Counting Integers with Restrictions on their Prime Factors

by

Jenna Downey

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

MASTER OF SCIENCE

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

April, 2019

The following individuals certify that they have read, and recommend to the Faculty of Graduate and Postdoctoral Studies for acceptance, a thesis/dissertation entitled:

Counting Integers with Restrictions on their Prime Factors

submitted by Jenna Downey in partial fulfillment of the requirement for

the degree of Master of Science

in Mathematics

Examining Committee:

Michael Bennett, Mathematics

Co-supervisor

Greg Martin, Mathematics

Co-supervisor

Abstract

In this thesis, we examine two problems that, on the surface, seem like pure group theory problems, but turn out to both be problems concerning counting integers with restrictions on their prime factors. Fixing an odd prime number q and a finite abelian q-group $H = \mathbb{Z}_{q^{\alpha_1}} \times \mathbb{Z}_{q^{\alpha_2}} \times \cdots \times \mathbb{Z}_{q^{\alpha_j}}$, our first aim is to find a counting function, $D(H, x)$, for the number of integers n up to x such that H is the Sylow q-subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. In Chapter 2, we prove that $D(H, x) \sim K_H x(\log\log x)^j/(\log x)^{1/(q-1)}$, where K_H is a constant depending on H.

The second problem that we examine in this thesis concerns counting the number of n up to x for which $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic and for which $(\mathbb{Z}/n\mathbb{Z})^\times$ is maximally non-cyclic, where $(\mathbb{Z}/n\mathbb{Z})^\times$ is said to be maximally non-cyclic if each of its invariant factors is squarefree. In Chapter 3, we prove that the number of n up to x such that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic is asymptotic to $\frac{3}{2}x/\log x$ and that the number of n up to x such that $(\mathbb{Z}/n\mathbb{Z})^\times$ is maximally non-cyclic is asymptotic to $C_f x/(\log x)^{1-\xi}$, where ξ is Artin's constant and C_f is the convergent product,

$$C_f = \frac{15}{14\Gamma(\xi)} \lim_{x\to\infty} \left(\prod_{\substack{p \le x \\ p-1 \text{ square-free}}} \left(1 + \frac{1}{p} + \frac{1}{p^2}\right) \prod_{p \le x} \left(1 - \frac{1}{p}\right)^{\xi} \right).$$

It turns out that both of these problems can be reduced to problems of counting integers with restrictions on their prime factors. This allows the problems to be addressed by classical techniques of analytic number theory.

Lay Summary

In mathematics, we have structures called groups, which are basically sets of objects which satisfy certain characteristics. If q is a prime number, a q-group is a group whose total number of elements is a power of q. A subgroup of a group G is a collection of elements in G who form a smaller group on their own and the Sylow q-subgroup of G, is a subgroup which has q^k elements, where q^k is the largest power of q which divides the total number of elements in G.

The first goal of this thesis is to fix an odd prime number q and a q-group H, and find a function that counts groups whose Sylow q-subgroup is H. The second goal of this thesis is to find functions that counts groups that are maximally non-cyclic. Note that we define maximally non-cyclic in Chapter 3.

Preface

This thesis is comprised of joint work with Dr. Greg Martin. We plan on submitting our results for publication.

Table of Contents

Chapter 1

Introduction

Problems concerning counting integers with restrictions on their prime factors has been a topic of interest to number theorists for many years. The study of squarefree integers, as well as friable integers (integers without large prime factors), are perfect examples of such problems. Of particular interest, in 1908, Landau published a paper [3] in which he investigated the question of counting integers up to x that can be written as the sum of two squares. Fermat had previously shown that this problem was equivalent to counting integers n that satisfied the following condition: if p is a prime congruent to 3 modulo 4 and r is the largest positive integer such that p^r divides n, then r is even. Similarly, in 2012, Ford, Luca and Moree published a paper [2] in which they investigated the problem of counting the number of integers n such that $\phi(n)$ is not divisible by q, where q is some fixed prime number. This is equivalent to counting the number of integers n such that q^2 does not divide n and if p is a prime divisor of n, then p is not congruent to 1 modulo q.

Abstract algebra, and in particular, group theory, can be a useful perspective from which to analyze such problems. For instance, it turns out that Ford, Luca and Moree's problem in [2] is equivalent to counting the integers n up to x for which the Sylow q-subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ is trivial. In response to a talk by Lee Troupe in 2017 at the Alberta Number Theory Days, Colin Weir asked if it was possible to count, for a fixed prime q and a fixed finite abelian q-group H, the number of n up to x for which H is the Sylow q-subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. This is the exact question that we will investigate throughout Chapter 2 of this thesis.

Let $\mathbb{Z}_n^\times = (\mathbb{Z}/n\mathbb{Z})^\times$ be the multiplicative group of integers modulo n. Also, let q be a fixed odd prime and let $G_q(n)$ denote the Sylow q-subgroup of $\mathbb{Z}_n^\times$, that is, the unique subgroup of $\mathbb{Z}_n^\times$ of order q^k, where q^k is the highest power of q that divides $\phi(n)$. Note that, throughout Chapter 2, q is always considered to be this fixed odd prime. Further, let $(q; \alpha_1, \alpha_2, \ldots, \alpha_j)$ denote the q-group $\mathbb{Z}_{q^{\alpha_1}} \times \mathbb{Z}_{q^{\alpha_2}} \times \cdots \times \mathbb{Z}_{q^{\alpha_j}}$, where $\alpha_1, \ldots, \alpha_j$ are positive integers, $\mathbb{Z}_{q^{\alpha_i}}$ is the cyclic group of integers modulo q^{α_i} for each i and $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_j$. Given a q-group, $(q; \alpha_1, \alpha_2, \ldots, \alpha_j)$, our goal is to count the number of positive integers n for which $G_q(n) = (q; \alpha_1, \alpha_2, \ldots, \alpha_j)$.

The main result of Chapter 2 is given in the following theorem.

Theorem 1.0.1. For a finite abelian q-group H, let $D(H,x) = \#\{n \leq x \colon G_q(n) = H\}$. Suppose that q is an odd prime and that $H = (q; \alpha_1, \alpha_2, \ldots, \alpha_j)$. Then,

$$D(H,x) = K_H\left(\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}}\right) + O\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right),$$

where K_H is a constant that depends on the group H that will be defined in Theorem 2.7.1.

In Chapter 3, we shift our focus to a different problem concerning counting integers with restrictions on their prime factors. This problem involves cyclic and maximally non-cyclic groups, where a finite abelian group is said to be maximally non-cyclic if each of its invariant factors is squarefree. Here, we show that the number of n up to x such that $\mathbb{Z}_n^\times$ is cyclic is asymptotic to $3/2 \cdot x/\log x$. The main result of this Chapter 3 is given in the following theorem.

Theorem 1.0.2. The number of integers n up to x such that $\mathbb{Z}_n^\times$ is maximally non-cyclic is asymptotic to $C_f x/(\log x)^{1-\xi}$, where

$$\xi = \prod_p \left(1 - \frac{1}{p(p-1)}\right)$$

is Artin's constant and C_f is the convergent product,

$$C_f = \frac{15}{14\Gamma(\xi)} \lim_{x\to\infty}\left(\prod_{\substack{p \leq x \\ p-1 \text{ square-free}}} \left(1 + \frac{1}{p} + \frac{1}{p^2}\right) \prod_{p\leq x}\left(1 - \frac{1}{p}\right)^{\xi}\right).$$

Chapter 2

Counting Finite Abelian Groups with a Prescribed Sylow q-Subgroup

2.1 Setup

In order to achieve our goal, we will introduce the following useful notation. For a finite abelian q-group H and a positive integer k, let $D(H,x)$ be defined as in Theorem 1.0.1 and let
$D_k(H,x) = \#\{n \leq x \colon q^k \parallel n, G_q(n) = H\}$, where $q^k \parallel n$ denotes that $q^k \mid n$ and $q^{k+1} \nmid n$.

We will spend most of this chapter evaluating $D_0((q;\alpha_1,\ldots,\alpha_j),x)$, since, as we will show in Sections 2.5 and 2.6, $D_k((q;\alpha_1,\ldots,\alpha_j),x)$ is closely related to $D_0((q;\alpha_1,\ldots,\alpha_j),x)$, for all $k \geq 1$. Since this is the case where $q \nmid n$, we can write n as the product of primes $n = 2^{\beta} p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$ where $\beta \geq 0$, $\beta_1, \beta_2, \ldots, \beta_t > 0$ and $q \neq p_i$ for each $1 \leq i \leq t$. Then, we can apply Chinese Remainder Theorem, to get that

$$\begin{aligned}
\mathbb{Z}_n^\times &\cong \mathbb{Z}_{2^\beta}^\times \times \mathbb{Z}_{p_1^{\beta_1}}^\times \times \mathbb{Z}_{p_2^{\beta_2}}^\times \times \cdots \times \mathbb{Z}_{p_t^{\beta_t}}^\times \\
&\cong \mathbb{Z}_{2^\beta}^\times \times \mathbb{Z}_{\phi(p_1^{\beta_1})} \times \mathbb{Z}_{\phi(p_2^{\beta_2})} \times \cdots \times \mathbb{Z}_{\phi(p_t^{\beta_t})} \\
&\cong \mathbb{Z}_{2^\beta}^\times \times \mathbb{Z}_{p_1^{\beta_1 - 1}} \times \mathbb{Z}_{p_1 - 1} \times \mathbb{Z}_{p_2^{\beta_2 - 1}} \times \mathbb{Z}_{p_2 - 1} \times \cdots \times \mathbb{Z}_{p_t^{\beta_t - 1}} \times \mathbb{Z}_{p_t - 1}.
\end{aligned}$$

Now, note that $\mathbb{Z}_{2^\beta}^\times$ will be isomorphic to the trivial group if β is 0 or 1, $\mathbb{Z}_2$ if β is 2 and $\mathbb{Z}_{2^{\beta-2}} \times \mathbb{Z}_2$ if β is at least 3. So, it follows that $\mathbb{Z}_{2^\beta}^\times$ will not contribute to the Sylow q-subgroup since for any odd prime q, $G_q(n)$ will be made up of only odd factors and the factorization of $\mathbb{Z}_{2^\beta}^\times$ only contains even factors. Also, note that since $q \neq p_i$ for each $1 \leq i \leq t$, it follows that none of the $\mathbb{Z}_{p_i^{\beta_i - 1}}$ factors will contribute to $G_q(n)$ either. So, it follows that $\mathbb{Z}_n^\times$ will have the same Sylow q-subgroup as $\mathbb{Z}_{p_1-1} \times \mathbb{Z}_{p_2-1} \times \cdots \times \mathbb{Z}_{p_t-1}$.

