The Iterated Carmichael Lambda Function

by

Nicholas Harland

B.Sc., The University of Manitoba, 2003
M.Math., The University of Waterloo, 2004

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

The Faculty of Graduate Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

October 2012

Abstract

The arithmetic function $\lambda(n)$ is the exponent of the cyclic group $(\mathbb{Z}/n\mathbb{Z})^{\times}$. The kth iterate of $\lambda(n)$ is denoted by $\lambda_k(n)$. In this work we will show the normal order for $\log(n/\lambda_k(n))$ is $(\log\log n)^{k-1}\log\log\log n/(k-1)!$. Second, we establish a similar normal order for other iterate involving a combination of λ and ϕ. Lastly, define $L(n)$ to be the smallest k such that $\lambda_k(n) = 1$. We determine new upper and lower bounds for $L(n)$ and conjecture a normal order.

Table of Contents

Appendices

List of Figures

Acknowledgements

I would like to thank my dedicated teachers throughout my academic career. I would like to thank my supervisor Greg Martin, who has helped me significantly throughout my Ph.D. Without his guidance I would never have been able to attain my mathematical achievements. Specifically his help with techniques to estimate summations was invaluable to this work. His advice in general has been, and will continue to be, helpful as I continue my academic career.

I would also like to thank Greg Martin and Nike Vatsal for their financial support over the last 3 years.

I would also like to acknowledge Mike Bennett. Not only has he been an outstanding instructor, but his advice involving research and presentation has and will assist me in my career.

Finally I would like to acknowledge my fellow students and postdocs for helpful conversations. Notably Carmen Bruni, Jay Heumann, Erick Wong, Kevin Doerkson, Vishaal Kapoor and Paul Pollack. Specifically I would like to thank Paul for his helpful suggestion in the proof of Lemma 2.4.

Dedication

I would like to dedicate my thesis to my wife Jamie. Her support over the last 3 years has been wonderful. I also dedicate my thesis to my son Miles. Finally to my parents and family for always encouraging me and helping me any way they could.

Chapter 1

Introduction

1.1 History and Results

The Carmichael lambda function $\lambda(n)$, first introduced by Carmichael [5], is defined to be the order of the largest cyclic subgroup of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, that is, the smallest postive integer m such that

$$a^m \equiv 1 \pmod{n}$$

for all integers a which are coprime to n. It can be computed at odd prime powers to be the same as $\phi(p^k) = p^{k-1}(p-1)$. As for even prime powers, $\lambda(2) = 1, \lambda(4) = 2$, and $\lambda(2^k) = \phi(2^k)/2 = 2^{k-2}$ for $k \geq 3$. By the Chinese Remainder Theorem, if $(a, b) = 1$, then $\lambda(ab) = \mathrm{lcm}\{\lambda(a), \lambda(b)\}$, which allows the calculation of the function for all positive integers.

In addition to being an interesting arithmetic function to study, the Carmichael lambda function has a connection with some primality testing algorithms [1], [15]. In [1], the authors create a prime testing algorithm. It is shown that the running time of the algorithm is connected to finding an upper bound of $\lambda(N)$ for specially created numbers N. In [15], the primality test involves looking at Carmichael numbers. That is numbers which satisfy $a^{n-1} \equiv 1 \pmod{n}$ for all $(a, n) = 1$. It is well known that composite numbers satisfy this conguence if and only if $\lambda(n)$ divdes $n-1$. Miller uses this idea to help create his algorithm to test primes.

Several properties of $\lambda(n)$ were studied by Erdős, Pomerance, and Schmutz in [9]. One of those results is the following. For an explicitly defined constant A,

$$\lambda(n) = n \exp\big(-(\log\log n)(\log\log\log n + A + O\big((\log\log\log n)^{-1+\epsilon}\big)\big) \quad (1.1)$$

as $n \to \infty$ for almost all n. Martin and Pomerance showed in [16] that

$$\lambda(\lambda(n)) = n \exp\bigg(-(1 + o(1))(\log\log n)^2 \log\log\log n\bigg) \qquad (1.2)$$

as $n \to \infty$ for almost all n.

Applications of this function included the power generator of pseudorandom numbers

$$u_n \equiv u_{n-1}^e \pmod{m}, \qquad 0 \leq u_n \leq m-1, \qquad n = 1, 2, \ldots.$$

This generator has lots of cryptographic applications (see [11]), and sequences of large period given by $\lambda(\lambda(m))$ are quite important. In [16], the authors provided lower bounds on the number of cycles of the power generator for almost all m by relating that number to $\lambda(\lambda(m))$ and then use their estimate.

This thesis studies the asymptotic properties of the following two functions.

Definition 1.1. The k–fold iterated Carmichael lambda function is defined recursively to be

$$\lambda_0(n) = n, \quad \lambda_k(n) = \lambda(\lambda_{k-1}(n)) \text{ for } k \geq 1.$$

We define $\phi_k(n)$ similarly. Next we study a related function.

Definition 1.2. For a positive integer n, let $L(n)$ denote the smallest k such that $\lambda_k(n) = 1$.

Throughout this work we are interested in finding normal orders for the preceding arithmetic functions. Next we define the meaning of normal order.

Definition 1.3. Let $f(n)$ be an arithmetic function. We say $f(n)$ has normal order $g(n)$ if for all $\epsilon > 0$,

$$(1-\epsilon)g(n) < f(n) < (1+\epsilon)g(n) \tag{1.3}$$

for almost all n. By "for almost all n" we mean the proportion of $n \leq x$ for which (1.3) does not hold goes to 0 as $n \to \infty$.

In [16] it is conjectured that

$$\lambda_k(n) = n \exp\left(-\frac{1}{(k-1)!}(1+o_k(1))(\log\log n)^k \log\log\log n\right)$$

for almost all n. Our first result is the proof of that conjecture.

Theorem 1.4. *For fixed positive integer k, the normal order of $\log \frac{n}{\lambda_k(n)}$ is $\frac{1}{(k-1)!}(\log\log n)^k \log\log\log n$.*

Note that Theorem 1.4 has been proved for $k = 1$ in [9]. Therefore from now on we will assume that $k \neq 1$. We'll prove the theorem in Chapter 3 in the following slightly stronger form. Let $\psi(x)$ be a function which satisifes the following two properties.

1. $\psi(x) = o(\log\log\log x)$ and
2. $\psi(x) \to \infty$ as $x \to \infty$.

We will show

$$\log\left(\frac{n}{\lambda_k(n)}\right) = \frac{1}{(k-1)!}(\log\log n)^k\Big(\log\log\log n + O_k\big(\psi(n)\big)\Big)$$

for all but $O(x/\psi(x))$ integers up to x.

The proof of Theorem 1.4 involves breaking down $n/\lambda_k(n)$ in terms of the iterated Euler ϕ function by using

$$\frac{n}{\lambda_k(n)} = \left(\frac{n}{\phi(n)}\right)\left(\frac{\phi(n)}{\phi_2(n)}\right)\cdots\left(\frac{\phi_{k-1}(n)}{\phi_k(n)}\right)\left(\frac{\phi_k(n)}{\lambda_k(n)}\right). \tag{1.4}$$

Estimates for all but the last term are known. Hence $\log(n/\lambda_k(n))$ can be written as a sum of the logarithms on the right side of (1.4). It will be necessary to analyze the term $\log(\phi_k(n)/\lambda_k(n))$.

Our second result is an asymptotic formula involving iterates involving λ and ϕ. Banks, Luca, Saidak and Stănică in [4] showed that for almost all n,

$$\lambda(\phi(n)) = n\exp(-(1+o(1))(\log\log n)^2\log\log\log n) \text{ and}$$
$$\phi(\lambda(n)) = n\exp(-(1+o(1))(\log\log n)\log\log\log n).$$

As a corollary to Theorem 1.4 we will obtain asymptotic formulas for higher iterates involving λ and ϕ. Specifically we prove the following.

Theorem 1.5. *For $l \geq 0$ and $k \geq 1$, let $g(n) = \phi_l(\lambda(f(n)))$, where $f(n)$ is a $(k-1)$ iterated arithmetic function consisting of iterates of ϕ and λ. The normal order of $\log(n/g(n))$ is $\frac{1}{(k-1)!}(\log\log n)^k\log\log\log n$.*

An example of the use of this theorem is for $\phi\phi\lambda\phi\phi\lambda\lambda\phi(n)$. Since $l = 2, k = 5$, we get that the normal order of $\log\frac{n}{\phi\phi\lambda\phi\phi\lambda\lambda\phi(n)}$ is

$$\frac{1}{24}(\log\log n)^5\log\log\log n.$$

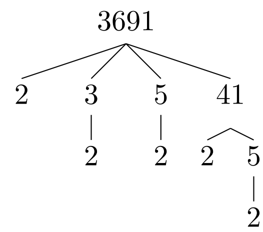

Figure 1.1: The Pratt tree for the prime 3691

A result by Erdős, Granville, Pomerance and Spiro in [8] established that $n/\phi_k(n)$ does not have a normal order. That result combined with Theorem 1.5 completes the picture of how all iterates of λ and ϕ relate to n. However it doesn't show how they relate to each other. For example $\log \frac{n}{\lambda\phi\phi\lambda\lambda\phi(n)} \sim \log \frac{n}{\lambda_6(n)}$ for almost all n, but is there a normal order for $\log \frac{\lambda\phi\phi\lambda\lambda\phi(n)}{\lambda_6(n)}$? Kapoor [14] found results for $k = 2$, but the problem remains open for higher iterates.

We then turn our attention to $L(n)$. In order to study this function, we use the Pratt tree for a prime p which is defined as follows. The root node is p. Below p are nodes labelled with the primes q such that $q \mid p-1$. The nodes below q are primes dividing $q-1$ and so on until we are left with just 2. For example, if we want to take the prime 3691, the primes dividing 3690 are $2, 3, 5$ and 41. Then we take the primes dividing one less than each of these and obtain the tree in Figure 1.1. In 1975, Pratt [19] introduced these trees to show that every prime has a short certificate (proof of primality). The Pratt tree is of interest to us because the way the primes go down a branch of the tree is similar to how those same primes divide iterates of $\lambda(n)$. The height of the Pratt tree $H(p)$ is the length of the longest branch. That height is related to $L(n)$.

Since $\lambda(n)$ is either even or 1, and $\lambda(n) \leq n/2$ for even n, we easily see that $L(n) \leq \lfloor \log n/\log 2 + 1 \rfloor$. By considering when n is a power of 3 we can note that $L(n) \geq 1 + (1/\log 3)\log n$ for infinitely many values of n. As for upper bounds, Martin and Pomerance [16] gave a construction for which $L(n) < (1/\log 2 + o(1))\log\log n$ for infinitely many n. The number of such $n \leq x$ have asymptotic density 0. It is conjectured that for a set of positive integers with asymptotic density 1, that $L(n) \asymp \log\log n$ however no previous results have shown $L(n) = o(\log n)$ for almost all n.

It's easy to see that $H(p) \leq L(p)$, so any lower bound on H acts as a lower bound on L. Bounds for the height of the Pratt tree $H(p)$ were obtained in a 2010 paper by Ford, Konyagin and Luca [10]. The bound depends on the exponent arising from the Elliot–Halberstam conjecture. Recall the Bombieri–Vinogradov Theorem [7, Chapter 28] implies

$$\sum_{n\le Q}\max_{y\le x}\left|\pi(y;n,1)-\frac{\mathrm{li}(y)}{\phi(m)}\right| \ll x(\log x)^{-A} \tag{1.5}$$

holds for any $Q \le x^{1/2}(\log x)^{-B}$ and any $A > 0$, where $B = B(A)$. The Elliot–Halberstam conjecture says that (1.5) holds for $Q = x^{\theta}$ for any $\theta < 1$. Let θ' be such that (1.5) holds for $Q = x^{\theta'}$. In [10] Ford, Konyagin and Luca showed for any $c < 1/(e^{-1} - \log\theta')$,

$$H(p) > c\log\log p \tag{1.6}$$

for all but $O\big(x/(\log x)^K\big)$ primes p, for some $K > 1$. Under Elliot–Halberstam, we can take any $c < e$, but unconditionally, Bombieri–Vinogradov gives any $c < 1/(e^{-1} + \log 2)$.

In Chapter 5 we show that if $n = \prod p_i^{\alpha_i}$, then

$$L(n) = \max_i\{L(p_i^{\alpha_i})\} \tag{1.7}$$

and

$$L(p^{\alpha}) = \alpha - 1 + L(p) \ge L(p). \tag{1.8}$$

These two equations imply $L(n) \ge L(p)$ for any $p \mid n$. This motivates the following theorem which will be proved in Chapter 5

Theorem 1.6. *There exists some $c > 0$ such that*

$$L(n) \ge c\log\log n$$

for almost all $n \le x$.

For an upper bound, in [10] it was shown that

$$H(p) \le (\log p)^{0.95022} \tag{1.9}$$

for all $p \le x$ outside a set of size $O\big(x\exp(-(\log x)^{\delta}\big)$ for some $\delta > 0$. We extend this to a result about $L(n)$.

Theorem 1.7. *If $H(p) \le (\log p)^{\gamma}$ for almost all $p \le x$ outside a set of size $O\big(x\exp(-(\log x)^{\delta})\big)$ for some $\delta > 0$, then for some function η,*

$$L(n) \ll (\log n)^{\gamma}\eta(n)$$

for almost all n as $n \to \infty$.

The function $\eta(x)$ can be taken to be as small as $O(\log\log\log x)$. Equation (1.9) yields the following corollary.

Corollary 1.8. *For almost all n,*

$$L(n) \ll (\log n)^{0.9503}.$$

In [10], the authors also came up with a nice probabilistic model which suggested a conjecture that the normal order for $H(p)$ is $e \log\log p$. Assuming this conjecture, we give some evidence to suggest a related conjecture for $L(n)$.

Conjecture 1.9. The normal order of $L(n)$ is $e \log\log n$.

Chapter 2

Notation and Required Estimates

2.1 Notation

The following notations and conventions will be used throughout this thesis. The letters p, q, r, s and their subscripts will always denote primes. In Chapters 3 and 4, $k \geq 2$ will be a fixed integer. In Chapter 3 any implicit constant may depend on k, otherwise the constants are absolute. Let $v_p(n)$ be the largest power of p which divides n, so that

$$n = \prod_p p^{v_p(n)}.$$

Let the set $\mathcal{P}_n$ be $\{p : p \equiv 1 \pmod{n}\}$. The notation $q \prec q'$ is defined to mean that $q' \in \mathcal{P}_q$. In Chapter 3 we will assume $x > e^{e^e}$. The function $y = y(x)$ is defined to be $\log \log x$. Also let $\psi(x)$ be any function going to ∞ such that $\psi(x) = o(\log y) = o(\log \log \log x)$. Whenever we use the phrase "for almost all $n \leq x$" in a result, we mean that the result is true for all $n \leq x$ except a set of size $o(x)$. In Chapter 3 the exceptional set will be $O(x/\psi(x))$.

2.2 Required Estimates

The following estimates will be used throughout this thesis. Let $\Lambda(n)$ be the Von–Mangoldt function defined by

$$\Lambda(n) = \begin{cases} \log p & n = p^l \\ 0 & \text{otherwise.} \end{cases}$$

We use the Chebyshev bound

$$\sum_{n \leq x} \Lambda(n) = \sum_{p^l \leq x} \log p \ll x. \tag{2.1}$$

Also define the related function

$$\theta(x) = \sum_{p \le x} \log p.$$

It follows from (2.1) that

$$\theta(x) \ll x. \tag{2.2}$$

We also require a formula of Mertens (see [17, Theorem 2.7(b)])

$$\sum_{q \le x} \frac{\log q}{q} = \log x + O(1). \tag{2.3}$$

We use partial summation on (2.2) to obtain some tail estimates.

Lemma 2.1. *For all $x > 2$, we have the following sums over primes.*

(a)

$$\sum_{q > x} \frac{\log q}{q^2} \ll \frac{1}{x}. \tag{2.4}$$

(b)

$$\sum_{q > x} \frac{1}{q^2} \ll \frac{1}{x \log x}. \tag{2.5}$$

Proof. Equation (2.5) follows from (2.4) since $\log x < \log q$. As for Equation (2.4),

$$\begin{aligned} \sum_{q > x} \frac{\log q}{q^2} &= \int_x^\infty \frac{d(\theta(t))}{t^2} \\ &= \frac{2\theta(x)}{x^3} + \int_x^\infty \frac{2\theta(t)dt}{t^3} \\ &= \frac{2\theta(x)}{x^3} + O\left(\int_x^\infty \frac{dt}{t^2} \right) \ll \frac{1}{x}. \end{aligned}$$

□

Given $m, x \ge 2$, let A be the smallest a for which $m^a > x$. We can then manipulate the sums

$$\sum_{a \in \mathbb{N}} \frac{P(a)}{m^a} = \frac{1}{m} \sum_{a=0}^{\infty} \frac{P(a)}{m^a} \quad \text{and} \quad \sum_{\substack{a \in \mathbb{N} \\ m^a > x}} \frac{1}{m^a} \ll \frac{1}{x} \left| \sum_{a=A}^{\infty} \frac{1}{m^{a-A}} \right| = \frac{1}{x} \left| \sum_{a=0}^{\infty} \frac{1}{m^a} \right|$$

for any polynomial $P(x)$. Then by noting that $\sum_{a=A}^{\infty}\frac{P(a)}{m^a} \ll_P 1$ uniformly for $m \geq 2$ and $A \geq 0$ we obtain the estimates

$$\sum_{a\in\mathbb{N}} \frac{P(a)}{m^a} \ll_P \frac{1}{m}, \sum_{\substack{a\in\mathbb{N}\\ m^a>x}} \frac{1}{m^a} \ll \frac{1}{x}. \tag{2.6}$$

From [17, Corollary 1.15] we get

$$\sum_{s\leq x} \frac{1}{s} = \log x + O(1) \tag{2.7}$$

We will also make frequent use of the Brun-Titchmarsh inequality [17, Theorem 3.9] which says for all $n \leq t$,

$$\pi(t;n,a) \ll \frac{t}{\phi(n)\log(t/n)}. \tag{2.8}$$

By partial summation on (2.8) we can obtain

$$\sum_{\substack{p\leq t\\ p\in\mathcal{P}_n}} \frac{1}{p} \ll \frac{\log\log t}{\phi(n)}. \tag{2.9}$$

Whenever $n/\phi(n)$ is bounded, as it will be whenever n is a prime, prime power or a product of two prime powers, we can replace (2.9) with

$$\sum_{\substack{p\leq t\\ p\in\mathcal{P}_n}} \frac{1}{p} \leq \frac{c\log\log t}{n} \tag{2.10}$$

for some absolute constant c. We include the c because occasionally we require an inequality as opposed to an estimate. From [18, Theorem 1] we obtain the asymptotic

$$\sum_{\substack{p\in\mathcal{P}_n\\ p\leq t}} \frac{1}{p} = \frac{\log\log t}{\phi(n)} + O\left(\frac{\log n}{\phi(n)}\right). \tag{2.11}$$

Equation (2.11) easily implies

$$\sum_{\substack{p\in\mathcal{P}_n\\ p\leq t}} \frac{1}{p-1} = \frac{\log\log t}{\phi(n)} + O\left(\frac{\log n}{\phi(n)}\right), \tag{2.12}$$

since the difference is

$$\sum_{\substack{p \in \mathcal{P}_n \\ p \leq t}} \frac{1}{p(p-1)} \leq \sum_{m=1}^{\infty} \frac{1}{mn(mn+1)} < \frac{1}{n^2} \sum_{m=1}^{\infty} \frac{1}{m^2} \ll \frac{1}{n^2}.$$

The Bombieri–Vinogradov Theorem [7, Chapter 28] implies

$$\sum_{n \leq Q} \max_{y \leq x} \left| \pi(y; n, 1) - \frac{\mathrm{li}(y)}{\phi(m)} \right| \ll x(\log x)^{-A} \tag{2.13}$$

with $Q \leq x^{1/2}(\log x)^{-B}$ for any $A > 0$ and $B = B(A)$. We will use this repeatedly in Chapter 3 with $Q = x^{1/3}$. We also often use the Cauchy–Schwarz inequality in the following form. If $f(n)$ and $g(n)$ are arithmetic functions, then for any $t \geq 1$,

$$\left| \sum_{n \leq t} f(n) g(n) \right|^2 \leq \sum_{n \leq t} |f(n)|^2 \sum_{n \leq t} |g(n)|^2. \tag{2.14}$$

2.3 Early Results

In Chapters 3 and 5 we will require the following technical lemma.

Lemma 2.2. *Fix a prime q and positive integers k, α. The number of $n \leq x$ such that there exists $p, q_1, \ldots, q_{k-1}$ satisfying $q^\alpha \mid q_{k-1} - 1, q_{k-1} \mid q_{k-2} - 1, \ldots, q_1 \mid p - 1$ and $p \mid n$ is at most*

$$\frac{x(cy)^k}{q^\alpha}$$

for some absolute constant c.

Proof. By repeated uses of Equation (2.10), the number of such n is bounded by

$$
\begin{aligned}
&\sum_{n\le x}\sum_{p|n}\sum_{q_1|p-1}\cdots\sum_{q_{k-1}|q_{k-2}-1}\sum_{q^\alpha|q_{k-1}-1} 1 \\
&\qquad = \sum_{q_{k-1}\equiv 1 \pmod{q^\alpha}}\ \sum_{q_{k-2}\equiv 1 \pmod{q_{k-1}}}\cdots\sum_{p\equiv 1 \pmod{q_1}}\ \sum_{\substack{n\le x\\ n\equiv 0 \pmod p}} 1 \\
&\qquad \le \sum_{q_{k-1}\equiv 1 \pmod{q^\alpha}}\ \sum_{q_{k-2}\equiv 1 \pmod{q_{k-1}}}\cdots\sum_{p\equiv 1 \pmod{q_1}} \frac{x}{p} \\
&\qquad \le \sum_{q_{k-1}\equiv 1 \pmod{q^\alpha}}\ \sum_{q_{k-2}\equiv 1 \pmod{q_{k-1}}}\cdots\sum_{q_1\equiv 1 \pmod{q_2}} \frac{xcy}{q_1} \\
&\qquad \le \cdots \le \sum_{q_{k-1}\equiv 1 \pmod{q^\alpha}} \frac{x(cy)^{k-1}}{q_{k-1}} \\
&\qquad \le \frac{x(cy)^k}{q^\alpha}.
\end{aligned}
$$

□

In our proofs of Propositions 3.13 and 3.14 we will see that $M_1(x)$ and $M_2(x)$ will reduce to summations involving $\pi(x;p,1)$. We will be using some sieve techniques to bound these sums and those will require some bounds on sums on multiplicative functions involving $\phi(m)$. The following involves the estimation of the latter sums.

