$$F_{\omega_q}(a) = \sum_{p \leq x} \omega_q(p) f_p(a).$$

Notice that, for any $n \le x$, we have the exact identity

$$\omega_q(n) = \mu(\omega_q) + F_{\omega_q}(n). \tag{17}$$

We have thereby decomposed an additive function into its mean value on the integers up to x (which is asymptotically equal to $\mu(\omega_q)$) and a term $F_{\omega_q}(n)$ that oscillates as n varies. This innovation, due to Granville and Soundararajan [8], allows for a more direct identification of the main terms that arise in the calculations of the hth moments

$$M_h(x) = \sum_{n\le x} (P_n(x) - D(x))^h$$

of the difference between $P_n(x)$ and its mean value. We approach these moments by first rewriting $P_n(x)$ using equation (17):

$$\begin{aligned} P_n(x) &= \log 2 \cdot \omega_0(n) + \frac{1}{4} \sum_{2\le q\le X} \omega_q(n)^2 \Lambda(q) \\ &= \log 2 \cdot (\mu(\omega_0) + F_{\omega_0}(n)) + \frac{1}{4} \sum_{2\le q\le X} (\mu(\omega_q) + F_{\omega_q}(n))^2 \Lambda(q). \end{aligned}$$

Upon expanding the square inside the sum and then subtracting $D(x)$, we obtain

$$P_n(x) - D(x) = \log 2 \cdot F_{\omega_0}(n) + \frac{1}{2} \sum_{2\le q\le X} \mu(\omega_q) F_{\omega_q}(n) + \frac{1}{4} \sum_{2\le q\le X} F_{\omega_q}(n)^2. \tag{18}$$

We then estimate the hth moment by taking the entire right-hand side to the hth power, expanding into a sum of 3^h terms, and estimating each term separately. The terms with the fewest F-factors will comprise the main term for $M_h(x)$, while the others contribute only to the error term. The bookkeeping and notation involved with tracking all of these terms is quite messy, and we have organized the remainder of the paper as follows to minimize the trauma to the reader.

The aim of Section 4 is to introduce a general algebraic framework for handling the terms that arise upon expanding the hth power of the right-hand side of equation (18). Section 5 is devoted to proving asymptotic estimates and formulas for those individual terms as x tends to infinity. In Section 6, we complete the proof of Proposition 1.3 using the results of previous sections. Finally, in Section 7, we quickly justify our use of probabilistic language in the statement of Theorem 1.1 by deducing Theorem 1.1 from Theorem 1.3.

4. Polynomial accounting

The main goal of this section is to establish Proposition 4.7, which is used to identify and simplify the main term of the moments $M_h(x)$ (for h even) at the end of Section 6. The proof begins with some combinatorial arguments, concerning polynomials in many variables, which are elementary but extremely notation-intensive. Along the way, we also introduce some polynomial-related notation (Definition 4.5) for future use.

Definition 4.1. For any positive integer k, define Σ_k to be the set of all permutations of $\{1, \ldots, k\}$ (that is, the set of all bijections from $\{1, \ldots, k\}$ to itself). A typical element of Σ_k will be denoted by σ.

For any positive even integer k, define T_k to be the set of all 2-to-1 functions from $\{1,\dots,k\}$ to $\{1,\dots,k/2\}$. A typical element of T_k will be denoted by τ. We let τ_0 denote the order-preserving element of T_k defined by $\tau_0(j) = \lceil \frac{j}{2} \rceil$ for each $1 \le j \le k$.

For $\tau \in T_k$ and $j \in \{1,\dots,k/2\}$, define $\Upsilon_1(j)$ and $\Upsilon_2(j)$ to be the two distinct preimages of j in $\{1,\dots,k\}$; we will never need to distinguish between the two.

Lemma 4.2. *Let k be a positive even integer. The function $\psi\colon \Sigma_k \to T_k$ defined by $\psi(\sigma) = \tau_0 \circ \sigma^{-1}$ is surjective and $2^{k/2}$-to-1.*

Proof. Given any $\tau \in T_k$, the equality $\psi(\sigma) = \tau$ holds for a particular $\sigma \in \Sigma_k$ if and only if

$$\{\Upsilon_1(j), \Upsilon_2(j)\} = \{\sigma(2j-1), \sigma(2j)\} \text{ for every } 1 \le j \le \tfrac{k}{2}. \tag{19}$$

This specifies each of the $\frac{k}{2}$ unordered pairs $\{\sigma(2j-1), \sigma(2j)\}$, each of which provides a choice of two options for which element equals $\Upsilon_1(j)$ and which equals $\Upsilon_2(j)$; the total number of preimages σ is thus exactly $2^{k/2}$. □

The following definition and lemma provide one of our main tools for dealing with arbitrary powers of finite sums.

Definition 4.3. Let h and ℓ be positive integers with h even. Let R be a commutative ring of characteristic zero with a unit element, and define two commutative polynomial rings over R with $\ell+1$ and $(\ell+1)^2$ variables: let $x_0,\dots,x_\ell$ be indeterminates and define $S = R[x_0,\dots,x_\ell]$, and let $\{z_{ij} \colon 0 \le i,j \le \ell\}$ be indeterminates and define $\tilde{S} = R[z_{00},\dots,z_{\ell\ell}]$. Let S_h be the R-submodule of S spanned by monomials of total degree h, and let $\tilde{S}_{h/2}$ be the R-submodule of $\tilde{S}$ spanned by monomials of total degree $h/2$.

We define an R-module homomorphism $\Phi_h\colon S_h \to \tilde{S}_{h/2}$ in the following way. Given a monic monomial $M = x_{m_1}\cdots x_{m_h}$ in S_h (where $m_1,\dots,m_h \in \{0,\dots,\ell\}$ are not necessarily distinct), set

$$\Phi_h(M) = \frac{1}{h!}\sum_{\sigma\in\Sigma_h} z_{m_{\sigma 1}m_{\sigma 2}}\cdots z_{m_{\sigma(h-1)}m_{\sigma h}}.$$

(Note that the order of the indices $m_1,\dots,m_h$ is not uniquely defined by M, but this is not problematic since the sum defining $\Phi_h(M)$ averages over all permutations σ.) Then we extend Φ_h R-linearly to S_h, so that $\Phi_h(\sum_j r_j M_j) = \sum_j r_j \Phi_h(M_j)$ for any monic monomials $M_j \in S_h$ and elements $r_j \in R$.

For example, with $h = 4$ and $\ell = 2$,

$$\Phi_4(x_0^2x_1x_2 - 7x_1^3x_2) = \tfrac16 z_{12}z_{00} + \tfrac16 z_{21}z_{00} + \tfrac16 z_{10}z_{20} + \tfrac16 z_{10}z_{02} + \tfrac16 z_{20}z_{01} + \tfrac16 z_{01}z_{02} - \tfrac72 z_{11}z_{12} - \tfrac72 z_{11}z_{21}.$$

Lemma 4.4. *Let h and ℓ be positive integers with h even. Let R be a commutative ring of characteristic zero with a unit element, and let Φ_h be defined as in Definition 4.3. For any elements $r_0,\dots,r_\ell \in R$,*

$$\Phi_h\big((r_0x_0+\dots+r_\ell x_\ell)^h\big) = \bigg(\sum_{0\le i,j\le\ell} r_ir_jz_{ij}\bigg)^{h/2}.$$

Proof. The key to the calculation is to purposefully avoid expanding $(r_0x_0 + \cdots + r_\ell x_\ell)^h$ using multinomial coefficients; allowing repetition such as $(x_1+x_2)^2 = x_1^2 + x_1x_2 + x_2x_1 + x_2^2$ makes the counting argument much easier. By the definition of Φ_h,

$$\begin{aligned}\Phi_h\bigg(\Big(\sum_{i=0}^{\ell} r_i x_i\Big)^h\bigg) &= \Phi_h\bigg(\sum_{m_1=0}^{\ell}\cdots\sum_{m_h=0}^{\ell} r_{m_1}\cdots r_{m_h} x_{m_1}\cdots x_{m_h}\bigg)\\ &= \sum_{m_1=0}^{\ell}\cdots\sum_{m_h=0}^{\ell} r_{m_1}\cdots r_{m_h}\frac{1}{h!}\sum_{\sigma\in\Sigma_h} z_{m_{\sigma1}m_{\sigma2}}\cdots z_{m_{\sigma(h-1)}m_{\sigma h}}\\ &= \frac{1}{h!}\sum_{\sigma\in\Sigma_h}\sum_{m_1=0}^{\ell}\cdots\sum_{m_h=0}^{\ell} r_{m_1}\cdots r_{m_h} z_{m_{\sigma1}m_{\sigma2}}\cdots z_{m_{\sigma(h-1)}m_{\sigma h}}.\end{aligned}$$

Since $r_{m_1}\cdots r_{m_h} = r_{m_{\sigma1}}\cdots r_{m_{\sigma h}}$ for any $\sigma\in\Sigma_h$, we can rewrite this identity as

$$\Phi_h\bigg(\Big(\sum_{i=0}^{\ell} r_i x_i\Big)^h\bigg) = \frac{1}{h!}\sum_{\sigma\in\Sigma_h}\sum_{m_1=0}^{\ell}\cdots\sum_{m_h=0}^{\ell} r_{m_{\sigma1}}\cdots r_{m_{\sigma h}} z_{m_{\sigma1}m_{\sigma2}}\cdots z_{m_{\sigma(h-1)}m_{\sigma h}}.$$

Now the only effect of any fixed σ on the inner h-fold sum is to permute the order of the indices; therefore setting $j_1 = m_{\sigma_1}$, $j_2 = m_{\sigma_2}$, and so on, we may write

$$\Phi_h\bigg(\Big(\sum_{i=0}^{\ell} r_i x_i\Big)^h\bigg) = \frac{1}{h!}\sum_{\sigma\in\Sigma_h}\sum_{j_1=0}^{\ell}\cdots\sum_{j_h=0}^{\ell} r_{j_1}\cdots r_{j_h} z_{j_1j_2}\cdots z_{j_{h-1}j_h}.$$

The inner h-fold sum no longer depends on σ, and so

$$\Phi_h\bigg(\Big(\sum_{i=0}^{\ell} r_i x_i\Big)^h\bigg) = \sum_{j_1=0}^{\ell}\cdots\sum_{j_h=0}^{\ell} r_{j_1}\cdots r_{j_h} z_{j_1j_2}\cdots z_{j_{h-1}j_h} = \bigg(\sum_{j_1=0}^{\ell}\sum_{j_2=0}^{\ell} r_{j_1}r_{j_2}z_{j_1j_2}\bigg)^{h/2},$$

which is equivalent to the statement of the lemma. □

Remark. The map Φ_h can also be interpreted as a rather natural R-module homomorphism from $\mathrm{Sym}^{2h}(M)$ to $\mathrm{Sym}^h(M\otimes_R M)$, where $M = R^{\oplus(\ell+1)} \cong S_1$. However, this interpretation does not seem to shorten the verification of the desired identity.

We now wish to apply these results to a specific polynomial related to the moments of $\log G(n)$. Given a real number x, let $X = (\log\log x)^{1/2}(\log\log\log x)^2$ as before, and let $\rho(X)$ denote the number of prime powers up to X. Define the polynomial

$$Q(x_0, x_1, \ldots, x_{\rho(X)}) = \log 2\cdot x_0 + \frac{1}{4}\sum_{i=1}^{\rho(X)}\Lambda(q_i)x_i^2.$$

Note that the polynomial $P_n(x)$ defined in the introduction is equal to this polynomial Q evaluated at the tuple $(x_0, x_1, \ldots, x_{\rho(X)}) = (\omega_0(n), \omega_{q_1}(n), \ldots, \omega_{q_{\rho(X)}}(n))$. For consistency, we will abuse notation and set $q_0 = 0$; this will be convenient when applying the results of this section to $P_n(x)$ in Section 6.

Let Q_i denote the partial derivative of Q with respect to x_i. Observe that

$$\begin{aligned} Q(x_0+y_0,\dots,x_{\rho(X)}+y_{\rho(X)}) - Q(y_0,\dots,y_{\rho(X)}) &= \log 2\cdot x_0 + \frac{1}{2}\sum_{i=1}^{\rho(X)} \Lambda(q_i)x_iy_i + \sum_{i=1}^{\rho(X)} \Lambda(q_i)x_i^2 \\ &= \sum_{i=0}^{\rho(X)} x_iQ_i(y_0,\dots,y_{\rho(X)}) + \sum_{i=1}^{\rho(X)} \Lambda(q_i)x_i^2. \end{aligned} \tag{20}$$

Definition 4.5. Let h be a positive integer. Define

$$R_h(x_0,\dots,x_{\rho(X)},y_0,\dots,y_{\rho(X)}) = \big(Q(x_0+y_0,\dots,x_{\rho(X)}+y_{\rho(X)}) - Q(y_0,\dots,y_{\rho(X)})\big)^h.$$

To expand this out in gruesome detail, R_h can be written as the sum of some number B_h of monomials:

$$R_h(x_0,\dots,x_{\rho(X)},y_0,\dots,y_{\rho(X)}) = \sum_{\beta=1}^{B_h} r_{h\beta}\prod_{i=1}^{k_{h\beta}} x_{v(h,\beta,i)} \prod_{j=1}^{\tilde{k}_{h\beta}} y_{w(h,\beta,j)}, \tag{21}$$

where each $v(h,\beta,i)$ and $w(h,\beta,j)$ is an integer in $\{0,1,\dots,\rho(X)\}$; the total x-degree of the βth monomial in the sum is $k_{h\beta}$, while its total y-degree is $\tilde{k}_{h\beta}$. From equation (20), we see that each $k_{h\beta}$ is between h and $2h$ (inclusive), each $\tilde{k}_{h\beta}$ is at most h, and each $k_{h\beta}+\tilde{k}_{h\beta}$ is also between h and $2h$.

As it turns out, the most significant monomials on the right-hand side of equation (21) are those of minimal x-degree, that is, those monomials with $k_{h\beta}=h$. (These monomials will contribute to the main term of the calculation of the hth moment in Section 6 when h is even, while the other monomials contribute only to the error term.) Consequently we focus on these special monomials for the remainder of this section.