Thus, we have that $G_q(n) = (q;\alpha_1,\ldots,\alpha_j)$ if and only if the following conditions are satisfied:

- For each α_i in $\{\alpha_1, \ldots, \alpha_j\}$ such that $\alpha_i \neq \alpha_k$ for all $k \neq i$, there exists a unique prime divisor p_i of n such that $p_i \equiv 1 \pmod{q^{\alpha_i}}$ and $p_i \not\equiv 1 \pmod{q^{\alpha_i+1}}$.
- If there is a subset $\{\alpha_k, \alpha_{k+1}, \ldots, \alpha_{k+m}\}$ of $\{\alpha_1, \ldots, \alpha_j\}$ such that $\alpha_k = \alpha_{k+1} = \cdots = \alpha_{k+m}$, then, there exists a unique set of $m+1$ distinct primes, $\{p_k, p_{k+1}, \ldots, p_{k+m}\}$, up to relabelling, such that if p_i is in $\{p_k, p_{k+1}, \ldots, p_{k+m}\}$, then $p_i \equiv 1 \pmod{q^{\alpha_i}}$ and $p_i \not\equiv 1 \pmod{q^{\alpha_i+1}}$.
- For all prime divisors p of n such that $p \neq p_i$ for any $1 \leq i \leq j$, we have that $p \not\equiv 1 \pmod{q}$.

Now, by definition of D and D_k, notice that,

$$\begin{aligned} D((q;\alpha_1,\ldots,\alpha_j),x) &= \#\{n \leq x \colon G_q(n) = (q;\alpha_1,\ldots,\alpha_j)\} \\ &= \sum_{k=0}^{\infty} D_k((q;\alpha_1,\ldots,\alpha_j),x). \end{aligned}$$

Using similar reasoning as above, if q^{α_1+2} divides n, then the Sylow q-subgroup of $\mathbb{Z}_n^\times$ will include a $\mathbb{Z}_{q^{\alpha_1+1}}$, and thus, will not be $(q;\alpha_1,\ldots,\alpha_j)$. Therefore, we can see that $D_k((q;\alpha_1,\ldots,\alpha_j),x)$ will be equal to zero if k is greater than or equal to α_1+2 and so,

$$D((q;\alpha_1,\ldots,\alpha_j),x) = \sum_{k=0}^{\alpha_1+1} D_k((q;\alpha_1,\ldots,\alpha_j),x). \tag{2.1}$$

Before we can say more about D_0, we need the following two definitions.

Definition 2.1.1. For a nonzero integer x, define $\nu_q(x)$ to be the largest nonnegative integer k such that q^k divides x.

Definition 2.1.2 (Conjugate Partition)**.** Let $(\beta_1, \beta_2, \ldots)$ be a partition. Then, we define the conjugate partition $(b_1, b_2, \ldots)$ of $(\beta_1, \beta_2, \ldots)$ to be the partition whose Ferrers diagram is the transpose of the Ferrers diagram of $(\beta_1, \beta_2, \ldots)$. In other words, we define $(b_1, b_2, \ldots)$ to be the conjugate partition of $(\beta_1, \beta_2, \ldots)$ if $b_i = \#\{k \colon \beta_k \geq i\}$ for each natural number i.

The following proposition will be very useful in evaluating D_0.

Proposition 2.1.3. Let $H = (q;\alpha_1,\alpha_2,\ldots,\alpha_j)$. Then,

$$D_0(H,x) = C_H \sum_{\substack{p_1 \leq x \\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2 \leq x/p_1 \\ p_2 \neq p_1 \\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_j \leq x/p_1\cdots p_{j-1} \\ p_j \neq p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \sum_{\substack{m \leq x/p_1\cdots p_j \\ q \nmid m \\ (t \neq p_1,\ldots,p_j \text{ and } t \mid m) \Rightarrow t \not\equiv 1 \pmod{q}}} 1, \tag{2.2}$$

where t is prime. Here,

$$C_H = \prod_{k=1}^{\alpha_1-1} \frac{1}{(a_k - a_{k+1})!},$$

where $(a_1, \ldots, a_{\alpha_1})$ is the conjugate partition of $(\alpha_1, \ldots, \alpha_j)$.

Proof. First, notice that

$$\sum_{\substack{p_1 \le x \\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2 \le x/p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_j \le x/p_1\cdots p_{j-1} \\ p_j \ne p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \sum_{\substack{m \le x/p_1\cdots p_j \\ q\nmid m \\ (t\ne p_1,\ldots,p_j \text{ and } t\mid m)\Rightarrow t\not\equiv 1 \pmod q}} 1,$$

counts the number of natural numbers $n = p_1p_2\cdots p_jm$ up to x where $p_1,\ldots,p_j$ are primes and the following two statements hold:

- for each $i = 1,2,\ldots,j$, $p_i \equiv 1 \pmod{q^{\alpha_i}}$ and $p_i \not\equiv 1 \pmod{q^{\alpha_i+1}}$,
- m is an integer not divisible by q such that if t is a prime divisor of m, with $t \ne p_1,\ldots,p_j$, then q does not divide $t-1$.

Comparing this sum to our above conditions on D_0, we can see that the only difference between it and D_0, is that, in this sum, we count the 'good' n up to x multiple times if the α_i are not distinct. So, every time we get a sequence of m repeated α values, we need to multiply by $1/m!$ to ensure that we only count distinct values of n.

Notice that for each $k = 1,2,\ldots$, by definition of conjugate partitions, $a_k - a_{k+1} \ge 0$ since $\{\ell\colon \alpha_\ell > k+1\} \subset \{\ell\colon \alpha_\ell > k\}$. For any k, such that $a_k - a_{k+1}$ is equal to 0 or 1, $1/(a_k - a_{k+1})! = 1$, and thus, multiplying the above nested sum by $1/(a_k - a_{k+1})!$ will have no effect. Now, notice that, $a_k - a_{k+1} = m > 1$ for some k, m if and only if there is some $1 \le i < j$ such that $\alpha_i = \alpha_{i+1} = \cdots = \alpha_{i+m-1} = k+1$. Thus, if we have m repeated α values all equal to $k+1$, we need to multiply by $1/(a_k - a_{k+1})! = 1/m!$.

The above proposition follows from here. $\square$

2.2 Selberg–Delange Method

We will start by introducing the version of the Selberg–Delange Method given in [5]. In order to do so, we will first define two important properties of Dirichlet series.

Definition 2.2.1 (From [5])**.** Let $z \in \mathbb{C}, c_0 > 0, 0 < \delta \le 1, M > 0$. We say that a Dirichlet series $F(s)$ has the property $\mathcal{P}(z; c_0, \delta, M)$ if the Dirichlet series $G(s; z) := F(s)\zeta(s)^{-z}$ may be continued as a holomorphic function for $\sigma \ge 1 - c_0/(1 + \log^+ |\tau|)$, and, in this domain, satisfies the bound $|G(s; z)| \le M(1 + |\tau|)^{1-\delta}$.

Note that, for $\tau > 0$, $\log^+ |\tau| = \max\{0, \log \tau\}$.

Definition 2.2.2 (From [5])**.** Let $z \in \mathbb{C}, c_0 > 0, 0 < \delta \le 1, M > 0$. We say that a Dirichlet series $F(s) = \sum_{n\ge 1} a_n n^{-s}$ has the property $\mathcal{T}(z, w; c_0, \delta, M)$ if $F(s)$ has property $\mathcal{P}(z; c_0, \delta, M)$ and if there exists a sequence of non-negative real numbers $\{b_n\}_{n=1}^{\infty}$ such that $|a_n| \le b_n (n = 1, 2, \ldots)$, and the series $\sum_{n\ge 1} b_n n^{-s}$ satisfies $\mathcal{P}(w; c_0, \delta, M)$ for some complex number w.

Now, we can state a version of the Selberg–Delange method, adapted from Theorem 5.2 of [5], by setting $N = 0$.

Theorem 2.2.3 (Selberg–Delange Method)**.** Let $F(s) := \sum_{n\geq 1} a_n n^{-s}$ be a Dirichlet series that has the property $\mathcal{T}(z, w; c_0, \delta, M)$. Then, for $x \geq 3$, $A > 0$, $|z| \leq A$, and $|w| \leq A$, we have

$$\sum_{n\leq x} a_n = x(\log x)^{z-1}\left\{\frac{G(1;z)}{\Gamma(z)} + O\left(\frac{M}{\log x}\right)\right\},$$

where G is as in Definition 2.2.1 and Γ is the Euler Gamma function.

Proof. Let $F(s) := \sum_{n\geq 1} a_n n^{-s}$ be a Dirichlet series that has the property $\mathcal{T}(z, w; c_0, \delta, M)$, $x \geq 3$, $A > 0$, $|z| \leq A$, and $|w| \leq A$. Then, setting $N = 0$ in Theorem 5.2 of [5], we get that

$$\begin{aligned}\sum_{n\leq x} a_n &= x(\log x)^{z-1}\left\{\frac{\lambda_0(z)}{(\log x)^0} + O(MR_0(x))\right\}\\ &= x(\log x)^{z-1}\Big\{\lambda_0(z) + O(MR_0(x))\Big\}.\end{aligned}$$

Now, by Equation (5.16) of [5], we have that

$$R_0(x) = e^{-c_1\sqrt{\log x}} + \frac{1}{\log x},$$

where c_1 is some positive constant. Then, since $e^{-c_1\sqrt{\log x}} \ll 1/\log x$, it follows that $R_0(x) \ll 1/\log x$, and thus,

$$\sum_{n\leq x} a_n = x(\log x)^{z-1}\left\{\lambda_0(z) + O\left(\frac{M}{\log x}\right)\right\}.$$

Now, by Equation (5.13) in [5], we have that

$$\lambda_0(z) = \frac{1}{\Gamma(z)}\sum_{h+j=0}\frac{1}{h!j!}G^{(h)}(1;z)\gamma_j(z) = \frac{G(1;z)\gamma_0(z)}{\Gamma(z)},$$

where the γ_j are entire functions of z, that satisfy

$$Z(s;z) = \sum_{j\geq 0}\frac{1}{j!}\gamma_j(z)(s-1)^j,$$

on the disk $|s - 1| < 1$ where

$$Z(s;z) = \frac{((s-1)\zeta(s))^z}{s}.$$

Then, since $Z(1; z) = 1$ (p.279 of [5]), we can see that,

$$1 = Z(1;z) = \frac{1}{0!}\gamma_0(z) = \gamma_0(z).$$

Therefore, $\lambda_0(z) = G(1;z)/\Gamma(z)$, and thus,

$$\sum_{n\le x} a_n = x(\log x)^{z-1}\left\{\frac{G(1;z)}{\Gamma(z)} + O\left(\frac{M}{\log x}\right)\right\}.$$

$\square$

In this section, our goal is to find an asymptotic formula for the following sum:

$$\sum_{\substack{m\le x/p_1\cdots p_j \\ q\nmid m \\ (t\ne p_1,\dots,p_j \text{ and } t|m)\Rightarrow t\not\equiv 1 \ (\mathrm{mod}\ q)}} 1,$$

where t is prime.

However, in order to achieve this goal, we will start by using the Selberg Delange theorem to find an asymptotic formula for:

$$\sum_{\substack{n\le x \\ p|n\Rightarrow p\not\equiv 1 \ (\mathrm{mod}\ q)}} 1.$$

First, as setup, let

$$a_n = \begin{cases} 1, & \text{if } p \not\equiv 1 \ (\mathrm{mod}\ q) \text{ for all } p \mid n \\ 0, & \text{otherwise} \end{cases}$$

and let $F(s) := \sum_{n=1}^{\infty} a_n n^{-s}$. Then, since a_n is a multiplicative function of n, we can write F as an Euler product in the following way: $F(s) = \prod_{p\not\equiv 1 \ (\mathrm{mod}\ q)} (1-p^{-s})^{-1}$. Now, let $G(s;z) := F(s)\zeta(s)^{-z}$. In order to find an asymptotic formula for

$$\sum_{\substack{n\le x \\ p|n\Rightarrow p\not\equiv 1 \ (\mathrm{mod}\ q)}} 1,$$

we need the following series of three propositions.