Lemma 2.3. *For any non-negative integer L we have*

$$\sum_{m\le t}\frac{m^L}{\phi(m)^{L+1}} \ll_L \log t. \tag{2.15}$$

Proof. If $f(n)$ is a non-negative multiplicative function, we know that

$$\sum_{n\le t} f(n) \le \prod_{p\le t}\sum_{r=0}^{\infty} f(p^r). \tag{2.16}$$

Applying (2.16) with $\frac{n^L}{\phi(n)^{L+1}}$ yields

$$\begin{aligned}
\sum_{m\le t}\frac{m^L}{\phi(m)^{L+1}} &\le \prod_{p\le t}\left(1+\sum_{r=1}^{\infty}\frac{p^{rL}}{(p^r-p^{r-1})^{L+1}}\right)\\
&= \prod_{p\le t}\left(1+\sum_{r=1}^{\infty}\frac{p^{L-r+1}}{(p-1)^{L+1}}\right)\\
&= \prod_{p\le t}\left(1+\frac{1}{(p-1)^{L+1}}\frac{p^L}{1-\frac{1}{p}}\right)\\
&= \prod_{p\le t}\left(1+\frac{p^{L+1}}{(p-1)^{L+2}}\right)\\
&\le \exp\left(\sum_{p\le t}\log\left(1+\frac{p^{L+1}}{(p-1)^{L+2}}\right)\right)\\
&= \exp\left(\sum_{p\le t}\left(\frac{p^{L+1}}{(p-1)^{L+2}}+O_L\left(\frac{1}{p^2}\right)\right)\right)\\
&= \exp\left(\sum_{p\le t}\left(\frac{1}{p}+O_L\left(\frac{1}{p^2}\right)\right)\right)\\
&\ll_L \log t
\end{aligned}$$

using (2.3). □

Lemma 2.4. *Let L be a nonnegative integer and γ a positive real number. Given a positive integer $C \le t^\gamma$ and non-negative integer L we have*

$$\sum_{m\le t}\frac{(Cm+1)^L}{\phi(Cm+1)^L\phi(m)} \ll_{L,\gamma} \log t. \tag{2.17}$$

Proof. It will suffice to show

$$\sum_{m\le t}\frac{(Cm+1)^{2L-1}}{\phi(Cm+1)^{2L}} \ll_{L,\gamma} \frac{\log t}{C} \tag{2.18}$$

as then by Cauchy–Schwarz (2.14) we can get that

$$\begin{aligned}\left(\sum_{m\le t}\frac{(Cm+1)^L}{\phi(Cm+1)^L\phi(m)}\right)^2 &\le \sum_{m\le t}\frac{(Cm+1)^{2L-1}}{\phi(Cm+1)^{2L}}\sum_{m\le t}\frac{(Cm+1)}{\phi(m)^2}\\ &\ll_{L,\gamma}\left(\frac{\log t}{C}\right)C\log t\\ &\ll_{L,\gamma}\log^2 t\end{aligned}$$

by using Lemma 2.3 and (2.18). Let

$$G(t)=\sum_{m\le t}\frac{(Cm+1)^{2L}}{\phi(Cm+1)^{2L}}.$$

We show Equation (2.18) by first showing $G(t)\ll_{L,\gamma} t$. This implies Equation (2.18) since

$$\begin{aligned}\sum_{m\le t}\frac{(Cm+1)^{2L-1}}{\phi(Cm+1)^{2L}} &< \frac{1}{C}\sum_{m\le t}\frac{(Cm+1)^{2L}}{m\phi(Cm+1)^{2L}}\\ &= \frac{1}{C}\int_{1^-}^{t}\frac{d(G(u))}{u}\\ &= \frac{1}{C}\left(\frac{G(t)}{t}+\int_{1^-}^{t}\frac{G(u)}{u^2}\right)\\ &\ll_{L,\gamma}\frac{1}{C}\left(1+\int_{1^-}^{t}\frac{1}{u}\right)\\ &\ll_{L,\gamma}\frac{1}{C}(\log t)\end{aligned}$$

To show Equation (2.18) we start by defining $s(n)$ to be the multiplicative function defined by

$$\frac{n^{2L}}{\phi(n)^{2L}}=1*s=\sum_{d|n}s(d).$$

Testing at prime powers, we can easily see that

$$s(1)=1, s(p)=\left(1-\frac{1}{p}\right)^{-2L}-1 \text{ and } s(p^k)=0 \text{ for all } k\ge 2.$$

Hence

$$\begin{aligned}
\sum_{m\le t}\frac{(Cm+1)^{2L}}{\phi(Cm+1)^{2L}} &= \sum_{\substack{n\le Ct+1\\ n\equiv 1 \pmod{C}}}\frac{n^{2L}}{\phi(n)^{2L}}\\
&= \sum_{\substack{n\le Ct+1\\ n\equiv 1 \pmod{C}}}\sum_{d|n} s(d)\\
&= \sum_{d\le Ct+1} s(d) \sum_{\substack{n\le Ct+1\\ d|n\\ n\equiv 1 \pmod{C}}} 1\\
&= \sum_{d\le Ct+1} s(d)\left(\frac{t}{d}+O(1)\right)\\
&= t\sum_{d\le Ct+1}\frac{s(d)}{d}+O\left(\sum_{d\le Ct+1} s(d)\right).
\end{aligned}$$

We require some estimates on $s(d)$. For the sum of the multiplicative function $s(d)/d$,

$$\begin{aligned}
\sum_{d\le Ct+1}\frac{s(d)}{d} &\le \prod_{p\le Ct+1}\left(1+\frac{(1-1/p)^{-2L}-1}{p}\right)\\
&\le \prod_{p\le Ct+1}\left(1+O_L\left(\frac{1}{p^2}\right)\right)\\
&= \exp\left(\sum_{p\le Ct+1}\log\left(1+O_L\left(\frac{1}{p^2}\right)\right)\right)\\
&= \exp\left(\sum_{p\le Ct+1}O_L\left(\frac{1}{p^2}\right)\right)\\
&= \exp(O_L(1))\\
&\ll_L 1.
\end{aligned}$$

For the sum of $s(d)$,

$$\begin{aligned}
\sum_{d \le Ct+1} s(d) &\le \prod_{p \le Ct+1} \left(1 + (1-1/p)^{-2L} - 1\right) \\
&= \prod_{p \le Ct+1} (1-1/p)^{-2L} \\
&= \exp\left(\sum_{p \le Ct+1} \log\left(1 + O_L\left(\frac{1}{p}\right)\right)\right) \\
&= \exp\left(\sum_{p \le Ct+1} O_L\left(\frac{1}{p}\right)\right) \\
&= \exp\big(O_L(\log\log(Ct+1))\big) \\
&\ll \exp\big(O_{L,\gamma}(\log\log t)\big) \\
&\ll (\log t)^{O_{L,\gamma}(1)} \\
&\ll_{L,\gamma} t
\end{aligned}$$

Therefore

$$G(t) = t \sum_{d \le Ct+1} \frac{s(d)}{d} + O\Bigg(\sum_{d \le Ct+1} s(d)\Bigg) \ll_{L,\gamma} t$$

as needed. □

The following sum seems more complicated. However, we can handle it using repeated applications of Lemma 2.4.

Lemma 2.5. *For positive integers $C_1, C_2, \dots, C_r \le t^\gamma$ and non-negative integers $L_1, L_2, \dots, L_r$ we have*

$$\sum_{m \le t} \frac{(C_1 m+1)^{L_1}(C_2 m+1)^{L_2} \dots (C_r m+1)^{L_r}}{\phi(C_1 m+1)^{L_1}\phi(C_2 m+1)^{L_2} \dots \phi(C_r m+1)^{L_r}\phi(m)} \ll_{L_1,\dots,L_r,\gamma} \log t. \tag{2.19}$$

Proof. We proceed by induction. The case $r = 1$ is covered by Lemma 2.4. Suppose

$$\sum_{m \le t} \frac{(C_1 m+1)^{L_1}(C_2 m+1)^{L_2} ... (C_r m+1)^{L_r}}{\phi(C_1 m+1)^{L_1}\phi(C_2 m+1)^{L_2} \dots \phi(C_r m+1)^{L_r}\phi(m)} \ll_{L_1,\dots,L_r,\gamma} \log t.$$

By Cauchy–Schwarz (2.14), we get that

$$\begin{aligned}
&\left(\sum_{m\le t}\frac{(C_1m+1)^{L_1}(C_2m+1)^{L_2}\dots(C_{r+1}m+1)^{L_{r+1}}}{\phi(C_1m+1)^{L_1}\phi(C_2m+1)^{L_2}\dots\phi(C_{r+1}m+1)^{L_{r+1}}\phi(m)}\right)^2\\
&\qquad\le\sum_{m\le t}\frac{(C_1m+1)^{2L_1}(C_2m+1)^{2L_2}\dots(C_rm+1)^{2L_r}}{\phi(C_1m+1)^{2L_1}\phi(C_2m+1)^{2L_2}\dots\phi(C_rm+1)^{2L_r}\phi(m)}\\
&\qquad\qquad\cdot\sum_{m\le t}\frac{(C_{r+1}m+1)^{2L_{r+1}}}{\phi(C_{r+1}m+1)^{2L_{r+1}}\phi(m)}\\
&\qquad\ll_{L_1,\dots,L_{r+1},\gamma}\log^2 t
\end{aligned}$$

by the induction hypothesis and Lemma 2.4, completing the proof. □

Now here is the lemma that we will use in Section 3.7.

Lemma 2.6. *For positive integers $C_1, C_2, ..., C_r \le t^\gamma$ and non-negative integers $L_1, L_2, ..., L_r, L$ we have*

$$\sum_{m\le t}\frac{(C_1m+1)^{L_1}(C_2m+1)^{L_2}...(C_rm+1)^{L_r}m^{L-1}}{\phi(C_1m+1)^{L_1}\phi(C_2m+1)^{L_2}\dots\phi(C_rm+1)^{L_r}\phi(m)^L}\ll_{L_1,\dots,L_r,L,\gamma}\log t. \tag{2.20}$$

Proof. Once again we'll use Cauchy–Schwarz (2.14) and the previous lemmas.

$$\begin{aligned}
&\left(\sum_{m\le t}\frac{(C_1m+1)^{L_1}(C_2m+1)^{L_2}\dots(C_rm+1)^{L_r}m^{L-1}}{\phi(C_1m+1)^{L_1}\phi(C_2m+1)^{L_2}\dots\phi(C_rm+1)^{L_r}\phi(m)^L}\right)^2\\
&\qquad\le\sum_{m\le t}\frac{(C_1m+1)^{2L_1}(C_2m+1)^{2L_2}\dots(C_rm+1)^{2L_r}}{\phi(C_1m+1)^{2L_1}\phi(C_2m+1)^{2L_2}\dots\phi(C_rm+1)^{2L_r}\phi(m)}\\
&\qquad\qquad\cdot\sum_{m\le t}\frac{m^{2L-2}}{\phi(m)^{2L-1}}\\
&\qquad\ll_{L_1,\dots,L_r,L,\gamma}\log^2 t
\end{aligned}$$

by Lemmas 2.3 and 2.5. □

Chapter 3

Iterated Carmichael Lambda Function

3.1 Required Propositions and Proof of Theorem 1.4

As mentioned in Chapter 1, the main contribution to $\log(n/\lambda_k(n))$ will come from $\log(\phi_k(n)/\lambda_k(n))$. Estimating this term will involve a summation over prime powers which divide each of $\phi_k(n)$ and $\lambda_k(n)$. It turns out that the largest contribution to this term will come from small primes which divide $\phi_k(n)$. By small, we mean primes $q \leq (\log\log x)^k = y^k$. We will split the sum into small primes and large primes $q > y^k$. To prove Theorem 1.4 we will require the following propositions. The first summations deal with the large primes which divide $\phi_k(n)$ and the second involves the large primes whose prime powers divide $\phi_k(n)$. We will show that the contribution of these primes to the main sum is small and hence it will end up as part of the error term.

Proposition 3.1.

$$\sum_{\substack{q>y^k \\ \nu_q(\phi_k(n))=1}} (\nu_q(\phi_k(n)) - \nu_q(\lambda_k(n))) \log q \ll y^k \psi(x)$$

for almost all $n \leq x$.

Proposition 3.2.

$$\sum_{\substack{q>y^k \\ \nu_q(\phi_k(n))\geq 2}} \nu_q(\phi_k(n)) \log q \ll y^k \psi(x)$$

for almost all $n \leq x$.

Since the main contribution will come from small primes dividing $\phi_k(n)$, the next proposition will show that the contribution of small primes dividing $\lambda_k(n)$ to the main sum can also be merged into the error term.

Proposition 3.3.

$$\sum_{q \le y^k} \nu_q(\lambda_k(n)) \log q \ll y^k \psi(x)$$

for almost all $n \le x$.

That will leave us with the contribution of small primes dividing $\phi_k(n)$. Recall the following definition of an additive function.

Definition 3.4. An arithmetic function $f(n)$ is called *additive* if for all $(m,n) = 1, f(mn) = f(m) + f(n)$. If in addition $f(p^k) = f(p)$ for all $k \ge 1$, then $f(n)$ is called *strongly additive*.

We will use a strongly additive function to approximate the remaining sum. Let $h_k(n)$ be the strongly additive function defined by

$$h_k(n) = \sum_{p_1 | n} \sum_{p_2 | p_1 - 1} \cdots \sum_{p_k | p_{k-1} - 1} \sum_{q \le y^k} \nu_q(p_k - 1) \log q.$$

The following proposition shows that the difference between the sum involving the small primes dividing $\phi_k(n)$ and the term $h_k(n)$ is small.

Proposition 3.5.

$$\sum_{q \le y^k} \nu_q(\phi_k(n)) \log q = h_k(n) + O(y^{k-1} \log y \cdot \psi(x))$$

for almost all $n \le x$.

That leaves us with $\log(\phi_k(n)/\lambda_k(n))$ being approximated by $h_k(n)$. The last proposition will obtain an asymptotic formula for $h_k(n)$. From there we will have enough armoury to tackle Theorem 1.4. Since $h_k(n)$ is strongly additive, we use the Turan–Kubilius inequality (Corollary A.2) which will show the final proposition.

Proposition 3.6.

$$h_k(n) = \frac{1}{(k-1)!} y^k \log y + O(y^k)$$

for almost all $n \le x$.

Proof of Theorem 1.4. We start by breaking down the function $\log(n/\lambda_k(n))$.

$$\begin{aligned}\log\left(\frac{n}{\lambda_k(n)}\right) &= \log\left(\frac{n}{\phi(n)}\right) + \log\left(\frac{\phi(n)}{\phi_2(n)}\right) \\ &\qquad + \cdots + \log\left(\frac{\phi_{k-1}(n)}{\phi_k(n)}\right) + \log\left(\frac{\phi_k(n)}{\lambda_k(n)}\right).\end{aligned} \tag{3.1}$$

Using the lower bound $\phi(m) \gg m/\log\log m$ from [17, Theorem 2.3] we have that

$$\log\left(\frac{n}{\phi(n)}\right) + \log\left(\frac{\phi(n)}{\phi_2(n)}\right) + \cdots + \log\left(\frac{\phi_{k-1}(n)}{\phi_k(n)}\right) \ll \log\log\log n. \tag{3.2}$$

Inserting equation (3.2) into equation (3.1) yields

$$\log\left(\frac{n}{\lambda_k(n)}\right) = \log\left(\frac{\phi_k(n)}{\lambda_k(n)}\right) + O(\log\log\log n).$$

In fact we could have used a more precise estimate for $\phi_i(n)/\phi_{i+1}(n)$ for $i \geq 1$ which can be found in [8] but the one we used is good enough. Next we break down the remaining term into summations. We will break it up into small primes and large primes.

$$\begin{aligned}\log\left(\frac{\phi_k(n)}{\lambda_k(n)}\right) &= \sum_{q>y^k} (\nu_q(\phi_k(n)) - \nu_q(\lambda_k(n)))\log q \\ &\qquad + \sum_{q\leq y^k} (\nu_q(\phi_k(n)) - \nu_q(\lambda_k(n)))\log q \\ &= \sum_{\substack{q>y^k \\ \nu_q(\phi_k(n))=1}} (\nu_q(\phi_k(n)) - \nu_q(\lambda_k(n)))\log q \\ &\qquad + \sum_{\substack{q>y^k \\ \nu_q(\phi_k(n))\geq 2}} (\nu_q(\phi_k(n)) - \nu_q(\lambda_k(n)))\log q \\ &\qquad + \sum_{q\leq y^k} \nu_q(\phi_k(n))\log q - \sum_{q\leq y^k} \nu_q(\lambda_k(n))\log q.\end{aligned}$$

Note that if $a \mid b$, then $\lambda(a) \mid \phi(b)$ since $\lambda(a) \mid \phi(a) \mid \phi(ma)$ for any integer m. This quickly implies that $\lambda_k(n)$ always divides $\phi_k(n)$ for all k and so we get

$$0 \leq \sum_{\substack{q>y^k \\ \nu_q(\phi_k(n))\geq 2}} (\nu_q(\phi_k(n)) - \nu_q(\lambda_k(n)))\log q \leq \sum_{\substack{q>y^k \\ \nu_q(\phi_k(n))\geq 2}} (\nu_q(\phi_k(n))\log q.$$

Using Propositions 3.1,3.2,3.3 and 3.5 we get

$$\log\left(\frac{n}{\lambda_k(n)}\right) = h_k(n) + O\Big(y^k\psi(x)\Big)$$

for almost all $n \le x$. Finally by using Proposition 3.6 we get

$$\log\left(\frac{n}{\lambda_k(n)}\right) = \frac{1}{(k-1)!}y^k \log y + O\Big(y^k\psi(x)\Big)$$

for almost all $n \le x$, finishing the proof of Theorem 1.4. □

3.2 Prime Power Divisors of $\phi_k(n)$

For various reasons thoughout this paper, we are concerned with the number of $n \le x$ such that q^a can divide $\phi_k(n)$. We will analyze a few of those situations here:

Case 1: $q^2 \mid n$. Clearly the number of such n is at most $\frac{x}{q^2}$.

Case 2: There exists $p_1 \in \mathcal{P}_{q^2}, p_2 \in \mathcal{P}_{p_1}, p_3 \in \mathcal{P}_{p_2}, ..., p_l \in \mathcal{P}_{p_{l-1}}$ where $p_l \mid n$. By using Lemma 2.2 we know the number of such $n \le x$ is $O_l(xy^l/q^2)$.

Cases 1 and 2 deal with any case where $p \in \mathcal{P}_{q^2}$, we are just left with the possibilities not containing any powers of q. Unfortunately these cases still allow for many possibilities which we will display in an array. There are lots of ways for a prime power q^a to divide $\phi_k(n)$. We now define various sets of primes that are involved in generating these powers of q, and we will eventually sum over all possibilities for these sets of primes. The set $\mathcal{L}_{h,i}$ will denote a finite set of primes. To begin, the set $\mathcal{L}_{1,2}$ will be an arbitrary finite set of primes in $\mathcal{P}_q$ and let $\mathcal{L}_{1,1}$ be empty. That is:

Case 3:

Level (1,2)

$$\mathcal{L}_{1,2} \subseteq \mathcal{P}_q.$$

Level (2,1) (Obtaining the primes in the previous level)

$\mathcal{L}_{2,1}$ is any set of primes with the property that for all $p \in \mathcal{L}_{1,1} \cup \mathcal{L}_{1,2}$, there exists a unique prime $r \in \mathcal{L}_{2,1}$ such that $r \in \mathcal{P}_p$. In other words p will divide $\phi(r)$ and hence the primes in $\mathcal{L}_{2,1}$ will create the primes in $\mathcal{L}_{1,1} \cup \mathcal{L}_{1,2}$.

Level (2,2) (New primes in $\mathcal{P}_q$)

$$\mathcal{L}_{2,2} \subseteq \mathcal{P}_q.$$

In general for all $1 < h \leq k$ we have for all $p \in \mathcal{L}_{h-1,1} \cup \mathcal{L}_{h-1,2}$ there exists a unique prime $r \in \mathcal{L}_{h,1}$ such that $r \in \mathcal{P}_p, \mathcal{L}_{h,2}$ is an arbitrary subset of $\mathcal{P}_q$, and

$$r \in \mathcal{L}_{k,1} \cup \mathcal{L}_{k,2} \Rightarrow r \mid n.$$

Some description of the terms are in order including some helpful definitions.

Definition 3.7. An incarnation I of Case 3 is some specified description of how the primes in a lower level create the primes in the level directly above.

For example, for $k = 3$, an incarnation I for which $q^4 \mid \phi_3(n)$ would be $s_1, s_2, s_3, r_3, r_4 \in \mathcal{P}_q$ where $r_1 \in \mathcal{P}_{s_1}, r_2 \in \mathcal{P}_{s_2 s_3}, p_1 \in \mathcal{P}_{r_1 r_2}, p_2 \in \mathcal{P}_{r_3 r_4}$, with $p_1 p_2 \mid n$.

Definition 3.8. An subincarnation of I is an incarnation with added conditions. In other words if J is a subincarnation of I and an integer n satisfies incarnation J, then it will also satisfy incarnation I.

For example, I is a subincarnation of the incarnation $s_1, s_3, r_3, r_4 \in \mathcal{P}_q$ where $r_1 \in \mathcal{P}_{s_1}, r_2 \in \mathcal{P}_{s_3}, p_1 \in \mathcal{P}_{r_1 r_2}, p_2 \in \mathcal{P}_{r_3 r_4}$, with $p_1 p_2 \mid n$.

Let p be a prime in $\mathcal{L}_{h,i}$ which we need to divide $\phi_{k-h+1}(n)$. The definition of $\mathcal{L}_{h,i}$ ensures that there is a unique prime r dividing $\phi_{k-h}(n)$ for which $p \mid r - 1$. The primes in levels $(k, 1), (k, 2)$ dividing n are for the base case of the recursion, so that each prime divides $\phi_0(n) = n$. When $i = 2$ we are introducing new primes to get greater powers of q in $\phi_k(n)$. Note that it's not necessary to have any primes on the levels $(h, 2)$. In fact the "worst case scenario" that we will see has no primes on these except Level (1,2).

Now that we've described the way to get $q^a \mid \phi_k(n)$, what is our exponent a? Let $m_{h,i} = \#\mathcal{L}_{h,i}$. From the recursion above we can see that $q^{m_{k,2}} \mid \phi(n)$ and so do the primes in $\mathcal{L}_{k-1,1}$. For the second iteration of ϕ, $q^{m_{k,2}-1+m_{k-1,2}} \mid \phi_2(n)$ and so do the primes in $\mathcal{L}_{k-2,1}$. Hence the power of q which divides $\phi_k(n)$ is

$$\max_{1 \leq j \leq k} (m_{1,1} + \sum_{2 \leq h \leq j} (m_{h,2} - 1)) \tag{3.3}$$

where the sum can be empty if there are no primes in the second level $(j, 2)$ or there are not enough to survive, i.e. $m_{j,2} < j-1$ and hence $q \nmid \phi_j(\prod_{\mathcal{L}_{j,2}} p)$. Without loss of generality, we can assume the former, since the later is a subincarnation of the former.

Now we'll introduce some notation to be used in future propositions. For any fixed incarnation of Case 3, let M be the total number of primes, N be the total number of new primes introduced at the levels $(h, 2)$ and H be the maximum necessary level $(h, 2)$. Specifically

$$M = \sum_h (m_{h,1} + m_{h,2}) \quad N = \sum_{h \le H} m_{h,2}$$

and H yields the maximum value in (3.3). Note that under this notation, $q^{N-H+1} \mid \phi_k(n)$. For example, in the incarnation I above,

$$\mathcal{L}_{1,2} = \{s_1, s_2, s_3\}, \mathcal{L}_{2,1} = \{r_1, r_2\}, \mathcal{L}_{2,2} = \{r_3, r_4\}, \mathcal{L}_{3,1} = \{p_1, p_2\}, \mathcal{L}_{3,2} = \emptyset$$

as well as

$$m_{1,2} = 3, m_{2,1} = 2, m_{2,2} = 2, m_{3,1} = 2, m_{3,2} = 0.$$

Hence $M = 9, N = 5, H = 2$ and so the power of q which divides $\phi_3(n)$ is $5 - 2 + 1 = 4$ as expected.