Lemma 4.6. *The part of R_h of total x-degree h is*

$$\sum_{\substack{\beta\le B_h \\ k_{h\beta}=h}} r_{h\beta}\prod_{i=1}^{h} x_{v(h,\beta,i)} \prod_{j=1}^{\tilde{k}_{h\beta}} y_{w(h,\beta,j)} = \bigg(\sum_{i=0}^{\rho(X)} x_iQ_i(y_0,\dots,y_{\rho(X)})\bigg)^h. \tag{22}$$

Proof. The left-hand side is exactly the definition of the part of R_h of total x-degree h, or equivalently (since $k_{h\beta}\ge h$ always) the part of R_h of total x-degree at most h. But R_h is the hth power of the polynomial $Q(x_0+y_0,\dots,x_{\rho(X)}+y_{\rho(X)}) - Q(y_1,\dots,y_{\rho(X)})$, whose part of total x-degree at most 1 equals $\sum_{i=0}^{\rho(X)} x_iQ_i(y_0,\dots,y_{\rho(X)})$ by equation (20). □

We are now ready to establish the proposition that will be used in Section 6 when analyzing the main term of the even moments. For any positive even integer h, define

$$s_h = \frac{h!}{2^{h/2}(h/2)!}. \tag{23}$$

Proposition 4.7. *Let h be a positive even integer. In the notation of Definitions 4.1 and 4.5,*

$$\frac{1}{(h/2)!}\sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{j=1}^{\tilde{k}_{h\beta}} y_{w(h,\beta,j)}\sum_{\tau\in T_h}\prod_{i=1}^{h/2} z_{v(h,\beta,\Upsilon_1(i))v(h,\beta,\Upsilon_2(i))}$$
$$= s_h\Bigg(\sum_{i=0}^{\rho(X)}\sum_{j=0}^{\rho(X)} Q_i(y_0,\ldots,y_{\rho(X)})Q_j(y_0,\ldots,y_{\rho(X)})z_{ij}\Bigg)^{h/2}. \quad (24)$$

Proof. Consider the operator Φ_h from Definition 4.3, using the ring $R=\mathbb{R}[y_0,\ldots,y_{\rho(X)}]$. We establish the lemma by showing that the left- and right-hand sides of equation (24) are the results of applying Φ_h to s_h times the left- and right-hand sides, respectively, of equation (22).

Checking the right-hand side is easy: since Φ_h is an R-module homomorphism,

$$\Phi_h\Bigg(s_h\Bigg(\sum_{j=0}^{\rho(X)} x_jQ_j(y_1,\ldots,y_{\rho(X)})\Bigg)^h\Bigg) = s_h\Phi_h\Bigg(\Bigg(\sum_{j=0}^{\rho(X)} Q_j(y_1,\ldots,y_{\rho(X)})x_j\Bigg)^h\Bigg)$$
$$= s_h\Bigg(\sum_{i=0}^{\rho(X)}\sum_{j=0}^{\rho(X)} Q_i(y_0,\ldots,x_{\rho(X)})Q_j(y_0,\ldots,y_{\rho(X)})z_{ij}\Bigg)^{h/2}$$

by Lemma 4.4 with $r_j=Q_j(y_1,\ldots,y_{\rho(X)})\in R$. As for the left-hand side: by R-linearity we have

$$\Phi_h\Bigg(s_h\sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{i=1}^{h} x_{v(h,\beta,i)}\prod_{j=1}^{\tilde{k}_{h\beta}} y_{w(h,\beta,j)}\Bigg)$$
$$= s_h\sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{j=1}^{\tilde{k}_{h\beta}} y_{w(h,\beta,j)}\Phi_h\Bigg(\prod_{i=1}^{h} x_{v(h,\beta,i)}\Bigg)$$
$$= s_h\sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{j=1}^{\tilde{k}_{h\beta}} y_{w(h,\beta,j)}\frac{1}{h!}\sum_{\sigma\in\Sigma_h} z_{v(h,\beta,\sigma1)v(h,\beta,\sigma2)}\cdots z_{v(h,\beta,\sigma(h-1))v(h,\beta,\sigma h)}.$$

But by Lemma 4.2, the set Σ_h can be partitioned into subsets of size $2^{h/2}$, each subset corresponding to a particular $\tau\in T_K$ and consisting of those σ for which equation (19) holds. Therefore

$$\Phi_h\Bigg(s_h\sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{i=1}^{h} x_{v(h,\beta,i)}\prod_{j=1}^{\tilde{k}_{h\beta}} y_{w(h,\beta,j)}\Bigg)$$
$$= s_h\sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{j=1}^{\tilde{k}_{h\beta}} y_{w(h,\beta,j)}\frac{2^{h/2}}{h!}\sum_{\tau\in T_h} z_{v(h,\beta,\Upsilon_1(1))v(h,\beta,\Upsilon_2(1))}\cdots z_{v(h,\beta,\Upsilon_1(h/2))v(h,\beta,\Upsilon_2(h/2))}.$$

The lemma now follows upon noting that $s_h 2^{h/2}/h! = 1/(\frac{h}{2})!$. $\square$

5. Covariances of two additive functions

The goal of this section is to evaluate certain expressions, arising from expanding the hth power of the right-hand side of equation (18), in terms of certain "covariances" which we now define.

Throughout this section, k is a fixed positive integer, $x > 1$ is a real number, and $z = x^{1/2k}$. For any two additive functions g_1 and g_2, define their *covariance* to be

$$\operatorname{cov}(g_1, g_2) = \operatorname{cov}(g_1, g_2; z) = \sum_{p \le z} \frac{g_1(p) g_2(p)}{p} \left(1 - \frac{1}{p}\right).$$

Whenever $g_1(p), g_2(p) \ll \log p$ (as will be the case in our application), this definition can be simplified to

$$\operatorname{cov}(g_1, g_2) = \sum_{p \le z} \frac{g_1(p) g_2(p)}{p} + O\biggl(\sum_{p \le z} \frac{\log^2 p}{p^2}\biggr) = \sum_{p \le z} \frac{g_1(p) g_2(p)}{p} + O(1). \tag{25}$$

We begin by finding asymptotic formulas for these covariances when each of g_1 and g_2 is equal to one of the ω_q $(q \ge 0)$.

The Bombieri–Vinogradov theorem will be an essential tool here and later in the paper; see for example [9, Theorem 17.1] for the statement for the function $\psi(x; q, a)$, from which it is simple to derive the analogous versions for the functions $\theta(x; q, a)$ and $\pi(x; q, a)$ (an example of such a derivation is the proof of [1, Corollary 1.4]).

Theorem 5.1. *For any positive real number A, there exists a positive real number $B = B(A)$ such that the estimates*

$$\sum_{2 \le q \le Q} \max_{(a,q)=1} \left| \theta(x; q, a) - \frac{x}{\phi(q)} \right| \ll_A \frac{x}{(\log x)^A} \tag{26}$$

$$\sum_{2 \le q \le Q} \max_{(a,q)=1} \left| \pi(x; q, a) - \frac{\operatorname{li}(x)}{\phi(q)} \right| \ll_A \frac{x}{(\log x)^A} \tag{27}$$

hold for all $x > 1$, where $Q = x^{1/2}(\log x)^{-B}$.

The following three lemmas provide the desired evaluations of the relevant covariances; we must attend separately to the cases where neither, one, or both of the two additive functions equals ω_0.

Lemma 5.2. *Let q_1 and q_2 be powers of primes (possibly of the same prime), and let $[q_1, q_2]$ denote the least common multiple of q_1 and q_2. Then*

$$\operatorname{cov}(\omega_{q_1}, \omega_{q_2}) = \frac{\log \log z}{\phi([q_1, q_2])} + O(1)$$

uniformly for $q_1, q_2 \le \sqrt{z}$.

Proof. Since each ω_{q_i} is uniformly bounded, and $\omega_{q_1}(p)\omega_{q_2}(p) = 1$ precisely when p is congruent to 1 modulo $[q_1, q_2]$, equation (25) becomes

$$\operatorname{cov}(\omega_{q_1}, \omega_{q_2}) = \sum_{\substack{p \le z \\ p \equiv 1 \pmod{[q_1,q_2]}}} \frac{1}{p} + O(1) = \frac{\log\log z}{\phi([q_1,q_2])} + O\left(\frac{\log[q_1,q_2]}{\phi([q_1,q_2])}\right) + O(1)$$

by Lemma 2.12; and the first error term can be absorbed into the $O(1)$. $\square$

Lemma 5.3. *If $q \le z^{1/4}$ is a prime power, then*

$$\operatorname{cov}(\omega_q, \omega_0) = \frac{(\log\log z)^2}{2\phi(q)} + O(\log\log z).$$

Proof. We emulate the proof of [6, Lemma 2.1]. In preparation for a partial summation calculation, we first show that

$$\sum_{p \le t} \omega_q(p)\omega_0(p) = \sum_{\substack{p \le t \\ p \equiv 1 \pmod q}} \omega(p-1) = \frac{t \log\log t}{\phi(q)\log t} + O\left(\frac{t}{\log t}\right) \tag{28}$$

for all $t > q$; the first equality follows from Definition 2.7 of ω_q and Definition 3.1 of ω_0. When $q > \log^2 t$ this estimate is simple: the trivial bounds $\pi(t; q, 1) < t/q$ and $\omega(p-1) \ll \log p$ result in

$$\sum_{\substack{p \le t \\ p \equiv 1 \pmod q}} \omega(p-1) \ll \pi(t; q, 1)\log t < \frac{t \log t}{q} \ll \frac{t}{\log t},$$

which is consistent with the right-hand side of equation (28) since $q > \log^2 t$ implies that $(\log\log t)/\phi(q) \ll (\log\log t \log\log\log t)/\log^2 t \ll 1$. Consequently, we may assume that $q \le \log^2 t$.

Letting ℓ denote a variable of summation taking only prime values, and noting that at most 2 primes greater than $p^{1/3}$ can divide $p-1$,

$$\begin{aligned}
\sum_{\substack{p \le t \\ p \equiv 1 \pmod q}} \omega(p-1) &= \sum_{\substack{p \le t \\ p \equiv 1 \pmod q}} \Bigg(\sum_{\substack{\ell \mid (p-1) \\ \ell \le t^{1/3}}} 1 + \sum_{\substack{\ell \mid (p-1) \\ \ell > t^{1/3}}} 1 \Bigg) \\
&= \sum_{\ell \le t^{1/3}} \sum_{\substack{p \le t \\ p \equiv 1 \pmod q \\ p \equiv 1 \pmod \ell}} 1 + O\Bigg(\sum_{\substack{p \le t \\ p \equiv 1 \pmod q}} 2 \Bigg) \\
&= \Bigg(\sum_{\substack{\ell \le t^{1/3} \\ \ell \nmid q}} \sum_{\substack{p \le t \\ p \equiv 1 \pmod{q\ell}}} 1 + O\Bigg(\sum_{\substack{\ell \le t^{1/3} \\ \ell \mid q}} \sum_{\substack{p \le t \\ p \equiv 1 \pmod q}} 1 \Bigg) \Bigg) + O(\pi(t; q, 1)) \\
&= \sum_{\substack{\ell \le t^{1/3} \\ \ell \nmid q}} \pi(t; q\ell, 1) + O\big(\omega(q)\pi(t; q, 1)\big) = \sum_{\substack{\ell \le t^{1/3} \\ \ell \nmid q}} \pi(t; q\ell, 1) + O\left(\frac{t}{\log t}\right),
\end{aligned} \tag{29}$$

where the last step follows from the Brun–Titchmarsh theorem (see [10, Theorem 3.9]) and the assumption $q \le \log^2 t$:

$$\omega(q)\pi(t;q,1) \ll \omega(q)\frac{t}{\phi(q)\log(t/q)} \ll \frac{\omega(q)}{\phi(q)}\frac{t}{\log t} \ll \frac{t}{\log t}. \tag{30}$$

By the Bombieri–Vinogradov estimate (27) with $A = 1$ (noting that every modulus $q\ell$ in the sum is at most $t^{1/3}\log^2 t \ll t^{1/2}(\log t)^{-B}$),

$$\begin{aligned}
\sum_{\substack{\ell \le t^{1/3} \\ \ell \nmid q}} \pi(t;q\ell,1) &= \sum_{\substack{\ell \le t^{1/3} \\ \ell \nmid q}} \frac{\mathrm{li}(t)}{\phi(q\ell)} + O\biggl(\sum_{\substack{\ell \le t^{1/3} \\ \ell \nmid q}} \biggl| \pi(t;q\ell,1) - \frac{\mathrm{li}(t)}{\phi(q\ell)} \biggr| \biggr) \\
&= \frac{\mathrm{li}(t)}{\phi(q)} \sum_{\substack{\ell \le t^{1/3} \\ \ell \nmid q}} \frac{1}{\ell - 1} + O\biggl(\frac{t}{\log t}\biggr) \qquad (31) \\
&= \frac{\mathrm{li}(t)}{\phi(q)}\bigl(\log\log t^{1/3} + O(\omega(q))\bigr) + O\biggl(\frac{t}{\log t}\biggr) = \frac{t\log\log t}{\phi(q)\log t} + O\biggl(\frac{t}{\log t}\biggr)
\end{aligned}$$

by partial summation. Together with the estimate (29), this evaluation establishes the claim (28).