Proposition 2.2.4. Let $A(s) = F(s)^{q-1}\zeta(s)^{-(q-1)}\prod_{\chi \ (\mathrm{mod}\ q)} L(s,\chi)$. Then, $A(s)$ can be analytically continued to $\sigma > 1/2$, where σ is the real part of s.

Proof. First, we can replace $F(s), \zeta(s)$, and $L(s,\chi)$ by their Euler products in the definition of $A(s)$ to get

$$\begin{aligned} A(s) &= \prod_{p\not\equiv 1 \ (\mathrm{mod}\ q)} \left(1-\frac{1}{p^s}\right)^{-(q-1)} \prod_{p} \left(1-\frac{1}{p^s}\right)^{q-1} \prod_{\chi \ (\mathrm{mod}\ q)} \prod_{p} \left(1-\frac{\chi(p)}{p^s}\right)^{-1} \\ &= \prod_{p\equiv 1 \ (\mathrm{mod}\ q)} \left(1-\frac{1}{p^s}\right)^{q-1} \prod_{\chi \ (\mathrm{mod}\ q)} \prod_{p} \left(1-\frac{\chi(p)}{p^s}\right)^{-1} \end{aligned}$$

So, we can write,

$$A(s) = \prod_p g_p\left(\frac{1}{p^s}\right)$$

where

$$g_p(x) = \left\{ \begin{array}{ll} (1-x)^{q-1} & \text{, if } p \equiv 1 \pmod q \\ 1 & \text{, if } p \not\equiv 1 \pmod q \end{array} \right\} \prod_{\chi \pmod q} (1-\chi(p)x)^{-1}.$$

By the generalized binomial theorem, $(1-x)^{q-1} = 1-(q-1)x + O(x^2)$, and $(1-\chi(p)x)^{-1} = 1+\chi(p)x + O(x^2)$. From this, we get that,

$$\prod_{\chi \pmod q} (1-\chi(p)x)^{-1} = \prod_{\chi \pmod q} (1+\chi(p)x + O(x^2)) = 1 + \left(\sum_{\chi \pmod q} \chi(p)\right) x + O(x^2).$$

By the orthogonality relations for χ, we know that

$$\sum_{\chi \pmod q} \chi(p) = \begin{cases} q-1, & \text{if } p \equiv 1 \pmod q, \\ 0, & \text{if } p \not\equiv 1 \pmod q. \end{cases}$$

Thus,

$$\prod_{\chi \pmod q} (1-\chi(p)x)^{-1} = \begin{cases} 1+(q-1)x+O(x^2), & \text{if } p \equiv 1 \pmod q, \\ 1+O(x^2), & \text{if } p \not\equiv 1 \pmod q. \end{cases}$$

So,

$$\begin{aligned} g_p(x) &= \left\{ \begin{array}{ll} 1-(q-1)x+O(x^2), & \text{if } p \equiv 1 \pmod q \\ 1, & \text{if } p \not\equiv 1 \pmod q \end{array} \right\} \left\{ \begin{array}{ll} 1+(q-1)x+O(x^2), & \text{if } p \equiv 1 \pmod q \\ 1+O(x^2), & \text{if } p \not\equiv 1 \pmod q \end{array} \right\} \\ &= 1+O(x^2), \end{aligned}$$

and thus,

$$A(s) = \prod_p \left(1 + O\left(\frac{1}{p^{2s}}\right)\right), \tag{2.3}$$

which converges for $\sigma > 1/2$. $\square$

Proposition 2.2.5. Let $A(s)$ be defined as in Proposition 2.2.4. Then, $G(s, 1-1/(q-1))$ can be analytically continued to $s = 1$.

Proof. First, notice that by rearranging the functions in the definition of $A(s)$, we get that

$$F(s)^{q-1} = A(s)\zeta(s)^{q-1} \prod_{\chi \pmod q} L(s,\chi)^{-1}. \tag{2.4}$$

Consider $L(s,\chi_0)^{-1}$, where χ_0 is the principal Dirichlet character modulo q. Notice that we can use algebraic manipulations to rewrite $L(s,\chi_0)^{-1}$ in the following way:

$$\begin{aligned} L(s,\chi_0)^{-1} = \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right) = \prod_{p\neq q} \left(1 - \frac{1}{p^s}\right) &= \left(1 - \frac{1}{q^s}\right)^{-1} \prod_p \left(1 - \frac{1}{p^s}\right) \\ &= \left(1 - \frac{1}{q^s}\right)^{-1} \zeta(s)^{-1}. \end{aligned} \tag{2.5}$$

Therefore, from equation (2.4), we have that

$$\begin{aligned} F(s)^{q-1} &= A(s)\zeta(s)^{q-1} \left(1 - \frac{1}{q^s}\right)^{-1} \zeta(s)^{-1} \prod_{\chi\neq\chi_0} L(s,\chi)^{-1} \\ &= A(s)\zeta(s)^{q-2} \left(1 - \frac{1}{q^s}\right)^{-1} \prod_{\chi\neq\chi_0} L(s,\chi)^{-1}. \end{aligned} \tag{2.6}$$

Thus, since $G(s;z) = F(s)\zeta(s)^{-z}$, we have that,

$$\begin{aligned} G\left(s; 1 - 1/(q-1)\right) &= F(s)\zeta(s)^{-(q-2)/(q-1)} \\ &= F(s)^{(q-1)/(q-1)}\zeta(s)^{-(q-2)/(q-1)} \\ &= \left(F(s)^{q-1}\zeta(s)^{-(q-2)}\right)^{1/(q-1)} \\ &= \left(A(s)\zeta(s)^{q-2}\left(1 - \frac{1}{q^s}\right)^{-1} \prod_{\chi\neq\chi_0} L(s,\chi)^{-1}\zeta(s)^{-(q-2)}\right)^{1/(q-1)} \\ &= \left(A(s)\left(1 - \frac{1}{q^s}\right)^{-1} \prod_{\chi\neq\chi_0} L(s,\chi)^{-1}\right)^{1/(q-1)}. \end{aligned} \tag{2.7}$$

Note that the analytic continuation of $G(s; 1 - 1/(q-1))$ to $s = 1$ follows from equations (2.3) and (2.7), since $L(1,\chi)$ is non-zero for χ non-principal. □

Before stating Proposition 2.2.7, we need the following definition.

Definition 2.2.6. Let m be an integer and let n be a positive integer such that $(m,n) = 1$. Then, we say that k is the order of m modulo n if k is the smallest positive integer such that $m^k \equiv 1 \pmod{n}$.

Proposition 2.2.7. For a prime number p, let k_p be the order of p modulo q. Then,

$$G(1; 1 - 1/(q-1)) = (1 - 1/q)^{-1/(q-1)} \prod_{\substack{p\neq q \\ p\not\equiv 1 \ (\mathrm{mod}\ q)}} (1 - 1/p^{k_p})^{-1/k_p} \prod_{\chi\neq\chi_0} L(1,\chi)^{-1/(q-1)}.$$

Proof. First, from equation (2.6), we get that

$$A(s) = F(s)^{q-1}\zeta(s)^{-(q-2)}\left(1 - \frac{1}{q^s}\right)\prod_{\chi\neq\chi_0} L(s,\chi)$$
$$= (1-1/q^s)\prod_{p\not\equiv 1 \pmod q}(1-1/p^s)^{-(q-1)}\prod_p (1-1/p^s)^{q-2}\prod_{\chi\neq\chi_0}\left(\prod_p (1-\chi(p)/p^s)^{-1}\right).$$

Now, when $p \equiv 1 \pmod q$, the local factor is

$$(1-1/p^s)^{q-2}\prod_{\chi\neq\chi_0}(1-\chi(p)/p^s)^{-1} = (1-1/p^s)^{q-2}(1-1/p^s)^{-(q-2)} = 1.$$

Similarly, when $p = q$, the local factor is

$$(1-1/p^s)(1-1/p^s)^{-(q-1)}(1-1/p^s)^{q-2}\prod_{\chi\neq\chi_0}(1-\chi(p)/p^s)^{-1} = \prod_{\chi\neq\chi_0}(1-0/p^s)^{-1} = 1.$$

For all other p, the local factor is

$$(1-1/p^s)^{-(q-1)}(1-1/p^s)^{q-2}\prod_{\chi\neq\chi_0}(1-\chi(p)/p^s)^{-1} = (1-1/p^s)^{-1}\prod_{\chi\neq\chi_0}(1-\chi(p)/p^s)^{-1}$$
$$= \prod_{\chi \pmod q}(1-\chi(p)/p^s)^{-1}.$$

Now, by the generalized binomial theorem, we have that $(1-\chi(p)/p^s)^{-1} = 1 + \chi(p)/p^s + O(1/p^{2s})$. So,

$$\prod_{\chi \pmod q}\left(1-\chi(p)p^{-s}\right)^{-1} = \prod_{\chi \pmod q}(1+\chi(p)p^{-s} + O(p^{-2s}))$$
$$= 1 + \left(\sum_{\chi \pmod q}\chi(p)\right)p^{-s} + O(p^{-2s}))$$
$$= 1 + O(p^{-2s}),$$

as expected since $A(s)$ converges for $\sigma > 1/2$ by Proposition 2.2.4.

Thus, we have that

$$A(s) = \prod_{\substack{p\neq q \\ p\not\equiv 1 \pmod q}}\prod_{\chi \pmod q}(1-\chi(p)/p^s)^{-1},$$

where A(s) converges for $\sigma > 1/2$, and hence,

$$A(1) = \prod_{\substack{p\neq q \\ p\not\equiv 1 \pmod q}}\prod_{\chi \pmod q}(1-\chi(p)/p)^{-1},$$

is convergent.