Now that we've described Case 3, how many possible n are in that case?

Lemma 3.9. *The number of $n \le x$ satisfying any incarnation of Case 3 is*

$$O\left(c^M \frac{xy^M}{q^N}\right)$$

where c is the constant from equation (2.10)*.*

Proof. Let $\mathcal{L}_h = \mathcal{L}_{h,1} \cup \mathcal{L}_{h,2}$. We use Brun-Titchmarsh (2.10) for all the primes at each level of Case 3, so the number of n is

$$\begin{aligned}\sum_{n \le x} \sum_{p_1 \in \mathcal{L}_1} \sum_{p_2 \in \mathcal{L}_2} \cdots \sum_{p_k \in \mathcal{L}_k} 1 &= \sum_{p_1 \in \mathcal{L}_1} \sum_{p_2 \in \mathcal{L}_2} \cdots \sum_{p_k \in \mathcal{L}_k} \sum_{\substack{p_k \mid n \\ n \le x}} 1 \\ &\ll \sum_{p_1 \in \mathcal{L}_1} \sum_{p_2 \in \mathcal{L}_2} \cdots \sum_{p_k \in \mathcal{L}_k} \frac{x}{\prod_{p_k \in \mathcal{L}_k} p_k}.\end{aligned}$$

Note that we have repeatedly counted the same primes in the sum as we can reorder the primes in each level. It won't be important here, but will need to be more carefully addressed later. Since the primes in level $(k, 1)$ gave us some $p_k \in \mathcal{P}_{p_{k-1}}$ for all the primes in $\mathcal{L}_{k-1}$, and for $p \in \mathcal{L}_{k,2}$ we have $p \in \mathcal{P}_q$. By Brun–Titchmarsh (2.10) we get that the above sum is

$$\ll \sum_{p_1 \in \mathcal{L}_1} \sum_{p_2 \in \mathcal{L}_2} \cdots \sum_{p_{k-1} \in \mathcal{L}_{k-1}} \frac{x(cy)^{m_{k,1}+m_{k,2}}}{\prod_{p_{k-1} \in \mathcal{L}_{k-1}} p_{k-1} q^{m_{k,2}}}.$$

Once again we get $m_{k-1,1} + m_{k-1,2}$ new applications of Brun-Titchmarsh giving the new primes in level $k-2$ as well as $m_{k-1,2}$ new powers of q. Continuing along in this manner we get:

$$\begin{aligned}
&\ll \sum_{p_1 \in \mathcal{L}_1} \frac{x(cy)^{\sum_{2\le i\le k}(m_{i,1}+m_{i,2})}}{\prod_{p_1\in\mathcal{L}_1} p_1 q^{\sum_{2\le i\le k} m_{i,2}}} \\
&\ll \frac{x(cy)^{\sum_{1\le i\le k}(m_{i,1}+m_{i,2})}}{q^{\sum_{1\le i\le k} m_{i,2}}} = \frac{x(cy)^M}{q^N}.
\end{aligned}$$

□

The last thing we'll consider in this section about the ways to obtain $\phi_k(n)$ is to determine the number of possible incarnations of Case 3. We note that there are lots of incarnations which are subincarnations of others. We will develop a concept of minimality.

Definition 3.10. An incarnation of Case 3 is minimal if it does not contain any strings of $p_1 \in \mathcal{P}_{p_2}, p_2 \in \mathcal{P}_{p_3} \dots p_{k-1} \in \mathcal{P}_{p_k}$ where $p_k \mid n$.

Note that any incarnation of Case 3 is a subincarnation of a minimal one. We now use this concept to show the number of necessary incarnations of Case 3 is small.

3.3 Large Primes Dividing $\phi_k(n)$

In this section we will prove the two propositions dealing with q being large. We'll start with the proposition where $\nu_q(\phi_k(n)) = 1$.

Proof of Proposition 3.1. It suffices to show

$$\sum_{n\le x} \sum_{\substack{q>y^k \\ \nu_q(\phi_k(n))=1}} (\nu_q(\phi_k(n)) - \nu_q(\lambda_k(n))) \log q \ll xy^k$$

as then there are at most $O\big(\frac{xy^k}{y^k\psi(x)}\big) = O\big(\frac{x}{\psi(x)}\big)$ such n where the bound for the sum in Proposition 3.1 fails to hold. We examine the cases where $\nu_q(\phi_k(n)) = 1$. Using the notation in Lemma 3.9 we have two subcases for Case 3, whether $N = 1$ or $N > 1$.

Suppose $N = 1$, then $H = 1$, $m_{1,2} = 1$ and $m_{h,2} = 0$ for $1 < h \le k$. Since $m_{h,1} \le m_{h-1,1} + m_{h-1,2}$ we get $m_{h,1} \le 1$ for all $1 \le h \le k$. Hence $m_{h,1} = 1$ for all $h \le k$. Therefore we are left with the case

$$p_1 \in \mathcal{P}_q, p_2 \in \mathcal{P}_{p_1}, p_3 \in \mathcal{P}_{p_2}, \ldots, p_k \in \mathcal{P}_{p_{k-1}}$$

where $p_k \mid n$. However in this case we also get $\nu_q(\lambda_k(n))) = 1$ giving us no additions to our sum.

Suppose $N > 1$, then by repeatedly using $m_{h,1} \leq m_{h-1,1} + m_{h-1,2}$ we have $M = \sum_h (m_{h,1} + m_{h,2}) \leq k \sum_h m_{h,2} = kN$. The number of cases we get are

$$O\left(c^M \frac{xy^M}{q^N}\right) \ll \frac{c^M xy^{kN}}{q^N} \ll \frac{c^M xy^{2k}}{q^2}$$

since $y > q^k$. Since $v_q(\phi_k(n)) = N - H + 1$ and $H \leq k$, we conclude $N \leq k$ implying that $M \leq k^2$. Hence c^M is bounded as a function of k. Also since M is bounded in terms of k, there are $O_k(1)$ possible incarnations of Case 3, and the bound already absorbs the possiblities from Cases 1 and 2. Hence we have

$$\begin{aligned} \sum_{q > y^k} \sum_{\substack{n \leq x \\ \nu_q(\phi_k(n))=1}} (\nu_q(\phi_k(n)) - \nu_q(\lambda_k(n))) \log q &\leq \sum_{q > y^k} \sum_{\substack{n \leq x \\ \nu_q(\phi_k(n))=1 \\ N>1}} \log q \\ &\ll \sum_{q > y^k} \frac{xy^{2k} \log q}{q^2} \\ &\ll xy^k \end{aligned}$$

by (2.4). $\square$

We turn our attention to $v_q(\phi_k(n)) > 1$. We have to be more careful here since we can't guarantee that the number of incarnations of Case 3 is $O_k(1)$. We'll start by proving a lemma which can eliminate a lot of those cases.

Lemma 3.11. *Let $q > y^k$ and $S_q = S_q(x)$ consist of all $n \leq x$ such that Case 1,2 or Case 3 where $M \leq k(N-1)$ occurs. Then*

$$\#S_q \ll \frac{xy^k}{q^2}.$$

Proof. There are clearly $O_k(1)$ incarnations of Cases 1 and 2 and each yield at most $O(xy^k/q^2)$ such n. By Lemma 3.9 for each incarnation of Case 3, we get at most

$$O\left(\frac{c^M xy^M}{q^N}\right) \ll \frac{c^M xy^k}{q^2}$$

such n since $M \leq k(N-1)$ and $q > y^k$. It remains to show we only require $O_k(1)$ such incarnations. Suppose n satisfies an incarnation with $M \leq k(N-1)$. Then it also satisfies a minimal incarnation with $M \leq k(N-1)$ since removing a string of $p_1 \in \mathcal{P}_{p_2}, p_2 \in \mathcal{P}_{p_3} \ldots p_{k-1} \in \mathcal{P}_{p_k}$, would decrease N by 1 and M by k leaving the inequality unchanged. Secondly we can assume that n also satisfies an incarnation where $k(N-2) < M \leq k(N-1)$ since we can keep eliminating primes in the $\mathcal{L}_{i,2}$, which decrease N by 1, but M by at most k. This must eventually produce an incarnation where $k(N-2) < M \leq k(N-1)$ since if we eliminate all primes in the $\mathcal{L}_{i,2}$ but 1, then $M > k(N-1)$. Also note that the condition $m_{h,1} \leq m_{h-1,1} + m_{h-1,2}$ forces $M \leq kN$. If M is bounded between $k(N-2)$ and kN and the incarnation is minimal, we get that N is bounded by $2k$ since eliminating a prime in $\mathcal{L}_{i,2}$ can only shrink M by at most $k-1$ since our incarnation is minimal.

Therefore n satisifies an incarnation where N and hence M are bounded functions of k. Since there are only $O_k(1)$ such incarnations, we get our result, noting that c^M can be absorbed into the constant as well. □

Proof of Proposition 3.2. Let $S = S(x) = \bigcup_{q>y^k} S_q$. Using Lemma 3.11 we have

$$\#S \leq \sum_{q>y^k} \#S_q \ll \sum_{q>y^k} \frac{xy^k}{q^2} \ll xy^k \sum_{q>y^k} \frac{1}{q^2} \ll \frac{xy^k}{\log(y^k)y^k} \ll \frac{x}{\psi(x)}$$

by (2.5). As for the n with $n \notin S$ and $a = \nu_q(\phi_k(n)) > 1$, the only remaining case is that $M > k(N-1)$. Recall that $a = N + H - 1$. If $H = 1$, then $N = m_{1,2} = a$. This implies $m_{2,1} = a-1$ or a, since otherwise for $k \geq 2$,

$$M = \sum_h m_{h,1} \leq a+(k-1)m_{2,1} \leq a+(k-1)(a-2) = k(a-1)-k+2 \leq (k-1)N$$

leading to a contradiction. If $H > 1$, then we again wish to show that $m_{2,1} \geq a-k$.

$$\begin{aligned} M &= \sum_h (m_{h,1} + m_{h,2}) \\ &\leq km_{1,2} + (k-1)\sum_{h>1} m_{h,2} \\ &= m_{1,2} + (k-1)N \\ &= k(N-1) - N + k + m_{1,2} \end{aligned}$$

which implies $m_{1,2} > N - k$ and so $\sum_{h>1} m_{h,2} = N - m_{1,1} < k$. Therefore if $m_{2,1} < a - k$, then

$$\begin{aligned} M &= \sum_h (m_{h,1} + m_{h,2}) \\ &\leq m_{1,2} + (k-1)m_{2,1} + (k-1)\sum_{h>1} m_{h,2} \leq a + (k-1)(a-k-1) + (k-1)(k-1) \\ &= ak - 2k \\ &\leq k(N-1) \end{aligned}$$

as $N > a$ again leading to a contradiction. Hence $m_{2,1} \geq a - k$ and so we conclude

$$\begin{aligned} \sum_{\substack{n \notin S \\ n \leq x}} \sum_{\substack{q > y^k \\ \nu_q(\phi_k(n)) > 1}} (\nu_q(\phi_k(n)) \log q &\leq 2 \sum_{\substack{n \notin S \\ n \leq x}} \sum_{\substack{q > y^k \\ \nu_q(\phi_k(n)) > 1}} (\nu_q(\phi_k(n)) - 1) \log q \\ &\ll \sum_{q > y^k} \log q \sum_{a \geq 2} a \sum_{\substack{n \leq x \\ n \notin S \\ \nu_q(\phi_k(n)) = a}} 1. \end{aligned}$$

Unfortunately, just blindly using the Brun-Titchmarsh inequality in (2.10) won't be good enough as we must sum over all a. Let $g(a,k) = (a-k)!$ if $a \geq k$ or 1 otherwise and note that since we have $m_{1,2} \geq a - k$, we have at least $g(a,k)$ permutations of the same primes. Thus by using Lemma 3.9 we get

$$a \sum_{q > y^k} \log q \sum_{\substack{n \leq x \\ n \notin S \\ \nu_q(\phi_k(n)) = a}} 1 \ll a \frac{x(cy)^M}{q^N g(a,k)} \ll \frac{ac^{k(a+k-1)} x y^{2k}}{q^2 g(a,k)}$$

using the assumption that $q > y^k$ and $M \leq kN \leq k(a+k-1)$. Hence we get that our sum is

$$\begin{aligned} \sum_{\substack{n \notin S \\ n \leq x}} \sum_{\substack{q > y^k \\ \nu_q(\phi_k(n)) > 1}} (\nu_q(\phi_k(n)) \log q &\ll \sum_{q > y^k} \log q \sum_{a \geq 2} \frac{ac^{k(a+k-1)} x y^{2k}}{q^2 g(a,k)} \\ &= x y^{2k} \sum_{q > y^k} \frac{\log q}{q^2} \sum_{a \geq 2} \frac{ac^{k(a+k-1)}}{g(a,k)} \end{aligned}$$

However the latter sum converges to some function depending on k, and so we get

$$\ll xy^{2k} \sum_{q>y^k} \frac{\log q}{q^2} \ll xy^k$$

by (2.4). □

3.4 Small Primes Dividing $\lambda_k(n)$

We now turn our attention to the bound involving $\lambda_k(n)$ in the summand. Just like when we were dealing with the number of cases where $q^a \mid \phi_k(n)$, we will need a lemma to deal with the number of cases where $q^a \mid \lambda_k(n)$. Fortunately this case is much simpler as the only two ways for $q^a \mid \lambda(n)$ is for $q^{a+1} \mid n$ or for there to exist $p \mid n$ with $p \in \mathcal{P}_{q^a}$. Note that these conditions aren't sufficient, but are necessary when $q = 2$.

Lemma 3.12. *The number of positive integers $n \leq x$ for which $q^a \mid \lambda_k(n)$ is $O(\frac{xy^k}{q^a})$.*

Proof. We'll proceed by induction on k. If $k = 1$, then $q^a \mid \lambda(n)$ if $q^{a+1} \mid n$ or $p \in \mathcal{P}_{q^a}$ with $p \mid n$. The number of such n is at most

$$\sum_{\substack{n\leq x\\ q^{a+1}\mid n}} 1 + \sum_{\substack{n\leq x\\ p\in\mathcal{P}_{q^a}\\ p\mid n}} 1 \ll \frac{x}{q^{a+1}} + \sum_{p\in\mathcal{P}_{q^a}} \frac{x}{p} \ll \frac{x}{q^{a+1}} + \frac{xy}{q^a} \ll \frac{xy}{q^a}.$$

using (2.10). Suppose the number of $n \leq x$ for which $q^a \mid \lambda_{k-1}(n)$ is $O(\frac{xy^{k-1}}{q^a})$. If $q^a \mid \lambda_k(n)$, then either $q^{a+1} \mid \lambda_{k-1}(n)$ or $p \in \mathcal{P}_{q^a}$ with $p \mid \lambda_{k-1}(n)$. Hence the number of such n is bounded by

$$\sum_{\substack{n\leq x\\ q^{a+1}\mid\lambda_{k-1}(n)}} 1 + \sum_{\substack{n\leq x\\ p\in\mathcal{P}_{q^a}\\ p\mid\lambda_{k-1}(n)}} 1 \ll \frac{xy^{k-1}}{q^{a+1}} + \sum_{p\in\mathcal{P}_{q^a}} \frac{xy^{k-1}}{p} \ll \frac{xy^{k-1}}{q^{a+1}} + \frac{xy^k}{q^a} \ll \frac{xy^k}{q^a}$$

as needed. □

Proof of Proposition 3.3. Like in the proof of previous propositions, we'll show

$$\sum_{n\leq x}\sum_{q\leq y^k} \nu_q(\lambda_k(n)) \log q \ll xy^k.$$

The left hand side is equal to

$$\sum_{n\le x}\sum_{q\le y^k}\nu_q(\lambda_k(n))\log q = \sum_{n\le x}\sum_{q\le y^k}\log q \sum_{\substack{a\in\mathbb{N}\\ q^a|\lambda_k(n)}} 1$$
$$\le \sum_{n\le x}\sum_{q\le y^k}\log q \sum_{\substack{a\in\mathbb{N}\\ q^a\le y^k}} 1 + \sum_{n\le x}\sum_{q\le y^k}\log q \sum_{\substack{a\in\mathbb{N}\\ q^a|\lambda_k(n)\\ q^a>y^k}} 1.$$

The first sum is

$$\sum_{n\le x}\sum_{q\le y^k}\log q \sum_{\substack{a\in\mathbb{N}\\ q^a\le y^k}} 1 = \sum_{n\le x}\sum_{m\le y^k}\Lambda(m) \ll \sum_{n\le x} y^k \ll xy^k,$$

using the definition of $\Lambda(m)$ and equation (2.1). Using Lemma 3.12, the geometric estimate in (2.6) and equation (2.1) the second sum becomes

$$\sum_{n\le x}\sum_{q\le y^k}\log q \sum_{\substack{a\in\mathbb{N}\\ q^a|\lambda_k(n)\\ q^a>y^k}} 1 \ll \sum_{q\le y^k}\log q \sum_{\substack{a\in\mathbb{N}\\ q^a>y^k}} \frac{xy^k}{q^a} \ll \sum_{q\le y^k}\log q\frac{xy^k}{y^k} \ll xy^k.$$

□

3.5 Reduction to $h_k(n)$ for Small Primes

The small primes dividing $\phi_k(n)$ are what contributes to the asymptotic term of $\log(n/\lambda_k(n))$. In this section we show that the important case is the supersquarefree case of p dividing $\phi_k(n)$ which is when

$$p \prec p_1 \prec p_2 \prec \cdots \prec p_k, p_k \mid n.$$

For this reason we will approximate the sum $\sum_{q\le y^k} v_q(\phi_k(n))\log q$ with

$$h_k(n) = \sum_{p_1|n}\sum_{p_2|p_1-1}\cdots\sum_{p_k|p_{k-1}-1}\sum_{q\le y^k}\nu_q(p_k-1)\log q. \tag{3.4}$$

Proof of Proposition 3.5. For any fixed prime q, we know that

$$v_q(\phi(m)) = \max\{0, v_q(m)-1\} + \sum_{p|m} v_q(p-1),$$

which implies

$$\sum_{p|m} v_q(p-1) \leq v_q(\phi(m)) \leq v_q(m) + \sum_{p|m} v_q(p-1).$$

Repeated use of this inequality for $m = \phi_l(n)$ where l ranges from $k-1$ to 0 yields

$$\begin{aligned} \sum_{p|\phi_{k-1}(n)} v_q(p-1) &\leq v_q(\phi_k(n)) \\ &\leq \sum_{p|\phi_{k-1}(n)} v_q(p-1) + \sum_{p|\phi_{k-2}(n)} v_q(p-1) \\ &\qquad + \cdots + \sum_{p|\phi(n)} v_q(p-1) + v_q(n). \end{aligned} \tag{3.5}$$

A prime p divides $\phi_{k-1}(n)$ either in the supersquarefree case (ssf), or not in the supersquarefree case (nssf), yielding

$$\begin{aligned} \sum_{ssf} v_q(p-1) &\leq \sum_{p|\phi_{k-1}(n)} v_q(p-1) \\ &\leq \sum_{ssf} v_q(p-1) + \sum_{nssf} v_q(p-1). \end{aligned}$$

Combining this inequality with (3.5) yields

$$\begin{aligned} \sum_{ssf} v_q(p-1) &\leq v_q(\phi_k(n)) \\ &\leq \sum_{ssf} v_q(p-1) + \sum_{nssf} v_q(p-1) + \sum_{p|\phi_{k-2}(n)} v_q(p-1) \\ &\qquad + \cdots + \sum_{p|\phi(n)} v_q(p-1) + v_q(n). \end{aligned}$$

Subtracting the sum over the supersquarefree case, multiplying through by $\log q$ and summing over $q \leq y^k$ yields

$$\begin{aligned}
0 &\le \sum_{q \le y^k} \nu_q(\phi_k(n)) \log q - h_k(n) \\
&\le \sum_{q \le y^k} \sum_{nssf} v_q(p-1)\log q + \sum_{q \le y^k} \sum_{p \mid \phi_{k-2}(n)} v_q(p-1)\log q \\
&\qquad + \cdots + \sum_{q \le y^k} \sum_{p \mid n} v_q(p-1)\log q
\end{aligned}$$

where we get $h_k(n)$ from (3.4). It suffices to show that the sum on the right side becomes our error term. For the sum

$$\begin{aligned}
\sum_{n \le x} \sum_{q \le y^k} \sum_{p \mid \phi_m(n)} v_q(p-1)\log q &= \sum_{n \le x} \sum_{q \le y^k} \sum_{p \mid \phi_m(n)} \sum_{\substack{a \in \mathbb{N} \\ q^a \mid p-1}} \log q \\
&= \sum_{n \le x} \sum_{q \le y^k} \log q \sum_{a \in \mathbb{N}} \sum_{\substack{p \in \mathcal{P}_{q^a} \\ p \mid \phi_m(n)}} 1,
\end{aligned}$$

we'll split the sum over values of $p \le y^{k-1}$ and $p > y^{k-1}$. For $p \le y^{k-1}$ we uniformly get for all n that

$$\begin{aligned}
\sum_{q \le y^k} \log q \sum_{a \in \mathbb{N}} \sum_{\substack{p \in \mathcal{P}_{q^a} \\ p \le y^{k-1} \\ p \mid \phi_m(n)}} 1 &\le \sum_{q \le y^k} \log q \sum_{a \in \mathbb{N}} \pi(y^{k-1}; q^a, 1) \\
&\ll \sum_{q \le y^k} \log q \sum_{a \in \mathbb{N}} \frac{y^{k-1}}{\phi(q^a)} \\
&\ll y^{k-1} \sum_{q \le y^k} \frac{\log q}{q} \\
&\ll y^{k-1} \log y
\end{aligned}$$

using the geometric estimate (2.6) and the prime number theorem for arithmetic progressions. As for $p > y^{k-1}$ we fix an M and N from case 3 for which $p \mid \phi_m(n)$, of which there are at most $O_k(1)$ such M, N since $v_p(\phi(m)) = 1$. Therefore

$$\begin{aligned}
\sum_{n\le x}\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p>y^{k-1}\\ p\in\mathcal{P}_{q^a}\\ p\mid\phi_m(n)}}1 &\ll \sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p\in\mathcal{P}_{q^a}\\ p>y^{k-1}}}\frac{xy^M}{p^N}\\
&\le \sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{p\in\mathcal{P}_{q^a}}\frac{xy^{M-(k-1)(N-1)}}{p}\\
&\ll \sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\frac{xy^{M-(k-1)(N-1)+1}}{q^a}\\
&\ll \sum_{q\le y^k}\frac{xy^{M-(k-1)(N-1)+1}\log q}{q}\\
&\ll xy^{M-(k-1)(N-1)+1}\log y^k\\
&\ll xy^{M-(k-1)(N-1)+1}\log y.
\end{aligned}$$

Since the M, N were chosen for $\phi_m(n)$ we know that $M \le mN$ where equality holds if and only if we are in the supersquarefree case. Now either $m \le k-2$ or $m = k-1$ and we are not in the supersquarefreecase. In the former case we have an error of

$$O(xy^{(k-2)N-(k-1)(N-1)+1}\log y) = O(xy^{k-N}\log y) = O(xy^{k-1}\log y)$$

since $N \ge 1$, or in the latter case

$$O(xy^{(k-1)N-1-(k-1)(N-1)+1}\log y) = O(xy^{k-1}\log y).$$

Thus we get

$$\begin{aligned}
\sum_{n\le x}\Bigg(\sum_{q\le y^k}\sum_{nssf}v_q(p-1)\log q + \sum_{q\le y^k}\sum_{p\mid\phi_{k-2}(n)}v_q(p-1)\log q + \dots\\
+\sum_{q\le y^k}\sum_{p\mid n}v_q(p-1)\log q\Bigg) \ll xy^{k-1}\log y
\end{aligned}$$

and so

$$\sum_{q\le y^k}\sum_{nssf} v_q(p-1)\log q + \sum_{q\le y^k}\sum_{p|\phi_{k-2}(n)} v_q(p-1)\log q + \dots$$
$$+\sum_{q\le y^k}\sum_{p|n} v_q(p-1)\log q \ll y^{k-1}\log y\cdot\psi(x)$$

for almost all $n \le x$ as required. □

3.6 Reduction to the First and Second Moments

The Turán-Kubilius inequality, which is discussed further in the appendix, asserts that if $f(n)$ is a complex strongly additive function, then there exists an absolute constant C such that

$$\sum_{n\le x}|f(n)-M_1(x)|^2 \le CxM_2(x) \tag{3.6}$$

where $M_1(x) = \sum_{p\le x}|f(p)|/p$ and $M_2(x) = \sum_{p\le x}|f(p)|^2/p$. Since $h_k(n)$ is strongly additive we apply this inequality where $M_1(x) = \sum_{p\le x} h_k(p)/p$, $M_2(x) = \sum_{p\le x} h_k(p)^2/p$. We will need to find bounds on M_1 and M_2 therefore it's our goal to prove the following two propositions:

Proposition 3.13. *For all $x > e^{e^e}$,*

$$M_1(x) = \frac{1}{(k-1)!}y^k\log y + O(y^k)$$

Proposition 3.14. *For all $x > e^{e^e}$,*

$$M_2(x) \ll y^{2k-1}\log^{k-1} y.$$

These will lead to a proof of Proposition 3.6.