Define $S(t) = \sum_{p \le t} \omega_q(p)\omega_0(p)$ to be the left-hand side of equation (28). Noting that $\omega_q(p) = 0$ for all $p \le q$, we use partial summation to estimate

$$\operatorname{cov}(\omega_q, \omega_0) = \sum_{q < p \le z} \omega_q(p)\omega_0(p)\frac{1}{p} = \int_q^z \frac{1}{t}\,dS(t) = \frac{S(z)}{z} + \int_q^z \frac{S(t)}{t^2}\,dt.$$

By equation (28), the first term satisfies

$$\frac{S(z)}{z} = \frac{\log\log z}{\phi(q)\log z} + O\biggl(\frac{1}{\log z}\biggr) \ll 1$$

while

$$\begin{aligned}
\int_q^z \frac{S(t)}{t^2}\,dt &= \int_q^z \biggl(\frac{\log\log t}{\phi(q)\,t\log t} + O\biggl(\frac{1}{t\log t}\biggr)\biggr)\,dt \\
&= \frac{(\log\log t)^2}{2\phi(q)}\bigg|_q^z + O\bigl(\log\log t\big|_q^z\bigr) = \frac{(\log\log z)^2}{2\phi(q)} + O(\log\log z).
\end{aligned}$$

as required. ∎

Lemma 5.4. *For $z > 2$,*

$$\operatorname{cov}(\omega_0, \omega_0) = \frac{(\log\log z)^3}{3} + O\bigl((\log\log z)^2\bigr).$$

Proof. Now we emulate the proof of [6, Lemma 2.2]. In preparation for a partial summation calculation, we first show that

$$\sum_{p \le t} \omega_0(p)^2 = \sum_{p \le t} \omega(p-1)^2 = \frac{t(\log\log t)^2}{\log t} + O\biggl(\frac{t|\log\log t|}{\log t}\biggr) \tag{32}$$

for all $t > 2$; again the first equality follows from Definition 3.1 of ω_0. Letting ℓ denote a variable of summation taking only prime values, and noting that at most 4 primes greater than $p^{1/5}$ can divide $p-1$,

$$\begin{aligned}
\sum_{p\le t}\omega(p-1)^2 &= \sum_{p\le t}\bigg(\sum_{\substack{\ell|(p-1)\\ \ell\le t^{1/5}}} 1 + O(4)\bigg)^2 \\
&= \sum_{p\le t}\sum_{\substack{\ell_1|(p-1)\\ \ell\le t^{1/5}}}\sum_{\substack{\ell_2|(p-1)\\ \ell\le t^{1/5}}} 1 + O\bigg(\sum_{p\le t}\sum_{\substack{\ell|(p-1)\\ \ell\le t^{1/5}}} 1 + \sum_{p\le t} 1\bigg) \\
&= \sum_{\ell_1\le t^{1/5}}\sum_{\ell_2\le t^{1/5}}\sum_{\substack{p\le t\\ p\equiv 1 \pmod{\ell_1}\\ p\equiv 1 \pmod{\ell_2}}} 1 + O\bigg(\sum_{p\le t}\omega(p-1)+\pi(t)\bigg) \\
&= \sum_{\ell_1\le t^{1/5}}\sum_{\substack{\ell_2\le t^{1/5}\\ \ell_2\ne\ell_1}}\pi(t;\ell_1\ell_2,1) + \sum_{\ell\le t^{1/5}}\pi(t;\ell,1) + O\bigg(\frac{t|\log\log t|}{\log t}\bigg),
\end{aligned}$$

where the error term in the last step was controlled using the $q=2$ case of equation (28). Using the Bombieri–Vinogradov estimate (27) in a manner similar to the argument in equation (31) now yields

$$\begin{aligned}
\sum_{p\le t}\omega(p-1)^2 &= \sum_{\ell_1\le t^{1/5}}\sum_{\substack{\ell_2\le t^{1/5}\\ \ell_2\ne\ell_1}}\frac{\mathrm{li}(t)}{(\ell_1-1)(\ell_2-1)} + \sum_{\ell\le t^{1/5}}\frac{\mathrm{li}(t)}{\ell-1} + O\bigg(\frac{t|\log\log t|}{\log t}\bigg) \\
&= \mathrm{li}(t)\bigg(\bigg(\sum_{\ell\le t^{1/5}}\frac{1}{\ell-1}\bigg)^2 + O\bigg(\sum_{\ell\le t^{1/5}}\frac{1}{\ell}\bigg)\bigg) + O\bigg(\frac{t|\log\log t|}{\log t}\bigg) \\
&= \mathrm{li}(t)\big((\log\log t^{1/5})^2 + O(\log\log t)\big) + O\bigg(\frac{t|\log\log t|}{\log t}\bigg),
\end{aligned}$$

which is enough to establish the claim (32).

Define $S(t) = \sum_{p\le t}\omega_0(p)^2$ to be the left-hand side of equation (32), and again use partial summation to estimate

$$\mathrm{cov}(\omega_0,\omega_0) = \sum_{q<p\le z}\omega_0(p)^2\frac{1}{p} = \int_2^z \frac{1}{t}\,dS(t) = \frac{S(z)}{z} + \int_2^z \frac{S(t)}{t^2}\,dt.$$

By equation (32), the first term satisfies

$$\frac{S(z)}{z} = \frac{(\log\log z)^2}{\log z} + O\bigg(\frac{|\log\log z|}{\log z}\bigg) \ll 1$$

while

$$\begin{aligned}
\int_2^z \frac{S(t)}{t^2}\,dt &= \int_2^z \bigg(\frac{(\log\log t)^2}{t\log t} + O\bigg(\frac{|\log\log t|}{t\log t}\bigg)\bigg)\,dt \\
&= \frac{(\log\log t)^3}{3}\bigg|_2^z + O\big((\log\log t)^2\big|_2^z\big) = \frac{(\log\log z)^3}{3} + O\big((\log\log z)^2\big)
\end{aligned}$$

as required. $\square$

When we expand the hth power in the calculation of the moments $M_h(x)$ (as in equation (36)), we will need to estimate products of the additive functions ω_q ($q \ge 0$) from Definitions 2.7 and 3.1, summed over many prime variables. Because of the presence of the multiplicative function H, defined momentarily, in these sums, it will be important how many distinct prime values are taken by these prime variables. The next three lemmas provide the details.

Definition 5.5. Define a multiplicative function $H(n)$ by setting, for each prime power p^γ,

$$H(p^\gamma) = \frac{1}{p}\bigg(1-\frac{1}{p}\bigg)^\gamma + \bigg(-\frac{1}{p}\bigg)^\gamma\bigg(1-\frac{1}{p}\bigg).$$

For any prime p, we note that $H(p^2) = \frac{1}{p}(1-\frac{1}{p})$ and $H(p) = 0$; in particular, $H(n) = 0$ unless n is squarefull. It is easy to check that $0 \le H(p^\gamma) \le H(p^2)$ for every prime p and every positive integer γ.

Lemma 5.6. *Let k be a positive even integer, and let $0 \le \ell \le k$ be an integer. Suppose that $g_1 = \cdots = g_\ell = \omega_0$, while the remaining functions g_j ($\ell < j \le k$) equal ω_{q_j} for some prime powers q_j. Then*

$$\sum_{\substack{p_1,\dots,p_k \le z \\ p_1\cdots p_k \text{ squarefull} \\ \#\{p_1,\dots,p_k\}=k/2}} H(p_1\cdots p_k) g_1(p_1)\cdots g_k(p_k)$$
$$= \frac{1}{(k/2)!}\sum_{\tau\in T_k}\prod_{j=1}^{k/2}\operatorname{cov}(g_{\Upsilon_1(j)}, g_{\Upsilon_2(j)}) + O_k\big((\log\log x)^{(2\ell+k)/2-1}\big). \quad (33)$$

Proof. All implicit constants in this proof may depend upon k. To each k-tuple $(p_1,\dots,p_k)$ counted by the sum on the left-hand side, we can uniquely associate a $(k/2)$-tuple $(q_1,\dots,q_{k/2})$ of primes satisfying $q_1 < \cdots < q_{k/2}$ such that each q_j equals exactly two of the p_i. This correspondence defines a unique $\tau \in T_k$, for which $\tau(i)$ equals the integer j such that $p_i = q_j$.

Therefore, by Definition 5.5,

$$\begin{aligned}
&\sum_{\substack{p_1,\dots,p_k\le z\\ p_1\cdots p_k \text{ squarefull}\\ \#\{p_1,\dots,p_k\}=k/2}} H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k)\\
&\qquad= \sum_{\tau\in T_k}\sum_{q_1<\dots<q_{k/2}\le z} H(q_1^2\cdots q_{k/2}^2)g_1(q_{\tau(1)})\cdots g_k(q_{\tau(k)})\\
&\qquad= \frac{1}{(k/2)!}\sum_{\tau\in T_k}\sum_{\substack{q_1,\dots,q_{k/2}\le z\\ q_1,\dots,q_{k/2}\text{ distinct}}} H(q_1^2\cdots q_{k/2}^2)g_1(q_{\tau(1)})\cdots g_k(q_{\tau(k)})\\
&\qquad= \frac{1}{(k/2)!}\sum_{\tau\in T_k}\sum_{\substack{q_1,\dots,q_{k/2}\le z\\ q_1,\dots,q_{k/2}\text{ distinct}}} g_1(q_{\tau(1)})\cdots g_k(q_{\tau(k)})\prod_{j=1}^{k/2}\frac{1}{q_j}\left(1-\frac{1}{q_j}\right)\\
&\qquad= \frac{1}{(k/2)!}\sum_{\tau\in T_k}\sum_{\substack{q_1,\dots,q_{k/2}\le z\\ q_1,\dots,q_{k/2}\text{ distinct}}} \prod_{j=1}^{k/2} g_{\Upsilon_1(j)}(q_j)g_{\Upsilon_2(j)}(q_j)\frac{1}{q_j}\left(1-\frac{1}{q_j}\right).
\end{aligned}$$

If we fix τ and $q_1,\dots,q_{k/2-1}$, the innermost sum over $q_{k/2}$ is

$$\begin{aligned}
&\sum_{\substack{q_{k/2}\le z\\ q_{k/2}\notin\{q_1,\dots,q_{k/2-1}\}}} g_{\Upsilon_1(k/2)}(q_{k/2})g_{\Upsilon_2(k/2)}(q_{k/2})\frac{1}{q_{k/2}}\left(1-\frac{1}{q_{k/2}}\right)\\
&\qquad= \operatorname{cov}(g_{\Upsilon_1(k/2)},g_{\Upsilon_2(k/2)}) - \sum_{j=1}^{k/2-1} g_{\Upsilon_1(k/2)}(q_j)g_{\Upsilon_2(k/2)}(q_j)\frac{1}{q_j}\left(1-\frac{1}{q_j}\right)\\
&\qquad= \operatorname{cov}(g_{\Upsilon_1(k/2)},g_{\Upsilon_2(k/2)}) + O(1),
\end{aligned}$$

since each $g_i(q)\ll \log z$ for $q\le z$. Summing in turn over $q_{k/2-1},\dots,q_1$ in the same way, we obtain

$$\begin{aligned}
&\sum_{\substack{p_1,\dots,p_k\le z\\ p_1\cdots p_k \text{ squarefull}\\ \#\{p_1,\dots,p_k\}=k/2}} H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k)\\
&\qquad= \frac{1}{(k/2)!}\sum_{\tau\in T_k}\prod_{j=1}^{k/2}\big(\operatorname{cov}(g_{\Upsilon_1(j)},g_{\Upsilon_2(j)})+O(1)\big).
\end{aligned}$$

Upon multiplying out the product corresponding to some $\tau\in T_k$, we obtain the leading term

$$\prod_{j=1}^{k/2}\operatorname{cov}(g_{\Upsilon_1(j)},g_{\Upsilon_2(j)})$$

together with terms that involve at most $k/2-1$ covariances. An examination of Lemmas 5.2–5.4 reveals that the order of magnitude of the leading term (as a function of z) is $(\log\log z)^{(2\ell+k)/2}$, regardless of how the g_j are paired with one another by τ, and that every non-leading term is $\ll (\log\log z)^{(2\ell+k)/2-1}$ uniformly in the possibilities for the g_j, We conclude that

$$\sum_{\substack{p_1,\dots,p_k\le z\\ p_1\cdots p_k \text{ squarefull}\\ \#\{p_1,\dots,p_k\}=k/2}} H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k)$$
$$= \frac{1}{(k/2)!}\sum_{\tau\in T_k}\prod_{j=1}^{k/2}\operatorname{cov}(g_{\Upsilon_1(j)},g_{\Upsilon_2(j)}) + O_k((\log\log x)^{(2\ell+k)/2-1})$$

as desired (where we have used $z=x^{1/2k}$ in the error term). □

Lemma 5.7. *Let k be a positive integer, and let $g_1,\dots,g_k$ be functions satisfying $g_1(p),\dots,g_k(p)\ll \log p$. Then for any $1\le i\le k$,*

$$\sum_{\substack{p_1,\dots,p_k\le z\\ \omega_0(p_i)>4k\log\log z}} H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k)\ll_k \frac{1}{(\log z)^{1/2}}.$$

Proof. All implicit constants in this proof may depend upon k. Suppose that $q_1,\cdots,q_s$ are the distinct primes such that $\{p_1,\dots,p_k\}=\{q_1,\cdots,q_s\}$, and let m denote any integer such that $q_m=p_i$. From Definition 5.5, we know that $0\le H(p_1\cdots p_k)\le H(q_1^2\cdots q_s^2)\le 1/q_1\cdots q_s$. Therefore, from the hypothesis on the sizes of the $g_j(p)$,

$$\sum_{\substack{p_1,\dots,p_k\le z\\ \omega_0(p_i)>4k\log\log z}} H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k)$$
$$\ll_k (\log z)^k\sum_{s=1}^{k}\sum_{m=1}^{s}\sum_{\substack{q_1,\dots,q_s\le z\\ \omega_0(q_m)>4k\log\log z}}\frac{1}{q_1\cdots q_s}$$
$$\ll_k (\log z)^k\sum_{s=1}^{k}\sum_{m=1}^{s}\Bigg(\sum_{\substack{q_m\le z\\ \omega_0(q_m)>4k\log\log z}}\frac{1}{q_m}\Bigg)\prod_{\substack{1\le i\le k\\ i\ne m}}\sum_{q_i\le z}\frac{1}{q_i}$$
$$\ll_k (\log z)^k\sum_{s=1}^{k}(\log\log z)^s\sum_{m=1}^{s}\sum_{\substack{q_m\le z\\ \omega_0(q_m)>4k\log\log z}}\frac{1}{q_m} \tag{34}$$

by Mertens's theorem. Note that

$$\sum_{\substack{q_m\le z\\ \omega_0(q_m)>4k\log\log z}}\frac{1}{q_m}=\sum_{\substack{q_m\le z\\ \omega(q_m-1)>4k\log\log z}}\frac{1}{q_m}\le\sum_{\substack{n\le z\\ \omega(n)>4k\log\log z}}\frac{1}{n}.$$

A result of Erdős and Nicolas [5] implies that the number of $n\le x$ satisfying $\omega(n)>4k\log\log x$ is $\ll x/(\log x)^{1+4k\log 4k-4k}$; partial summation then implies that the right-hand sum is $\ll 1/(\log x)^{4k\log 4k-4k}$. Equation (34) therefore implies

$$\sum_{\substack{p_1,\dots,p_k\le z\\ \omega_0(p_i)>4k\log\log z}} H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k)\ll_k (\log z)^k(\log\log z)^k\frac{1}{(\log z)^{4k\log 4k-4k}},$$

and the lemma follows from the fact that $4k\log 4k - 5k > \frac{1}{2}$ for $k \ge 1$. $\square$

Lemma 5.8. *Let k be a positive integer, and let $0 \le \ell \le k$ be an integer. Suppose that $g_1 = \cdots = g_\ell = \omega_0$, while the remaining functions g_j ($\ell < j \le k$) equal ω_{q_j} for some prime powers q_j. When k is even,*

$$\sum_{\substack{p_1,\dots,p_k \le z \\ p_1\cdots p_k \text{ squarefull} \\ \#\{p_1,\dots,p_k\} < k/2}} H(p_1\cdots p_k) g_1(p_1)\cdots g_k(p_k) \ll_k (\log\log x)^{(2\ell+k)/2-1},$$

while when k is odd,

$$\sum_{\substack{p_1,\dots,p_k \le z \\ p_1\cdots p_k \text{ squarefull} \\ \#\{p_1,\dots,p_k\} < k/2}} H(p_1\cdots p_k) g_1(p_1)\cdots g_k(p_k) \ll_k (\log\log x)^{(2\ell+k-1)/2}.$$

We remark that when k is odd, the condition of summation $\#\{p_1,\dots,p_k\} < k/2$ is always satisfied; we have nevertheless included the condition, for later convenience.