Now, we will evaluate the innermost product. First, letting $x = 1/p$, we get that

$$\prod_{\chi \text{ (mod } q)} (1 - \chi(p)/p)^{-1} = \prod_{\chi \text{ (mod } q)} (1 - \chi(p)x)^{-1}.$$

For any prime p, let k_p be the order of p modulo q. Then, since each k_p^{th} root of unity occurs exactly $(q-1)/k_p$ times among the values $\chi(p)$ as χ varies over all Dirichlet characters modulo q, we have that

$$\prod_{\chi \text{ (mod } q)} (1 - \chi(p)x)^{-1} = \prod_{j=1}^{k_p} (1 - e^{2\pi ij/k_p}x)^{-(q-1)/k_p}.$$

Now, since

$$x^{k_p} - 1 = \prod_{j=1}^{k_p} (x - e^{2\pi ij/k_p}),$$

we have that,

$$1 - 1/x^{k_p} = \prod_{j=1}^{k_p} (1 - e^{2\pi ij/k_p}/x).$$

Thus, replacing x by $1/x$, we see that

$$1 - x^{k_p} = \prod_{j=1}^{k_p} (1 - e^{2\pi ij/k_p}x).$$

Thus,

$$\prod_{j=1}^{k_p} (1 - e^{2\pi ij/k_p}x)^{-(q-1)/k_p} = (1 - x^{k_p})^{-(q-1)/k_p}.$$

So, it follows that,

$$\prod_{\chi \text{ (mod } q)} (1 - \chi(p)x)^{-1} = (1 - x^{k_p})^{-(q-1)/k_p},$$

and thus,

$$A(1) = \prod_{\substack{p \neq q \\ p \not\equiv 1 \text{ (mod } q)}} (1 - 1/p^{k_p})^{-(q-1)/k_p}.$$

Now, setting $s = 1$ in

$$G\left(s; 1 - 1/(q-1)\right) = \left(A(s) \left(1 - \frac{1}{q^s}\right)^{-1} \prod_{\chi \neq \chi_0} L(s, \chi)^{-1} \right)^{1/(q-1)}$$

we get that

$$
\begin{aligned}
G\left(1;1-1/(q-1)\right) &= A(1)^{1/(q-1)}\left(1-1/q\right)^{-1/(q-1)} \prod_{\chi\neq\chi_0} L(1,\chi)^{-1/\phi(q)} \\
&= \left(1-1/q\right)^{-1/(q-1)} \prod_{\substack{p\neq q \\ p\not\equiv 1 \ (\mathrm{mod}\ q)}} \left(1-1/p^{k_p}\right)^{-(q-1)/k_p} \prod_{\chi\neq\chi_0} L(1,\chi)^{-1/(q-1)}
\end{aligned}
$$

□

The following corollary to the Selberg–Delange Theorem gives an asymptotic formula for the desired sum.

Corollary 2.2.8. Let p be a prime number. Then, for $x \geq 3$,

$$
\sum_{\substack{n\leq x \\ p|n \Rightarrow p\not\equiv 1 \ (\mathrm{mod}\ q)}} 1 = B_q x(\log x)^{-1/(q-1)} + O(x(\log x)^{-1-1/(q-1)}),
$$

where

$$
B_q = \frac{G(1;1-1/(q-1))}{\Gamma(1-1/(q-1))},
$$

and $G(1;1-1/(q-1))$ is as in Proposition 2.2.7.

Proof. We will start by establishing some of the parameters required for the Selberg–Delange Theorem. First, let $z = 1-1/(q-1)$ and recall that

$$
G(s;1-1/(q-1)) = A(s)^{1/(q-1)}\left(1-\frac{1}{q^s}\right)^{-1/(q-1)} \prod_{\chi\neq\chi_0} L(s,\chi)^{-1/(q-1)}.
$$

Note that $A(s)$ converges for $\sigma > 1/2$ and $(1-1/q^s)^{-1/(q-1)}$ is well-defined for $\sigma > 0$. Now, from Theorem 11.3 of [4], it follows that if none of the Dirichlet characters χ (mod q) have an exceptional zero, then there exists an absolute constant $c > 0$ such that $L(s,\chi)$ has no zeros in the region $\sigma > 1 - c/\log(q(|\tau|+4))$. Note that since $\log^+|\tau|$ and $\log(|\tau|+4)$ differ by at most $\log(5)$, it follows that there exists a constant $c > 0$ such that $L(s,\chi)$ has no zeros in the region $\sigma > 1 - c/\log^+(q|\tau|)$. Now, since

$$
1 - c/\log^+(q|\tau|) = 1 - \frac{c/\log q}{1+\log^+|\tau|/\log q} < 1 - \frac{c/\log q}{1+\log^+|\tau|},
$$

we have that if $L(s,\chi)$ has no zeros in the region $\sigma > 1 - \frac{c/\log q}{1+\log^+|\tau|/\log q}$, then, $L(s,\chi)$ has no zeros in the region $\sigma > 1 - \frac{c/\log q}{1+\log^+|\tau|}$, and thus, $\prod_{\chi\neq\chi_0} L(s,\chi)^{-1/(q-1)}$ will be analytic for $\sigma > 1 - \frac{c/\log q}{1+\log^+|\tau|}$. Now, suppose that some Dirichlet character χ modulo q has an exceptional zero, $\beta \in \mathbb{R}, 1-c/\log^+(q|\tau|) < \beta < 1$. Then, we have that $L(s,\chi)$ has no zeros in the region $\sigma > 1-(1-\beta)/(1+\log^+|\tau|)$. Indeed, if $\sigma > 1-(1-\beta)/(1+\log^+|\tau|)$, then $1-\beta > (1-\beta)/(1+\log^+|\tau|) > 1-\sigma$, and thus, $\sigma > \beta$.

Therefore, putting everything together, we can see that $G(s; 1 - 1/(q-1))$ is analytic in the region $\sigma > 1 - \frac{c_0}{1+\log^+|\tau|}$, where $c_0 = c/\log q$, where c is the constant defined in Theorem 11.3 of [4], if every Dirichlet character χ (mod q) has no exceptional zero, and $c_0 = 1 - \beta$ if there is some Dirichlet character χ modulo q such that χ has an exceptional zero β.

Now, since $A(s)$ converges for $\sigma > 1/2$, we have that $|A(s)|^{1/(q-1)} \ll 1$ in the region $\sigma > 1 - \frac{c_0}{1+\log^+|\tau|}$. Similarly, since $(1 - 1/q^s)^{-1/(q-1)}$ is well-defined for $\sigma > 0$, $(1 - 1/q^s)^{-1/(q-1)} \ll 1$ in the region $\sigma > 1 - \frac{c_0}{1+\log^+|\tau|}$. Therefore, we have that

$$|G(s; 1 - 1/(q-1))| = |A(s)|^{1/(q-1)} \left|1 - \frac{1}{q^s}\right|^{-1/(q-1)} \prod_{\chi \neq \chi_0} |L(s,\chi)|^{-1/(q-1)} \ll \prod_{\chi \neq \chi_0} |L(s,\chi)|^{-1/(q-1)}.$$

Now, by Theorem 11.4 of [4], we know that $L(s;\chi)^{-1} \ll \log(q(|\tau|+4))$. From this, it follows that

$$\prod_{\chi \neq \chi_0} |L(s,\chi)|^{-1/(q-1)} \ll \prod_{\chi \neq \chi_0} |\log(q(|\tau|+4))|^{1/(q-1)} = |\log(q(|\tau|+4))|^{1-1/(q-1)}.$$

Fix $\epsilon > 0$. Then, since

$$\lim_{|\tau| \to \infty} \frac{\log(q(|\tau|+4))}{(1+|\tau|)^\epsilon} = 0,$$

we have that $\log(q(|\tau|+4)) = o((1+|\tau|)^\epsilon)$, and thus, $\log(q(|\tau|+4)) \ll (1+|\tau|)^\epsilon$.

Therefore, we get that

$$|G(s; 1 - 1/(q-1))| \ll \prod_{\chi \neq \chi_0} |L(s,\chi)|^{-1/(q-1)} \ll (\log(q(|\tau|+4)))^{1-1/(q-1)} \ll (1+|\tau|)^{\epsilon(1-1/(q-1))}.$$

Since this is true for arbitrarily small positive values of ϵ, it follows that $|G(s; 1 - 1/(q-1))| \ll (1+|\tau|)^{1-\delta}$, for $0 < \delta \leq 1$, and thus that, $|G(s; 1 - 1/(q-1))| \leq M(1+|\tau|)^{1-\delta}$, for some $M > 0$.

So, at this point, we can apply Theorem 2.2.3 with $z = 1 - 1/(q-1)$ to get that, for $x \geq 3$,

$$\begin{aligned}
\sum_{n \leq x} a_n &= x(\log x)^{-1/(q-1)} \left\{ \frac{G(1; 1 - 1/(q-1)}{\Gamma(1 - 1/(q-1))} + O\left(\frac{M}{\log x}\right) \right\} \\
&= x(\log x)^{-1/(q-1)} \left\{ B_q + O\left(\frac{1}{\log x}\right) \right\} \\
&= B_q x(\log x)^{-1/(q-1)} + O\left(x(\log x)^{-1-1/(q-1)}\right).
\end{aligned}$$

Therefore, for $x \geq 3$,

$$\sum_{\substack{n \leq x \\ p|n \Rightarrow p \not\equiv 1 \text{ (mod } q)}} 1 = B_q x(\log x)^{-1/(q-1)} + O(x(\log x))^{-1-1/(q-1)}.$$

$\square$

The following proposition will be useful in evaluating the innermost sum of equation (2.2).

Corollary 2.2.9. Let x be a real number and let $p_1, \ldots, p_j$ be distinct prime numbers such that $x/p_1 \cdots p_j \geq 3$ and $q \neq p_i$ for any $1 \leq i \leq j$. Then,

$$\sum_{\substack{m \leq x/p_1\cdots p_j \\ q\nmid m \\ (t\neq p_1,\ldots,p_j \text{ and } t|m)\Rightarrow t\not\equiv 1 \text{ (mod } q)}} 1 = B_q \frac{x}{p_1\cdots p_j}\left(\log \frac{x}{p_1\cdots p_j}\right)^{-1/(q-1)}\left(1-\frac{1}{q}\right)\prod_{i=1}^{j}\left(1-\frac{1}{p_i}\right)^{-1}$$
$$+ O\left(\frac{x}{p_1\cdots p_j}\left(\log \frac{x}{p_1\cdots p_j}\right)^{-1-1/(q-1)}\right),$$

where t is prime.

Proof. We will start by rewriting the sum as follows,

$$\sum_{\substack{m \leq x/p_1\cdots p_j \\ q\nmid m \\ (t\neq p_1,\ldots,p_j \text{ and } t|m)\Rightarrow t\not\equiv 1 \text{ (mod } q)}} 1 = \sum_{m \leq x/p_1\cdots p_j} b_m,$$

where

$$b_m = \begin{cases} 1, & \text{if } q \nmid m \text{ and, for } t \neq p_1,\ldots,p_j, \text{ we have } t \mid m \Rightarrow t \not\equiv 1 \text{ (mod } q), \\ 0, & \text{otherwise .} \end{cases}$$

Define $F_2(s) = \sum_{m=1}^{\infty} b_m m^{-s}$. Then,

$$\begin{aligned} F_2(s) = \sum_{m=1}^{\infty} b_m m^{-s} &= \prod_{r \text{ prime}} \left(1 + \frac{b_r}{r^s} + \frac{b_{r^2}}{r^{2s}} + \cdots\right) \\ &= \prod_{i=1}^{j}\left(1+\frac{1}{p_i^s}+\frac{1}{p_i^{2s}}+\cdots\right) \prod_{\substack{r \text{ prime} \\ r\neq q \\ r\not\equiv 1 \text{ (mod } q)}} \left(1+\frac{1}{r^s}+\frac{1}{r^{2s}}+\cdots\right) \\ &= \prod_{i=1}^{j}\left(1-\frac{1}{p_i^s}\right)^{-1} \prod_{\substack{r \text{ prime} \\ r\neq q \\ r\not\equiv 1 \text{ (mod } q)}} \left(1-\frac{1}{r^s}\right)^{-1} \\ &= \left(1-\frac{1}{q^s}\right)\prod_{i=1}^{j}\left(1-\frac{1}{p_i^s}\right)^{-1} \prod_{\substack{r \text{ prime} \\ r\not\equiv 1 \text{ (mod } q)}} \left(1-\frac{1}{r^s}\right)^{-1}. \end{aligned}$$

Now, define $G_2(s;z) = F_2(s)\zeta(s)^{-z}$. Our next aim is to find an explicit formula for G_2. We will start by defining $A_2(s)$ such that $F_2(s)^{q-1} = A_2(s)\zeta(s)^{q-1}\prod_{\chi \pmod q} L(s,\chi)^{-1}$. Then,

$$\begin{aligned}
A_2(s) &= F_2(s)^{q-1}\zeta(s)^{-(q-1)} \prod_{\chi \pmod q} L(s,\chi) \\
&= \left(1-\frac{1}{q^s}\right)^{q-1}\prod_{i=1}^{j}\left(1-\frac{1}{p_i^s}\right)^{-(q-1)} \prod_{\substack{r \text{ prime} \\ r\equiv 1 \pmod q}} \left(1-\frac{1}{r^s}\right)^{q-1} \prod_{\chi \pmod q}\left(\prod_{r \text{ prime}}\left(1-\frac{\chi(r)}{r^s}\right)^{-1}\right) \\
&= \left(1-\frac{1}{q^s}\right)^{q-1}\prod_{i=1}^{j}\left(1-\frac{1}{p_i^s}\right)^{-(q-1)} A(s),
\end{aligned}$$

where $A(s)$ is defined as in the proof of Proposition 2.2.4. Thus, since $A(s)$ converges for $\sigma > 1/2$, it follows that $A_2(s)$ also converges for $\sigma > 1/2$.