Proof of Proposition 3.6. Let N denote the number of $n \le x$ for which $|h_k(n) - M_1(x)| > y^k$. The contribution of such n to the sum in (3.6) is at least Ny^{2k}. Thus Proposition 3.14 implies $N \ll x\log^{k-1} y/y$ and so Proposition 3.13 implies that $h_k(n) = \frac{1}{(k-1)!}y^k\log y + O(y^k)$ except for a set of size $O(x(\log y)^{k-1}/y)$. □

3.7 Summations Involving $\pi(t, p, 1)$

The proofs of Propositions 3.13 and 3.14 involve multiple summations over primes. Those sums can be re–written as sums including terms such as $\pi(t, p, 1)$. A lot of these summations will involve sieving techniques. This section will be split into proofs of two lemmas involving the summations required for the sums arising from the Propositions 3.13 and 3.14.

Lemma 3.15. *Let b, k, l be positive integers with $2 \le l \le k$. Let $t > e^e$ be a real number and let constants $\alpha, \alpha_1, \alpha_2$ satisfy $0 < \alpha < 1/2$ and $0 < \alpha_1 < \alpha_2 < 1/2$.*

(a) If $b > t^{\alpha}$, then

$$\sum_{p_k \in \mathcal{P}_b} \sum_{p_{k-1} \in \mathcal{P}_{p_k}} \cdots \sum_{p_2 \in \mathcal{P}_{p_3}} \pi(t; p_2, 1) \ll \frac{t \log t (\log\log t)^{k-2}}{b}. \tag{3.7}$$

(b) If $b \le t^{\alpha_1}$, then

$$\sum_{\substack{p_l \in \mathcal{P}_b \\ p_l > t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_{p_l}} \cdots \sum_{p_2 \in \mathcal{P}_{p_3}} \pi(t; p_2, 1) \ll \frac{b^{l-1} t}{\phi(b)^l \log t}. \tag{3.8}$$

(c) If $b \le t^{\alpha_1}$, then

$$\sum_{p_l \in \mathcal{P}_b} \sum_{p_{l-1} \in \mathcal{P}_{p_l}} \cdots \sum_{p_2 \in \mathcal{P}_{p_3}} \pi(t; p_2, 1) \ll \frac{t (\log\log t)^{l-1}}{\phi(b) \log t}. \tag{3.9}$$

The implicit constants in $(a) - (c)$ depend on the choices of the α.

Proof. For (3.7) we just use the trivial estimate $\pi(t; p_2, 1) \le t/p_2$ and several uses of Brun-Titchmarsh (2.10) to get

$$\begin{aligned}
\sum_{p_k \in \mathcal{P}_b} \sum_{p_{k-1} \in \mathcal{P}_k} \cdots \sum_{p_2 \in \mathcal{P}_3} \pi(t; p_2, 1) &\leq \sum_{p_k \in \mathcal{P}_b} \sum_{p_{k-1} \in \mathcal{P}_k} \cdots \sum_{p_2 \in \mathcal{P}_3} \frac{t}{p_2} \\
&\ll t \sum_{p_k \in \mathcal{P}_b} \sum_{p_{k-1} \in \mathcal{P}_k} \cdots \sum_{p_3 \in \mathcal{P}_4} \frac{\log\log t}{p_3} \\
&\ll t \sum_{p_k \in \mathcal{P}_b} \frac{(\log\log t)^{k-2}}{p_k} \\
&\leq t \sum_{\substack{m \equiv 1 \pmod{b} \\ t^{\alpha} \leq m \leq t}} \frac{(\log\log t)^{k-2}}{m} \\
&\leq \frac{t \log t (\log\log t)^{k-2}}{b}
\end{aligned}$$

where $m > 1$ and $m \equiv 1 \pmod{b}$ imply that $m > b$ and by using (2.7). As for (3.8) we get

$$\begin{aligned}
&\sum_{\substack{p_l \in \mathcal{P}_b \\ l > t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_l} \cdots \sum_{p_2 \in \mathcal{P}_3} \pi(t; p_2, 1) \\
&\quad = \sum_{\substack{p_l \in \mathcal{P}_b \\ l > t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_l} \cdots \sum_{p_3 \in \mathcal{P}_4} \#\{(m_1, p_2) : p_2 = 1 \pmod{p_3}, p_2 > t^{\alpha_2}, \\
&\qquad\qquad m_1 p_2 + 1 \leq t, p_2, m_1 p_2 + 1 \text{ prime}\} \\
&\quad = \sum_{\substack{p_l \in \mathcal{P}_b \\ l > t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_l} \cdots \sum_{p_4 \in \mathcal{P}_5} \#\{(m_1, m_2, p_3) : p_3 = 1 \pmod{p_4}, p_3 > t^{\alpha_2}, \\
&\qquad\quad m_1(m_2 p_3 + 1) + 1 \leq t, \{p_3, m_2 p_3 + 1, m_1(m_2 p_3 + 1) + 1\} \text{ prime}\} \\
&\quad = \#\{(m_1, m_2, \ldots, m_{l-1}, p_l) : p_l = 1 \pmod{b}, p_l > t^{\alpha_2}, \\
&\qquad\qquad m_1(m_2 \ldots (m_{l-2}(m_{l-1} p_l + 1) + 1) + \cdots + 1 \leq t, \{p_l, m_{l-1} p_l + 1, \\
&\qquad\qquad\quad m_{l-2}(m_{l-1} p_l + 1) + 1, \ldots, \\
&\qquad\qquad\qquad m_1(m_2 \ldots (m_{l-2}(m_{l-1} p_l + 1) + 1) + \cdots + 1\} \text{ prime}\} \\
&\quad \leq \sum_{m_1 \ldots m_{l-1} \leq t^{1-\alpha_2}} \#\{p_l < t/m_1 \ldots m_{l-1} : p_l = 1 \pmod{b}, \\
&\qquad\qquad \{p_l, m_{l-1} p_l + 1, m_{l-2}(m_{l-1} p_l + 1) + 1, \ldots, \\
&\qquad\qquad\qquad m_1(m_2 ... (m_{l-2}(m_{l-1} p_l + 1) + 1) + \cdots + 1\} \text{ prime}\}.
\end{aligned}$$

From here will need to use Brun's Sieve method (see [12, Theorem 2.4]) to get that

$$\begin{aligned}\#\{p_l <&t/m_1\dots m_{l-1} : p_l = 1 \pmod b), \{p_l, m_{l-1}p_l+1, m_{l-2}(m_{l-1}p_l+1)+1,\\ &\dots, m_1(m_2\dots(m_{l-2}(m_{l-1}p_l+1)+1)+\dots+1\} \text{ prime}\}\\ &\ll \frac{E^{l-1}}{\phi(E)^{l-1}}\frac{b^{l-1}}{\phi(b)^{l-1}}\frac{bc_1\dots c_{l-1}}{\phi(bc_1\dots c_{l-1})}\frac{t/m_1\dots m_{l-1}b}{(\log t/m_1\dots m_{l-1}b)^l}\end{aligned}$$

where the c_i and E are

$$\begin{aligned}E =&\left(\prod_{i=1}^{l-1} m_i^{i(i+1)/2}\right)(1+m_1+m_1m_2+\dots+m_1\dots m_{l-3})(1+m_2+m_2m_3\\ &+\dots+m_2\dots m_{l-3})\dots(1+m_{l-3})(1+m_1+m_1m_2+\dots\\ &+m_1\dots m_{l-4})(1+m_2+m_2m_3+\dots+m_2\dots m_{l-4})\\ &\dots(1+m_{l-4})\dots(1+m_1)\end{aligned}$$

and for $1 \le i \le l-1$,

$$c_i = 1+m_i+m_im_{i+1}+\dots+m_i\dots m_{l-2}, c_{l-1} = 1.$$

Using $\phi(mn) \ge \phi(m)\phi(n)$ and $m_1\dots m_{l-1}b \le t^{1+\alpha_1-\alpha_2}$ where $1+\alpha_1-\alpha_2 < 1$ we get

$$\ll \frac{E^{l-1}}{\phi(E)^{l-1}}\frac{b^{l-1}}{\phi(b)^{l}}\frac{c_1}{\phi(c_1)}\dots\frac{c_{l-1}}{\phi(c_{l-1})}\frac{t}{m_1\dots m_{l-1}(\log t)^l}.$$

Using

$$\frac{m^L}{\phi(m^L)} = \frac{m}{\phi(m)},$$

we get the sum is

$$\begin{aligned}&\sum_{m_1\dots m_{l-1}\le t^{1-\alpha_2}} \frac{E^{l-1}}{\phi(E)^{l-1}}\frac{c_1}{\phi(c_1)}\dots\frac{c_{l-1}}{\phi(c_{l-1})}\frac{1}{m_1\dots m_{l-1}}\\ &\quad= \sum_{m_1\dots m_{l-1}\le t^{1-\alpha_2}} \frac{(E^*)^{l-1}}{\phi(E^*)^{l-1}}\frac{c_1}{\phi(c_1)}\dots\frac{c_{l-1}}{\phi(c_{l-1})}\frac{1}{m_1\dots m_{l-1}}\end{aligned}$$

where

$$
\begin{aligned}
E^* =&(1 + m_1 + m_1 m_2 + \cdots + m_1 \ldots m_{l-3})(1 + m_2 + m_2 m_3 + \cdots + \\
&m_2 \ldots m_{l-3}) \ldots (1 + m_{l-3})(1 + m_1 + m_1 m_2 + \cdots + m_1 \ldots m_{l-4}) \\
&(1 + m_2 + m_2 m_3 + \cdots + m_2 \ldots m_{l-4}) \ldots (1 + m_{l-4}) \ldots (1 + m_1).
\end{aligned}
$$

We have that every factor in E^* as well as the c_i are of the form $1+Cm_i$ for some i or of the form m_i^L. Hence using $l-1$ applications of Lemmas 2.3, 2.5 or 2.6 we can pick off the factors of the form $(1+Cm_i)$ one at a time. Let $E^{(e)}, c_i^{(e)}$ denote the E^* and c_i terms with the factors of the form $1+Cm_1$ through $1+Cm_e$ removed.

$$
\begin{aligned}
&\sum_{m_1 \ldots m_{l-1} \le t^{1-\alpha_2}} \frac{E^{l-1}}{\phi(E)^{l-1}} \frac{c_1}{\phi(c_1)} \cdots \frac{c_{l-1}}{\phi(c_{l-1})} \frac{1}{m_1 \ldots m_{l-1}} \\
&\qquad \ll \sum_{m_2 \ldots m_{l-1} \le t^{1-\alpha_2}} \frac{(E')^{l-1}}{\phi(E')^{l-1}} \frac{c_1'}{\phi(c_1')} \cdots \frac{c_{l-1}'}{\phi(c_{l-1}')} \frac{1}{m_2 \ldots m_{l-1}} (\log t) \\
&\qquad \ll \sum_{m_3 \ldots m_{l-1} \le t^{1-\alpha_2}} \frac{(E'')^{l-1}}{\phi(E'')^{l-1}} \frac{c_1''}{\phi(c_1'')} \cdots \frac{c_{l-1}''}{\phi(c_{l-1}'')} \frac{1}{m_3 \ldots m_{l-1}} (\log^2 t) \\
&\qquad \ll \cdots \ll (\log t)^{l-1}.
\end{aligned}
$$

Note that the C are at most $1 + t + t^2 + \cdots + t^{k-3} \le t^{k-2}$ and $l \le k$ so the implied constant only depends on k. Therefore

$$
\sum_{\substack{p_l \in \mathcal{P}_b \\ l > t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_l} \cdots \sum_{p_2 \in \mathcal{P}_3} \pi(t; p_2, 1) \ll \frac{t b^{l-1}}{\phi(b)^l (\log t)^l} (\log t)^{l-1} = \frac{t b^{l-1}}{\phi(b)^l \log t}.
$$

As for part (c), first note that $b/\phi(b) \ll \log\log b$, so for $p_l > t^{\alpha_2}$, we get that part (b) implies our bound. As for $p_l \le t^{\alpha_2}$ we'll split it into cases where p_3 is less than or greater than t^{α_2}. If $p_3 \le t^{\alpha_2}$, then

$$\begin{aligned}\sum_{\substack{p_l \in \mathcal{P}_b \\ p_l \le t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_l} \cdots \sum_{\substack{p_2 \in \mathcal{P}_3 \\ p_2 \le t^{\alpha_2}}} \pi(t; p_2, 1) &\ll \sum_{\substack{p_l \in \mathcal{P}_b \\ p_l \le t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_l} \cdots \sum_{\substack{p_2 \in \mathcal{P}_3 \\ p_2 \le t^{\alpha_2}}} \frac{t}{\phi(p_2) \log t/p_2} \\ &\ll \sum_{\substack{p_l \in \mathcal{P}_b \\ p_l \le t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_l} \cdots \sum_{\substack{p_2 \in \mathcal{P}_3 \\ p_2 \le t^{\alpha_2}}} \frac{t}{p_2 \log t} \\ &\ll \sum_{p_l \in \mathcal{P}_b} \frac{t (\log \log t)^{l-2}}{p_l \log t} \\ &\ll \frac{t (\log \log t)^{l-1}}{\phi(b) \log t}\end{aligned}$$

If $p_3 > t^{\alpha_2}$, then since $b \le t^{\alpha_2}$ there is a minimum m such that $p_m \le t^{\alpha_2}$. So using part (b) with $l = m$ we get

$$\begin{aligned}\sum_{\substack{p_l \in \mathcal{P}_b \\ p_l \le t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_l} \cdots \sum_{\substack{p_2 \in \mathcal{P}_3 \\ p_2 > t^{\alpha_2}}} \pi(t; p_2, 1) &\ll \sum_{\substack{p_l \in \mathcal{P}_b \\ p_l \le t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_l} \cdots \sum_{p_{m+1} \in \mathcal{P}_{m+2}} \frac{(p_{m-1})^{m-1} t}{\phi(p_{m-1})^m \log t} \\ &\ll \sum_{\substack{p_l \in \mathcal{P}_b \\ p_l \le t^{\alpha_2}}} \sum_{p_{l-1} \in \mathcal{P}_l} \cdots \sum_{p_{m+1} \in \mathcal{P}_{m+2}} \frac{t}{p_{m-1} \log t} \\ &\ll \frac{t (\log \log t)^{l-m}}{\phi(b) \log t} \\ &\ll \frac{t (\log \log t)^{l-1}}{\phi(b) \log t}\end{aligned}$$

since $m \ge 2$ and by using Brun-Titchmarsh (2.10) which finishes part (c) and the lemma. □

As for the summations requires for the second moment, we'll note that we need twice as many sums due to $h_k(p)^2$. However the techniques required are similar.

Lemma 3.16. *Let $t > e^e$ and $0 < 2\alpha_1 < \alpha_2 < 1/2$. Then*

(a) If $b_1 > t^{\alpha_1}$ or $b_2 > t^{\alpha_1}$ then

$$\sum_{\substack{p_2 \in \mathcal{P}_{b_1} \\ r_2 \in \mathcal{P}_{b_2}}} \pi(t; p_2 r_2, 1) \ll \frac{t \log^2 t}{b_1 b_2}. \tag{3.10}$$

(b) If neither b_1 nor b_2 exceeds t^{α_1}, then

$$\sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ r_k \in \mathcal{P}_{b_2} \\ p_k r_k > t^{\alpha_2}}} \cdots \sum_{\substack{p_2 \in \mathcal{P}_{p_3} \\ r_2 \in \mathcal{P}_{r_3}}} \pi(t; p_2 r_2, 1) \ll \frac{t(\log\log t)^{k-1} b_2^{k-1}}{\phi(b_1)\phi(b_2)^k \log t} + \frac{t(\log\log t)^{k-1} b_1^{k-1}}{\phi(b_2)\phi(b_1)^k \log t}. \tag{3.11}$$

(c) If neither b_1 nor b_2 exceeds t^{α_1}, then

$$\sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ r_k \in \mathcal{P}_{b_2}}} \cdots \sum_{\substack{p_2 \in \mathcal{P}_{p_3} \\ r_2 \in \mathcal{P}_{r_3}}} \pi(t; p_2 r_2, 1) \ll \frac{t(\log\log t)^{2k-2}}{\phi(b_1)\phi(b_2) \log t}. \tag{3.12}$$

(d) If neither b_1 nor b_2 exceeds t^{α_1}, then

$$\sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ r_k \in \mathcal{P}_{b_2}}} \cdots \sum_{\substack{p_3 \in \mathcal{P}_{p_4} \\ r_3 \in \mathcal{P}_{r_4}}} \sum_{s \in \mathcal{P}_{p_3} \cap \mathcal{P}_{r_3}} \pi(t; s, 1) \ll \frac{t(\log\log t)^{2k-2}}{\phi(b_1)\phi(b_2) \log t}. \tag{3.13}$$

Again the implicit constants depend on our choice of the α.

Proof. (a) is similar to part (a) of Lemma 3.15. For part (b) we first assume that $p_k \leq r_k$, then

$$\begin{aligned}
&\sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ r_k \in \mathcal{P}_{b_2} \\ p_k \leq r_k \\ p_k r_k > t^{\alpha_2}}} \dots \sum_{\substack{p_2 \in \mathcal{P}_{p_3} \\ r_2 \in \mathcal{P}_{r_3}}} \pi(t; p_2 r_2, 1) \\
&\quad = \sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ r_k \in \mathcal{P}_{b_2} \\ p_k r_k > t^{\alpha_2}}} \cdots \sum_{\substack{p_3 \in \mathcal{P}_{p_4} \\ r_3 \in \mathcal{P}_{r_4}}} \#\{(m_1, p_2, r_2) : p_2 = 1 \pmod{p_3}, r_2 = 1 \pmod{r_3}, \\
&\qquad\qquad r_2 p_2 > t^{\alpha_2}, m_1 r_2 p_2 + 1 \leq t, p_2, m_1 r_2 p_2 + 1 \text{ prime}\} \\
&\quad = \sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ p_k \leq r_k}} \sum_{p_{k-1} \in \mathcal{P}_k} \cdots \sum_{p_2 \in \mathcal{P}_3} \sum_{\substack{r_k \in \mathcal{P}_{b_2} \\ p_k r_k > t^{\alpha_2}}} \sum_{r_{k-1} \in \mathcal{P}_{r_k}} \cdots \sum_{r_4 \in \mathcal{P}_{r_5}} \#\{(m_1, m_2, r_3) : \\
&\qquad\qquad r_3 = 1 \pmod{r_4}, r_3 p_2 > t^{\alpha_2}, m_1 p_2 (m_2 r_3 + 1) + 1 \leq t, \\
&\qquad\qquad\quad \{r_3, m_2 r_3 + 1, m_1 p_2 (m_2 r_3 + 1) + 1\} \text{ prime}\} \\
&\quad = \sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ p_k \leq r_k}} \sum_{p_{k-1} \in \mathcal{P}_k} \cdots \sum_{p_2 \in \mathcal{P}_3} \#\{(m_1, m_2, \dots, m_{l-1}, r_l) : r_l = 1 \pmod{b_2}, \\
&\qquad\quad p_2 r_k > t^{\alpha_2}, m_1 p_2 (m_2 \dots (m_{k-2}(m_{k-1} r_k + 1) + 1) + \dots + 1 \leq t, \\
&\qquad\qquad \{r_k, m_{k-1} r_k + 1, m_{k-2}(m_{k-1} r_k + 1) + 1, \dots, \\
&\qquad\qquad\quad m_1 p_2 (m_2 \dots (m_{k-2}(m_{k-1} r_k + 1) + 1) + \dots + 1\} \text{ prime}\} \\
&\quad \leq \sum_{m_1 \dots m_{l-1} \leq t^{1-\alpha_2}} \sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ p_k \leq r_k}} \sum_{p_{k-1} \in \mathcal{P}_k} \cdots \sum_{p_2 \in \mathcal{P}_3} \#\{r_k < t/p_2 m_1 \dots m_{k-1} : \\
&\qquad\quad r_k = 1 \pmod{b_2}, \{r_k, m_{k-1} r_k + 1, m_{k-2}(m_{k-1} r_k + 1) + 1, \dots, \\
&\qquad\qquad p_2 m_1 (m_2 \dots (m_{k-2}(m_{k-1} r_k + 1) + 1) + \dots + 1\} \text{ prime}\}
\end{aligned}$$