Proof. All implicit constants in this proof may depend upon k. We begin by noting that by Lemma 5.7, it suffices to consider the sum on the left-hand side with the extra summation condition $\max \omega_0(p_i) \le 4k\log\log z$ inserted.

To each k-tuple $(p_1,\dots,p_k)$ counted by the sum on the left-hand side, we associate the positive integer $s = \#\{p_1,\dots,p_k\}$, the primes $q_1 < \cdots < q_s$ such that $\{q_1,\dots,q_s\} = \{p_1,\dots,p_k\}$, and the integers $\gamma_1,\dots,\gamma_s \ge 2$ such that q_j equals exactly γ_j of the p_i; note that $\boldsymbol{\gamma} = (\gamma_1,\dots,\gamma_s)$ is a composition, not a partition, of k, since we are not assuming any monotonicity of the γ_j. Let $T_{\boldsymbol{\gamma}}$ denote the set of functions from $\{1,\dots,k\}$ to $\{1,\dots,s\}$ such that for each $1 \le j \le s$, exactly γ_j elements of $\{1,\dots,k\}$ are mapped to j. Given any $\tau \in T_{\boldsymbol{\gamma}}$, define $\Upsilon_1(j)$ and $\Upsilon_2(j)$ to be two distinct preimages of j in $\{1,\dots,k\}$; we will never need to know exactly which two preimages or to distinguish between the two. Finally, for any such τ, define ℓ' to be the number of functions among $g_{\Upsilon_1(1)}, g_{\Upsilon_2(1)}, \dots, g_{\Upsilon_1(s)}, g_{\Upsilon_2(s)}$ that equal ω_0, and set $M_\tau = (4k\log\log z)^{\ell-\ell'}$.

First, observe that

$$\sum_{\substack{p_1,\dots,p_k \le z \\ p_1\cdots p_k \text{ squarefull} \\ \#\{p_1,\dots,p_k\} < k/2 \\ \max\omega_0(p_i) \le 4k\log\log z}} H(p_1\cdots p_k) g_1(p_1)\cdots g_k(p_k)$$
$$= \sum_{1 \le s < k/2} \sum_{\substack{q_1 < \cdots < q_s \le z \\ \max\omega_0(q_i) \le 4k\log\log z}} \sum_{\substack{\gamma_1,\dots,\gamma_s \ge 2 \\ \gamma_1+\cdots+\gamma_s = k}} H(q_1^{\gamma_1}\cdots q_s^{\gamma_s}) \sum_{\tau \in T_{\boldsymbol{\gamma}}} g_1(q_{\tau(1)})\cdots g_k(q_{\tau(k)}).$$

By Definition 5.5, we may bound $H(q_1^{\gamma_1}\cdots q_s^{\gamma_s})$ by $H(q_1^2\cdots q_s^2)$. Moreover, in the innermost summand, we retain all of the factors of the form $g_{\Upsilon_1(j)}(q_j)$ and $g_{\Upsilon_2(j)}(q_j)$ while bounding all of the other $g_i(q_{\tau(i)})$ by their pointwise upper bounds, which results in a factor of M_τ:

$$\sum_{\substack{p_1,\dots,p_k\le z\\ p_1\cdots p_k \text{ squarefull}\\ \#\{p_1,\dots,p_k\}<k/2\\ \max\omega_0(p_i)\le 4k\log\log z}} H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k)$$

$$\le \sum_{1\le s<k/2}\sum_{q_1<\cdots<q_s\le z}\sum_{\substack{\gamma_1,\dots,\gamma_s\ge 2\\ \gamma_1+\cdots+\gamma_s=k}} H(q_1^2\cdots q_s^2)\sum_{\tau\in T_\gamma} M_\tau \prod_{j=1}^{s} g_{\Upsilon_1(j)}(q_j)g_{\Upsilon_2(j)}(q_j)$$

$$= \sum_{1\le s<k/2}\frac{1}{s!}\sum_{q_1,\dots,q_s\le z}\sum_{\substack{\gamma_1,\dots,\gamma_s\ge 2\\ \gamma_1+\cdots+\gamma_s=k}}\sum_{\tau\in T_\gamma} M_\tau \prod_{j=1}^{s} g_{\Upsilon_1(j)}(q_j)g_{\Upsilon_2(j)}(q_j)\frac{1}{q_j}\Big(1-\frac{1}{q_j}\Big).$$

Moving the sum over the q_j to the inside and summing, we obtain

$$\sum_{\substack{p_1,\dots,p_k\le z\\ p_1\cdots p_k \text{ squarefull}\\ \#\{p_1,\dots,p_k\}<k/2\\ \max\omega_0(p_i)\le 4k\log\log z}} H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k)$$

$$\le \sum_{1\le s<k/2}\frac{1}{s!}\sum_{\substack{\gamma_1,\dots,\gamma_s\ge 2\\ \gamma_1+\cdots+\gamma_s=k}}\sum_{\tau\in T_\gamma} M_\tau\prod_{j=1}^{s}\operatorname{cov}(g_{\Upsilon_1(j)},g_{\Upsilon_2(j)}).$$

An examination of Lemmas 5.2–5.4 reveals that each product on the right-hand side is $\ll (\log\log z)^{s+\ell'}$ regardless of how the g_j are paired with one another by τ; consequently,

$$M_\tau\prod_{j=1}^{s}\operatorname{cov}(g_{\Upsilon_1(j)},g_{\Upsilon_2(j)}) \ll_k (\log\log z)^{\ell-\ell'}(\log\log z)^{s+\ell'}$$

$$= (\log\log z)^{s+\ell} \le \begin{cases}(\log\log x)^{k/2-1+\ell}, & \text{if } k \text{ is even},\\ (\log\log x)^{(k-1)/2+\ell}, & \text{if } k \text{ is odd}.\end{cases}$$

The lemma follows upon summing over τ, the γ_i and s, which results in a constant that depends only on k. □

We are now ready to establish the main result of this section, which will be used repeatedly in Section 6. Recall that the functions f_p and F_g were defined in Definition 3.2.

Proposition 5.9. *Let k be a positive even integer, and let $0\le \ell\le k$ be an integer. Suppose that $g_1=\cdots=g_\ell=\omega_0$, while the remaining functions g_j ($\ell<j\le k$) equal ω_{q_j} for some prime powers q_j. When k is even,*

$$\sum_{n\le x}\prod_{j=1}^{k}F_{g_j}(n) = \frac{x}{(k/2)!}\sum_{\tau\in T_k}\prod_{j=1}^{k/2}\operatorname{cov}(g_{\Upsilon_1(j)},g_{\Upsilon_2(j)}) + O_k\big(x(\log\log x)^{(2\ell+k)/2-1}\big),$$

while when k is odd,

$$\sum_{n\le x}\prod_{j=1}^{k}F_{g_j}(n) \ll_k x(\log\log x)^{(2\ell+k-1)/2}.$$

Proof. All implicit constants in this proof may depend upon k. Expanding out the left-hand side using Definition 3.2 results in

$$\begin{aligned}\sum_{n\le x}\prod_{j=1}^{k}F_{g_j}(n) &= \sum_{n\le x}\prod_{j=1}^{k}\sum_{p\le z}g_j(p)f_p(n)\\ &= \sum_{p_1,\dots,p_k\le z}g_1(p_1)\cdots g_k(p_k)\sum_{n\le x}f_{p_1\cdots p_k}(n)\\ &= \sum_{p_1,\dots,p_k\le z}g_1(p_1)\cdots g_k(p_k)\big(H(p_1\cdots p_k)x+O\big(2^{\omega(p_1\cdots p_k)}\big)\big),\end{aligned}$$

where the last equality follows from [8, equation before equation (9)] with a slight change of notation. Each ω_q is bounded by 1, while $\omega_0(p)=\omega(p-1)$ is trivially bounded by $\log p/\log 2$; in particular, $2g_j(p_j)\ll \log z$ for all $p_j\le z$. Therefore

$$\sum_{p_1,\dots,p_k\le z}g_1(p_1)\cdots g_k(p_k)2^{\omega(p_1\cdots p_k)}\ll \sum_{p_1,\dots,p_k\le z}\prod_{j=1}^{k}\log z=(\pi(z)\log z)^k\ll z^k=\sqrt{x},$$

and so

$$\sum_{n\le x}\prod_{j=1}^{k}F_{g_j}(n)=x\sum_{p_1,\dots,p_k\le z}H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k)+O(\sqrt{x}).$$

Since $H(p_1\cdots p_k)$ vanishes unless $p_1\cdots p_k$ is squarefull by Definition 5.5, there are at most $k/2$ distinct primes among $p_1,\dots,p_k$, and so we can write

$$\begin{aligned}\sum_{p_1,\dots,p_k\le z}H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k) &= \sum_{\substack{p_1,\dots,p_k\le z\\ p_1\cdots p_k\text{ squarefull}\\ \#\{p_1,\dots,p_k\}=k/2}}H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k)\\ &\quad+\sum_{\substack{p_1,\dots,p_k\le z\\ p_1\cdots p_k\text{ squarefull}\\ \#\{p_1,\dots,p_k\}<k/2}}H(p_1\cdots p_k)g_1(p_1)\cdots g_k(p_k).\end{aligned}$$

The proposition now follows upon appealing to Lemmas 5.6 and 5.8. □

6. Calculating the moments

We are now ready to carry out, for $h\ge 1$, the computation of the moments $M_h(x)$. In particular, the proof of Proposition 1.3 requires some preparatory work, which we organize into Lemmas 6.1–6.3. We also find an asymptotic formula for the function $D(x)$ in Proposition 6.5; together with Lemmas 6.4 and 6.6, this calculation reveals the origins of the perhaps mysterious constants A, B, and C appearing in Theorem 1.1. Finally, we proof Proposition 1.3 at the end of this section.

Recall that $X=(\log\log x)^{1/2}(\log\log\log x)^2$, a notation that will persist throughout this section; we shall always assume that $X\ge 2$. As our starting point, we define

$$S_1=\sum_{2\le q\le X}\Lambda(q)F_{\omega_q}(n)^2\quad\text{and}\quad S_2=\sum_{2\le q\le X}2\Lambda(q)\mu(\omega_q)F_{\omega_q}(n)\tag{35}$$

and use equations (6) and (18) to write

$$
\begin{aligned}
M_h(x) = \sum_{n\le x} \big(P_n(x) - D(x)\big)^h &= \sum_{n\le x} \big(\log 2\cdot F_{\omega_0}(n) + S_1 + S_2\big)^h \\
&= \sum_{\substack{h_0,h_1,h_2\ge 0\\ h_0+h_1+h_2=h}} \binom{h}{h_0,h_1,h_2} \sum_{n\le x} \big(\log 2\cdot F_{\omega_0}(n)\big)^{h_0} S_1^{h_1} S_2^{h_2},
\end{aligned} \tag{36}
$$

where the $\binom{h}{h_0,h_1,h_2}$ are multinomial coefficients. Since $\mu(\omega_q)$ is large and positive while F_{ω_q} is an oscillatory function, and F_{ω_0} is significantly larger on average than any F_{ω_q} with $q\ge 2$, our intuition should be that the largest summands on the right-hand side correspond to $h_1=0$. Indeed, the following lemma gives an alternate expression for the sum of these large summands, in a notation that will allow us to apply our work from Section 4. Recall that, for convenience, we set $q_0=0$ (so that $\omega_{q_0}=\omega_0$).

Lemma 6.1. *Let h be a positive integer. In the notation of Definition 4.5 and equation* (35),

$$
\begin{aligned}
\sum_{\substack{h_0,h_1,h_2\ge 0\\ h_0+h_1+h_2=h\\ h_1=0}} \binom{h}{h_0,h_1,h_2} \big(\log 2\cdot F_{\omega_0}(n)\big)^{h_0} S_2^{h_2} &= \sum_{h_0=0}^{h} \binom{h}{h_0} \sum_{n\le x} \big(\log 2\cdot F_{\omega_0}(n)\big)^{h_0} S_2^{h-h_0} \\
&= \sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta} \prod_{j=1}^{\tilde k_{h\beta}} \mu(\omega_{q_{w(h,\beta,j)}}) \sum_{n\le x} \prod_{i=1}^{h} F_{\omega_{q_{v(h,\beta,i)}}}(n).
\end{aligned}
$$

Proof. The first equality is a simple change of variables, so we focus on the second equality. Since $\omega_q(n)=\mu(\omega_q)+F_{\omega_q}(n)$ by equation (17), the formulas (16) can be combined as

$$
\begin{aligned}
P_n(x)-D(x) &= \log 2\cdot\big(\omega_0(n)-\mu(\omega_q)\big) + \frac14 \sum_{2\le q\le X} \big(\omega_q(n)^2-\mu(\omega_q)^2\big)\Lambda(q) \\
&= \log 2\cdot F_{\omega_0}(n) + \frac14 \sum_{2\le q\le X} \big(2\mu(\omega_q)F_{\omega_q}(n)+F_{\omega_q}(n)^2\big)\Lambda(q) \\
&= \log 2\cdot F_{\omega_{q_0}}(n) + \frac12 \sum_{i=1}^{\rho(X)} \Lambda(q_i)F_{\omega_{q_i}}(n)\mu(\omega_{q_i}) + \sum_{i=1}^{\rho(X)} \Lambda(q_i)F_{\omega_{q_i}}(n)^2 \\
&= Q\big(F_{\omega_{q_0}}(n)+\mu(\omega_{q_0}),\dots,F_{\omega_{q_{\rho(X)}}}(n)+\mu(\omega_{q_{\rho(X)}})\big) - Q\big(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\big)
\end{aligned}
$$

by comparison to equation (20). Therefore, by equation (6) and Definition 4.5,

$$
\begin{aligned}
M_h(x) = \sum_{n\le x}\big(P_n(x)-D(x)\big)^h &= \sum_{n\le x} R_h(F_{\omega_0}(n),\dots,F_{\omega_{q_\ell}}(n),\mu(\omega_0),\dots,\mu(\omega_{q_\ell})) \\
&= \sum_{n\le x}\sum_{\beta=1}^{B_h} r_{h\beta} \prod_{i=1}^{k_{h\beta}} F_{\omega_{q_{v(h,\beta,i)}}}(n) \prod_{j=1}^{\tilde k_{h\beta}} \mu(\omega_{q_{w(h,\beta,j)}}) \\
&= \sum_{\beta=1}^{B_h} r_{h\beta} \prod_{j=1}^{\tilde k_{h\beta}} \mu(\omega_{q_{w(h,\beta,j)}}) \sum_{n\le x} \prod_{i=1}^{k_{h\beta}} F_{\omega_{q_{v(h,\beta,i)}}}(n).
\end{aligned} \tag{37}
$$

Note that each monomial on the right-hand side has $k_{h\beta}$ factors of the form F_{ω_q} for various $0 \le q \le X$.