Now recall from equation (2.5) that $L(s,\chi_0)^{-1} = \zeta(s)^{-1}(1-q^{-s})^{-1}$. Therefore, we have that

$$\begin{aligned}
F_2(s)^{q-1} &= A_2(s)\zeta(s)^{q-1}\zeta(s)^{-1}\left(1-\frac{1}{q^s}\right)^{-1}\prod_{\chi\neq\chi_0} L(s,\chi)^{-1} \\
&= \left(1-\frac{1}{q^s}\right)^{q-1}\prod_{i=1}^{j}\left(1-\frac{1}{p_i^s}\right)^{-(q-1)} A(s)\zeta(s)^{q-2}\left(1-\frac{1}{q^s}\right)^{-1}\prod_{\chi\neq\chi_0} L(s,\chi)^{-1}.
\end{aligned}$$

Then,

$$\begin{aligned}
G_2(s;1-1/(q-1)) &= F_2(s)\zeta(s)^{-(q-2)/(q-1)} \\
&= (F_2(s)^{(q-1)}\zeta(s)^{-(q-2)})^{1/(q-1)} \\
&= \left(\left(1-\frac{1}{q^s}\right)^{q-1}\prod_{i=1}^{j}\left(1-\frac{1}{p_i^s}\right)^{-(q-1)} A(s)\left(1-\frac{1}{q^s}\right)^{-1}\prod_{\chi\neq\chi_0} L(s,\chi)^{-1}\right)^{1/(q-1)} \\
&= \left(1-\frac{1}{q^s}\right)\prod_{i=1}^{j}\left(1-\frac{1}{p_i^s}\right)^{-1} G(s;1-1/(q-1)),
\end{aligned}$$

where G is defined as in Proposition 2.2.7.

Then, since $x \geq 3p_1\cdots p_j$, we can apply Theorem 2.2.3 with $z = (q-2)/(q-1)$ to get:

$$\begin{aligned}
\sum_{m\leq x/p_1\cdots p_j} b_m = &\frac{x}{p_1\cdots p_j}\left(\log\frac{x}{p_1\cdots p_j}\right)^{-1/(q-1)}\left(\frac{G_2(1;1-1/(q-1))}{\Gamma(1-1/(q-1))}\right) \\
&+ O\left(\frac{x}{p_1\cdots p_j}\left(\log\frac{x}{p_1\cdots p_j}\right)^{-1-1/(q-1)}\right).
\end{aligned}$$

Now, since

$$G_2(1;1-1/(q-1)) = \left(1-\frac{1}{q}\right)\prod_{i=1}^{j}\left(1-\frac{1}{p_i}\right)^{-1} G(1;1-1/(q-1)),$$

it follows that,

$$\begin{aligned}
&\sum_{\substack{m \le x/p_1\cdots p_j \\ q \nmid m \\ t \ne p_1,\ldots,p_j \text{ and } t|m \Rightarrow t \not\equiv 1 \text{ (mod } q)}} 1 \\
&\quad = B_q \frac{x}{p_1\cdots p_j}\left(\log \frac{x}{p_1\cdots p_j}\right)^{-1/(q-1)}\left(1-\frac{1}{q}\right)\prod_{i=1}^{j}\left(1-\frac{1}{p_i}\right)^{-1} \\
&\quad\quad + O\left(\frac{x}{p_1\cdots p_j}\left(\log\frac{x}{p_1\cdots p_j}\right)^{-1-1/(q-1)}\right).
\end{aligned}$$

□

2.3 Other Important Tools

We will start this section by giving a lemma and a proposition that will be very useful throughout this thesis.

Lemma 2.3.1. Let $\delta > 0$. Then, for $x > y^{1+\delta}$,

$$\log x \ll_\delta \log \frac{x}{y}.$$

Proof. First, since $x > y^{1+\delta}$, we have that $x^{1/\delta} > y^{(1+\delta)/\delta}$. Now, notice that we can rewrite $x^{1/\delta}$ as follows:

$$x^{1/\delta} = x^{1/\delta+1-1} = x^{(1+\delta)/\delta-1} = x^{(1+\delta)/\delta}/x.$$

So, we have that $x^{(1+\delta)/\delta}/x > y^{(1+\delta)/\delta}$. From here, we get the following biconditional statements:

$$x^{(1+\delta)/\delta}/x > y^{(1+\delta)/\delta} \iff x < (x/y)^{(1+\delta)/\delta}.$$

Thus, it follows that

$$\log(x) < \frac{1+\delta}{\delta}\log\left(\frac{x}{y}\right) \ll_\delta \log\left(\frac{x}{y}\right).$$

□

Proposition 2.3.2. Let y be a positive real number. Then, for $x > y^2$,

$$\left(\log \tfrac{x}{y}\right)^{-\alpha} = (\log x)^{-\alpha} + O_\alpha\left((\log x)^{-1-\alpha}\log y\right).$$

Proof. First, we can see that

$$\begin{aligned}
\left(\log \tfrac{x}{y}\right)^{-\alpha} &= (\log x - \log y)^{-\alpha} \\
&= (\log x)^{-\alpha}\left(1-\frac{\log y}{\log x}\right)^{-\alpha}.
\end{aligned}$$

Now, let $f(t) = (1-t)^{-\alpha}$. Then, since $f(0) = 1$, f is differentiable at $t = 0$ and f is continuous for $|t| \leq 1/2$, it follows that $f(t) = 1 + O_\alpha(t)$ for $|t| \leq 1/2$. Since $x > y^2$, we have that $\log y / \log x < 1/2$. So,

$$\left(1 - \frac{\log y}{\log x}\right)^{-\alpha} = 1 + O_\alpha\left(\frac{\log y}{\log x}\right).$$

Substituting this back in to our above product, we get that

$$\begin{aligned}\left(\log \tfrac{x}{y}\right)^{-\alpha} &= (\log x)^{-\alpha}\left(1 + O_\alpha\left(\frac{\log y}{\log x}\right)\right)\\ &= (\log x)^{-\alpha} + O_\alpha\left((\log x)^{-1-\alpha}\log y\right).\end{aligned}$$

□

The next seven propositions lead to Propositions 2.3.11 and 2.3.12 which will both be useful in evaluating the nested sum in equation (2.2).

Before stating the next proposition we need the following definition.

Definition 2.3.3. Let α be a real number such that $\alpha \notin \mathbb{N}$. Then,

$$H_\alpha(z) = -\sum_{n=0}^{\infty} \frac{\alpha}{n-\alpha} z^n.$$

Note that, by the ratio test, $H_\alpha(z)$ converges for $|z| < 1$.

Proposition 2.3.4. Let $\alpha > 0$ such that $\alpha \notin \mathbb{N}$ and let $x > 1$. Then, for u in the domain $(1, x)$,

$$\int \log(x/u)^{-\alpha}\left(\frac{1}{u\log u}\right) du = \frac{H_\alpha(1 - \log u/\log x) - 1}{\alpha(\log(x/u))^\alpha} + C.$$

Proof. We will prove the above proposition by showing that

$$\frac{d}{du}\left[\frac{H_\alpha(1 - \log u/\log x) - 1}{\alpha(\log(x/u))^\alpha}\right] = \log(x/u)^{-\alpha}\left(\frac{1}{u\log u}\right).$$

Let $z = 1 - \log u/\log x$. Then, $z\log x = \log x - \log u = \log(x/u)$, and thus,

$$\frac{d}{du}\left[\frac{H_\alpha(1 - \log u/\log x) - 1}{\alpha(\log(x/u))^\alpha}\right] = \frac{d}{dz}\left[\frac{H_\alpha(z) - 1}{\alpha(z\log x)^\alpha}\right]\left(\frac{dz}{du}\right).$$

Since $1 < u < x$, we have that $0 < 1 - \log u/\log x < 1$, and thus, $|z| = |1 - \log u/\log x| < 1$. So, z is in the region of convergence of $H_\alpha(z)$, which allows us to differentiate the infinite sum term by term in the following computation. Using quotient rule to differentiate the first part, we see that

$$\begin{aligned}
\frac{d}{dz}\left[\frac{H_\alpha(z)-1}{\alpha(z\log x)^\alpha}\right] &= \frac{d}{dz}\left[\frac{-\sum_{n=1}^{\infty}\frac{\alpha}{n-\alpha}z^n}{\alpha(z\log x)^\alpha}\right] \\
&= \frac{-\alpha(z\log x)^\alpha\sum_{n=1}^{\infty}\frac{n\alpha}{n-\alpha}z^{n-1}+\alpha^2(\log x)^\alpha z^{\alpha-1}\sum_{n=1}^{\infty}\frac{\alpha}{n-\alpha}z^n}{\alpha^2(z\log x)^{2\alpha}} \\
&= \frac{-\alpha^2(\log x)^\alpha z^\alpha\left[\sum_{n=1}^{\infty}\frac{n}{n-\alpha}z^{n-1}-\sum_{n=1}^{\infty}\frac{\alpha}{n-\alpha}z^{n-1}\right]}{\alpha^2(z\log x)^{2\alpha}} \\
&= \frac{-\sum_{n=1}^{\infty}z^{n-1}}{(z\log x)^\alpha} \\
&= \frac{-\sum_{n=0}^{\infty}z^{n}}{(z\log x)^\alpha}.
\end{aligned}$$

Then, since

$$\frac{1}{1-z}=\sum_{n=0}^{\infty}z^n,$$

we have that

$$\frac{d}{dz}\left[\frac{H_\alpha(z)-1}{\alpha(z\log x)^\alpha}\right] = -\frac{1}{(1-z)(z\log x)^\alpha}.$$