Just like in Lemma 3.15 we use Brun's Sieve. However, notice that we have almost the same set, except with m_1 replaced with $m_1 p_2$. Hence we have

$$\begin{aligned}
&\#\{r_k < t/p_2 m_1 \cdots_{k-1} : r_k = 1 \pmod{b_1}, \{r_k, m_{k-1} r_k + 1, m_{k-2}(m_{k-1} r_k + 1) \\
&\qquad + 1, \dots, p_2 m_1 (m_2 \dots (m_{k-2}(m_{k-1} r_k + 1) + 1) + \dots + 1\} \text{ prime}\} \\
&\qquad\qquad \ll \frac{E^{k-1}}{\phi(E)^{k-1}} \frac{b_2^{k-1}}{\phi(b_2)^{k-1}} \frac{b_2 c_1 \dots c_{k-1}}{\phi(b_2 c_1 \dots c_{k-1})} \frac{t/p_2 m_1 \dots m_{k-1} b_2}{(\log t/p_2 m_1 \dots m_{k-1} b_2)^k}
\end{aligned}$$

where the c_i and E are

$$E = p_2\left(\prod_{i=1}^{l-1} m_i^{i(i+1)/2}\right)(1 + p_2m_1 + p_2m_1m_2 + ... + p_2m_1 \dots m_{k-3})$$
$$(1 + m_2 + m_2m_3 + \cdots + m_2 \dots m_{k-3}) \dots (1 + m_{k-3})$$
$$(1 + p_2m_1 + p_2m_1m_2 + \cdots + p_2m_1 \dots m_{k-4})(1 + m_2$$
$$+ m_2m_3 + \cdots + m_2 \dots m_{k-4}) \dots (1 + m_{k-4}) \dots (1 + p_2m_1)$$

and for $2 \leq i \leq k-2$,

$$\begin{aligned} c_1 &= 1 + p_2m_1 + p_2m_1m_2 + \cdots + p_2m_1 \dots m_{k-2}, \\ c_i &= 1 + m_i + m_im_{i+1} + \cdots + m_i \dots m_{k-2}, \\ c_{k-1} &= 1. \end{aligned}$$

By the same methods as Lemma 3.15, using that $p_2/\phi(p_2)$ is bounded and noting that

$$\frac{t}{p_2m_1...m_{k-1}b_2} > \frac{r_k}{b_1} > t^{\alpha_2/2-\alpha_1} = t^{\epsilon}$$

for some $\epsilon > 0$ since $\alpha_2 > 2\alpha_1$, we get that

$$\begin{aligned} \sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ r_k \in \mathcal{P}_{b_2} \\ p_kr_k > t^{\alpha_2}}} \cdots \sum_{\substack{p_2 \in \mathcal{P}_{p_3} \\ r_2 \in \mathcal{P}_{r_3}}} \pi(t; p_2r_2, 1) &\ll \frac{tb_2^{k-1}}{\phi(b_2)^k \log t} \sum_{p_k \in \mathcal{P}_{b_1}} \sum_{p_{k-1} \in \mathcal{P}_k} \cdots \sum_{p_2 \in \mathcal{P}_3} \frac{1}{p_2} \\ &\ll \frac{tb_2^{k-1}}{\phi(b_2)^k \log t} \sum_{p_k \in \mathcal{P}_{b_1}} \frac{(\log\log t)^{k-2}}{p_k} \\ &\ll \frac{t(\log\log t)^{k-1}b_2^{k-1}}{\phi(b_1)\phi(b_2)^k \log t}. \end{aligned}$$

The case for $r_k \leq p_k$ is similar. As for part (c), first note that $b_i/\phi(b_i) \ll \log\log b_i$ for $i \in \{1, 2\}$. taking care of the case where $p_kr_k > t^{\alpha_2}$. As for

$p_k r_k \leq t^{\alpha_2}$ we get

$$\sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ r_k \in \mathcal{P}_{b_2} \\ p_k r_k \leq t^{\alpha_2}}} \cdots \sum_{\substack{p_2 \in \mathcal{P}_{p_3} \\ r_2 \in \mathcal{P}_{r_3}}} \pi(t; p_2 r_2, 1) \ll \sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ r_k \in \mathcal{P}_{b_2} \\ p_k r_k \leq t^{\alpha_2}}} \cdots \sum_{\substack{p_2 \in \mathcal{P}_{p_3} \\ r_2 \in \mathcal{P}_{r_3}}} \frac{t}{\phi(p_2 r_2) \log t / p_2 r_2}$$
$$\ll \sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ r_k \in \mathcal{P}_{b_2} \\ p_k r_k \leq t^{\alpha_2}}} \cdots \sum_{\substack{p_2 \in \mathcal{P}_{p_3} \\ r_2 \in \mathcal{P}_{r_3}}} \frac{t}{p_2 r_2 \log t}$$
$$\ll \sum_{\substack{p_k \in \mathcal{P}_{b_1} \\ r_k \in \mathcal{P}_{b_2} \\ p_k r_k \leq t^{\alpha_2}}} \frac{t (\log\log t)^{2k-4}}{p_k r_k \log t}$$
$$\ll \frac{t (\log\log t)^{2k-2}}{\phi(b_1)\phi(b_2) \log t}$$

using Brun-Titchmarsh (2.10), finishing part (c). As for part (d) we note that

$$\sum_{\substack{p_3 \in \mathcal{P}_{p_4} \\ r_3 \in \mathcal{P}_{r_4}}} \sum_{s \in \mathcal{P}_{p_3} \cap \mathcal{P}_{r_3}} \pi(t; s, 1)$$
$$= \sum_{\substack{p_3 \in \mathcal{P}_{p_4} \\ r_3 \in \mathcal{P}_{r_4}}} \#\{(m_1, s) : s = 1 \pmod{p_3 r_3}, m_1 s + 1 \leq t, s, m_1 s + 1 \text{ prime}\}$$
$$= \sum_{p_3 \in \mathcal{P}_{p_4}} \#\{(m_1, m_2, r_3) : r_3 = 1 \pmod{r_4}, m_1(m_2 p_3 r_3 + 1) + 1 \leq t,$$
$$\{m_2 p_3 r_3 + 1, m_1(m_2 p_3 r_3 + 1) + 1 \text{ prime}\}$$

and so on, yielding a similar sieve as part (b). □

3.8 Reduction of $\sum h_k(p)$ to Small Values of p_k

We will be using Euler Summation on the sum $\sum_{p \leq t} h_k(p)$ in our efforts to find our estimate for $M_1(x)$. It will turn out that the large primes do not contribute much to the sum. The sum will involve estimating $\pi(t; p, 1)$ by $\mathrm{li}(t)/p - 1$. The following lemma will deal with those errors and will involve the Bombieri–Vinogradov Theorem (2.13).

Lemma 3.17. *For all $2 \le l \le k$, $x > e^{e^e}$ and $v > e^e$,*

$$\sum_{q \le y^k} \log q \sum_{a \in \mathbb{N}} \sum_{\substack{p_k \in \mathcal{P}_{q^a} \\ p_k \le v^{1/3^{l-1}}}} \sum_{\substack{p_{k-1} \in \mathcal{P}_{p_k} \\ p_{k-1} \le v^{1/3^{l-2}}}} \cdots \sum_{\substack{p_{k-l+2} \in \mathcal{P}_{p_{k-l+3}} \\ p_{k-l+2} \le v^{1/3}}} \left(\pi(v, p_{k-l+2}, 1) - \frac{\mathrm{li}(v)}{p_{k-l+2}} \right) \ll \frac{v \log y}{\log v} + \mathrm{li}(v)(\log\log v)^{l-2}.$$

Proof. Let $E(t; r, 1) = \pi(t; r, 1) - \frac{\mathrm{li}(t)}{r-1}$. Then we have

$$\begin{aligned}
&\sum_{q \le y^k} \log q \sum_{a \in \mathbb{N}} \sum_{\substack{p_k \in \mathcal{P}_{q^a} \\ p_k \le v^{1/3^{l-1}}}} \sum_{\substack{p_{k-1} \in \mathcal{P}_{p_k} \\ p_{k-1} \le v^{1/3^{l-2}}}} \cdots \\
&\qquad \sum_{\substack{p_{k-l+2} \in \mathcal{P}_{p_{k-l+3}} \\ p_{k-l+2} \le v^{1/3}}} \left(\pi(v, p_{k-l+2}, 1) - \frac{\mathrm{li}(v)}{p_{k-l+2} - 1} \right) \\
&= \sum_{q \le y^k} \log q \sum_{a \in \mathbb{N}} \sum_{\substack{p_k \in \mathcal{P}_{q^a} \\ p_k \le v^{1/3^{l-1}}}} \sum_{\substack{p_{k-1} \in \mathcal{P}_{p_k} \\ p_{k-1} \le v^{1/3^{l-2}}}} \cdots \sum_{\substack{p_{k-l+2} \in \mathcal{P}_{p_{k-l+3}} \\ p_{k-l+2} \le v^{1/3}}} E(v; p_{k-l+2}, 1) \\
&\ll \sum_{q \le y^k} \log q \sum_{a \in \mathbb{N}} \sum_{\substack{p_k \in \mathcal{P}_{q^a} \\ p_k \le v^{1/3^{l-1}}}} \sum_{\substack{p_{k-1} \in \mathcal{P}_{p_k} \\ p_{k-1} \le v^{1/3^{l-2}}}} \cdots \sum_{\substack{p_{k-l+2} \in \mathcal{P}_{p_{k-l+3}} \\ p_{k-l+2} \le v^{1/3}}} |E(v; p_{k-l+2}, 1)|.
\end{aligned}$$

Let $\Omega(m)$ denote the number of divisors of m which are primes or prime powers. We use the estimate $\Omega(m) \ll \log m$ to get

$$\begin{aligned}
&\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}}\cdots\sum_{\substack{p_{k-l+2}\in\mathcal{P}_{p_{k-l+3}}\\ p_{k-l+2}\le v^{1/3}}}|E(v;p_{k-l+2},1)|\\
&\quad\le\log(y^k)\sum_{\substack{p_{k-l+2}\in\mathcal{P}_{p_{k-l+3}}\\ p_{k-l+2}\le v^{1/3}}}|E(v;p_{k-l+2},1)|\sum_{\substack{p_{k-l+3}|p_{k-l+2}-1\\ p_3\le v^{1/9}}}\sum_{\substack{p_{k-l+4}|p_{k-l+3}-1\\ p_{k-l+4}\le v^{1/27}}}\\
&\qquad\cdots\sum_{q\le y^k}\sum_{\substack{a\in\mathbb{N}\\ q^a|p_k-1}}1\\
&\quad\le\log(y^k)\sum_{\substack{p_{k-l+2}\in\mathcal{P}_{p_{k-l+3}}\\ p_{k-l+2}\le v^{1/3}}}|E(v;p_{k-l+2},1)|\sum_{\substack{p_{k-l+3}|p_{k-l+2}-1\\ p_3\le v^{1/9}}}\sum_{\substack{p_{k-l+4}|p_{k-l+3}-1\\ p_{k-l+4}\le v^{1/27}}}\\
&\qquad\cdots\sum_{\substack{p_k\le v^{1/3^{k-1}}\\ p_k|p_{k-1}-1}}\Omega(p_k-1)\\
&\quad\ll\log y\sum_{\substack{p_{k-l+2}\in\mathcal{P}_{p_{k-l+3}}\\ p_{k-l+2}\le v^{1/3}}}|E(v;p_{k-l+2},1)|\sum_{\substack{p_{k-l+3}|p_{k-l+2}-1\\ p_3\le v^{1/9}}}\sum_{\substack{p_{k-l+4}|p_{k-l+3}-1\\ p_{k-l+4}\le v^{1/27}}}\\
&\qquad\cdots\sum_{\substack{p_k\le v^{1/3^{k-1}}\\ p_k|p_{k-1}-1}}\log v.
\end{aligned}$$

Continuing in this manner we obtain

$$\begin{aligned}
&\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}}\cdots\sum_{\substack{p_{k-l+2}\in\mathcal{P}_{p_{k-l+3}}\\ p_{k-l+2}\le v^{1/3}}}|E(v;p_{k-l+2},1)|\\
&\qquad\ll\log y(\log v)^{l-1}\sum_{\substack{p_{k-l+2}\in\mathcal{P}_{p_{k-l+3}}\\ p_{k-l+2}\le v^{1/3}}}|E(v;p_{k-l+2},1)|\ll\frac{v\log y}{\log v}
\end{aligned}$$

using Bombieri–Vinogradov (2.13). As for the difference between

$$\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}}\cdots\sum_{\substack{p_{k-l+2}\in\mathcal{P}_{p_{k-l+3}}\\ p_{k-l+2}\le v^{1/3}}}\frac{\mathrm{li}(v)}{p_{k-l+2}-1}$$

and

$$\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}}\cdots\sum_{\substack{p_{k-l+2}\in\mathcal{P}_{p_{k-l+3}}\\ p_{k-l+2}\le v^{1/3}}}\frac{\mathrm{li}(v)}{p_{k-l+2}} \tag{3.14}$$

we get that it is

$$\begin{aligned}
&\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}}\cdots\sum_{\substack{p_{k-l+2}\in\mathcal{P}_{p_{k-l+3}}\\ p_{k-l+2}\le v^{1/3}}}\frac{\mathrm{li}(v)}{p_{k-l+2}(p_{k-l+2}-1)}\\
&\quad\le\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}}\cdots\sum_{i=1}^{\infty}\frac{\mathrm{li}(v)}{(ip_{k-l+3}+1)(ip_{k-l+3})}\\
&\quad\ll\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}}\cdots\sum_{\substack{p_{k-l+3}\in\mathcal{P}_{p_{k-l+4}}\\ p_{k-l+3}\le v^{1/9}}}\frac{\mathrm{li}(v)}{p_{k-l+3}^2}\\
&\quad\ll\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}}\cdots\sum_{\substack{p_{k-l+3}\in\mathcal{P}_{p_{k-l+4}}\\ p_{k-l+3}\le v^{1/9}}}\frac{\mathrm{li}(v)}{p_{k-l+3}q^a}\\
&\quad\ll\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\frac{\mathrm{li}(v)(\log\log v)^{l-2}}{q^{2a}}\\
&\quad\ll\sum_{q\le y^k}\frac{\mathrm{li}(v)(\log\log v)^{l-2}\log q}{q^2}\\
&\quad\ll\mathrm{li}(v)(\log\log v)^{l-2}.
\end{aligned}$$

The estimate used the Brun–Titchmarsh inequality (2.10), the inequality $p_{k-l+3}\ge q^a$ and noting that the sum over q converges. □

Lemma 3.18. *For all $x>e^{e^e}$ and $t>e^e$,*

$$\begin{aligned}
\sum_{p\le t}h_k(p)&=\sum_{q\le y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le t^{1/3^{k-1}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le t^{1/3^{k-2}}}}\cdots\sum_{\substack{p_2\in\mathcal{P}_{p_3}\\ p_2\le t^{1/3}}}\pi(t;p_2,1)\\
&\qquad+O\biggl(t^{1-1/3^k}\log t(\log\log t)^{k-2}y^k+\frac{t(\log\log t)^{k-2}\log y}{\log t}\biggr).
\end{aligned}$$

Proof. For a prime p,

$$\begin{aligned} h_k(p) &= \sum_{p_1|p} \sum_{p_2|p_1-1} \cdots \sum_{p_k|p_{k-1}-1} \sum_{q\le y^k} \nu_q(p_k-1)\log q \\ &= \sum_{p_2|p-1} \cdots \sum_{p_k|p_{k-1}-1} \sum_{q\le y^k} \nu_q(p_k-1)\log q \end{aligned}$$

since the only prime which can divide p is p itself. Hence

$$\begin{aligned} \sum_{p\le t} h_k(p) &= \sum_{p\le t} \sum_{p_2|p-1} \cdots \sum_{p_k|p_{k-1}-1} \sum_{q\le y^k} \nu_q(p_k-1)\log q \\ &= \sum_{p\le t} \sum_{p_2|p_1-1} \cdots \sum_{p_k|p_{k-1}-1} \sum_{q\le y^k} \sum_{\substack{p_k\in\mathcal{P}_{q^a} \\ a\in\mathbb{N}}} \log q \\ &= \sum_{q\le y^k} \log q \sum_{a\in\mathbb{N}} \sum_{p_k\in\mathcal{P}_{q^a}} \sum_{p_{k-1}\in\mathcal{P}_{p_k}} \cdots \sum_{p_2\in\mathcal{P}_{p_3}} \sum_{\substack{p\le t \\ p\in\mathcal{P}_{p_2}}} 1 \\ &= \sum_{q\le y^k} \log q \sum_{a\in\mathbb{N}} \sum_{p_k\in\mathcal{P}_{q^a}} \sum_{p_{k-1}\in\mathcal{P}_{p_k}} \cdots \sum_{p_2\in\mathcal{P}_{p_3}} \pi(t;p_2,1). \end{aligned}$$

We wish to approximate $\pi(t;p_2,1)$ by $\frac{\mathrm{li}(t)}{p_2-1}$ and use the Bombieri-Vinogradov Theorem to deal with the error. However this approximation only allows primes up to say $t^{1/3}$. So we use the estimations in Lemma 3.15 to bound these errors. We will see that the main contribution comes from $p_i \le t^{1/3^{i-1}}$ and $q^a \le t^{1/3^k}$.

Using Lemma 3.15, we get for large q^a

$$\begin{aligned} &\sum_{q\le y^k} \log q \sum_{\substack{a\in\mathbb{N} \\ q^a>t^{1/3^k}}} \sum_{p_k\in\mathcal{P}_{q^a}} \sum_{p_{k-1}\in\mathcal{P}_{p_k}} \cdots \sum_{p_3\in\mathcal{P}_{p_2}} \pi(t;p_2,1) \\ &\qquad \ll \sum_{q\le y^k} \log q \sum_{\substack{a\in\mathbb{N} \\ q^a>t^{1/3^k}}} \frac{t\log t(\log\log t)^{k-2}}{q^a}. \end{aligned}$$

By geometric estimates, if a^* is the smallest a where $q^a > t^{1/3^k}$, then we get that the above is bounded by

$$
\begin{aligned}
&O\Bigg(t\log t(\log\log t)^{k-2}\sum_{q\le y^k}\frac{\log q}{q^{a^*}}\Bigg)\\
&\ll t^{1-1/3^k}\log t(\log\log t)^{k-2}\sum_{q\le y^k}\log q\\
&\ll t^{1-1/3^k}\log t(\log\log t)^{k-2}y^k.
\end{aligned}
$$

Now suppose $q^a\le t^{1/3^k}$. Let l be the last index (supposing one exists) where $p_i>t^{1/3^{i-1}}$ By using (3.8) where l ranges from 2 to k, we can bound the large values of the p_i.

$$
\begin{aligned}
&\sum_{q\le y^k}\log q\sum_{\substack{a\in\mathbb{N}\\ q^a\le t^{1/3^k}}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p^k\le t^{1/3^{k-1}}}}\cdots\sum_{\substack{p_{l+1}\in\mathcal{P}_{p_{l+2}}\\ p_{l+1}\le t^{1/3^l}}}\sum_{\substack{p_l\in\mathcal{P}_{p_{l+1}}\\ p_l>t^{1/3^{l-1}}}}\sum_{p_{l-1}\in\mathcal{P}_{p_l}}\cdots\sum_{p_2\in\mathcal{P}_{p_3}}\pi(t;p_2,1)\\
&\qquad\ll\sum_{q\le y^k}\log q\sum_{\substack{a\in\mathbb{N}\\ q^a\le t^{1/3^k}}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le t^{1/3^{k-1}}}}\cdots\sum_{\substack{p_{l+2}\in\mathcal{P}_{p_{l+3}}\\ p_{l+2}\le t^{1/3^{l+1}}}}\sum_{\substack{p_{l+1}\in\mathcal{P}_{p_{l+2}}\\ p_{l+1}>t^{1/3^l}}}\frac{p_{l+1}^{l-1}t}{\phi(p_{l+1})^l\log t}\\
&\qquad\ll\sum_{q\le y^k}\log q\sum_{\substack{a\in\mathbb{N}\\ q^a\le t^{1/3^k}}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le t^{1/3^{k-1}}}}\cdots\sum_{\substack{p_{l+2}\in\mathcal{P}_{p_{l+3}}\\ p_{l+2}\le t^{1/3^{l+1}}}}\sum_{\substack{p_{l+1}\in\mathcal{P}_{p_{l+2}}\\ p_{l+1}>t^{1/3^l}}}\frac{t}{p_{l+1}\log t}
\end{aligned}
$$

since p_l is prime and $l\le k$. By Brun-Titchmarsh (2.10) we get

$$
\begin{aligned}
&\ll\sum_{q\le y^k}\log q\sum_{\substack{a\in\mathbb{N}\\ q^a\le t^{1/3^k}}}\frac{t(\log\log t)^{k-l}}{q^a\log t}\\
&\ll\sum_{q\le y^k}\frac{t(\log\log t)^{k-l}\log q}{q\log t}\\
&\ll\frac{t(\log\log t)^{k-2}\log y}{\log t}
\end{aligned}
$$

by (2.3) and since $l \geq 2$. Hence we get

$$\sum_{p \leq t} h_k(p) = \sum_{q \leq y^k} \log q \sum_{\substack{a \in \mathbb{N} \\ q^a \leq t^{1/3^k}}} \sum_{\substack{p_k \in \mathcal{P}_{q^a} \\ p_k \leq t^{1/3^{k-1}}}} \sum_{\substack{p_{k-1} \in \mathcal{P}_{p_k} \\ p_{k-1} \leq t^{1/3^{k-2}}}} \cdots \sum_{\substack{p_2 \in \mathcal{P}_{p_3} \\ p_2 \leq t^{1/3}}} \pi(t, p_2, 1)$$
$$+ O\left(t^{1-1/3^k} \log t (\log\log t)^{k-2} y^k + \frac{t(\log\log t)^{k-2}\log y}{\log t}\right)$$

finishing the lemma. $\square$

3.9 Evaluation of the Main Term

Now we'll deal with the main term from Lemma 3.18. We will deal with estimating the individual sums recursively. Hence we wish to make the following definition.

Definition 3.19. Let $2 \leq l \leq k$ and $2 \leq u \leq t$. Then define

$$g_{k,l}(u) = \sum_{q \leq y^k} \log q \sum_{a \in \mathbb{N}} \sum_{\substack{p_k \in \mathcal{P}_{q^a} \\ p_k \leq u^{1/3^{l-1}}}} \sum_{\substack{p_{k-1} \in \mathcal{P}_{p_k} \\ p_{k-1} \leq u^{1/3^{l-2}}}} \cdots \sum_{\substack{p_{k-l+2} \in \mathcal{P}_{p_{k-l+3}} \\ p_{k-l+2} \leq u^{1/3}}} \pi(u; p_{k-l+2}, 1).$$

Note that $g_{k,k}(t)$ is the summation in Lemma 3.18. Next we'll exhibit a recursive formula satisfied by the $g_{k,l}$.