On the other hand, if we insert the definitions (35) into the right-hand side of equation (36) and expand out the powers $S_1^{h_1} S_2^{h_2}$, each resulting monomial will have $h_0 + 2h_1 + h_2$ factors of the form F_{ω_q}. Therefore, for any integer $h \le m \le 2h$,

$$\sum_{\substack{h_0,h_1,h_2\ge 0\\ h_0+h_1+h_2=h\\ h_0+2h_1+h_2=m}} \binom{h}{h_0,h_1,h_2} \sum_{n\le x} \big(\log 2\cdot F_{\omega_0}(n)\big)^{h_0} S_1^{h_1} S_2^{h_2} = \sum_{\substack{\beta\le B_h\\ k_{h\beta}=m}} r_{h\beta} \prod_{j=1}^{\tilde{k}_{h\beta}} \mu(\omega_{q_{w(h,\beta,j)}}) \sum_{n\le x} \prod_{i=1}^{k_{h\beta}} F_{\omega_{q_{v(h,\beta,i)}}}(n).$$

In particular, $h_0 + 2h_1 + h_2 = m$ in these sums precisely when $h_1 = 0$, so the $m = h$ case of the above equation is equivalent to the statement of the lemma. □

The following preliminary lemma estimates a sum that appears more than once in the proof of Lemma 6.3 below. For the remainder of this section, all implicit constants may depend upon h, h_0, h_1, and h_2.

Lemma 6.2. *For any nonnegative integers h_1 and h_2,*

$$\sum_{2\le q_1,\dots,q_{h_1+h_2}\le X} \prod_{i=1}^{h_1+h_2} \Lambda(q_i) \prod_{i=h_1+1}^{h_1+h_2} \mu(\omega_{q_i}) \ll (\log\log x)^{(h_1+2h_2)/2} (\log\log\log x)^{2h_1+h_2}.$$

Proof. We sum on each q_i separately. For each $1 \le i \le h_1$, we simply have

$$\sum_{2\le q_i\le X} \Lambda(q_i) \ll X = (\log\log x)^{1/2} (\log\log\log x)^2$$

by the prime number theorem, giving a total contribution of $(\log\log x)^{h_1/2}(\log\log\log x)^{2h_1}$. On the other hand, when $h_1 + 1 \le i \le h_1 + h_2$, equation (45) gives

$$\mu(\omega_{q_i}) \ll \frac{\log\log x}{\phi(q_i)}$$

since $q \le X < \log x$. Therefore, for each $h_1 + 1 \le i \le h_1 + h_2$,

$$\sum_{2\le q_i\le X} \Lambda(q_i)\mu(\omega_{q_i}) \ll \log\log x \sum_{2\le q_i\le X} \frac{\Lambda(q_i)}{\phi(q_i)} \ll \log\log x \cdot \log\log\log x$$

by partial summation, giving a total contribution of $(\log\log x \cdot \log\log\log x)^{h_2}$. Collecting exponents yields the lemma. □

We now handle all the terms on the right-hand side of equation (36) when h is odd, and the lower-order terms in the case when h is even, with the following lemma. We do so by brute-force expansion of the hth power and using the results of Section 5.

Lemma 6.3. *Let h_0, h_1, and h_2 be nonnegative integers, and set $h = h_0 + h_1 + h_2$. Suppose that either h is odd, or h is even and $h_1 \ne 0$. Then with S_1 and S_2 defined as in equation* (35)*,*

$$\sum_{n\le x} (\log 2 \cdot F_{\omega_0}(n))^{h_0} S_1^{h_1} S_2^{h_2} \ll x(\log\log x)^{3h/2-1/4} (\log\log\log x)^{2h}$$

for $x \ge e^{e^3}$.

Proof. Since

$$S_1^{h_1} = \bigg(\sum_{2\le q\le X} \Lambda(q) F_{\omega_q}(n)^2 \bigg)^{h_1} = \sum_{2\le q_1,\dots,q_{h_1}\le X} \prod_{i=1}^{h_1} \Lambda(q_i) F_{\omega_{q_i}}(n)^2$$

and

$$S_2^{h_2} = \bigg(\sum_{2\le q\le X} 2\Lambda(q)\mu(\omega_q) F_{\omega_q}(n) \bigg)^{h_2} \ll \sum_{2\le q_1,\dots,q_{h_2}\le X} \prod_{i=1}^{h_2} \Lambda(q_i)\mu(\omega_{q_i}) F_{\omega_{q_i}}(n),$$

the sum under consideration satisfies

$$\begin{aligned}
&\sum_{n\le x} (\log 2\cdot F_{\omega_0}(n))^{h_0} S_1^{h_1} S_2^{h_2} \qquad (38)\\
&\quad \ll \sum_{n\le x} \sum_{2\le q_1,\dots,q_{h_1+h_2}\le X} F_{\omega_0}(n)^{h_0} \prod_{i=1}^{h_1+h_2} \Lambda(q_i) \prod_{i=h_1+1}^{h_1+h_2} \mu(\omega_{q_i}) \prod_{i=1}^{h_1} F_{\omega_{q_i}}(n)^2 \prod_{i=h_1+1}^{h_1+h_2} F_{\omega_{q_i}}(n)\\
&\quad = \sum_{2\le q_1,\dots,q_{h_1+h_2}\le X} \prod_{i=1}^{h_1+h_2} \Lambda(q_i) \prod_{i=h_1+1}^{h_1+h_2} \mu(\omega_{q_i}) \bigg(\sum_{n\le x} F_{\omega_0}(n)^{h_0} \prod_{i=1}^{h_1} F_{\omega_{q_i}}(n)^2 \prod_{i=h_1+1}^{h_1+h_2} F_{\omega_{q_i}}(n) \bigg).
\end{aligned}$$

We will consider two cases, depending on the parity of $h_0 + h_2$; when $h_0 + h_2$ is even, we additionally assume that $h_1 \ne 0$. A moment's thought verifies that these two cases do exhaust the possibilities for h_0, h_1, and h_2.

Case 1: $h_0 + h_2$ is odd. In the inner sum on the right-hand side of equation (38), each summand is the product of $h_0 + 2h_1 + h_2$ values of F-functions. By Proposition 5.9 with $\ell = h_0$ and $k = h_0 + 2h_1 + h_2$ (which is odd),

$$\sum_{n\le x} F_{\omega_0}(n)^{h_0} \prod_{i=1}^{h_1} F_{\omega_{q_i}}(n)^2 \prod_{i=h_1+1}^{h_1+h_2} F_{\omega_{q_i}}(n) \ll x(\log\log x)^{(3h_0+2h_1+h_2-1)/2}.$$

Inserting this upper bound into the right-hand side of equation (38) yields

$$\begin{aligned}
&\sum_{n\le x} \big(\log 2\cdot F_{\omega_0}(n)\big)^{h_0} S_1^{h_1} S_2^{h_2}\\
&\qquad \ll x(\log\log x)^{(3h_0+2h_1+h_2-1)/2} \sum_{2\le q_1,\dots,q_{h_1+h_2}\le X} \prod_{i=1}^{h_1+h_2} \Lambda(q_i) \prod_{i=h_1+1}^{h_1+h_2} \mu(\omega_{q_i})\\
&\qquad \ll x(\log\log x)^{(3h_0+2h_1+h_2-1)/2} \cdot (\log\log x)^{(h_1+2h_2)/2} (\log\log\log x)^{2h_1+h_2}\\
&\qquad \le x(\log\log x)^{(3h-1)/2} (\log\log\log x)^{2h}
\end{aligned}$$

by Lemma 6.2 (since $h = h_0 + h_1 + h_2$), which establishes the lemma in this case.

Case 2: $h_0 + h_2$ is even and $h_1 \ne 0$. In the inner sum on the right-hand side of equation (38), each summand is again the product of $h_0 + 2h_1 + h_2$ values of F-functions. By

Proposition 5.9 with $\ell = h_0$ and $k = h_0 + 2h_1 + h_2$ (which is now even),

$$\sum_{n\le x} F_{\omega_0}(n)^{h_0} \prod_{i=1}^{h_1} F_{\omega_{q_i}}(n)^2 \prod_{i=h_1+1}^{h_1+h_2} F_{\omega_{q_i}}(n) \\ \ll x \sum_{\tau\in T_k} \prod_{j=1}^{k/2} \operatorname{cov}(\omega_{q_{\Upsilon_1(j)}}, \omega_{q_{\Upsilon_2(j)}}) + x(\log\log x)^{(3h_0+2h_1+h_2)/2-1}.$$

Inserting this upper bound into the right-hand side of equation (38) yields

$$\begin{aligned} &\sum_{n\le x} \big(\log 2\cdot F_{\omega_0}(n)\big)^{h_0} S_1^{h_1} S_2^{h_2} \\ &\quad\ll x \sum_{2\le q_1,\dots,q_{h_1+h_2}\le X} \prod_{i=1}^{h_1+h_2} \Lambda(q_i) \prod_{i=h_1+1}^{h_1+h_2} \mu(\omega_{q_i}) \sum_{\tau\in T_k} \prod_{j=1}^{k/2} \operatorname{cov}(\omega_{q_{\Upsilon_1(j)}}, \omega_{q_{\Upsilon_2(j)}}) \\ &\qquad + x(\log\log x)^{(3h_0+2h_1+h_2)/2-1} \sum_{2\le q_1,\dots,q_{h_1+h_2}\le X} \prod_{i=1}^{h_1+h_2} \Lambda(q_i) \prod_{i=h_1+1}^{h_1+h_2} \mu(\omega_{q_i}) \\ &\quad\ll x \sum_{\tau\in T_k} \sum_{2\le q_1,\dots,q_{h_1+h_2}\le X} \prod_{i=1}^{h_1+h_2} \Lambda(q_i) \prod_{i=h_1+1}^{h_1+h_2} \mu(\omega_{q_i}) \prod_{j=1}^{k/2} \operatorname{cov}(\omega_{q_{\Upsilon_1(j)}}, \omega_{q_{\Upsilon_2(j)}}) \\ &\qquad + x(\log\log x)^{3h/2-1}(\log\log\log x)^{2h} \end{aligned} \tag{39}$$

by Lemma 6.2 and an examination of exponents similar to the end of the proof of Case 1.

Now, by Lemmas 5.2–5.4, for any $0 \le q, q' \le X$ we have

$$\operatorname{cov}(\omega_q, \omega_{q'}) \ll \begin{cases} (\log\log x)/\phi(q), & \text{if } q, q' \ge 2, \\ (\log\log x)^2/\phi(q), & \text{if } q \ge 2 \text{ and } q' = 0, \\ (\log\log x)^2/\phi(q'), & \text{if } q' \ge 2 \text{ and } q = 0, \\ (\log\log x)^3, & \text{if } q = q' = 0. \end{cases} \tag{40}$$

Notice that the first upper bound is, intentionally, crude in general: by Lemma 5.2, we could divide not just by $\phi(q)$ but by $\phi([q,q'])$. However, $\phi([q,q'])$ can be as small as $\phi(q)$ in the worst case (when q' divides q). Fortunately, our argument will succeed even with this worst-case assumption. (We have also bounded $\log\log z$ above by $\log\log x$, which is fairly insignificant.)

For a given $\tau \in T_k$ (which is a two-to-one function), define $\Delta(\tau)$ to be a subset of $\{1,\dots,h_1\}$ of size at least $h_1/2$ such that τ is one-to-one when restricted to $\Delta(\tau)$. When we use the upper bounds (40) in the innermost product on the right-hand side of equation (39), the resulting estimate will include a factor of $\prod_{i\in\Delta(\tau)} 1/\phi(q_i)$. Furthermore, the resulting exponent of $\log\log x$ is $k/2 + h_0 = (3h_0 + 2h_1 + h_2)/2$, regardless of how the g_j are paired with one another by τ. In other words, equation (39) becomes

$$\sum_{n\le x}\big(\log 2\cdot F_{\omega_0}(n)\big)^{h_0}S_1^{h_1}S_2^{h_2} \tag{41}$$
$$\ll x(\log\log x)^{(3h_0+2h_1+h_2)/2}\sum_{\tau\in T_k}\sum_{2\le q_1,\dots,q_{h_1+h_2}\le X}\prod_{i\in\Delta(\tau)}\frac{\Lambda(q_i)}{\phi(q_i)}\prod_{\substack{1\le i\le h_1+h_2\\ i\notin\Delta(\tau)}}\Lambda(q_i)\prod_{i=h_1+1}^{h_1+h_2}\mu(\omega_{q_i})$$
$$+\,x(\log\log x)^{3h/2-1}(\log\log\log x)^{2h}.$$

We now sum on each q_i separately (still fixing τ for the moment), in a similar manner to the proof of Lemma 6.2. For each $1\le i\le h_1$ such that $i\notin\Delta(\tau)$, the prime number theorem gives

$$\sum_{2\le q_i\le X}\Lambda(q_i)\ll X=(\log\log x)^{1/2}(\log\log\log x)^2$$

resulting in a total contribution of $(\log\log x)^{(h_1-\#\Delta(\tau))/2}(\log\log\log x)^{2(h_1-\#\Delta(\tau))}$. On the other hand, for each $1\le i\le h_1$ such that $i\in\Delta(\tau)$, partial summation gives

$$\sum_{2\le q_i\le X}\frac{\Lambda(q_i)}{\phi(q_i)}\ll\log X\ll\log\log\log x,$$

resulting in a total contribution of $(\log\log\log x)^{\#\Delta(\tau)}$. Lastly, when $h_1+1\le i\le h_1+h_2$, equation (45) gives

$$\sum_{2\le q_i\le X}\Lambda(q_i)\mu(\omega_{q_i})\ll\log\log x\sum_{2\le q_i\le X}\frac{\Lambda(q_i)}{\phi(q_i)}\ll\log\log x\cdot\log\log\log x$$

as above, resulting in a total contribution of $(\log\log x\cdot\log\log\log x)^{h_2}$. The product of all these contributions is

$$\begin{aligned}(\log\log x)^{(h_1-\#\Delta(\tau))/2+h_2}(\log\log\log x)^{2h_1+h_2-\#\Delta(\tau)}&\le(\log\log x)^{h_1/4+h_2}(\log\log\log x)^{2h}\\&\le(\log\log x)^{h_1/2+h_2-1/4}(\log\log\log x)^{2h},\end{aligned}$$

where we have used the assumption $h_1>0$ in the last inequality.