Since $z = 1-\log u/\log x$, we can see that

$$\frac{d}{dz}\left[\frac{H_\alpha(z)-1}{\alpha(z\log x)^\alpha}\right] = -\frac{1}{(\log u/\log x)(\log(x/u))^\alpha} = -\frac{\log x}{(\log u)(\log(x/u))^\alpha},$$

and

$$\frac{dz}{du} = -\frac{1}{u\log x}.$$

Therefore, putting everything together, we get the following:

$$\begin{aligned}
\frac{d}{du}\left[\frac{H_\alpha(1-\log u/\log x)-1}{\alpha(\log(x/u))^\alpha}+C\right] &= \frac{d}{dz}\left[\frac{H_\alpha(z)-1}{\alpha(z\log x)^\alpha}\right]\left(\frac{dz}{du}\right) \\
&= \left(-\frac{\log x}{\log u(\log(x/u))^\alpha}\right)\left(-\frac{1}{u\log x}\right) \\
&= \frac{1}{u(\log u)(\log(x/u))^\alpha}
\end{aligned}$$

Thus, we have shown that

$$\frac{d}{du}\left[\frac{H_\alpha(1-\log u/\log x)-1}{\alpha(\log(x/u))^\alpha}+C\right] = (\log(x/u))^{-\alpha}\left(\frac{1}{u(\log u)}\right),$$

which proves the proposition. $\square$

Proposition 2.3.5. Let $\alpha > 0$ such that $\alpha \notin \mathbb{N}$. For $y \geq 9$,

$$\int_{2^-}^{\sqrt{y}} \log(y/u)^{-\alpha} \left(\frac{1}{u \log u}\right) du = \frac{\log\log y}{(\log y)^{\alpha}} + O_\alpha\left(\frac{1}{(\log y)^\alpha}\right).$$

Proof. First, by Proposition 2.3.4, we have that

$$\begin{aligned}
\int_{2^-}^{\sqrt{y}} \log(y/u)^{-\alpha} \left(\frac{1}{u \log u}\right) du &= \frac{H_\alpha(1 - \frac{\log u}{\log y}) - 1}{\alpha(\log(y/u))^\alpha}\bigg|_{2^-}^{\sqrt{y}} \\
&= \frac{H_\alpha\left(1 - \frac{\log y}{2\log y}\right) - 1}{\alpha\left(\frac{1}{2}\log y\right)^\alpha} - \frac{H_\alpha\left(1 - \frac{\log 2}{\log y}\right) - 1}{\alpha(\log(y/2))^\alpha} \\
&= \frac{H_\alpha\left(\frac{1}{2}\right) - 1}{\frac{\alpha}{2^\alpha}(\log y)^\alpha} - \frac{H_\alpha\left(1 - \frac{\log 2}{\log y}\right) - 1}{\alpha(\log(y/2))^\alpha}.
\end{aligned}$$

We will start by simplifying the minuend of the above subtraction. By definition of H_α, we have that

$$H_\alpha\left(\frac{1}{2}\right) - 1 = -\sum_{n=1}^{\infty} \frac{\alpha}{n-\alpha}\left(\frac{1}{2}\right)^n.$$

Now, since $1/2$ is inside the region of convergence for $H_\alpha(z)$, we can see that this sum converges. So, we have that,

$$H_\alpha\left(\frac{1}{2}\right) - 1 \ll_\alpha 1,$$

and thus,

$$\frac{H_\alpha\left(\frac{1}{2}\right) - 1}{\frac{\alpha}{2^\alpha}(\log y)^\alpha} = O_\alpha\left(\frac{1}{(\log y)^\alpha}\right).$$

Now, we will find an asymptotic formula for the subtrahend. To do this, let $z = 1 - \log 2/(\log y)$ and consider $H_\alpha(z) - 1 - \alpha\log(1-z)$. Rewriting H_α and $\log(1-z)$ as sums and simplifying, we get,

$$\begin{aligned}
H_\alpha(z) - 1 - \alpha\log(1-z) &= -\sum_{n=1}^{\infty} \frac{\alpha}{n-\alpha} z^n - \alpha\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}(-z)^n \\
&= -\alpha\sum_{n=1}^{\infty}\frac{1}{n-\alpha}z^n + \alpha\sum_{n=1}^{\infty}\frac{1}{n}z^n \\
&= \alpha\sum_{n=1}^{\infty}\frac{-\alpha}{n(n-\alpha)}z^n \\
&= -\alpha^2\sum_{n=1}^{\infty}\frac{1}{n(n-\alpha)}z^n.
\end{aligned}$$

Since $y \geq 9$, we have that $|z| = |1 - \log 2/\log y| < 1$, and so,

$$-\alpha^2\sum_{n=1}^{\infty}\frac{1}{n(n-\alpha)}z^n \leq \left|-\alpha^2\sum_{n=1}^{\infty}\frac{1}{n(n-\alpha)}z^n\right| \leq \alpha^2\sum_{n=1}^{\infty}\left|\frac{1}{n(n-\alpha)}\right| \ll_\alpha 1.$$

It follows that,

$$H_\alpha(z) - 1 - \alpha \log(1-z) \ll_\alpha 1,$$

and thus,

$$H_\alpha(1 - \log 2/\log y) - 1 = \alpha \log(\log 2/\log y) + O_\alpha(1).$$

Therefore, we have that:

$$\begin{aligned}
\frac{H_\alpha\left(1 - \frac{\log 2}{\log y}\right) - 1}{\alpha(\log(y/2))^\alpha} &= \frac{\alpha \log(\log 2/\log y) + O_\alpha(1)}{\alpha(\log(y/2))^\alpha} \\
&= \frac{\log\log 2 - \log\log y}{(\log(y/2))^\alpha} + O_\alpha\left(\frac{1}{(\log(y/2))^\alpha}\right) \\
&= -\frac{\log\log y}{(\log(y/2))^\alpha} + O_\alpha\left(\frac{1}{(\log(y/2))^\alpha}\right).
\end{aligned}$$

Now, since $y \geq 3 > 2^{1+1/2}$, we can apply Lemma 2.3.1 to the above error term, to get

$$\frac{H_\alpha\left(1 - \frac{\log 2}{\log y}\right) - 1}{\alpha(\log(y/2))^\alpha} = -\frac{\log\log y}{(\log(y/2))^\alpha} + O_\alpha\left(\frac{1}{(\log y)^\alpha}\right).$$

Also, since $y \geq 9 > 2^2$, we can apply Proposition 2.3.2 to the denominator of the above main term, to get

$$\begin{aligned}
\frac{H_\alpha\left(1 - \frac{\log 2}{\log y}\right) - 1}{\alpha(\log(y/2))^\alpha} &= -\frac{\log\log y}{(\log y)^\alpha} + O\left(\frac{\log 2 \log\log y}{(\log y)^{1+\alpha}}\right) + O_\alpha\left(\frac{1}{(\log y)^\alpha}\right) \\
&= -\frac{\log\log y}{(\log y)^\alpha} + O\left(\frac{\log\log y}{(\log y)^{1+\alpha}}\right) + O_\alpha\left(\frac{1}{(\log y)^\alpha}\right) \\
&= -\frac{\log\log y}{(\log y)^\alpha} + O_\alpha\left(\frac{1}{(\log y)^\alpha}\right).
\end{aligned}$$

Putting everything together, we can see that,

$$\int_{2^-}^{\sqrt{y}} \log(y/u)^{-\alpha} \left(\frac{1}{u \log u}\right) du = \frac{\log\log y}{(\log y)^\alpha} + O_\alpha\left(\frac{1}{(\log y)^\alpha}\right).$$

$\square$

Proposition 2.3.6. Let $\alpha > 0$ such that $\alpha \notin \mathbb{N}$, let $\beta \in \mathbb{N}$, and let $y \geq 9$. Then,

$$\sum_{\substack{p \leq \sqrt{y} \\ \nu_q(p-1) = \beta}} \frac{1}{p} \left(\log \frac{y}{p}\right)^{-\alpha} = \frac{\log\log y}{q^\beta (\log y)^\alpha} + O_\alpha\left(\frac{1}{(\log y)^\alpha}\right).$$

Proof. Define $M(x)$ as follows:

$$M(x) = \sum_{\substack{p \le x \\ \nu_q(p-1)=\beta}} 1/p = \sum_{\substack{p \le x \\ p \equiv 1 \ (\mathrm{mod}\ q^\beta) \\ p \not\equiv 1 \ (\mathrm{mod}\ q^{\beta+1})}} 1/p$$
$$= \sum_{\substack{p \le x \\ p \equiv 1 \ (\mathrm{mod}\ q)^\beta}} 1/p - \sum_{\substack{p \le x \\ p \equiv 1 \ (\mathrm{mod}\ q^{\beta+1})}} 1/p.$$

Then, using Mertens' Theorem [4, Corollary 4.12], we can simplify $M(x)$ as follows:

$$M(x) = \left(\frac{1}{\phi(q^\beta)} - \frac{1}{\phi(q^{\beta+1})}\right) \log\log(x) + c_{q^\beta} - c_{q^{\beta+1}} + O(1/\log x)$$
$$= \frac{1}{q^\beta} \log\log(x) + c + O(1/\log x)$$

where c is a constant depending on q^β. Then, we have that

$$\sum_{\substack{p \le \sqrt{y} \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log\frac{y}{p}\right)^{-\alpha} = \int_{2^-}^{\sqrt{y}} \log\left(\frac{y}{u}\right)^{-\alpha} d(M(u))$$
$$= \int_{2^-}^{\sqrt{y}} \log\left(\frac{y}{u}\right)^{-\alpha} d\left(\frac{1}{q^\beta}\log\log u + c + O\left(\frac{1}{\log u}\right)\right)$$
$$= \frac{1}{q^\beta}\int_{2^-}^{\sqrt{y}} \log\left(\frac{y}{u}\right)^{-\alpha} \left(\frac{du}{u\log u}\right)$$
$$+ \int_{2^-}^{\sqrt{y}} \log\left(\frac{y}{u}\right)^{-\alpha} d\left(O\left(\frac{1}{\log u}\right)\right).$$

By Proposition 2.3.5, we know that

$$\int_{2^-}^{\sqrt{y}} \log(y/u)^{-\alpha}\left(\frac{1}{u\log u}\right) du = \frac{\log\log y}{(\log y)^\alpha} + O_\alpha\left(\frac{1}{(\log y)^\alpha}\right),$$

and thus,

$$\sum_{\substack{p \le \sqrt{y} \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log\frac{y}{p}\right)^{-\alpha} = \frac{\log\log y}{q^\beta\,(\log y)^\alpha} + O_\alpha\left(\frac{1}{(\log y)^\alpha}\right) + \int_{2^-}^{\sqrt{y}} \log\left(\frac{y}{u}\right)^{-\alpha} d\left(O\left(\frac{1}{\log u}\right)\right).$$