Lemma 3.20. *Let $3 \leq l \leq k$, then*

$$g_{k,l}(v) = \mathrm{li}(v) \int_2^{v^{1/3}} \frac{1}{u^2} g_{k,l-1}(u)du + O\left(\frac{v(\log\log v)^{l-2}\log y}{\log v}\right). \tag{3.15}$$

Proof. We'll proceed by approximating π by li and then use partial summation to recover π. Using Lemma 3.17 we get

$$g_{k,l}(v) = \sum_{q \leq y^k} \log q \sum_{a \in \mathbb{N}} \sum_{\substack{p_k \in \mathcal{P}_{q^a} \\ p_k \leq v^{1/3^{l-1}}}} \sum_{\substack{p_{k-1} \in \mathcal{P}_{p_k} \\ p_{k-1} \leq v^{1/3^{l-2}}}} \cdots \sum_{\substack{p_{k-l+2} \in \mathcal{P}_{p_{k-l+3}} \\ p_{k-l+2} \leq v^{1/3}}} \pi(v; p_{k-l+2}, 1)$$
$$= \sum_{q \leq y^k} \log q \sum_{a \in \mathbb{N}} \sum_{\substack{p_k \in \mathcal{P}_{q^a} \\ p_k \leq v^{1/3^{l-1}}}} \sum_{\substack{p_{k-1} \in \mathcal{P}_{p_k} \\ p_{k-1} \leq v^{1/3^{l-2}}}} \cdots \sum_{\substack{p_{k-l+2} \in \mathcal{P}_{p_{k-l+3}} \\ p_{k-l+2} \leq v^{1/3}}} \frac{\mathrm{li}(v)}{p_{k-l+2}}$$
$$+ O\left(\frac{v \log y}{\log v} + \mathrm{li}(v)(\log\log v)^{l-2}\right).$$

We use Euler summation on the inner sum to get

$$\sum_{\substack{p_{k-l+2}\in\mathcal{P}_{p_{k-l+3}}\\ p_{k-l+2}\le v^{1/3}}} \frac{1}{p_{k-l+2}} = \frac{\pi(v^{1/3};p_{k-l+3},1)}{v^{1/3}} + \int_2^{v^{1/3}} \frac{\pi(u;p_{k-l+3},1)}{u^2}du.$$

Our function then becomes

$$\begin{aligned} g_{k,l}(v) = \mathrm{li}(v) \sum_{q\le y^k} \log q \sum_{a\in\mathbb{N}} \sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}} \sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}} \cdots \\ \sum_{\substack{p_{k-l+3}\in\mathcal{P}_{p_{k-l+4}}\\ p_{k-l+3}\le v^{1/3}}} \left(\frac{\pi(v^{1/3};p_{k-l+3},1)}{v^{1/3}} + \int_2^{v^{1/3}} \frac{\pi(u;p_{k-l+3},1)}{u^2}du\right) \\ + O\left(\frac{v\log y}{\log v} + \mathrm{li}(v)(\log\log v)^{l-2}\right). \end{aligned}$$

We trivially estimate $\pi(x;q,1)$ by x/q inside the sum and then use Brun–Titchmarsh (2.10) to get

$$\begin{aligned} &\sum_{q\le y^k} \log q \sum_{a\in\mathbb{N}} \sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}} \sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}} \cdots \sum_{\substack{p_{k-l+3}\in\mathcal{P}_{p_{k-l+4}}\\ p_{k-l+3}\le v^{1/3}}} \frac{\pi(v^{1/3};p_{k-l+3},1)}{v^{1/3}} \\ &\quad\ll \sum_{q\le y^k} \log q \sum_{a\in\mathbb{N}} \sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\le v^{1/3^{l-1}}}} \sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ p_{k-1}\le v^{1/3^{l-2}}}} \cdots \sum_{\substack{p_{k-l+3}\in\mathcal{P}_{p_{k-l+4}}\\ p_{k-l+3}\le v^{1/3}}} \frac{1}{p_{k-l+3}} \\ &\quad\ll \sum_{q\le y^k} \log q \sum_{a\in\mathbb{N}} \frac{(\log\log v)^{l-2}}{q^a} \\ &\quad\ll \sum_{q\le y^k} \log q \frac{(\log\log v)^{l-2}}{q} \\ &\quad\ll (\log\log v)^{l-2}\log y. \end{aligned}$$

Multiplying through by $\mathrm{li}(v)$ finishes the lemma. $\square$

We now require a lemma to find the asymptotic formula for h_k using the previous recurrence relation.

Lemma 3.21. *Let* $2 \leq l \leq k$.

$$g_{k,l}(u) = \frac{ku(\log\log u)^{l-1}\log y}{(l-1)!\log u} + O\left(\frac{u(\log\log u)^{l-1}}{\log u} + \frac{u(\log\log u)^{l-2}\log^2 y}{\log u}\right)$$

which implies

$$\sum_{p\leq t} h_k(p) = \frac{kt(\log\log t)^{k-1}\log y}{(k-1)!\log t} + O\left(\frac{t(\log\log t)^{k-1}}{\log t}\right.$$
$$\left. + \frac{t(\log\log t)^{k-2}\log^2 y}{\log t} + t^{1-1/3^k}\log t(\log\log t)^{k-2}y^k\right).$$

Proof. The second formula is derived from the first by setting $l = k$, $u = t$ and using Lemma 3.18. We'll proceed with the first formula by induction on l. Using the estimates we obtained via Bombieri–Vinogradov (2.13) in Lemma 3.17, we have for $l = 2$

$$\begin{aligned} g_{k,2}(u) &= \sum_{q\leq y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\leq u^{1/3}}}\pi(u;p_k,1) \\ &= \mathrm{li}(u)\sum_{q\leq y^k}\log q\sum_{a\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q^a}\\ p_k\leq u^{1/3}}}\frac{1}{p_k} + O\left(\mathrm{li}(u) + \frac{u\log y}{\log u}\right). \end{aligned}$$

We then use (2.12) and

$$\log\log(u^{1/3}) = \log\log u + O(1)$$

to get

$$\begin{aligned}
g_{k,2}(u) &= \mathrm{li}(u) \sum_{q \le y^k} \log q \sum_{a \in \mathbb{N}} \left(\frac{\log\log u^{1/3}}{\phi(q^a)} + O\left(\frac{\log(q^a)}{\phi(q^a)} \right) \right) + O\left(\frac{u \log y}{\log u} \right) \\
&= \mathrm{li}(u)(\log\log u + O(1)) \sum_{q \le y^k} \log q \sum_{a \in \mathbb{N}} \left(\frac{1}{q^a} \right. \\
&\qquad \left. + O\left(\frac{1}{q^{a+1}} \right) \right) + O\left(\mathrm{li}(u) \sum_{q \le y^k} \log^2 q \sum_{a \in \mathbb{N}} \frac{a}{q^a} \right) + O\left(\frac{u \log y}{\log u} \right) \\
&= \mathrm{li}(u)(\log\log u + O(1)) \sum_{q \le y^k} \left(\frac{\log q}{q} + O\left(\frac{\log q}{q^2} \right) \right) \\
&\qquad + O\left(\mathrm{li}(u) \sum_{q \le y^k} \frac{\log^2 q}{q} + \frac{u \log y}{\log u} \right) \\
&= \mathrm{li}(u) \log\log u \log(y^k) + O\left(\mathrm{li}(u)(\log y + \log\log u + \log^2 y) + \frac{u \log y}{\log u} \right) \\
&= \frac{ku \log\log u \log y}{\log u} + O\left(\frac{u \log\log u}{\log u} + \frac{u \log^2 y}{\log u} \right),
\end{aligned}$$

using equation (2.3), completing the base case. Now using Lemma 3.20 we get

$$\begin{aligned}
g_{k,l}(v) &= \mathrm{li}(v) \int_2^{v^{1/3}} \frac{1}{u^2} g_{k,l-1}(u) du + O\left(\frac{v (\log\log v)^{l-2} \log y}{\log v} \right) \\
&= \mathrm{li}(v) \int_2^{v^{1/3}} \frac{1}{u^2} \left(\frac{ku (\log\log u)^{l-2} \log y}{(l-2)! \log u} + O\left(\frac{u (\log\log u)^{l-2}}{\log u} \right. \right. \\
&\qquad \left. \left. + \frac{u (\log\log u)^{l-3} \log^2 y}{\log u} \right) \right) du + O\left(\frac{v (\log\log v)^{l-2} \log y}{\log v} \right) \\
&= \mathrm{li}(v) \int_2^{v^{1/3}} \left(\frac{k (\log\log u)^{l-2} \log y}{(l-2)! u \log u} + O\left(\frac{(\log\log u)^{l-2}}{u \log u} \right. \right. \\
&\qquad \left. \left. + \frac{(\log\log u)^{l-3} \log^2 y}{u \log u} \right) \right) du + O\left(\frac{v (\log\log v)^{l-2} \log y}{\log v} \right) \\
&= \frac{k \, \mathrm{li}(v) (\log\log v^{1/3})^{l-1} \log y}{(l-1)!} + O\left(\mathrm{li}(v) (\log\log v^{1/3})^{l-1} \right. \\
&\qquad \left. + \mathrm{li}(v) (\log\log v^{1/3})^{l-2} \log^2 y + \frac{v (\log\log v)^{l-2} \log y}{\log v} \right).
\end{aligned}$$

Once again by using

$$\log\log v^{1/3} = \log\log v + O(1)$$

we get

$$\begin{aligned}
&\frac{kv(\log\log v)^{l-1}\log y}{(l-1)!\log v} + O\bigg(\frac{v(\log\log v)^{l-1}}{\log v} \\
&\qquad + \frac{v(\log\log v)^{l-2}\log^2 y}{\log v} + \frac{v(\log\log v)^{l-2}\log y}{\log v}\bigg) \\
&\quad = \frac{kv(\log\log v)^{l-1}\log y}{(l-1)!\log v} + O\bigg(\frac{v(\log\log v)^{l-1}}{\log v} + \frac{v(\log\log v)^{l-2}\log^2 y}{\log v}\bigg),
\end{aligned}$$

completing the induction. □

3.10 The Proof of the First Moment

We now are in a position to prove the proposition for the first moment.

Proof of Proposition 3.13.

$$\begin{aligned}
M_1(x) &= \sum_{p\le x}\frac{h_k(p)}{p} \\
&= \sum_{p\le e^e}\frac{h_k(p)}{p} + \sum_{e^e<p\le x}\frac{h_k(p)}{p} \\
&= O(1) + \sum_{e^e<p\le x} h_k(p)\bigg(\frac{1}{x} + \int_p^x \frac{dt}{t^2}\bigg) \\
&= O(1) + \frac{1}{x}\sum_{e^e<p\le x} h_k(p) + \int_{e^e}^x \frac{dt}{t^2}\sum_{e^e<p\le t} h_k(p).
\end{aligned}$$

Using $t = x$ in Lemma 3.21 we get that

$$\sum_{e^e<p\le x} h_k(p) \ll \frac{xy^{k-1}\log y}{\log x}.$$

Since

$$\sum_{e^e<p\le t} h_k(p) \text{ and } \sum_{p\le t} h_k(p)$$

differ by a constant, we get that

$$\begin{aligned}M_1(x) = O(1) + \frac{1}{x}O\left(\frac{xy^{k-1}\log y}{\log x}\right) + \int_{e^e}^{x}\frac{dt}{t^2}\left(\frac{kt(\log\log t)^{k-1}\log y}{(k-1)!\log t}\right.\\ + O\left(\frac{t(\log\log t)^{k-1}}{\log t} + \frac{t(\log\log t)^{k-2}\log^2 y}{\log t}\right.\\ \left.\left. + t^{1-1/3^k}\log t(\log\log t)^{k-2}y^k\right)\right)\end{aligned}$$

using Lemma 3.21. Noting that

$$\begin{aligned}&\int_{e^e}^{x}\frac{dt}{t^2}t^{1-1/3^k}\log t(\log\log t)^{k-2}y^k\\ &\quad= \int_{e^e}^{x}\frac{y^k dt}{t^{1+\epsilon}}\\ &\quad\ll y^k,\end{aligned}$$

we conclude that $M_1(x)$ is

$$\begin{aligned}&O(y^k) + O\left(\frac{y^{k-1}\log y}{\log x}\right) + \int_{e^e}^{x}\frac{dt}{t^2}\left(\frac{kt(\log\log t)^{k-1}\log y}{(k-1)!\log t} + O\left(\frac{t(\log\log t)^{k-1}}{\log t}\right.\right.\\ &\qquad\left.\left. + \frac{t(\log\log t)^{k-2}\log^2 y}{\log t}\right)\right)\\ &\quad= O(y^k) + \frac{k(\log\log x)^k\log y}{k(k-1)!} + O\left((\log\log x)^k + (\log\log x)^{k-1}\log^2 y\right)\\ &\quad= \frac{y^k\log y}{(k-1)!} + O(y^k)\end{aligned}$$

as needed. □

3.11 The Proof of the Second Moment

We now turn our attention to the second moment. Our first lemma will bound the case where $p_3 = r_3$ and then we'll use the summations from Lemma 3.16 to take care of the rest.

Lemma 3.22.
$$\sum_{q_1,q_2\le y^k}\log q_1\log q_2\sum_{a_1,a_2\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q_1^{a_1}}\\ r_k\in\mathcal{P}_{q_2^{a_2}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ r_{k-1}\in\mathcal{P}_{r_k}}}\cdots\sum_{\substack{p_3\in\mathcal{P}_{p_4}\\ r_3\in\mathcal{P}_{r_4}}}\sum_{s\in\mathcal{P}_{p_3}\cap\mathcal{P}_{r_3}}\sum_{\substack{p\le t\\ p\in\mathcal{P}_s}}1$$
$$\ll t^{1-\epsilon}y^k\log y+\frac{t(\log\log t)^{2k-2}}{\log t}\log^2 y$$

for some $\epsilon>0$.

Proof. Our sum is
$$\sum_{q_1,q_2\le y^k}\log q_1\log q_2\sum_{a_1,a_2\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q_1^{a_1}}\\ r_k\in\mathcal{P}_{q_2^{a_2}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ r_{k-1}\in\mathcal{P}_{r_k}}}\cdots\sum_{\substack{p_3\in\mathcal{P}_{p_4}\\ r_3\in\mathcal{P}_{r_4}}}\sum_{s\in\mathcal{P}_{p_3}\cap\mathcal{P}_{r_3}}\sum_{\substack{p\le t\\ p\in\mathcal{P}_s}}1$$
$$=\sum_{q_1,q_2\le y^k}\log q_1\log q_2\sum_{a_1,a_2\in\mathbb{N}}\sum_{\substack{p_k\in\mathcal{P}_{q_1^{a_1}}\\ r_k\in\mathcal{P}_{q_2^{a_2}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ r_{k-1}\in\mathcal{P}_{r_k}}}\cdots\sum_{\substack{p_3\in\mathcal{P}_{p_4}\\ r_3\in\mathcal{P}_{r_4}}}\sum_{s\in\mathcal{P}_{p_3r_3}}\pi(t;s,1).$$

We split up into two cases. If $q_1^{a_1}q_2^{a_2}>t^\alpha$, then suppose $q_1^{a_1}>t^{\alpha/2}$. (the other case is analogous) Thus $p_3r_3>t^{\alpha/2}$. Hence Lemma 3.15 part (a) yields
$$\sum_{q_1,q_2\le y^k}\log q_1\log q_2\sum_{\substack{a_1,a_2\in\mathbb{N}\\ q_1^{a_1}>t^{\frac{\alpha}{2}}}}\sum_{\substack{p_k\in\mathcal{P}_{q_1^{a_1}}\\ r_k\in\mathcal{P}_{q_2^{a_2}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ r_{k-1}\in\mathcal{P}_{r_k}}}\cdots\sum_{\substack{p_3\in\mathcal{P}_{p_4}\\ r_3\in\mathcal{P}_{r_4}}}\sum_{s\in\mathcal{P}_{p_3r_3}}\pi(t;s,1)$$
$$\ll\sum_{q_1,q_2\le y^k}\log q_1\log q_2\sum_{\substack{a_1,a_2\in\mathbb{N}\\ q_1^{a_1}>t^{\frac{\alpha}{2}}}}\sum_{\substack{p_k\in\mathcal{P}_{q_1^{a_1}}\\ r_k\in\mathcal{P}_{q_2^{a_2}}}}\sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ r_{k-1}\in\mathcal{P}_{r_k}}}\cdots\sum_{\substack{p_3\in\mathcal{P}_{p_4}\\ r_3\in\mathcal{P}_{r_4}}}\frac{t\log t}{p_3r_3}$$
$$\ll\sum_{q_1,q_2\le y^k}\log q_1\log q_2\sum_{\substack{a_1,a_2\in\mathbb{N}\\ q_1^{a_1}>t^{\frac{\alpha}{2}}}}\frac{t\log t(\log\log t)^{2k-4}}{q_1^{\alpha_1}q_2^{\alpha_2}}.$$

using Brun–Titchmarsh (2.10). By letting $A=\min\{a|q_1^{a_1}>t^{\frac{\alpha}{2}}\}$ we get

$$\ll\sum_{q_1,q_2\le y^k}\log q_1\log q_2\frac{t\log t(\log\log t)^{2k-4}}{q_1^A q_2}$$
$$\le t^{1-\frac{\alpha}{2}}\log t(\log\log t)^{2k-4}\sum_{q_1\le y^k}\log q_1\sum_{q_2\le y^k}\frac{\log q_2}{q_2}$$
$$\ll t^{1-\epsilon}y^k\log y$$

by equations (2.1) and (2.3). If $q_1^{a_1} q_2^{a_2} \le t^\alpha$, then by Lemma 3.16 part (d) we get

$$\begin{aligned}
&\sum_{q_1,q_2 \le y^k} \log q_1 \log q_2 \sum_{\substack{a_1,a_2 \in \mathbb{N} \\ q_1^{a_1} q_2^{a_2} \le t^\alpha}} \sum_{\substack{p_k \in \mathcal{P}_{q_1^{a_1}} \\ r_k \in \mathcal{P}_{q_2^{a_2}}}} \sum_{\substack{p_{k-1} \in \mathcal{P}_{p_k} \\ r_{k-1} \in \mathcal{P}_{r_k}}} \cdots \sum_{\substack{p_3 \in \mathcal{P}_{p_4} \\ r_3 \in \mathcal{P}_{r_4}}} \sum_{s \in \mathcal{P}_{p_3 r_3}} \pi(t; s, 1) \\
&\qquad \ll \sum_{q_1,q_2 \le y^k} \log q_1 \log q_2 \sum_{\substack{a_1,a_2 \in \mathbb{N} \\ q_1^{a_1} q_2^{a_2} \le t^\alpha}} \frac{t(\log\log t)^{2k-2}}{q_1^{a_1} q_2^{a_2} \log t} \\
&\qquad \ll \sum_{q_1,q_2 \le y^k} \log q_1 \log q_2 \frac{t(\log\log t)^{2k-2}}{q_1 q_2 \log t} \\
&\qquad = \frac{t(\log\log t)^{2k-2}}{\log t} \left(\sum_{q \le y^k} \frac{\log q}{q} \right)^2 \\
&\qquad \ll \frac{t(\log\log t)^{2k-2}}{\log t} \log^2 y
\end{aligned}$$

by (2.3), completing the lemma.

$\square$

We now have enough to finish the second moment which is the final piece of the puzzle.

Proof of Proposition 3.14.

$$\begin{aligned}
\sum_{p \le t} h_k(p)^2 &= \sum_{p \le x} \left(\sum_{p_1 \mid p} \sum_{p_2 \mid p_1 - 1} \cdots \sum_{p_k \mid p_{k-1} - 1} \sum_{q \le y^k} \nu_q(p_k - 1) \log q \right)^2 \\
&= \sum_{q_1,q_2 \le y^k} \log q_1 \log q_2 \sum_{a_1,a_2 \in \mathbb{N}} \sum_{\substack{p_k \in \mathcal{P}_{q_1^{a_1}} \\ r_k \in \mathcal{P}_{q_2^{a_2}}}} \sum_{\substack{p_{k-1} \in \mathcal{P}_{p_k} \\ r_{k-1} \in \mathcal{P}_{r_k}}} \cdots \sum_{\substack{p_2 \in \mathcal{P}_{p_3} \\ r_2 \in \mathcal{P}_{r_3}}} \sum_{\substack{p \le t \\ p \in \mathcal{P}_{p_2} \\ p \in \mathcal{P}_{r_2}}} 1
\end{aligned}$$

since the condition $p_1 \mid p$ only occurs if $p_1 = p$. We then split up the sum according to whether or not $p_2 = r_2$. Lemma 3.22 deals with the part where $s = p_2 = r_2$ leaving us with

$$\sum_{q_1,q_2\le y^k} \log q_1 \log q_2 \sum_{a_1,a_2\in\mathbb{N}} \sum_{\substack{p_k\in\mathcal{P}_{q_1^{a_1}}\\ r_k\in\mathcal{P}_{q_2^{a_2}}}} \sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ r_{k-1}\in\mathcal{P}_{r_k}}} \dots \sum_{\substack{p_2\in\mathcal{P}_{p_3}\\ r_2\in\mathcal{P}_{r_3}\\ p_2\neq r_2}} \sum_{\substack{p\le t\\ p\in\mathcal{P}_{p_2}\\ p\in\mathcal{P}_{r_2}}} 1$$
$$+ O\left(t^{1-\epsilon}y^k \log y + \frac{t(\log\log t)^{2k-2}}{\log t}\log^2 y\right).$$

The sum becomes

$$\sum_{q_1,q_2\le y^k} \log q_1 \log q_2 \sum_{a_1,a_2\in\mathbb{N}} \sum_{\substack{p_k\in\mathcal{P}_{q_1^{a_1}}\\ r_k\in\mathcal{P}_{q_2^{a_2}}}} \sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ r_{k-1}\in\mathcal{P}_{r_k}}} \cdots \sum_{\substack{p_2\in\mathcal{P}_{p_3}\\ r_2\in\mathcal{P}_{r_3}}} \pi(t;p_2r_2,1).$$

If $q_1^{a_1} > t^{\alpha_1}$, then so is p_2, and hence by (3.10) we get

$$\begin{aligned}
&\sum_{q_1,q_2\le y^k} \log q_1 \log q_2 \sum_{\substack{a_1,a_2\in\mathbb{N}\\ q_1^{a_1}>t^{\alpha_1}}} \sum_{\substack{p_k\in\mathcal{P}_{q_1^{a_1}}\\ r_k\in\mathcal{P}_{q_2^{a_2}}}} \sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ r_{k-1}\in\mathcal{P}_{r_k}}} \cdots \sum_{\substack{p_3\in\mathcal{P}_{p_4}\\ r_3\in\mathcal{P}_{r_4}}} \frac{t\log^2 t}{p_3r_3}\\
&\ll \sum_{q_1,q_2\le y^k} \log q_1 \log q_2 \sum_{\substack{a_1,a_2\in\mathbb{N}\\ q_1^{a_1}>t^{\alpha_1}}} \frac{t\log^2 t(\log\log t)^{2k-4}}{q_1^{a_1}q_2^{a_2}}\\
&\ll t^{1-\alpha_1}\log^2 t(\log\log t)^{2k-4} \sum_{q_1,q_2\le y^k} \log q_1 \log q_2 \sum_{a_2\in\mathbb{N}} \frac{1}{q_2^{a_2}}\\
&\ll t^{1-\alpha_1}\log^2 t(\log\log t)^{2k-4} \sum_{q_1,q_2\le y^k} \frac{\log q_1 \log q_2}{q_2}\\
&\ll t^{1-\alpha_1}\log^2 t(\log\log t)^{2k-4}(y^k\log y).
\end{aligned}$$

We similarly get the same bound if $q_2^{a_2} > t^{\alpha_1}$. If neither of $q_1^{a_1}, q_2^{a_2}$ exceed t^{α_1}, then by (3.12) and using that for $b_i = q_i^{a_i}$

$$\frac{b_i}{\phi(b_i)} \ll 1, \frac{1}{\phi(b_i)} \ll \frac{1}{b_i},$$

we get

$$\begin{aligned}
\sum_{q_1,q_2\le y^k} \log q_1 \log q_2 & \sum_{\substack{a_1,a_2\in\mathbb{N}\\ q_1^{a_1},q_2^{a_2}\le t^{\alpha_1}}} \sum_{\substack{p_k\in\mathcal{P}_{q_1^{a_1}}\\ r_k\in\mathcal{P}_{q_2^{a_2}}}} \sum_{\substack{p_{k-1}\in\mathcal{P}_{p_k}\\ r_{k-1}\in\mathcal{P}_{r_k}}} \cdots \\
& \sum_{\substack{p_i\in\mathcal{P}_{p_{i+1}}\\ r_i\in\mathcal{P}_{r_{i+1}}}} \sum_{\substack{p_{i-1}\in\mathcal{P}_{p_i}\\ r_{i-1}\in\mathcal{P}_{r_i}}} \cdots \sum_{\substack{p_2\in\mathcal{P}_{p_3}\\ r_2\in\mathcal{P}_{r_3}}} \pi(t;p_2r_2,1) \\
& \ll \sum_{q_1,q_2\le y^k} \log q_1 \log q_2 \sum_{\substack{a_1,a_2\in\mathbb{N}\\ q_1^{a_1},q_2^{a_2}\le t^{\alpha_1}}} \frac{t(\log\log t)^{2k-2}}{q_1^{a_1}q_2^{a_2}\log t} \\
& \ll \frac{t(\log\log t)^{2k-2}}{\log t} \sum_{q_1,q_2\le y^k} \frac{\log q_1 \log q_2}{q_1q_2} \\
& \ll \frac{t(\log\log t)^{2k-2}\log^2 y}{\log t}.
\end{aligned}$$

The above gives us

$$\sum_{p\le t} h_k(p)^2 \ll t^{1-\epsilon} y^k \log y + \frac{t(\log\log t)^{2k-2}\log^2 y}{\log t}.$$

Using partial summation we have

$$\begin{aligned}
M_2(x) = \sum_{p\le x}\frac{h_k(p)^2}{p} &= \sum_{p\le e^e}\frac{h_k(p)^2}{p} + \frac{1}{x}\sum_{e^e\le p\le x} h_k(p)^2 + \int_{e^e}^{x}\frac{dt}{t^2}\sum_{e^e\le p\le t} h_k(p)^2 \\
&\ll 1 + \frac{1}{x}\left(x^{1-\epsilon}y^k\log y + \frac{x(\log\log x)^{2k-2}\log^2 y}{\log x}\right) \\
&\quad + \int_{e^e}^{x}\left(t^{-1-\epsilon}y^k\log y + \frac{(\log\log t)^{2k-2}\log^2 y}{t\log t}\right)dt \\
&\ll \frac{y^{2k-2}\log^2 y}{\log x} + x^{-\epsilon}y^k\log y + (\log\log x)^{2k-1}\log^2 y \\
&\ll y^{2k-1}\log^2 y
\end{aligned}$$

completing the proof of Proposition 3.14 and hence Theorem 1.4. □

Chapter 4

Iterates Between ϕ and λ

We now turn our attention to the proof of Theorem 1.5. It will be necessary to use the following upper bound for the Carmichael function of a product.