Finally we insert this estimate back into equation (41), which gives

$$\begin{aligned}\sum_{n\le x}\big(\log 2\cdot F_{\omega_0}(n)\big)^{h_0}S_1^{h_1}S_2^{h_2}&\\ \ll x(\log\log x)^{(3h_0+2h_1+h_2)/2}&\sum_{\tau\in T_k}(\log\log x)^{h_1/2+h_2-1/4}(\log\log\log x)^{2h}\\ &+x(\log\log x)^{3h/2-1}(\log\log\log x)^{2h}\\ \ll x(\log\log x)^{3h/2-1/4}&(\log\log\log x)^{2h}\end{aligned}$$

(the sum over τ can now be ignored, since the implicit constant may depend upon h), which completes the proof of the lemma. □

Two particular sums of arithmetic functions will arise in the evaluation of the main term for $M_h(x)$; we asymptotically evaluate those sums in the following lemma, after which we give an asymptotic formula for the "mean" $D(x)$ that appears in the definition of $M_h(x)$.

Lemma 6.4. *Recall from Theorem 1.1 that*

$$A_0 = \frac{1}{4}\sum_p \frac{p^2\log p}{(p-1)^3(p+1)} \quad \textit{and} \quad B = \frac{1}{4}\sum_p \frac{p^3(p^4-p^3-p^3-p-1)(\log p)^2}{(p-1)^6(p+1)^2(p^2+p+1)}.$$

When $X > 2$,

(a) $\displaystyle \frac{1}{4}\sum_{2\le q\le X}\frac{\Lambda(q)}{\phi(q)^2} = A_0 + O\left(\frac{1}{X}\right)$;

(b) $\displaystyle \frac{1}{4}\sum_{2\le q_1\le X}\sum_{2\le q_2\le X}\frac{\Lambda(q_1)\Lambda(q_2)}{\phi(q_1)\phi(q_2)\phi([q_1,q_2])} = 4A_0^2 + B + O\left(\frac{\log X}{X}\right)$.

Proof. (a) We need only observe that

$$\sum_{q\ge 2}\frac{\Lambda(q)}{\phi(q)^2} = \sum_p\sum_{j=1}^{\infty}\frac{\Lambda(p^j)}{\phi(p^j)^2} = \sum_p \frac{\log p}{(p-1)^2}\sum_{j=1}^{\infty}\frac{1}{(p^{j-1})^2} = \sum_p \frac{\log p}{(p-1)^2}\frac{p^2}{p^2-1} = 4A_0, \quad (42)$$

while partial summation bounds the tail of this convergent series by

$$\frac{1}{4}\sum_{q>X}\frac{\Lambda(q)}{\phi(q)^2} \ll \frac{1}{X}.$$

(b) If $q_1 = p_1^r$ and $q_2 = p_2^s$ with $p_1 \ne p_2$, then $[q_1,q_2] = p_1^r p_2^s$; on the other hand, if $q_1 = p^r$ and $q_2 = p^s$ are powers of the same prime, then $[q_1,q_2] = p^{\max(r,s)}$. Therefore,

$$\begin{aligned}
&\sum_{q_1\ge 2}\sum_{q_2\ge 2}\frac{\Lambda(q_1)\Lambda(q_2)}{\phi(q_1)\phi(q_2)\phi([q_1,q_2])}\\
&\quad = \sum_{p_1^r}\sum_{\substack{p_2^s\\ p_2\ne p_1}}\frac{(\log p_1)(\log p_2)}{p_1^{r-1}(p_1-1)p_2^{s-1}(p_2-1)p_1^{r-1}(p_1-1)p_2^{s-1}(p_2-1)}\\
&\qquad + \sum_p\sum_{r=1}^{\infty}\sum_{s=1}^{\infty}\frac{(\log p)^2}{p^{r-1}(p-1)p^{s-1}(p-1)p^{\max(r,s)-1}(p-1)}\\
&\quad = \Bigg(\sum_{p_1^r}\sum_{p_2^s}\frac{(\log p_1)(\log p_2)}{p_1^{r-1}(p_1-1)p_2^{s-1}(p_2-1)p_1^{r-1}(p_1-1)p_2^{s-1}(p_2-1)}\\
&\qquad - \sum_p\sum_{r=1}^{\infty}\sum_{s=1}^{\infty}\frac{(\log p)(\log p)}{p^{r-1}(p-1)p^{s-1}(p-1)p^{r-1}(p-1)p^{s-1}(p-1)}\Bigg)\\
&\qquad + \sum_p\sum_{r=1}^{\infty}\sum_{s=1}^{\infty}\frac{(\log p)^2}{p^{r-1}(p-1)p^{s-1}(p-1)p^{\max(r,s)-1}(p-1)}.
\end{aligned} \quad (43)$$

By equation (42), the double sum on the right-hand side is simply

$$\left(\sum_{p^j}\frac{\log p}{(p^{j-1})^2(p-1)^2}\right)^2 = (4A_0)^2.$$

On the other hand, using the power series identities

$$\sum_{r=1}^{\infty}\sum_{s=1}^{\infty} x^r x^s x^r x^s = \left(\frac{x^2}{1-x^2}\right)^2$$

and

$$\begin{aligned}\sum_{r=1}^{\infty}\sum_{s=1}^{\infty} x^r x^s x^{\max\{r,s\}} &= 2\sum_{r=1}^{\infty}\sum_{s=r}^{\infty} x^r x^s x^s - \sum_{r=1}^{\infty} x^r x^r x^r \\ &= 2\sum_{r=1}^{\infty}\frac{x^{3r}}{1-x^2} - \sum_{r=1}^{\infty} x^{3r} = \frac{1+x^2}{1-x^2}\frac{x^3}{1-x^3},\end{aligned}$$

we may evaluate the pair of triple sums on the right-hand side of equation (43) as

$$\sum_p \left(-\frac{p^4(\log p)^2}{(p-1)^4}\left(\frac{p^{-2}}{1-p^{-2}}\right)^2 + \frac{p^3(\log p)^2}{(p-1)^3}\frac{1+p^{-2}}{1-p^{-2}}\frac{p^{-3}}{1-p^{-3}}\right) = 4B.$$

Thus equation (43) simplifies to

$$\frac{1}{4}\sum_{q_1\ge 2}\sum_{q_2\ge 2}\frac{\Lambda(q_1)\Lambda(q_2)}{\phi(q_1)\phi(q_2)\phi([q_1,q_2])} = 4A_0^2 + B,$$

and it therefore suffices to show that the tail

$$\begin{aligned}\sum_{q_1\ge 2}\sum_{q_2\ge 2}\frac{\Lambda(q_1)\Lambda(q_2)}{\phi(q_1)\phi(q_2)\phi([q_1,q_2])} &- \sum_{2\le q_1\le X}\sum_{2\le q_2\le X}\frac{\Lambda(q_1)\Lambda(q_2)}{\phi(q_1)\phi(q_2)\phi([q_1,q_2])} \\ &= \sum_{q_1>X}\sum_{q_2>X}\frac{\Lambda(q_1)\Lambda(q_2)}{\phi(q_1)\phi(q_2)\phi([q_1,q_2])} + 2\sum_{2\le q_1\le X}\sum_{q_2>X}\frac{\Lambda(q_1)\Lambda(q_2)}{\phi(q_1)\phi(q_2)\phi([q_1,q_2])} \qquad (44)\end{aligned}$$

is $\ll (\log X)/X$.

Since $\phi([q_1,q_2]) \ge \phi(q_2)$, the second sum on the right-hand side can be bounded crudely:

$$2\sum_{2\le q_1\le X}\sum_{q_2>X}\frac{\Lambda(q_1)\Lambda(q_2)}{\phi(q_1)\phi(q_2)^2} = 2\left(\sum_{2\le q_1\le X}\frac{\Lambda(q_1)}{\phi(q_1)}\right)\left(\sum_{q_2>X}\frac{\Lambda(q_2)}{\phi(q_2)^2}\right) \ll \log X\cdot\frac{1}{X}.$$

by partial summation. Finally, we handle the first sum on the right-hand side of equation (44) by splitting it as

$$\begin{aligned}
\sum_{q_1>X}\sum_{q_2>X}&\frac{\Lambda(q_1)\Lambda(q_2)}{\phi(q_1)\phi(q_2)\phi([q_1,q_2])}\\
&=\sum_{p_1^r>X}\sum_{\substack{p_2^s>X\\ p_2\ne p_1}}\frac{(\log p_1)(\log p_2)}{\phi(p_1^r)\phi(p_2^s)\phi(p_1^r p_2^s)}+\sum_p\sum_{\substack{r\\ p^r>X}}\sum_{\substack{s\\ p^s>X}}\frac{(\log p)^2}{\phi(p^r)\phi(p^s)\phi(p^{\max(r,s)})}\\
&\le\sum_{p_1^r>X}\sum_{\substack{p_2^s>X\\ p_2\ne p_1}}\frac{(\log p_1)(\log p_2)}{\phi(p_1^r)^2\phi(p_2^s)^2}+2\sum_p\sum_{\substack{r\\ p^r>X}}\sum_{s=r}^{\infty}\frac{(\log p)^2}{\phi(p^r)\phi(p^s)\phi(p^s)}\\
&\ll\biggl(\sum_{p^r>X}\frac{\log p}{p^{2r}}\biggr)^2+\sum_{p^r>X}\frac{(\log p)^2}{p^r}\sum_{s=r}^{\infty}\frac{1}{p^{2s}}\\
&\ll\Bigl(\frac{1}{X}\Bigr)^2+\sum_{p^r>X}\frac{(\log p)^2}{p^{3r}}\ll\frac{\log X}{X^2}
\end{aligned}$$

by partial summation. □

Proposition 6.5. *Recall that $D(x)$ was defined in equation* (16)*. When $x>e^e$,*

$$D(x)=A(\log\log x)^2+O\biggl(\frac{(\log\log x)^{3/2}}{(\log\log\log x)^2}\biggr),$$

where $A=\dfrac{\log 2}{2}+A_0$ as in Theorem 1.1.

Proof. We begin by establishing asymptotics for $\mu(\omega_0)$ and $\mu(\omega_q)$ for $q\le X$. First,

$$\mu(\omega_0)=\sum_{p\le x}\frac{\omega_0(p)}{p}=\sum_{p\le x}\frac{\omega_2(p)\omega_0(p)}{p}=\operatorname{cov}(\omega_2,\omega_0)+O(1)=\frac{1}{2}(\log\log x)^2+O(\log\log x)$$

by Lemma 5.3 (with x in place of z). On the other hand,

$$\mu(\omega_q)=\sum_{p\le x}\frac{\omega_q(p)}{p}=\sum_{\substack{p\le x\\ p\equiv 1\ (\mathrm{mod}\ q)}}\frac{1}{p}=\frac{\log\log x}{\phi(q)}+O\biggl(\frac{\log q}{\phi(q)}\biggr)\tag{45}$$

by Lemma 2.12. Squaring, and using the fact that $\log q=o(\log\log x)$ for q in the range of summation, yields

$$\mu(\omega_q)^2=\frac{(\log\log x)^2}{\phi(q)^2}+O\biggl(\frac{\log q}{\phi(q)^2}\log\log x\biggr).$$

Inserting these estimates for $\mu(\omega_0)$ and $\mu(\omega_q)$ into equation (16), we obtain

$$\begin{aligned}
D(x) &= \frac{\log 2}{2}(\log\log x)^2 + O(\log\log x) + \frac{1}{4}\sum_{2\le q\le X}\Lambda(q)\biggl(\frac{(\log\log x)^2}{\phi(q)^2} + O\biggl(\frac{\log q}{\phi(q)^2}\log\log x\biggr)\biggr) \\
&= \frac{\log 2}{2}(\log\log x)^2 + \frac{1}{4}(\log\log x)^2\sum_{2\le q\le X}\frac{\Lambda(q)}{\phi(q)^2} + O\biggl(\log\log x\sum_{2\le q\le X}\frac{\Lambda(q)\log q}{\phi(q)^2}\biggr) \\
&= \biggl(\frac{\log 2}{2} + \frac{1}{4}\sum_{2\le q\le X}\frac{\Lambda(q)}{\phi(q)^2}\biggr)(\log\log x)^2 + O(\log\log x)
\end{aligned}$$

by partial summation. By Lemma 6.4, we may replace the coefficient of $(\log\log x)^2$ by $A + O(1/X)$, obtaining

$$D(x) = A(\log\log x)^2 + O\biggl(\frac{(\log\log x)^{3/2}}{(\log\log\log x)^2}\biggr),$$

as claimed. □

The following lemma gives the asymptotic size of a double sum that will appear shortly in the proof of Proposition 1.3.