Now, we will evaluate the remaining integral, using Riemann-Stieltjes integration:

$$\begin{aligned}\int_{2^-}^{\sqrt{y}} \log{(y/u)}^{-\alpha}\, d\left(O\left(\frac{1}{\log u}\right)\right) &= \left(\log\left(\frac{y}{u}\right)\right)^{-\alpha} O\left(\frac{1}{\log u}\right)\Bigg|_{2^-}^{\sqrt{y}} \\ &\quad - \int_{2^-}^{\sqrt{y}} O\left(\frac{1}{\log u}\right)\left(-\alpha\left(\log\left(\frac{y}{u}\right)\right)^{-\alpha-1}\left(\frac{u}{y}\right)\left(-\frac{y}{u^2}\right)\right) du \\ &= \left(\frac{1}{2}\log y\right)^{-\alpha} O\left(\frac{2}{\log y}\right) - \left(\log\left(\frac{y}{2}\right)\right)^{-\alpha} O\left(\frac{1}{\log 2}\right) \\ &\quad + O\left(\int_{2^-}^{\sqrt{y}} \log(y/u)^{-\alpha-1}\left(\frac{1}{u\log u}\right) du\right) \\ &= O\left(\frac{1}{(\log y)^{1+\alpha}}\right) + O\left(\frac{1}{\left(\log{(y/2)}\right)^{\alpha}}\right) \\ &\quad + O\left(\int_{2^-}^{\sqrt{y}} \log(y/u)^{-\alpha-1}\left(\frac{1}{u\log u}\right) du\right).\end{aligned}$$

By Lemma 2.3.1, since $y \geq 9$, we have that

$$\frac{1}{\log(y/2)} \ll \frac{1}{\log y}.$$

Therefore, we have that

$$\begin{aligned}\int_{2^-}^{\sqrt{y}} \log{(y/u)}^{-\alpha}\, d\left(O\left(\frac{1}{\log u}\right)\right) &= O\left(\frac{1}{(\log y)^{1+\alpha}}\right) + O\left(\frac{1}{(\log y)^{\alpha}}\right) \\ &\quad + O\left(\int_{2^-}^{\sqrt{y}} \log(y/u)^{-\alpha-1}\left(\frac{1}{u\log u}\right) du\right) \\ &= O\left(\frac{1}{(\log y)^{\alpha}}\right) + O\left(\int_{2^-}^{\sqrt{y}} \log(y/u)^{-\alpha-1}\left(\frac{1}{u\log u}\right) du\right).\end{aligned}$$

Now, by Proposition 2.3.5, we have that

$$\begin{aligned}\int_{2^-}^{\sqrt{y}} \log(y/u)^{-\alpha-1}\left(\frac{1}{u\log u}\right) du &= \frac{\log\log y}{(\log y)^{1+\alpha}} + O_\alpha\left(\frac{1}{(\log y)^{1+\alpha}}\right) \\ &= O_\alpha\left(\frac{\log\log y}{(\log y)^{1+\alpha}}\right).\end{aligned}$$

Thus, we get that

$$\begin{aligned}\int_{2^-}^{\sqrt{y}} \log{(y/u)}^{-\alpha}\, d\left(O\left(\frac{1}{\log u}\right)\right) &= O\left(\frac{1}{(\log y)^{\alpha}}\right) + O_\alpha\left(\frac{\log\log y}{(\log y)^{1+\alpha}}\right) \\ &= O_\alpha\left(\frac{1}{(\log y)^{\alpha}}\right).\end{aligned}$$

Therefore, it follows that

$$\sum_{\substack{p\le\sqrt{y}\\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log\frac{y}{p}\right)^{-\alpha} = \frac{\log\log y}{q^{\beta}\left(\log y\right)^{\alpha}} + O_{\alpha}\left(\frac{1}{(\log y)^{\alpha}}\right).$$

□

Proposition 2.3.7. Let $\alpha > 0$ such that $\alpha \notin \mathbb{N}$. For $y \ge 9$,

$$\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha}\left(\frac{1}{u\log u}\right)du = O\left(\frac{1}{(\log y)^{\alpha}}\right) + O\left(\frac{1}{\log y}\right).$$

Proof. First, by Proposition 2.3.4, we have that

$$\begin{aligned}\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha}\left(\frac{1}{u\log u}\right)du &= \frac{H_{\alpha}(1-\frac{\log u}{\log y})-1}{\alpha(\log(y/u))^{\alpha}}\Bigg|_{\sqrt{y}}^{y/3}\\ &= \frac{H_{\alpha}\left(1-\frac{\log(y/3)}{\log y}\right)-1}{\alpha(\log 3)^{\alpha}} - \frac{H_{\alpha}\left(1-\frac{\log y}{2\log y}\right)-1}{\alpha\left(\frac{1}{2}\log y\right)^{\alpha}}\\ &= \frac{H_{\alpha}\left(\frac{\log 3}{\log y}\right)-1}{\alpha(\log 3)^{\alpha}} - \frac{H_{\alpha}\left(\frac{1}{2}\right)-1}{\frac{\alpha}{2^{\alpha}}(\log y)^{\alpha}}.\end{aligned} \tag{2.8}$$

As seen in the proof of Proposition 2.3.5,

$$\frac{H_{\alpha}\left(\frac{1}{2}\right)-1}{\frac{\alpha}{2^{\alpha}}(\log y)^{\alpha}} = O\left(\frac{1}{(\log y)^{\alpha}}\right).$$

Now, we will simplify the minuend of the right-hand side of equation (2.8). By definition of H_{α}, we have that

$$H_{\alpha}(\log 3/\log y)-1 = -\sum_{n=1}^{\infty}\frac{\alpha}{n-\alpha}\left(\frac{\log 3}{\log y}\right)^{n}.$$

Now, since this sum is bounded on the closed disc corresponding to $\log 3/\log y \le 1/2$, we have that, for $y \ge 9$,

$$H_{\alpha}(\log 3/\log y)-1 \ll \frac{\log 3}{\log y} \ll \frac{1}{\log y}.$$

Putting everything together, we can see that,

$$\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha}\left(\frac{1}{u\log u}\right)du = O\left(\frac{1}{(\log y)^{\alpha}}\right) + O\left(\frac{1}{\log y}\right).$$

□

Proposition 2.3.8. Let $\alpha > 0$ such that $\alpha \notin \mathbb{N}$, let $\beta \in \mathbb{N}$, and let $y \geq 9$. Then,

$$\sum_{\substack{\sqrt{y}<p\leq y/3 \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log\frac{y}{p}\right)^{-\alpha} = O\left(\frac{1}{(\log y)^{\alpha}}\right) + O\left(\frac{1}{\log y}\right).$$

Proof. Define $M(x)$ as in Proposition 2.3.6. Then, we have that

$$\begin{aligned}
\sum_{\substack{\sqrt{y}<p\leq y/3 \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log\frac{y}{p}\right)^{-\alpha} &= \int_{\sqrt{y}}^{y/3} \log\left(\frac{y}{u}\right)^{-\alpha} d(M(u)) \\
&= \int_{\sqrt{y}}^{y/3} \log\left(\frac{y}{u}\right)^{-\alpha} d\left(\frac{1}{q^{\beta}}\log\log u + c + O\left(\frac{1}{\log u}\right)\right) \\
&= \frac{1}{q^{\beta}}\int_{\sqrt{y}}^{y/3} \log\left(\frac{y}{u}\right)^{-\alpha}\left(\frac{du}{u\log u}\right) \\
&\quad + \int_{\sqrt{y}}^{y/3} \log\left(\frac{y}{u}\right)^{-\alpha} d\left(O\left(\frac{1}{\log u}\right)\right).
\end{aligned}$$

By Proposition 2.3.7, we know that

$$\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha}\left(\frac{1}{u\log u}\right) du = O\left(\frac{1}{(\log y)^{\alpha}}\right) + O\left(\frac{1}{\log y}\right),$$

and thus,

$$\sum_{\substack{\sqrt{y}<p\leq y/3 \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log\frac{y}{p}\right)^{-\alpha} = O\left(\frac{1}{(\log y)^{\alpha}}\right) + O\left(\frac{1}{\log y}\right) + \int_{\sqrt{y}}^{y/3} \log\left(\frac{y}{u}\right)^{-\alpha} d\left(O\left(\frac{1}{\log u}\right)\right).$$

Now, we will evaluate the remaining integral, using Riemann-Stieltjes integration:

$$\begin{aligned}
\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha} d\left(O\left(\frac{1}{\log u}\right)\right) &= \left(\log\left(\frac{y}{u}\right)\right)^{-\alpha} O\left(\frac{1}{\log u}\right)\Bigg|_{\sqrt{y}}^{y/3} \\
&\quad - \int_{\sqrt{y}}^{y/3} O\left(\frac{1}{\log u}\right)\left(-\alpha\left(\log\left(\frac{y}{u}\right)\right)^{-\alpha-1}\left(\frac{u}{y}\right)\left(-\frac{y}{u^2}\right)\right) du \\
&= (\log 3)^{-\alpha} O\left(\frac{1}{\log(y/3)}\right) - \left(\frac{1}{2}\log y\right)^{-\alpha} O\left(\frac{2}{\log y}\right) \\
&\quad + O\left(\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha-1}\left(\frac{1}{u\log u}\right) du\right) \\
&= O\left(\frac{1}{\log(y/3)}\right) + O\left(\frac{1}{(\log y)^{1+\alpha}}\right) \\
&\quad + O\left(\int_{2^-}^{\sqrt{y}} \log(y/u)^{-\alpha-1}\left(\frac{1}{u\log u}\right) du\right).
\end{aligned}$$

By Lemma 2.3.1, since $y \geq 9$, we have that

$$\frac{1}{\log(y/3)} \ll \frac{1}{\log(y)}.$$

Therefore, we have that

$$\begin{aligned}\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha}\, d\left(O\left(\frac{1}{\log u}\right)\right) &= O\left(\frac{1}{\log y}\right) + O\left(\frac{1}{(\log y)^{1+\alpha}}\right) \\ &\quad + O\left(\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha-1}\left(\frac{1}{u\log u}\right) du\right) \\ &= O\left(\frac{1}{\log y}\right) + O\left(\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha-1}\left(\frac{1}{u\log u}\right) du\right).\end{aligned}$$

Now, by Proposition 2.3.7, we have that

$$\begin{aligned}\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha-1}\left(\frac{1}{u\log u}\right) du &= O\left(\frac{1}{(\log y)^{1+\alpha}}\right) + O\left(\frac{1}{\log y}\right) \\ &= O\left(\frac{1}{\log y}\right).\end{aligned}$$

So, we get that

$$\int_{\sqrt{y}}^{y/3} \log(y/u)^{-\alpha}\, d\left(O\left(\frac{1}{\log u}\right)\right) = O\left(\frac{1}{\log y}\right),$$

and thus,

$$\sum_{\substack{\sqrt{y}<p\leq y/3 \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log\frac{y}{p}\right)^{-\alpha} = O\left(\frac{1}{(\log y)^{\alpha}}\right) + O\left(\frac{1}{\log y}\right).$$

$\square$

Proposition 2.3.9. Let $\alpha > 0$ such that $\alpha \notin \mathbb{N}$, let $\beta \in \mathbb{N}$, let $y \geq 9$ and let $\{w_1, w_2, \ldots, w_n\}$ be a set of primes. Then,

$$\sum_{\substack{p\leq y/3 \\ p\neq w_1,w_2,\ldots,w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log\frac{y}{p}\right)^{-\alpha} = \frac{\log\log y}{q^{\beta}\,(\log y)^{\alpha}} + O_n\left(\frac{1}{(\log y)^{\min\{\alpha,1\}}}\right).$$