Lemma 4.1. *Let a, b be natural numbers, then*

$$\lambda(ab) \leq b\lambda(a). \tag{4.1}$$

Proof. We first note that it suffices to show the inequality whenever b is prime, because if

$$b = p_1 \dots p_k$$

where the p_i are not necessarily distinct, then repeated use of the theorem where b is prime yields

$$\lambda(ab) = \lambda(ap_1 \dots p_k) \leq p_1\lambda(ap_2 \dots p_k) \leq \dots \leq p_1 \dots p_k\lambda(a) = b\lambda(a).$$

If b is a prime which divides a, then for some $e > 0$

$$a = b^e p_1^{e_1} \dots p_k^{e_k} \text{ and } ab = b^{e+1} p_1^{e_1} \dots p_k^{e_k}.$$

Therefore

$$\begin{aligned}
\lambda(ab) &= \operatorname{lcm}\left(\lambda(b^{e+1}), \lambda(p_1^{e_1}), \dots, \lambda(p_k^{e_k})\right) \\
&\leq \operatorname{lcm}\left(b\lambda(b^e), \lambda(p_1^{e_1}), \dots, \lambda(p_k^{e_k})\right) \\
&\leq b * \operatorname{lcm}\left(\lambda(b^e), \lambda(p_1^{e_1}), \dots, \lambda(p_k^{e_k})\right) \\
&= b\lambda(a)
\end{aligned}$$

where the first inequality is in fact an equality if $b^e = 4$. (Also note that in this case, it would not be hard to show that $\lambda(ab) \mid b\lambda(a)$.) If $(a, b) = 1$, then $e = 0$ and

$$\begin{aligned}
\lambda(ab) &= \operatorname{lcm}\Big(b-1, \lambda(p_1^{e_1}), \ldots, \lambda(p_k^{e_k})\Big) \\
&\le (b-1)\operatorname{lcm}\Big(\lambda(p_1^{e_1}), \ldots, \lambda(p_k^{e_k})\Big) \\
&< b\lambda(a),
\end{aligned}$$

ending the proposition. □

Suppose that $g(n)$ is an arithmetic function of the form $\phi(h(n))$ where $h(n)$ is a $(k-1)$–fold iterate involving ϕ and λ. Note that if $a \mid b$, then $\lambda(a) \mid \phi(b)$ since $\lambda(a) \mid \phi(a) \mid \phi(ma)$ for any m. More easily we see $\lambda(a) \mid \lambda(b)$ and $\phi(a) \mid \phi(b)$. Inductively we can therefore show $\lambda_k(n) \mid g(n)$. Thus we can use equation (4.1) to get

$$\lambda_{l+k}(n) \le \lambda_l(g(n)) = \lambda_l\left(\frac{g(n)}{\lambda_k(n)}\lambda_k(n)\right) \le \lambda_{l+k}(n)\frac{g(n)}{\lambda_k(n)}.$$

Since $g(n) \le n$ we have that

$$\frac{g(n)}{\lambda_k(n)} \le \frac{n}{\lambda_k(n)} = \exp\left(\frac{1}{(k-1)!}(1+o_k(1))(\log\log n)^k \log\log\log n\right)$$

by Theorem 1.4 for almost all n. Hence

$$\begin{aligned}
\lambda_{l+k}(n) &\le \lambda_l(g(n)) \\
&\le \lambda_l\left(\frac{g(n)}{\lambda_k(n)}\lambda_k(n)\right) \\
&\le \lambda_{l+k}(n)\exp\left(\frac{1}{(k-1)!}(\log\log n)^k(1+o_k(1))\log\log\log n\right)
\end{aligned}$$

for almost all n. From the fact that

$$\lambda_{l+k}(n) = n\exp\left(-\frac{1}{(k+l-1)!}(1+o_{l,k}(1))(\log\log n)^{k+l}\log\log\log n\right)$$

we get

$$\lambda_l(g(n)) = n\exp\left(-\frac{1}{(k+l-1)!}(1+o_{l,k}(1))(\log\log n)^{k+l}\log\log\log n\right)$$

for almost all n. As for $\phi(g(n))$ we note that unless $g(n) = \phi_k(n)$, $g(n)$ can be writen as $\phi_l(h(n))$ where $h(n)$ is a $(k-l)$–fold iterate beginning with a λ. From above we can see that

$$h(n) = n \exp\left(-\frac{1}{(k-l-1)!}(1+o_k(1))(\log\log n)^{k-l}\log\log\log n\right)$$

and so $\phi(h(n))$ is bounded above by $h(n)$ and below by

$$\begin{aligned}
&\frac{h(n)}{e^\gamma \log\log h(n) + \frac{3}{\log\log h(n)}} \\
&\quad = \frac{h(n)}{e^\gamma \log\big(\log n - \frac{1}{(k-l-1)!}(1+o_k(1))(\log\log n)^{k-l}\log\log\log n\big)} \\
&\quad = \frac{h(n)}{e^\gamma \log\log n - O\big(\frac{1}{(k-l-1)!\log n}(1+o_k(1))(\log\log n)^{k-l}\log\log\log n\big)} \\
&\quad = h(n)\exp\big(O(\log\log\log n)\big)
\end{aligned}$$

which is within the error of $h(n)$. Hence any string of ϕ will not change our estimate. Therefore if $j(n)$ is a k–fold iteration of ϕ and λ which is not $\phi_k(n)$, but which begins with l copies of ϕ, then

$$j(n) = n \exp\left(-\frac{1}{(k-l-1)!}(1+o_k(1))(\log\log n)^{k-l}\log\log\log n\right)$$

yielding our theorem.

Chapter 5

Bounds on $L(n)$

In this chapter, we will be showing upper and lower bounds for the arithmetic function $L(n)$. Recall $L(n)$ is the smallest k such that $\lambda_k(n) = 1$. The height of the Pratt Tree is $H(p)$. Our goal is to prove Theorems 1.6 and 1.7. The former says there exists some $c > 0$ such that $L(n) \geq c \log\log n$ for almost all $n \leq x$. The latter says if $H(p) \leq (\log p)^\gamma$ for almost all $p \leq x$ outside a set of size $O\big(x \exp(-(\log x)^\delta)\big)$ for some $\delta > 0$, then for some function η, we have $L(n) \ll (\log n)^\gamma \eta(n)$ for almost all n as $n \to \infty$. Finally we justify a conjecture about the normal order of $L(n)$.

5.1 Lower Bound for $L(n)$

We start with two lemmas which establishes that $L(n) \geq L(p)$ provided $p \mid n$. This will be essential in our proof of the lower bound.

Lemma 5.1. *For all natural numbers a, b,*

$$\lambda(\mathrm{lcm}(a,b)) = \mathrm{lcm}(\lambda(a), \lambda(b)).$$

Proof. Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ where at least one of $\alpha_i, \beta_i > 0$. Then

$$\begin{aligned}
\mathrm{lcm}(\lambda(a), \lambda(b)) &= \mathrm{lcm}\left(\lambda(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}), \lambda(p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r})\right) \\
&= \mathrm{lcm}(\lambda(p_1^{\alpha_1}), \lambda\big(p_2^{\alpha_2}), \dots, \lambda(p_r^{\alpha_r}), \lambda(p_1^{\beta_1}), \lambda(p_2^{\beta_2}), \dots, \lambda(p_r^{\beta_r})\big) \\
&= \mathrm{lcm}\left(\lambda\big(p_1^{\max(\alpha_1,\beta_1)}\big), \lambda\big(p_2^{\max(\alpha_2,\beta_2)}\big), \dots, \lambda\big(p_r^{\max(\alpha_r,\beta_r)}\big)\right) \\
&= \lambda\left(p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_r^{\max(\alpha_r,\beta_r)}\right) \\
&= \lambda(\mathrm{lcm}(a,b)).
\end{aligned}$$

□

Lemma 5.2. *Given a positive integer $n = \prod_i^r p_i^{\alpha_i}$,* *(a)* $L(n) = \max_i\{L(p_i^{\alpha_i})\}$.

(b) $L(p^\alpha) = \alpha - 1 + L(p) \geq L(p)$ *for* $\alpha \geq 1$.

Note that these two equations imply $L(n) \geq L(p)$ *for all* $p \mid n$.

Proof. We show both parts by induction. For part (a) we show

$$\lambda_k(n) = \operatorname{lcm}\left(\lambda_k(p_1^{\alpha_1}), \ldots, \lambda_k(p_r^{\alpha_r})\right) \tag{5.1}$$

for $k \geq 0$. For $k = 0$, it is true by the definition of n. Suppose it's true for some k, then by Lemma 5.1

$$\begin{aligned} \lambda_{k+1}(n) = \lambda(\lambda_k(n)) &= \lambda\big(\operatorname{lcm}\left(\lambda_k(p_1^{\alpha_1}), \ldots, \lambda_k(p_r^{\alpha_r})\right)\big) \\ &= \operatorname{lcm}\left(\lambda\big(\lambda_k(p_1^{\alpha_1})\big), \ldots, \lambda\big(\lambda_k(p_r^{\alpha_r})\big)\right) \\ &= \operatorname{lcm}\left(\lambda_{k+1}(p_1^{\alpha_1}), \ldots, \lambda_{k+1}(p_r^{\alpha_r})\right) \end{aligned}$$

proving the induction. Equation (5.1) implies part (a) since the least common multiple of a set is 1 if and only if each number in the set is 1.

For part (b), we prove this by induction on α. If $\alpha = 1$ then the theorem is clearly true. Suppose $L(p^\alpha) = \alpha - 1 + L(p)$ then for $\alpha + 1$,

$$\lambda(p^{\alpha+1}) = p^\alpha \lambda(p).$$

Since $(p^\alpha, \lambda(p))$, by part (a),

$$L(p^\alpha\lambda(p)) = \max\left(L(p^\alpha), L(\lambda(p))\right) = \max\left(\alpha - 1 + L(p), L(p) - 1\right) = \alpha - 1 + L(p).$$

Therefore $L(p^{\alpha+1}) = \alpha + L(p)$, completing the induction and the theorem. □

For any $p \mid n$, we know that $L(n) \geq L(p)$, which implies that $L(n) > c \log\log p$ for almost all p. However, if all the primes p dividing n are small relative to n, or if n is divisible by exceptional primes, this will not imply that $L(n) > c\log\log n$. The proof of Theorem 1.6 therefore relies on showing that not many n are composed entirely of small primes as well as dealing with the exceptional set for which (1.6) doesn't hold.

Proof of Theorem 1.6. Let $Y = Y(x) \leq x$. Given c from equation (1.6), define a set $S(x) = S(x, Y) = \{p : p \geq Y, H(p) < c \log\log p\}$. From [10, Theorem 3] we have that $\#S(x) \ll x/(\log x)^K$ for some $K > 1$. If $p \mid n$ for some $p \notin S(x)$, and $p \geq Y$,

$$L(n) \geq L(p) \geq H(p) \geq c \log\log p \geq c \log\log Y.$$

Either there exists $p \geq Y, p \in S(x)$ such that $p \mid n$ or else n is composed entirely of primes less than or equal to Y. The number of $n \leq x$ where there exists $p \mid n$ with $p \in S(x)$ is bounded by

$$\begin{aligned}
\sum_{n \leq x} \sum_{\substack{p \mid n \\ p \in S(x)}} 1 &= \sum_{\substack{p \leq x \\ p \in S(x)}} \sum_{\substack{n \leq x \\ n \equiv 0 \pmod p}} 1 \\
&\leq \sum_{\substack{p \leq x \\ p \in S(x)}} \frac{x}{p} \\
&= x \int_Y^x \frac{d(S(t))}{t} \\
&= x \left(\frac{|S(x)|}{x} + \int_Y^x \frac{S(t)dt}{t^2} \right) \\
&\ll \frac{x}{\log^K x} + \int_Y^x \frac{dt}{t \log^K t} \\
&\ll \frac{x}{\log^{K-1} Y}
\end{aligned}$$

using partial summation. Let $\Psi(x, z)$ be the number of $n \leq x$ composed of primes $p \leq z$ and let $z = x^{1/u}$. Let $U > 0$, and $\rho(u)$ be the Dickman function which goes to 0 as $u \to \infty$. By [17, Theorem 7.2],

$$\Psi(x, z) \ll x\rho(u)$$

uniformly for $0 \leq u \leq U$. Given $\epsilon > 0$, choose Y such that $\log Y = (\log x)^{1-\epsilon}$. Since $Y < x^\gamma$ for all $\gamma > 0$, this choice yields $L(n) \geq c(1-\epsilon) \log\log x$ for all but $O\big(x/(\log Y)^{K-1} + \Psi(x, Y)\big) = o(x)$ such $n \leq x$, completing the theorem. $\square$

5.2 Upper Bound for $L(n)$

The Pratt tree for a prime p describes the primes q where $q \prec \cdots \prec p$. This is useful in calculating $L(p)$. However $L(p)$ is also increased by prime powers which the Pratt tree does not describe. The proof of Theorem 1.7 hinges on bounding the contribution of these large prime powers. We will show Theorem 1.7 is a corollary to the following main propostion, that the difference between $H(p)$ and $L(p)$ cannot be too great.

Proposition 5.3. *Let $b > 0$ and c be the constant from* (2.10)*. Suppose $H(p) \leq (\log p)^\gamma$ for all $p \leq x$ outside a set of size $O\big(x \exp(-(\log x)^\delta)\big)$ and let $\eta(x)$ be a function such that*

$$\frac{x(cy)^{(\log x)^\gamma + 1}}{2^{b(\log x)^\gamma \eta(x) - 2}} = o(x). \tag{5.2}$$

Then

$$L(n) \ll (\log x)^\gamma \eta(x)$$

for almost all $n \leq x$, for which the excluded n are divisible by at least one prime p in the above excluded set.

Note that if $\eta^*(x)$ is some function such that $b\eta^*(x)(\log x)^\gamma - \log(cy) \to \infty$ and $\eta(x) > \frac{1}{b \log 2} \log(cy) + \eta^*(x)$, then

$$\begin{aligned}\frac{x(cy)^{(\log x)^\gamma + 1}}{2^{b(\log x)^\gamma \eta(x) - 2}} &= \frac{x \exp\big(((\log x)^\gamma + 1) \log(cy)\big)}{\exp\big((b\eta(x)(\log x)^\gamma - 2) \log 2\big)} \\ &\ll x \exp\big(\log(cy) - b\eta^*(x)(\log x)^\gamma\big) = o(x).\end{aligned}$$

Specifically we can choose $\eta(x) \ll_b \log\log\log x$. The proof of Propostion 5.3 begins by analyzing the ways that $L(p)$ can be much larger than $H(p)$ and then showing in those cases that it cannot happen for many p.

Proof of Proposition 5.3. Let $n = \prod p_i^{\alpha_i}$ be the prime factorization of n where $H(p) \leq (\log p)^\gamma$ for all p dividing n. By equations (1.7) and (1.8), $L(n) = \max_i\{\alpha_i - 1 + L(p)\}$. Our first goal is to show that the number of n for which there exists a large α with $p^\alpha \mid n$ is small. Fixing a prime p and $\alpha \geq 2$, the number $n \leq x$ such that $p^\alpha \mid n$ is at most x/p^α. Hence the number of bad n is bounded by

$$\sum_{p \leq x} \frac{x}{p^\alpha} \leq x \sum_{m=2}^{x} \frac{1}{m^\alpha} \ll x \int_2^\infty t^{-\alpha} dt = \frac{x}{(\alpha - 1)2^{\alpha - 1}}.$$

Therefore the number of bad n is bounded is $o(x)$ for any choice of $\alpha = \xi(x)$ with $\xi(x) \to \infty$. Therefore for almost all $n \leq x$ we can assume

$$L(n) \leq \max_{p \mid n}(L(p) + \xi(x)) = \max_{p \mid n}(L(p) + o((\log x)^\gamma)$$

by taking $\xi(x) = o((\log x)^\gamma)$.

Let $\eta(x)$ be a function satifying the hypothesis of the proposition. We must determine how $L(p)$ can be larger than $H(p)$ and by how much. First note that for any prime in the Pratt tree, the difference between the factors of $q-1$ and the primes in the Pratt tree are just the powers of that prime which divide $q-1$. Therefore, if we have a branch of the Pratt tree, $2 = q_k \prec q_{k-1} \prec \cdots \prec q_1 \prec q_0 = p$, then $L(p) \le \max\{H(p) + \sum_{i=1}^k (\alpha_i - 1)\}$ where $q_i^{\alpha_i} \| q_{i-1} - 1$ and the max is taken over all the branches of the Pratt tree. The inequality $q_i^{\alpha_i} < q_{i-1}$ holds for all i which implies

$$2^{\prod_{i=1}^k \alpha_i} < p.$$

Therefore we need to maximize the sum $\sum_{i=1}^k (\alpha_i - 1)$ subject to $\prod_{i=1}^k \alpha_i < \log x / \log 2$.

Suppose we have $rs = tu$, where $2 \le r, s, t, u \le M$. The larger of $r+s$ and $t+u$ will be where the two terms are further apart. Consequently if we wish to maximize a sum subject a fixed product and number of terms, we want some terms to be the lowest possible value, in this case 2, and the rest to be the largest value, in this case M.

Suppose for the purpose of contradiction, that $\sum_{i=1}^k (\alpha_i - 1) \gg \eta(x)(\log x)^\gamma$, where $2 \le \alpha_i \le M$ and $M \le b\eta(x)(\log x)^\gamma$ for any constant b. By the above reasoning we know the sum is bounded by $2(k-l) + lM$ for some $l \le k$. However, $M^l \le \log x / \log 2$ implying $l \le (\log\log x - \log\log 2)/\log M$. Since $k \ll \log\log x$, we conclude $2(k-l) + lM$ is bounded above by

$$O\Big(\log\log x + M(\log\log x - \log\log 2)/\log M\Big) = o\big(\eta(x)(\log x)^\gamma\big),$$

contradicting the fact that the sum is $\gg \eta(x)(\log x)^\gamma$. As a result, either $\sum_{i=1}^k (\alpha_i - 1) \ll \eta(x)(\log x)^\gamma$, completing the theorem, or $M \ge b\eta(x)(\log x)^\gamma$. In the latter case, there exists some $\alpha_i \ge b\eta(x)(\log x)^\gamma$ for some $b > 0$.

It remains to show that the number of $n \le x$ such that there exists $q^\alpha \mid q_{k-1} - 1, q_{k-1} \mid q_{k-2} - 1, \ldots, q_1 \mid p - 1, p \mid n$, with $\alpha \ge b\eta(x)(\log x)^\gamma$ is $o(x)$. Note that $k \le H(p) \le (\log x)^\gamma$. By Lemma 2.2, the number of n is bounded by

$$\sum_{\alpha \ge b\eta(x)(\log x)^\gamma} \sum_{k \le (\log x)^\gamma} \sum_q \frac{x(cy)^k}{q^\alpha}.$$

Summing q over all integers at least 2 instead of primes as above and using $\alpha \geq 2$ makes this

$$\ll \sum_{\alpha \geq b\eta(x)(\log x)^\gamma} \sum_{k \leq (\log x)^\gamma} \frac{x(cy)^k}{2^{\alpha-1}}.$$

Summing the geometric series under both α and k yields

$$\ll \frac{x(cy)^{(\log x)^\gamma+1}}{2^{b\eta(x)(\log x)^\gamma-2}}.$$

By the choice of η this is $o(x)$ and hence for almost all $n \leq x$,

$$\begin{aligned} L(n) &\leq o((\log x)^\gamma) + \max_{p|n} \left\{ H(p) + \sum_{i=1}^{k} (\alpha_i - 1) \right\} \\ &\ll (\log n)^\gamma + \eta(x)(\log x)^\gamma \\ &\ll \eta(x)(\log x)^\gamma. \end{aligned}$$

□

We are now in a position to prove Theorem 1.7. Proposition 5.3 yields the theorem provided n wasn't divisible by any primes for which (1.9) fails to hold, so it remains to consider when n is divisible by such a prime.