Lemma 6.6. *Recall from Theorem 1.1 that* $C = \frac{(\log 2)^2}{3} + 2A_0\log 2 + 4A_0^2 + B$. *We have*

$$\begin{aligned}
\sum_{i=0}^{\rho(X)}\sum_{j=0}^{\rho(X)} Q_i\bigl(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\bigr)Q_j\bigl(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\bigr)\operatorname{cov}(\omega_{q_i},\omega_{q_j}) \\
= C(\log\log x)^3 + O\biggl(\frac{(\log\log x)^{5/2}}{\log\log\log x}\biggr). \qquad (46)
\end{aligned}$$

Proof. We begin by computing the partial derivatives appearing in the double sum. We have

$$Q_0\bigl(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\bigr) = \log 2$$

and, for $i \ne 0$, we use equation (45) to write

$$Q_i\bigl(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\bigr) = \frac{1}{2}\Lambda(q_i)\mu(\omega_{q_i}) = \frac{1}{2}\frac{\Lambda(q_i)}{\phi(q_i)}\log\log x + O\biggl(\frac{\Lambda(q_i)\log q_i}{\phi(q_i)}\biggr).$$

So, by Lemma 5.4, the summand on the left-hand side of equation (46) corresponding to $i = j = 0$ is of the form

$$\begin{aligned}
Q_0\bigl(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\bigr)Q_0\bigl(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\bigr)\operatorname{cov}(\omega_{q_0},\omega_{q_0}) \\
= \frac{(\log 2)^2}{3}(\log\log x)^3 + O((\log\log x)^2);
\end{aligned}$$

similarly, by Lemma 5.3 the summands corresponding to $i = 0$ and $j \ne 0$ are of the form

$$\begin{aligned}
Q_0\bigl(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\bigr)Q_j\bigl(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\bigr)\operatorname{cov}(\omega_{q_0},\omega_{q_j}) \\
= \frac{\log 2}{4}\frac{\Lambda(q_j)}{\phi(q_j)^2}(\log\log x)^3 + O\biggl(\frac{\Lambda(q_i)(\log\log x)^2}{\phi(q_j)^2}\biggr).
\end{aligned}$$

and the summands corresponding to $i \neq 0$ and $j = 0$ are the same up to labeling. Finally, by Lemma 5.2 we have that the summands on the left-hand side of equation (46) corresponding to $i \neq 0$ and $j \neq 0$ are of the form

$$Q_i\big(\mu(\omega_{q_0}), \dots, \mu(\omega_{q_{\rho(X)}})\big) Q_j\big(\mu(\omega_{q_0}), \dots, \mu(\omega_{q_{\rho(X)}})\big) \operatorname{cov}(\omega_{q_i}, \omega_{q_j}) \\ = \frac{1}{4} \frac{\Lambda(q_i)\Lambda(q_j)}{\phi(q_i)\phi(q_j)\phi([q_i, q_j])} (\log\log x)^3 + O\bigg(\frac{\Lambda(q_i)\Lambda(q_j)}{\phi(q_i)\phi(q_j)} (\log\log x)^2 \bigg).$$

Combining these last three evaluations results in

$$\sum_{i=0}^{\rho(X)} \sum_{j=0}^{\rho(X)} Q_i\big(\mu(\omega_{q_0}), \dots, \mu(\omega_{q_{\rho(X)}})\big) Q_j\big(\mu(\omega_{q_0}), \dots, \mu(\omega_{q_{\rho(X)}})\big) \operatorname{cov}(\omega_{q_i}, \omega_{q_j})$$
$$= \frac{(\log 2)^2}{3} (\log\log x)^3 + O((\log\log x)^2)$$
$$+ 2 \sum_{j=1}^{\rho(X)} \bigg(\frac{\log 2}{4} \frac{\Lambda(q_j)}{\phi(q_j)^2} (\log\log x)^3 + O\bigg(\frac{\Lambda(q_i)(\log\log x)^2}{\phi(q_j)^2} \bigg) \bigg)$$
$$+ \sum_{i=1}^{\rho(X)} \sum_{j=1}^{\rho(X)} \bigg(\frac{1}{4} \frac{\Lambda(q_i)\Lambda(q_j)}{\phi(q_i)\phi(q_j)\phi([q_i, q_j])} (\log\log x)^3 + O\bigg(\frac{\Lambda(q_i)\Lambda(q_j)}{\phi(q_i)\phi(q_j)} (\log\log x)^2 \bigg) \bigg)$$
$$= \bigg(\frac{(\log 2)^2}{3} + \frac{\log 2}{2} \sum_{i=1}^{\rho(X)} \frac{\Lambda(q_i)}{\phi(q_j)^2} + \frac{1}{4} \sum_{i=1}^{\rho(X)} \sum_{j=1}^{\rho(X)} \frac{\Lambda(q_i)\Lambda(q_j)}{\phi(q_i)\phi(q_j)\phi([q_i, q_j])} \bigg) (\log\log x)^3$$
$$+ O((\log\log x)^2 (\log\log\log x)^2) \tag{47}$$

by partial summation. By Lemma 6.4, the coefficient of $(\log\log x)^3$ above is equal to

$$\frac{(\log 2)^2}{3} + 2\log 2 A_0 + 4A_0^2 + B + O\bigg(\frac{1}{(\log\log x)^{1/2} \log\log\log x} \bigg).$$

Inserting this expression into equation (47) finishes the proof. □

We now have all of the auxiliary results needed to carry out the asymptotic evaluation of the moments $M_h(x)$.

Proof of Proposition 1.3. We start from equation (36):

$$M_h(x) = \sum_{\substack{h_0, h_1, h_2 \geq 0 \\ h_0 + h_1 + h_2 = h}} \binom{h}{h_0, h_1, h_2} \sum_{n \leq x} \big(\log 2 \cdot F_{\omega_0}(n) \big)^{h_0} S_1^{h_1} S_2^{h_2}.$$

If $h \geq 1$ is odd, then Lemma 6.3 applies to every inner sum, yielding

$$M_h(x) \ll \sum_{\substack{h_0, h_1, h_2 \geq 0 \\ h_0 + h_1 + h_2 = h}} \binom{h}{h_0, h_1, h_2} x (\log\log x)^{3h/2 - 1/4} (\log\log\log x)^{2h}$$
$$\ll x (\log\log x)^{3h/2 - 1/4} (\log\log\log x)^{2h},$$

since the implicit constant may depend upon h. In particular, $M_h(x) = o\big(x(\log\log x)^{3h/2}\big)$ for each odd h, as required.

On the other hand, if $h \ge 2$ is even, then Lemma 6.3 applies to all summands except those for which $h_1 = 0$, so that

$$M_h(x) = \sum_{\substack{h_0,h_1,h_2\ge 0\\ h_0+h_1+h_2=h\\ h_1=0}} \binom{h}{h_0,h_1,h_2}\big(\log 2\cdot F_{\omega_0}(n)\big)^{h_0} S_2^{h_2} + O\big(x(\log\log x)^{3h/2-1/4}(\log\log\log x)^{2h}\big)$$

$$= \sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{j=1}^{\tilde{k}_{h\beta}} \mu(\omega_{q_{w(h,\beta,j)}}) \sum_{n\le x}\prod_{i=1}^{h} F_{\omega_{q_{v(h,\beta,i)}}}(n) + O\big(x(\log\log x)^{3h/2-1/4}(\log\log\log x)^{2h}\big) \tag{48}$$

by Lemma 6.1. Notice, in this translation of notation, that factors of the form $\mu(\omega_q)$ on the right-hand side all arise from the term $S_2^{h_2}$; in particular, $\tilde{k}_{h\beta} = h_2$, and each $q_{w(h,\beta,j)}$ is a prime power not exceeding X (rather than 0), so that $\mu(\omega_{q_{w(h,\beta,j)}}) \ll \log\log x$ by equation (45). Similarly, of the factors of the form F_{ω_q}, we see that h_0 of them are F_{ω_0}, while the other h_2 are of the form F_{ω_q} for prime powers q. Therefore, in the main term in equation (48), we may apply Proposition 5.9 with $\ell = h_0$ and $k = h = h_0 + h_2$ to obtain

$$\sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{j=1}^{\tilde{k}_{h\beta}} \mu(\omega_{q_{w(h,\beta,j)}}) \sum_{n\le x}\prod_{i=1}^{h} F_{\omega_{q_{v(h,\beta,i)}}}(n)$$

$$= \sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{j=1}^{\tilde{k}_{h\beta}} \mu(\omega_{q_{w(h,\beta,j)}}) \bigg(\frac{x}{(h/2)!}\sum_{\tau\in T_h}\prod_{i=1}^{h/2} \operatorname{cov}(\omega_{q_{v(h,\beta,\Upsilon_1(i))}},\omega_{q_{v(h,\beta,\Upsilon_2(i))}}) + O(x(\log\log x)^{(2h_0+h)/2-1})\bigg)$$

$$= \frac{x}{(h/2)!}\sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{j=1}^{\tilde{k}_{h\beta}} \mu(\omega_{q_{w(h,\beta,j)}}) \sum_{\tau\in T_h}\prod_{i=1}^{h/2} \operatorname{cov}(\omega_{q_{v(h,\beta,\Upsilon_1(i))}},\omega_{q_{v(h,\beta,\Upsilon_2(i))}})$$
$$+ O((\log\log x)^{h_2}\cdot x(\log\log x)^{(3h_0+h_2)/2-1}); \tag{49}$$

note that this last error term is exactly $x(\log\log x)^{3h/2-1}$. By Proposition 4.7 with $y_j = \mu(\omega_{q_j})$ and $z_{ij} = \operatorname{cov}(\omega_{q_i},\omega_{q_j})$,

$$\frac{x}{(h/2)!}\sum_{\substack{\beta\le B_h\\ k_{h\beta}=h}} r_{h\beta}\prod_{j=1}^{\tilde{k}_{h\beta}} \mu(\omega_{q_{w(h,\beta,j)}}) \sum_{\tau\in T_h}\prod_{i=1}^{h/2} \operatorname{cov}(\omega_{q_{v(h,\beta,\Upsilon_1(i))}},\omega_{q_{v(h,\beta,\Upsilon_2(i))}})$$

$$= s_h x\bigg(\sum_{i=0}^{\rho(X)}\sum_{j=0}^{\rho(X)} Q_i\big(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\big)Q_j\big(\mu(\omega_{q_0}),\dots,\mu(\omega_{q_{\rho(X)}})\big)\operatorname{cov}(\omega_{q_i},\omega_{q_j})\bigg)^{h/2}$$

$$= s_h x\bigg(C(\log\log x)^3 + O\bigg(\frac{(\log\log x)^{5/2}}{\log\log\log x}\bigg)\bigg)^{h/2}$$

$$= C^{h/2}s_h x(\log\log x)^{3h/2} + O(x(\log\log x)^{3(h-1)/2})$$

by Lemma 6.6. Combining this evaluation with equations (48) and (49) yields

$$\lim_{x\to\infty} \frac{M_h(x)}{C^{h/2}x(\log\log x)^{3h/2}} = s_h = \frac{h!}{(h/2)!2^{h/2}},$$

which completes the proof when h is even. $\square$

7. The method of moments

We now describe the argument that deduces the Erdős–Kac law for $\log G(n)$ (Theorem 1.1) from the asymptotic formula for the moments given in Proposition 1.3. While this deduction is fairly standard, for the sake of completeness we include the rest of the proof.

For any real number u and positive real number x, let $k_x(u)$ denote the number of integers $n \le x$ such that $P_n(x) < D(x)+u\cdot\sqrt{C}(\log\log x)^{3/2}$. Then $\sigma_x(u) = k_x(u)/x$ is the cumulative distribution function of the random variable Y_x obtained by choosing $n \le x$ uniformly at random and then calculating $(P_n(x) - D(x))/\sqrt{C}(\log\log x)^{3/2}$; the hth moment of this random variable equals

$$\int_{-\infty}^{\infty} u^h \, d\sigma_x(u) = \frac{1}{x}\sum_{n\le x}\left(\frac{P_n(x) - D(x)}{\sqrt{C}(\log\log x)^{3/2}}\right)^h = \frac{M_h(x)}{xC^{h/2}(\log\log x)^{3h/2}}.$$

For every fixed h, by Proposition 1.3, this hth moment converges (as $x \to \infty$) to $s_h = h!/2^{h/2}(\frac{h}{2})!$ when h is even and to 0 when h is odd. By the "method of moments" from probability (see [3, Theorem 30.2]), the sequence $\{Y_x\}$ of random variables converges in distribution to the unique random variable with these moments, which is the standard normal random variable. (This result is due to Chebyshev for the normal distribution and was later generalized to any random variable that is uniquely determined by its moments.) In other words, for any real number u,

$$\lim_{x\to\infty} \frac{1}{x}\#\left\{n \le x \colon \frac{P_n(x) - D(x)}{\sqrt{C}(\log\log x)^{3/2}} < u\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\, dt. \tag{50}$$

On the other hand, Propositions 1.2 and 6.5 imply that

$$\frac{P_n(x) - D(x)}{\sqrt{C}(\log\log x)^{3/2}} = \frac{\log G(n) - A(\log\log x)^2}{\sqrt{C}(\log\log x)^{3/2}} + O\left(\frac{1}{\log\log\log x}\right) \tag{51}$$

for all but $O(x/\log\log\log x)$ integers $n \le x$. Furthermore, $\log\log x = (\log\log n)\big(1 + O(1/\log\log x)\big)$ when $n > x/\log\log\log x$, and therefore we may modify equation (51) to

$$\frac{P_n(x) - D(x)}{\sqrt{C}(\log\log x)^{3/2}} = \frac{\log G(n) - A(\log\log n)^2}{\sqrt{C}(\log\log n)^{3/2}} + O\left(\frac{1}{\log\log\log x}\right)$$

for all but $O(x/\log\log\log x)$ integers $n \le x$. It follows from this estimate that we also have

$$\lim_{x\to\infty} \frac{1}{x}\#\left\{n \le x \colon \frac{\log G(n) - A(\log\log n)^2}{\sqrt{C}(\log\log n)^{3/2}} < u\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\, dt \tag{52}$$

(by bounding, for a given real number u, the left-hand side of equation (52) above and below by the left-hand side of equation (50) with u replaced, respectively, by $u + \varepsilon$ and $u - \varepsilon$), which is equivalent to the conclusion of Theorem 1.1.

8. Counting subgroups up to isomorphism, and maximal orders

Recall that $I(n)$ denotes the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$. We are able to quickly establish an Erdős–Kac law for $I(n)$ (Theorem 1.4) by relating $\log I(n)$ to two other ϕ-additive functions that have already been analyzed by Erdős and Pomerance.

Lemma 8.1. *For any positive integer n, we have $\omega(\phi(n))\log 2 \le \log I(n) \le \Omega(\phi(n))\log 2$.*

Proof. Let $I_p(n)$ denote the number of isomorphism classes of p-subgroups of $\mathbb{Z}_n^\times$; as we saw with $G(n)$, we again have

$$\log I(n) = \sum_{p\mid\phi(n)} \log I_p(n).$$

This is already enough to imply the lower bound $\omega(\phi(n))\log 2 \le \log I(n)$: for every prime $p \mid \phi(n)$, the quantity $I_p(n)$ counts at least two subgroups of $\mathbb{Z}_n^\times$, namely the Sylow p-subgroup and the trivial subgroup.

For any such prime p, write the Sylow p-subgroup of $\mathbb{Z}_n^\times$ as $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots$ for some partition $\boldsymbol{\alpha}$ of the integer $\nu_p(\phi(n))$. Then $I_p(n)$ is exactly the number of subpartitions of $\boldsymbol{\alpha}$. Certain subsets of the Ferrers diagram corresponding to $\boldsymbol{\alpha}$ correspond to subpartitions, while many subsets do not; but the total number of subsets, $2^{\nu_p(\phi(n))}$, is certainly an upper bound for the number of subpartitions. We conclude that

$$\sum_{p\mid\phi(n)} \log I_p(n) \le \sum_{p\mid\phi(n)} \log\left(2^{\nu_p(\phi(n))}\right) = \sum_{p\mid\phi(n)} \nu_p(\phi(n))\log 2 = \Omega(\phi(n))\log 2, \tag{53}$$

which is the desired upper bound. □

Proof of Theorem 1.4. Erdős and Pomerance [6] have shown that both $\omega(\phi(n))$ and $\Omega(\phi(n))$ satisfy Erdős–Kac laws, in both cases with mean $\frac{1}{2}(\log\log n)^2$ and variance is $\frac{1}{3}(\log\log n)^3$. Thus, as a consequence of Lemma 8.1, $\log I(n)$ satisfies an Erdős–Kac law with mean $\frac{\log 2}{2}(\log\log n)^2$ and variance $\frac{\log 2}{3}(\log\log n)^3$ as well. □

It might be surprising that the simple bounds from Lemma 8.1 suffice to establish this Erdős–Kac law, despite how seemingly wasteful the inequality (53) is. We view this as a reflection of the anatomical fact that typically, most primes dividing $\phi(n)$ are large and most large primes dividing $\phi(n)$ do so only to the first power.

We turn now to the question of determining how large the values of $G(n)$ and $I(n)$ can become. We start with a pair of arguments (an upper bound and a construction) that together show that the maximal order of $\log G(n)$ has order of magnitude $(\log x)^2/\log\log x$. In both arguments, it will be helpful to observe that

$$\lambda_p(n) = \sum_{j=1}^{\lambda_p(n)} 1 \le \sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n)$$

for any prime $p \mid \phi(n)$, and therefore

$$\sum_{p\mid\phi(n)} \lambda_p(n)\log p \le \sum_{p\mid\phi(n)} \sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n)\log p = \log\phi(n) < \log x \tag{54}$$

by equation (10).

Proof of the upper bound in Theorem 1.5. Proposition 2.11 gives

$$\begin{aligned}\log G(n) = \sum_{p\mid\phi(n)} \log G_p(n) &= \sum_{p\mid\phi(n)} \biggl(\frac{\log p}{4} \sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n)^2 + O(\lambda_p(n)\log p) \biggr) \\ &= \frac{1}{4} \sum_{p\mid\phi(n)} \sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n)^2 \log p + O\biggl(\sum_{p\mid\phi(n)} \lambda_p(n)\log p \biggr) \\ &= \frac{1}{4} \sum_{p\mid\phi(n)} \sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n)^2 \log p + O(\log x) \qquad (55)\end{aligned}$$

by equation (54). On the other hand,

$$\overline{\omega}_{p^j}(n) \le \omega_{p^j}(n) + 2 \le \omega(n) + 2 < \frac{\log x}{\log\log x}\biggl(1 + \frac{1}{\log\log x}\biggr) \qquad (56)$$

by the classical upper bound for $\omega(n)$ [10, Theorem 2.10]. We use this bound on one of the two factors of $\overline{\omega}_{p^j}(n)$ in each summand on the right-hand side of equation (55), obtaining

$$\begin{aligned}\log G(n) &< \frac{1}{4} \sum_{p\mid\phi(n)} \sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n) \log p \cdot \frac{\log x}{\log\log x}\biggl(1 + \frac{1}{\log\log x}\biggr) + O(\log x) \\ &= \frac{\log x}{4\log\log x}\biggl(1 + \frac{1}{\log\log x}\biggr)\log\phi(n) + O(\log x) < \frac{(\log x)^2}{4\log\log x}\biggl(1 + \frac{1}{\log\log x}\biggr)\end{aligned}$$

by equation (54) again. □

Proof of the lower bound in Theorem 1.5. Choose $B = B(3)$ so that Theorem 5.1 is valid, and set

$$\begin{aligned} V &= \frac{(\log x)^2}{(\log\log x)^{2B+1}}\biggl(1 - \frac{1}{\log\log x}\biggr) \\ Q &= \frac{\log x}{(\log\log x)^{2B+1}};\end{aligned}$$

note that $Q < V^{1/2}/(\log V)^B$ when x is large enough. Thus by equation (26),

$$\sum_{Q<p<2Q} \biggl| \theta(V;p,1) - \frac{V}{p-1} \biggr| \ll \frac{V}{(\log V)^3}.$$

Since the number of primes between Q and $2Q$ is $\gg Q/\log Q$, we may choose a prime p in that interval such that

$$\begin{aligned}\theta(V,p,1) &= \frac{V}{p-1} + O\biggl(\frac{V}{(\log V)^3} \frac{\log Q}{Q} \biggr) \\ &\le \frac{V}{Q} + O\biggl(\frac{V}{(\log V)^3} \frac{\log Q}{Q} \biggr) = \log x - \frac{\log x}{\log\log x} + O\biggl(\frac{\log x}{(\log\log x)^2} \biggr). \qquad (57)\end{aligned}$$

Now, fixing this prime p that was chosen above, consider the integer

$$n = \prod_{\substack{q \le V \\ q \equiv 1 \pmod{p}}} q = e^{\theta(V,p,1)},$$

where p is the prime chosen above; by equation (57), we see that $n < x$ when x is sufficiently large. Notice also that $\log p = \log\log x + O(\log\log\log x)$ and $\log V = 2\log\log x + O(\log\log\log x)$, and therefore

$$\omega_p(n) = \pi(V;p,1) \ge \frac{\theta(V;p,1)}{\log V} \ge \frac{\log x}{2\log\log x}\biggl(1 + O\biggl(\frac{\log\log\log x}{\log\log x}\biggr)\biggr)$$

by equation (57). Consequently,

$$\begin{aligned}
\log G(n) &\ge \log G_p(n) \\
&= \frac{\log p}{4}\sum_{j=1}^{\lambda_p(n)} \overline{\omega}_{p^j}(n)^2 + O(\lambda_p(n)\log p) \\
&\ge \frac{\log p}{4}\omega_p(n)^2 + O(\lambda_p(n)\log p) \\
&\ge \frac{\log\log x + O(\log\log\log x)}{4}\biggl(\frac{\log x}{2\log\log x}\biggr)^2\biggl(1 + O\biggl(\frac{\log\log\log x}{\log\log x}\biggr)\biggr) + O(\lambda_p(n)\log p) \\
&= \frac{\log^2 x}{16\log\log x}\biggl(1 + O\biggl(\frac{\log\log\log x}{\log\log x}\biggr)\biggr) + O(\lambda_p(n)\log\log x).
\end{aligned}$$

Since equation (54) implies that $\lambda_p(n) < \log x$, the above estimate establishes the desired lower bound. □

We believe that the upper bound (with leading constant $\frac{1}{4}$) gives the true asymptotic size of the maximal order of $\log G(n)$; in particular, if one assumes the Elliott–Halberstam conjecture, then the construction giving the lower bound can easily be modified to produce a leading constant $\frac{1}{4}$ instead of the current $\frac{1}{16}$.

Theorem 1.5 shows that the maximal order of $\log G(n)$ is substantially larger than the typical size of $\log G(n)$. The same phenomenon holds, to a somewhat lesser degree, for $\log I(n)$, which we now show via another pair of arguments (an upper bound and a construction) after the following preliminary lemma.

Lemma 8.2. *For any $x \ge 3$ and any integer $m \le x$,*

$$\sum_{p \mid m} \frac{1}{\log p} < \frac{\log x}{(\log\log x)^2} + O\biggl(\frac{\log x}{(\log\log x)^3}\biggr).$$

Proof. First suppose that $m_0 = \prod_{p \le y} p$ for some real number y. Then $\log x > \log m_0 = \sum_{p \le y} \log p = \theta(y) = y + O(y/\log y)$ by the prime number theorem, which implies that $y < \log x + O(\log x/\log\log x)$. Then, by partial summation,

$$\sum_{p \mid m_0} \frac{1}{\log p} = \sum_{p \le y} \frac{1}{\log p} = \frac{y}{\log^2 y} < \frac{\log x}{(\log\log x)^2} + O\biggl(\frac{\log x}{(\log\log x)^3}\biggr).$$

For general m, choose a real number y such that $\pi(y) = \omega(m)$, and define $m_0 = \prod_{p \le y} p$. Then $m_0 \le m \le x$, while $\sum_{p|m_0} 1/\log p \ge \sum_{p|m} 1/\log p$ since both sums have the same number of summands and each individual summand in the first sum is at least as large as the corresponding summand in the second sum. Consequently, the desired upper bound for $\sum_{p|m} 1/\log p$ follows from the already established upper bound for $\sum_{p|m_0} 1/\log p$. □

Proof of the upper bound in Theorem 1.6. Given $n \le x$, we write

$$\phi(n) = \prod_{p^{k_p} \| \phi(n)} p^{k_p};$$

since $\phi(n) \le n \le x$,

$$\sum_{p^{k_p} \| \phi(n)} k_p \log p = \log \phi(n) \le \log x. \tag{58}$$

For any prime p dividing $\phi(n)$, the p-Sylow subgroup of $\mathbb{Z}_n^\times$ is of the form $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots$ for some partition $\boldsymbol{\alpha}$ of the integer k_p. As discussed at the beginning of Section 2.1, $I_p(n)$ is the number of subpartitions of $\boldsymbol{\alpha}$. We bound this number crudely by noting that every subpartition of $\boldsymbol{\alpha}$ is a partition of some integer $j \in \{0, 1, \dots, k_p\}$; therefore, with $P(m)$ denoting the usual partition function,

$$I_p(n) \le \sum_{j=0}^{k_p} P(j) \le (k_p + 1) P(k_p). \tag{59}$$

A consequence of Lehmer's formula for the partition function, as described in [2, proof of Theorem 2.1], is that for every positive integer m,

$$(m+1)P(m) < (m+1) \cdot \frac{\sqrt{3}}{12m} \left(1 + \frac{1}{\sqrt{m}}\right) \exp\left(\frac{\pi}{6}\sqrt{24m-1}\right) < \exp\left(\pi\sqrt{\frac{2}{3}m}\right),$$

where the last inequality can be verified by an easy calculation. In particular, the upper bound (59) implies that $\log I_p(n) < \pi\sqrt{2k_p/3}$, and thus

$$\log I(n) = \sum_{p|\phi(n)} \log I_p(n) < \pi\sqrt{\frac{2}{3}} \sum_{p|\phi(n)} \sqrt{k_p}. \tag{60}$$

But by Cauchy–Schwarz,

$$\left(\sum_{p|\phi(n)} \sqrt{k_p}\right)^2 \le \left(\sum_{p|\phi(n)} k_p \log p\right)\left(\sum_{p|\phi(n)} \frac{1}{\log p}\right) \le \log x \cdot \frac{\log x}{(\log\log x)^2}\left(1 + O\left(\frac{1}{\log\log x}\right)\right)$$

by equation (58) and Lemma 8.2; combining this bound with equation (60) completes the proof of the upper bound. □

Proof of the lower bound in Theorem 1.6. We employ a strategy suggested by Pomerance (private communication). Set $U = \frac{1}{5}\log x - \log\log x$, define $m = \prod_{p \le U} p$, and let q be the smallest prime that is congruent to 1 (mod m). By Linnik's theorem, with the best current value of Linnik's constant due to Xylouris [14], we know that $q \ll m^5$. On the other hand, by the prime number theorem,

$$\log m = \theta(U) = U + O\left(\frac{U}{\log^2 U}\right) = \frac{1}{5}\log x - \log\log x + O\left(\frac{\log x}{(\log\log x)^2}\right),$$

which shows that $m = o(x^{1/5})$ and therefore $q < x$ when x is large enough.

Since m divides $q-1$, the prime number theorem also gives

$$\begin{aligned}\omega(\phi(q)) = \omega(q-1) \geq \omega(m) = \pi(U) &= \frac{U}{\log U} + O\left(\frac{U}{\log^2 U}\right)\\ &= \frac{\log x}{5\log\log x} + O\left(\frac{\log x}{(\log\log x)^2}\right).\end{aligned}$$

The lower bound now follows from inequality $\log I(q) \geq \log 2 \cdot \omega(\phi(q))$, as noted in the proof of Lemma 8.1. □

Note that the constant $\frac{1}{5}\log 2$ can be improved to any number less than $\log 2$ if one is willing to assume Montgomery's conjecture on the error term in the prime number theorem for arithmetic progressions (as stated by Friedlander and Granville [7, conjecture 1(b)]). However, even this assumption is not enough to close the gap between the constants in the upper and lower bounds (note that $\log 2 \approx 0.69315$ while $\pi\sqrt{2/3} \approx 2.56651$).

Acknowledgements

The authors thank Carl Pomerance for helpful conversations concerning some proofs in this paper. The authors were supported in part by a National Sciences and Engineering Research Council of Canada Discovery Grant.

References

1. A. Akbary and K. Hambrook, *A variant of the Bombieri–Vinogradov theorem with explicit constants and applications*, Math. Comp. **84** (2015), no. 294, 1901–1932.
2. C. Bessenrodt and K. Ono, *Maximal multiplicative properties of partitions*, Ann. Comb. **20** (2016), no. 1, 59–64.
3. P. Billingsley, *Probability and measure*, 3rd ed., Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, Inc., New York, 1995, A Wiley–Interscience Publication.
4. P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, American Journal of Mathematics **62** (1940), no. 1/4, 343–352.
5. P. Erdős and J-L. Nicolas, *Sur la fonction "nombre de facteurs premiers de n"*, Séminaire Delange–Pisot–Poitou. Théorie des nombres **20** (1978–1979), no. 2, 1–19.
6. P. Erdős and C. Pomerance, *The normal number of prime factors of $\varphi(n)$*, Rocky Mtn. J. Math. **15** (1985), 343–352.
7. J. Friedlander and A. Granville, *Limitations to the equi-distribution of primes. I*, Ann. of Math. (2) **129** (1989), no. 2, 363–382.
8. A. Granville and K. Soundararajan, *Sieving and the Erdős–Kac theorem*, Equidistribution in number theory, an introduction, NATO Sci. Ser. II Math. Phys. Chem., vol. 237, Springer, Dordrecht, 2007, pp. 15–27.
9. H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.
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. K.K. Norton, *On the number of restricted prime factors of an integer. I*, Illinois J. Math. **20** (1976), no. 4, 681–705.
12. C. Pomerance, *On the distribution of amicable numbers*, J. Reine Angew. Math. **293/294** (1977), 217–222.
13. T. Stehling, *On computing the number of subgroups of a finite abelian group*, Combinatorica **12** (1992), no. 4, 475–479.
14. T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, Bonner Mathematische Schriften [Bonn Mathematical Publications], vol. 404, Universität Bonn, Mathematisches Institut, Bonn, 2011, Dissertation for the degree of Doctor of Mathematics and Natural Sciences at the University of Bonn, Bonn, 2011.

Department of Mathematics, University of British Columbia, Room 121, 1984 Mathematics Road, Canada V6T 1Z2

E-mail address: gerg@math.ubc.ca

E-mail address: ltroupe@math.ubc.ca