Proof of Theorem 1.7. Let $Y = Y(x) \to \infty$ such that $\log Y \ll (\log x)^\gamma$. As in the proof of Theorem 1.6 we know that the set of $n \leq x$ which are composed entirely of primes less than or equal to Y has density 0. Therefore we only need to consider values of n for which there exists a prime greater than Y where $H(p) > (\log p)^\gamma$. Let $S(x)$ be the set $\{Y < p \leq x \mid L(p) > (\log p)^\gamma\}$. Since $L(p) > H(p)$, by (1.9) we know that $\#S(x) \ll x \exp\left(-(\log t)^\delta\right)$. The number of $n \leq x$ where n is divisible by a prime in $S(x)$ is bounded by

$$\begin{aligned} \sum_{n \leq x} \sum_{\substack{p \in S(x) \\ p|n}} 1 &\leq \sum_{p \in S(x)} \frac{x}{p} \\ &= \frac{x|S(x)|}{x} + x \int_Y^x \frac{|S(t)| dt}{t^2} \\ &\ll x \exp\left(-(\log x)^\delta\right) + x \int_Y^x \frac{\exp\left(-(\log t)^\delta\right) dt}{t} \\ &\ll x \exp\left(-(\log x)^\delta\right) + \frac{x}{\log x} + \frac{x}{\log Y} \end{aligned}$$

using partial summation and $\exp(-(\log t)^\delta) \ll (\log t)^{-2}$. By our choice of Y the number of n is $o(x)$ completing the theorem. □

5.3 Conjecture for the Normal Order of $L(n)$.

The purpose of this section is to justify Conjecture 1.9 assuming the conjecture in [10, Conjecture 2] which says $H(p) = e\log\log p - \frac{3}{2}\log\log\log p + E(p)$ for a slow growing function $E(p)$, and for almost all p. Note that this implies both that $H(p) \sim e\log\log p$ and that $H(p) \leq \log\log p$ for almost all p. To justify our conjecture, we wish to analyze the difference $L(p) - H(p)$ to show that it is not too large. As we saw in the previous section, this difference is created when a branch of the Pratt tree has $p_i^a \mid p_{i-1} - 1$ where $a > 1$. Let $Y = Y(x) \leq x$. Also let a branch of the Pratt tree be $p_1 \succ p_2 \succ \cdots \succ p_l \succ p_{l+1} \succ \cdots \succ p_k = 2$ where $p_i^{a_i} \| p_{i-1} - 1$ and let l be the largest index such that $p_l > Y$. We will separate our arguments into there parts. First is the trivial case to show there are not too many primes after p_{l+1}. Then we deal with $i < l+1$, and $i = l+1$, by some probability arguments.

By the trivial estimate $L(n) \ll \log n$ we know $L(p_{l+1}) \ll \log Y$. By a suitable choice of Y this will be made to be $o(\log\log x)$.

For $i \leq l$, we wish to know the probability that n has a factor p^a, where $p > Y$. We use the following lemma.

Lemma 5.4. *The number of $n \leq x$ for which there exists $p > Y$ where $p^a \| n$ is $O(x/Y^{a-1})$.*

Proof. The number of n is bounded by

$$\sum_{n \leq x} \sum_{\substack{p > Y \\ p^a \| n}} 1 \leq \sum_{p > Y} \frac{x}{p^a} \ll \frac{x}{Y^{a-1}}.$$

□

By Lemma 5.4 we should expect a proportion of at most c/Y^a. This implies that the probability of $p_i^{a_i} \| p_{i-1} - 1$ where $(a_2 - 1) + (a_3 - 1) + \cdots + (a_l - 1) = \eta(x)$ is bounded by $c^l / Y^{\eta(x)}$. Since the number of possible branches of the Pratt tree is trivially bounded by $\log x$, the probability of there existing such a string of a_i is bounded by

$$1 - \left(1 - \frac{c^l}{Y^{\eta(x)}}\right)^{\log x}.$$

This bound will approach 0 provided $\log x = o\big(Y^{\eta(x)}/c^l\big)$. Under the assumption that $H(p) \leq e\log\log(p)$, we have $l \leq H(p) \leq e\log\log(p)$. Therefore a choice of $Y = \exp((\log\log x)^{3/4})$ and $\eta(x) = (\log\log x)^{3/4}$ makes the contribution to $L(p) - H(p)$ be $o(\log\log x)$ for $i \neq l+1$.

For $i = l+1$, we have $p_{l+1}^{a_{l+1}} \mid p_l - 1$. The remaining contribution to $L(p) - H(p)$ is $a_{l+1} - 1$, if $p_{l+1} > 2$ and $\lceil (a_{l+1}+1)/2 \rceil$ if $p_{l+1} = 2$. For the a_{l+1} to contribute a lot to $L(p)$, it must be at the end of a long prime chain, i.e. $l \gg \log\log p$, otherwise the conjectured value of $H(p)$ being $e \log\log p$ would nullify the contribution. To show this is unlikely, we use a result from [3] which implies that the number of primes at a *fixed* level n of the Pratt tree is $\sim (\log\log p)^n/n!$. If we allow some dependence and use $n = c\log\log p$, for $0 < c < \log\log p$ we get roughly $(e/c)^{c\log\log p} = (\log p)^{c\log(e/c)}$ primes at level n. We show that the probability of none of these primes being congruent to 1 modulo $p_{l+1}^{a_{l+1}}$ goes to 1 provided $p_{l+1}^{a_{l+1}}$ is large enough.

Suppose we have N primes. The probability that any one of them is congruent to 1 modulo r^a for a prime r and positive integer a, is $1/\phi(r^a)$. Assuming independence, the probability that none of the N primes are congruent to 1 modulo r^a is

$$\left(1 - \frac{1}{\phi(r^a)}\right)^N.$$

Let η be a function going to infinity. Furthermore, let $r^a > N\eta(N)$ be a prime power. Since r is prime, we know $\phi(r^a) \geq r^a/2$. This bound implies the probability is bounded below by

$$\left(1 - \frac{2}{r^a}\right)^N.$$

Using our lower bound on r^a we get

$$\left(1 - \frac{2}{r^a}\right)^N \geq 1 - \left(1 - \frac{2}{N\eta(N)}\right)^N \to 1,$$

since $\eta(N) \to \infty$.

We know wish to use the lower bound on r^a to bound a_{l+1} and therefore our contribution to $L(p) - H(p)$. Suppose $q_{l+1} \neq 2$. If the level $l \approx c\log\log p$, for almost all p, we expect

$$a_{l+1} \leq \frac{\log(N\log N)}{\log q_{l+1}} = \frac{c\log(e/c)}{\log q_{l+1}} \log\log p + O(\log_3 p).$$

Combining all the contributions along any particular branch, we get

$$L(p) \leq \left(c + \frac{c\log(e/c)}{\log q_{l+1}}\right) \log\log p + o(\log\log p). \tag{5.3}$$

If $q_{l+1} = 2$, since, $\lambda(2^a) = 2^{a-2}$ we get

$$\left(c + \frac{c\log(e/c)}{2\log 2}\right)\log\log p + o(\log_2 p) = \left(c + \frac{c\log(e/c)}{\log 4}\right)\log\log p + o(\log_2 p).$$

Consequently, 3 is the value of q_{l+1} which yields the largest coefficient of $\log\log p$ in (5.3). Since $c + c\log(e/c)/\log 3 \leq e$ for $0 < c < e$, we conclude that for almost all $p \leq x$, $L(p) \sim e\log\log p$. The reason that we can replace p by n is the same reason as in Theorem 1.6.

It may seem obvious to conclude $L(p) \sim e\log\log p$, since $H(p) \sim e\log\log p$. However, note that the function $\left(c + \frac{c\log(e/c)}{\log 2}\right)$ does not yield a maximum value of e, but instead has its maximum of $2/\log(2)$ at $c = 2$. This may suggest if we had a function $L'(n)$ similar to $L(n)$ except that $\lambda'(2^a) = 2^{a-1}$ for all positive integers a, that we may get a different normal order, perhaps even $2\log\log n/\log(2)$.

Chapter 6

Open Problems

Here is a list of open problems regarding $\lambda(n), L(n)$ and $H(p)$. Theorem 1.4 showed that the normal order of $\log \frac{n}{\lambda_k(n)}$ is $\frac{1}{(k-1)!}(\log\log n)^k \log\log\log n$. Theorem 1.5 showed that if $g(n) = \phi_l(\lambda(f(n)))$, where $f(n)$ is a $(k-1)$ iterated arithmetic function consisting of iterates of ϕ and λ, then the normal order of $\log(n/g(n))$ is $\frac{1}{(k-1)!}(\log\log n)^k \log\log\log n$. This is because $g(n)$ relates to n in the same way as $\lambda_k(n)$. However this doesn't explain the relationship between $g(n)$ and $\lambda_k(n)$. The question has been solved for $k=2$ by Kapoor [14].

Theorem 6.1. *The normal order of* $\log\left(\frac{\lambda(\phi(n))}{\lambda(\lambda(n))}\right)$ *is* $\log\log n \log\log\log n$.

It would be interesting to see if a similar result could be proven for higher values of k. Based on Theorem 6.1 is seems reasonable to think that if $f_1(n)$ and $f_2(n)$ are compositions of λ and ϕ, then

$$\log\left(\frac{\lambda(f_1(n))}{\lambda(f_2(n))}\right) \sim \log\left(\frac{f_1(n)}{f_2(n)}\right). \tag{6.1}$$

For example the normal order of $\log \frac{\lambda\lambda\phi\lambda\lambda\phi(n)}{\lambda_6(n)}$ is conjecturally

$$\log \frac{\phi\lambda\lambda\phi(n)}{\lambda_4(n)} \sim \frac{1}{3!}(\log\log n)^4 \log\log\log n.$$

It would also be interesting to see if there can be a more precise result of Theorem 1.4. In [9], for $k=1$, there is an improved result. Instead of simply $\log(n/\lambda(n)) = \log\log n(\log\log\log n + O(\psi(n)))$, they more precisely showed

$$\log\left(\frac{n}{\lambda(n)}\right) = \log\log n\Big(\log\log\log n + A + O\big((\log\log\log n)^{-1+\epsilon}\big)\Big) \tag{6.2}$$

for almost all n as $n \to \infty$. There is no result like (6.2) even for $k=2$. For $k=1$, the authors in [9] split up the primes q into four regions, namely $q \le y/\log y$, $y/\log y < q \le y\log y$, $y\log y < q \le y^2$ and $y^2 < q$. On the other hand in Theorem 1.4, as well as the theorem of Martin and Pomerance in [16], the values of q were only split up into the two regions $q \leq y^k$ and $q > y^k$. Perhaps reasoning closer to [9] can obtain a more precise estimate.

Another improvement would be a more uniform result for Theorem 1.4. The implicit constant is at least exponential in k, meaning the best uniform result wouldn't even get $k < \log\log\log\log n$. It's unlikely the methods of Chapter 3 will produce a more uniform result even with more careful consideration.

In [9], Erdős, Pomerance, and Schmutz obtained a lower bound for $\lambda(n)$ of $\exp\left(c_1 \log\log n \log\log\log n\right)$. With a different constant, they also obtained an upper bound of the same form for infinitely many n. It would be interesting to see if something similar could be done for $\lambda(\lambda(n))$ or more generally $\lambda_k(n)$. Naively inputting the lower bound into itself recursively can show a lower bound to be

$$\exp\left(c_k \log_{k+1}(n) \log_{k+2}(n)\right), \tag{6.3}$$

where $\log_k(n)$ is the k–th iterate of the log function. However, this may or may not be the "best" lower bound. Perhaps there are infinitely many n with an upper bound of the form (6.3) for $\lambda_k(n)$. If that is true, then it can be shown that for those n,

$$L(n) = k + L(\lambda_k(n)) \leq k + \frac{\log(\lambda_k(n))}{\log 2} + 1 \ll_k \log_{k+1}(n) \log_{k+2}(n)$$

settling a conjecture given in [16]. Even showing this for $k = 2$ would yield a better result than is currently known. If (6.3) is not a desirable lower bound, perhaps a better one could be found, along with a sequence of n which obtain that lower bound.

Another notable open problems regarding $\lambda(n)$ is the analog of the famous Carmichael conjecture. In [6], R.D. Carmichael made the following conjecture:

Conjecture 6.2. For any natural number m, the equation $\phi(n) = m$ does not have exactly one solution.

The conjecture is open for both ϕ as well as λ, although it's known to be true for λ conditionally using the generalized Riemann hypothesis. For λ, it is known from [2] that any counterexample is a multiple of the smallest one. Much more is known see [2] about the (probably non–existent) counterexample of the λ case.

Bibliography

[1] L.M. Adleman, C. Pomerance and R.S. Rumely. On distiguishing prime numbers from composite numbers, Ann. of Math. **117** (1983), 173–206.

[2] W.D. Banks, J. Friedlander, F. Luca, F. Pappalardi, and I.E. Shparlinski, Coincidences in the values of the Euler and Carmichael functions, Acta Arith., **122** (2006), 207–234.

[3] N. L. Bassily, I. Kátai and M. Wijsmuller, Number of prime divisors of $\phi_k(n)$, where ϕ_k is the k–fold iterate of ϕ, J. Number Theory **65** (1997), 226–239.

[4] W.D. Banks, F. Luca, F. Saidak and P. Stănică. Compositions with the Euler and Carmichael functions, Abh. Math. Sem. Univ. Hamburg., **75** (2005), 215–244.

[5] R.D. Carmichael. Note on a new number theory function, Bull. Amer. Math. Soc., **5** (1910), 232–238.

[6] R.D. Carmichael. Note on Euler's ϕ function, Bull. Amer. Math. Soc., **28** (1922), 109–110.

[7] H. Davenport, *Multiplicative Number Theory Third Edition*, Graduate Texts in Math., New York: Springer-Verlag, Vol. 74 (2000).

[8] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, On the normal behavior of the iterates of some arithmetic functions, in Analytic Number Theory (Allerton Park, IL, 1989), Progr. Math., **85** Birkhäuser Boston, Boston, MA, (1990), 165–204.

[9] P. Erdős, C. Pomerance, and E. Schmutz, Carmichael's lambda function, Acta Arith., **58** (1991), 363–385.

[10] K. Ford, S.V. Konyagin and F. Luca, Prime chains and Pratt trees, Geom. Funct. Anal., **20** (2010), 1231–1258.

[11] J. Friedlander, C. Pomerance and I.E. Shparlinski, Period of the power generator and small values of the Carmichael function, Math. Comp., **70** (2001), 1591–1605.

[12] H. Halberstam and H. Richert *Sieve Methods*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York (2004) London Mathematical Society Monographs, No.4.

[13] J.P. Kubilius, *Probabilistic Methods in the Theory of Numbers*, Translations of Mathetical Monographs, Vol. 11, American Math. Soc., Providence (1964).

[14] V. Kapoor, Asymptotic formulae for arithmetic functions, Ph.D. Thesis, The University of British Columbia, April 2011.

[15] G. Miller. Riemann's hypothesis and tests for primality, J. Comput. System Sci., **13** (1976), 300–317.

[16] G. Martin and C. Pomerance, The iterated Carmichael λ–function and the number of cycles of the power generator, Acta Arith., **118** (2005), no. 4, 305–335.

[17] H. Montgomery and R. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge University Press, New York (2007).

[18] C. Pomerance, On the distribution of amicable numbers, J. Reine Angew. Math., 293/294 (1977), 217–222.

[19] V. Pratt, Every prime has a succinct certificate, SIAM J. Comput., **4** (1975), no. 3, 214–220.

[20] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press, New York (1995).

[21] P. Turán, On a theorem of Hardy and Littlewood, J. London Math. Soc. **9** (1934), 274–276.

Appendix A

The Turan–Kubilius Inequality

The Turán–Kubilius Inequality is a result in probabilistic number theor. It is useful in finding normal orders of additive arithmetic functions. The theorem was originally proved in a special case by Turán [21] to prove the following theorem of Hardy and Littlewood. Let $\omega(n)$ be the number of distinct prime divisors of n, and $\Omega(n)$ be the number of prime divisors including multiplicity. For any $\delta > 0$, the number of $n \leq x$ for which

$$\omega(n) = \log\log n + O\Big((\log\log n)^{1/2+\delta}\Big)$$

fails to hold is $o(x)$. The analagous result for Ω holds as well. The methods of Turán were subsequently extended by Kubilius to more general additive functions.

Theorem A.1 (Turán–Kubilius)**.** *For any complex additive function f we have*

$$\sum_{n\leq x} |f(n) - A(x)|^2 \ll xB(x)^2 \tag{A.1}$$

where

$$A(x) = \sum_{p^k \leq x} \frac{f(p^k)(1-p^{-1})}{p^k}, \qquad B(x)^2 = \sum_{p^k\leq x} \frac{|f(p^k)|^2}{p^k}.$$

For a strongly additive function, that is $f(p^k) = f(p)$ for all $k \geq 1$, the theorem reduces to the following corollary.

Corollary A.2. *For any complex completely additive function f we have*

$$\sum_{n\leq x} |f(n) - M_1(x)|^2 \ll xM_2(x)^2$$

where

$$M_1(x) = \sum_{p\leq x} \frac{f(p)}{p}, \qquad M_2(x)^2 = \sum_{p\leq x} \frac{|f(p)|^2}{p}.$$

To see the redution to the corollary for strongly additive function, note that we can replace $B(x)^2$ by $M_2(x)^2$ because

$$\begin{aligned}
B(x)^2 &= \sum_{p^k \le x} \frac{|f(p)|^2}{p^k} \\
&\le \sum_{p \le x} |f(p)|^2 \sum_{k \ge 1} \frac{1}{p^k} \\
&\ll \sum_{p \le x} |f(p)|^2 \frac{1}{p}.
\end{aligned}$$

As for $A(x)$, the sum becomes

$$\begin{aligned}
A(x) &= \sum_{p^k \le x} \frac{f(p)(1-p^{-1})}{p^k} \\
&= \sum_{p^k \le x} \left(\frac{f(p)}{p^k} - \frac{f(p)}{p^{k+1}} \right)
\end{aligned}$$

Using Cauchy–Schwarz (2.14) the difference between $A(x)$ and $M_1(x)$ is at most

$$\sum_{p \le x} \frac{|f(p)|}{p^2} \le \left(\sum_{p \le x} \frac{1}{p^2} \sum_{p \le x} \frac{|f(p)|^2}{p^2} \right)^{1/2} \ll B(x).$$

Therefore

$$\begin{aligned}
\sum_{n \le x} |f(n) - M_1(x)|^2 &\le 2 \sum_{n \le x} \left(|f(n) - A(x)|^2 + |A(x) - M_1(x)|^2 \right) \\
&\ll x B(x)^2 \ll x M_2(x)^2.
\end{aligned}$$

Our proof of Theorem A.1 is taken mostly from [20, III.3 Theorem 1]. We will prove it for f real and positive. Note that proof for f real can be done by combining the positive and negative parts of f. The proof for f complex can be done by combining the real and imaginary parts of f.

Proof of Theorem A.1. For notational convience, let $A = A(x), B = B(x)$ and $S = S(x)$ be the sum in equation (A.1). Then

$$S = \sum_{n \le x} f^2(n) - 2A \sum_{n \le x} f(n) + \lfloor x \rfloor A^2 := S_2 - 2AS_1 + \lfloor x \rfloor A^2. \tag{A.2}$$

Since $f(n)$ is additive, $f(n) = \sum_{p^k \| n} f(p^k)$. Inserting this into S_1 yields

$$S_1 = \sum_{n \le x} \sum_{p^k \| n} f(p^k) = \sum_{p^k \le x} f(p^k) \left(\left\lfloor \frac{x}{p^k} \right\rfloor - \left\lfloor \frac{x}{p^{k+1}} \right\rfloor \right)$$
$$\ge xA - \sum_{p^k \le x} f(p^k)$$

using $\lfloor x \rfloor - \lfloor y \rfloor \ge x - y - 1$. As for S_2 we obtain

$$S_2 = \sum_{n \le x} \left(\sum_{p^k \| n} f(p^k) \right)^2 = \sum_{n \le x} \sum_{p^k \| n} f(p^k) \sum_{q^l \| n} f(q^l).$$

Splitting this up into the two cases where $p = q$ or $p \ne q$ yields

$$\begin{aligned} S_2 &= \sum_{p^k \le x} f^2(p^k) \sum_{\substack{n \le x \\ p^k \| n}} 1 + \sum_{\substack{p^k \le x \\ q^l \le x \\ q \ne p}} f(p^k) f(q^l) \sum_{\substack{n \le x \\ p^k \| n \\ q^l \| n}} 1 \\ &\le x \sum_{p^k \le x} \frac{f^2(p^k)}{p^k} + \sum_{\substack{p^k \le x \\ q^l \le x \\ q \ne p}} f(p^k) f(q^l) \left(\left\lfloor \frac{x}{p^k q^l} \right\rfloor \right. \\ &\qquad \left. - \left\lfloor \frac{x}{p^k q^{l+1}} \right\rfloor - \left\lfloor \frac{x}{p^{k+1} q^l} \right\rfloor + \left\lfloor \frac{x}{p^{k+1} q^{l+1}} \right\rfloor \right) \\ &\le xB^2 + x \sum_{\substack{p^k \le x \\ q^l \le x \\ q \ne p}} \frac{f(p^k)}{p^k} (1 - p^{-1}) \frac{f(q^l)}{q^l} (1 - q^{-1}) + 2 \sum_{\substack{p^k \le x \\ q^l \le x \\ q \ne p}} f(p^k) f(q^l) \end{aligned}$$

using $\lfloor x \rfloor - \lfloor y \rfloor \le x - y + 1$. Let the last sum be S_3. Inserting these estimates into (A.2) yields

$$S \le xB^2 + 2A \sum_{p^k \le x} f(p^k) + 2S_3 + A^2. \tag{A.3}$$

Using Cauchy–Schwarz (2.14) on S_3 yields

$$S_3 \le \left(\sum_{\substack{p^k \le x \\ q^l \le x}} \frac{f(p^k) f(q^l)}{p^k q^l} \sum_{\substack{p^k \le x \\ q^l \le x}} p^k q^l \right)^{1/2} \ll B^2 \left(\sum_{n \le x} n \right)^{1/2} \ll xB^2.$$

Using Cauchy–Schwarz (2.14) again yields

$$\sum_{p^k \le x} f(p^k) \le \Bigg(\sum_{p^k \le x} \frac{f^2(p^k)}{p^k} \sum_{p^k \le x} p^k \Bigg)^{1/2} = B \Bigg(\sum_{p^k \le x} p^k \Bigg)^{1/2}.$$

We would like to bound the sum by a sum over all $n \le x$ like in our bound for S_3, however that would give us an estimate of Bx which is too large. Instead we bound each term by x and bound the sum over prime powers by $\pi(x) + \pi(x^{1/2}) + \cdots \ll x/\log x$. This bound implies

$$\sum_{p^k \le x} f(p^k) \ll B \bigg(\frac{x^2}{\log x} \bigg)^{1/2} = B \frac{x}{\sqrt{\log x}}.$$

As for A we use an estimate of Mertens [17, Theorem 2.7 (d)] and Cauchy–Schwarz (2.14), implying

$$A \ll \sum_{p^k \le x} \frac{f(p^k)}{p^k} \le \Bigg(\sum_{p^k \le x} \frac{f^2(p^k)}{p^k} \sum_{p^k \le x} \frac{1}{p^k} \Bigg)^{1/2} \ll B (\log\log x)^{1/2}.$$

Putting all these estimates together with (A.3) yields

$$S \ll xB^2 + 2\Big(B(\log\log x)^{1/2} \Big) \Big(B \frac{x}{(\log x)^{1/2}} \Big) + 2xB^2 + B^2(\log\log x) \ll xB^2$$

completing the theorem. □

It's worth noting that the strongly additive condition is not necessary for the replacement of $B(x)$ with $M_2(x)$. See [13, Lemma 3.1] for a proof. Also note that the function $h_k(n)$ in the proof of Theorem 1.4 is a strongly additive function justifying our use of Corollary A.2.