Proof. First, notice that

$$\sum_{\substack{p\leq y/3 \\ p\neq w_1,w_2,\ldots,w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log\frac{y}{p}\right)^{-\alpha} = \sum_{\substack{p\leq y/3 \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log\frac{y}{p}\right)^{-\alpha} + O\left(\sum_{i=1}^{n}\frac{1}{w_i}\left(\log\frac{y}{w_i}\right)^{-\alpha}\right).$$

Since, by Lemma 2.3.1
$$\left(\log \frac{y}{w_i}\right)^{-\alpha} \ll (\log y)^{-\alpha},$$
we have that
$$\sum_{i=1}^{n} \frac{1}{w_i} \left(\log \frac{y}{w_i}\right)^{-\alpha} \ll \sum_{i=1}^{n} \frac{1}{w_i} (\log y)^{-\alpha} = (\log y)^{-\alpha} \sum_{i=1}^{n} \frac{1}{w_i} \ll_n (\log y)^{-\alpha}.$$
Now, to simplify the main term, we can split it up as follows
$$\sum_{\substack{p \le y/3 \\ \nu_q(p-1)=\beta}} \frac{1}{p} \left(\log \frac{y}{p}\right)^{-\alpha} = \sum_{\substack{p \le \sqrt{y} \\ \nu_q(p-1)=\beta}} \frac{1}{p} \left(\log \frac{y}{p}\right)^{-\alpha} + \sum_{\substack{\sqrt{y} < p \le y/3 \\ \nu_q(p-1)=\beta}} \frac{1}{p} \left(\log \frac{y}{p}\right)^{-\alpha}.$$
From here, we can apply Propositions 2.3.6 and 2.3.8 directly to get that
$$\sum_{\substack{p \le y/3 \\ \nu_q(p-1)=\beta}} \frac{1}{p} \left(\log \frac{y}{p}\right)^{-\alpha} = \frac{\log\log y}{q^\beta (\log y)^\alpha} + O\left(\frac{1}{(\log y)^\alpha}\right) + O\left(\frac{1}{(\log y)^\alpha}\right) + O\left(\frac{1}{\log y}\right).$$
Therefore, we have that
$$\sum_{\substack{p \le y/3 \\ p \neq w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p} \left(\log \frac{y}{p}\right)^{-\alpha} = \frac{\log\log y}{q^\beta (\log y)^\alpha} + O_n\left(\frac{1}{(\log y)^{\min\{\alpha,1\}}}\right).$$

□

Proposition 2.3.10. Let $\alpha > 0$ such that $\alpha \notin \mathbb{N}$, $y \ge 9$, $\beta \in \mathbb{N}$ and let $\{w_1, \ldots, w_n\}$ be a set of primes. Then,
$$\sum_{\substack{p \le y/3 \\ p \neq w_1, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p^2} (\log(y/p))^{-\alpha} \ll (\log y)^{-\min\{\alpha,1\}}.$$

Proof. In order to prove the proposition, we will split the sum in the following way:
$$\sum_{\substack{p \le y/3 \\ p \neq w_1, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p^2} (\log(y/p))^{-\alpha} = \sum_{\substack{p \le y/3 \\ \nu_q(p-1)=\beta}} \frac{1}{p^2} (\log(y/p))^{-\alpha} + O\left(\sum_{i=1}^{n} \frac{1}{w_i^2} \left(\log \frac{y}{w_i}\right)^{-\alpha}\right).$$
Since, by Lemma 2.3.1
$$\left(\log \frac{y}{w_i}\right)^{-\alpha} \ll (\log y)^{-\alpha},$$
we have that
$$\sum_{i=1}^{n} \frac{1}{w_i^2} \left(\log \frac{y}{w_i}\right)^{-\alpha} \ll \sum_{i=1}^{n} \frac{1}{w_i^2} (\log y)^{-\alpha} = (\log y)^{-\alpha} \sum_{i=1}^{n} \frac{1}{w_i^2} \ll (\log y)^{-\alpha}.$$

Then, to bound the main term, we will split it up as follows:

$$\sum_{\substack{p\le y/3\\ \nu_q(p-1)=\beta}} \frac{1}{p^2}(\log(y/p))^{-\alpha} = \sum_{\substack{p\le \sqrt{y}\\ \nu_q(p-1)=\beta}} \frac{1}{p^2}(\log(y/p))^{-\alpha} + \sum_{\substack{\sqrt{y}<p\le y/3\\ \nu_q(p-1)=\beta}} \frac{1}{p^2}(\log(y/p))^{-\alpha}.$$

For the first sum on the right-hand side, since we are summing over primes p that are at most $\sqrt{y}$, we can bound the sum as follows:

$$\begin{aligned}\sum_{\substack{p\le \sqrt{y}\\ \nu_q(p-1)=\beta}} \frac{1}{p^2}(\log(y/p))^{-\alpha} &\le \sum_{\substack{p\le \sqrt{y}\\ \nu_q(p-1)=\beta}} \frac{1}{p^2}(\log(y/\sqrt{y}))^{-\alpha}\\ &= \left(\frac{1}{2}\log y\right)^{-\alpha} \sum_{\substack{p\le \sqrt{y}\\ \nu_q(p-1)=\beta}} \frac{1}{p^2}\\ &\ll (\log y)^{-\alpha},\end{aligned}$$

since the sum of $1/p^2$ over all primes p is convergent.

Then, we can bound the remaining sum as follows:

$$\begin{aligned}\sum_{\substack{\sqrt{y}<p\le y/3\\ \nu_q(p-1)=\beta}} \frac{1}{p^2}(\log(y/p))^{-\alpha} &\le (\pi(y/3)-\pi(\sqrt{y}))\left(\frac{1}{(\sqrt{y})^2}\right)\left(\log\left(\frac{y}{y/3}\right)\right)^{-\alpha}\\ &\le \pi(y/3)(1/y)(\log 3)^{-\alpha}\\ &\ll \frac{y/3}{\log(y/3)}\left(\frac{1}{y}\right)\\ &\ll \frac{1}{\log(y/3)}.\end{aligned}$$

Now, since $y \le 3^{1+1}$, we can apply Lemma 2.3.1 to get that

$$\sum_{\substack{\sqrt{y}<p\le y/3\\ \nu_q(p-1)=\beta}} \frac{1}{p^2}(\log(y/p))^{-\alpha} \ll 1/\log y.$$

Thus, we get that

$$\sum_{\substack{p\le y/3\\ p\ne w_1,\ldots,w_n\\ \nu_q(p-1)=\beta}} \frac{1}{p^2}(\log(y/p))^{-\alpha} \ll (\log y)^{-\alpha} + (\log y)^{-1} \ll (\log y)^{-\min\{\alpha,1\}}.$$

□

The following two propositions will be very useful in evaluating D_0.

Proposition 2.3.11. Let $\alpha > 0$ such that $\alpha \notin \mathbb{N}$, let $\beta \in \mathbb{N}$, let $y \geq 9$ and let $\{w_1, w_2, \ldots, w_n\}$ be a set of primes. Then,

$$\sum_{\substack{p \leq y/3 \\ p \neq w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log \frac{y}{p}\right)^{-\alpha}\left(1+O\left(\frac{1}{p}\right)\right) = \frac{\log\log y}{q^\beta (\log y)^\alpha} + O_n\left(\frac{1}{(\log y)^{\min\{\alpha,1\}}}\right).$$

Proof. First, notice that we can split the sum as follows,

$$\sum_{\substack{p \leq y/3 \\ p \neq w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log \frac{y}{p}\right)^{-\alpha}\left(1+O\left(\frac{1}{p}\right)\right)$$
$$= \sum_{\substack{p \leq y/3 \\ p \neq w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(\log \frac{y}{p}\right)^{-\alpha} + O\Bigg(\sum_{\substack{p \leq y/3 \\ p \neq w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p^2}\left(\log \frac{y}{p}\right)^{-\alpha}\Bigg).$$

Then, we can apply Propositions 2.3.9 and 2.3.10 to get the desired result. □

Proposition 2.3.12. Let $\alpha > 0$ such that $\alpha \notin \mathbb{N}$, let $\beta, k \in \mathbb{N}$, let $y \geq 9$ and let $\{w_1, w_2, \ldots, w_n\}$ be a set of primes. Then,

$$\sum_{\substack{p \leq y/3 \\ p \neq w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(1+O\left(\frac{1}{p}\right)\right)\left(\frac{(\log\log(y/p))^k}{(\log(y/p))^\alpha} + O\left(\frac{(\log\log y)^{k-1}}{(\log(y/p))^{\min\{\alpha,1\}}}\right)\right)$$
$$= \frac{(\log\log y)^{k+1}}{q^\beta \log^\alpha y} + O_n\left(\frac{(\log\log y)^k}{(\log y)^{\min\{\alpha,1\}}}\right).$$

Proof. First, we can break the above sum into multiple sums as follows:

$$\sum_{\substack{p \leq y/3 \\ p \neq w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p}\left(1+O\left(\frac{1}{p}\right)\right)\left(\frac{(\log\log(y/p))^k}{(\log(y/p))^\alpha} + O\left(\frac{(\log\log y)^{k-1}}{(\log(y/p))^{\min\{\alpha,1\}}}\right)\right)$$
$$= \sum_{\substack{p \leq y/3 \\ p \neq w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\,(\log(y/p))^\alpha} + O\Bigg(\sum_{\substack{p \leq y/3 \\ p \neq w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p^2\,(\log(y/p))^\alpha}\Bigg)$$
$$+ O\Bigg(\sum_{\substack{p \leq y/3 \\ p \neq w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{(\log\log y)^{k-1}}{p(\log(y/p))^{\min\{\alpha,1\}}}\Bigg).$$

We will start by simplifying the error terms. Starting with the first error term, notice that

$$\sum_{\substack{p \le y/3 \\ p \ne w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p^2\left(\log(y/p)\right)^{\alpha}} \ll \sum_{\substack{p \le y/3 \\ p \ne w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{(\log\log y)^k}{p^2\left(\log(y/p)\right)^{\alpha}}$$

$$= (\log\log y)^k \sum_{\substack{p \le y/3 \\ p \ne w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p^2\left(\log(y/p)\right)^{\alpha}}.$$

Then, by Proposition 2.3.10, we get that

$$\sum_{\substack{p \le y/3 \\ p \ne w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p^2\left(\log(y/p)\right)^{\alpha}} \ll \frac{1}{(\log y)^{\min\{\alpha,1\}}},$$

and thus

$$\sum_{\substack{p \le y/3 \\ p \ne w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{\log\log(y/p)}{p^2\left(\log(y/p)\right)^{\alpha}} \ll \frac{(\log\log y)^k}{(\log y)^{\min\{\alpha,1\}}}.$$

Now, to simplify the second error term, we can apply Proposition 2.3.9 to get that

$$\sum_{\substack{p \le y/3 \\ p \ne w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{(\log\log y)^{k-1}}{p(\log(y/p))^{\min\{\alpha,1\}}} = (\log\log y)^{k-1} \sum_{\substack{p \le y/3 \\ p \ne w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{1}{p(\log(y/p))^{\min\{\alpha,1\}}}$$

$$\ll (\log\log y)^{k-1} \frac{\log\log y}{(\log y)^{\min\{\alpha,1\}}}$$

$$= \frac{(\log\log y)^k}{(\log y)^{\min\{\alpha,1\}}}.$$

Now, we will evaluate the main term. First, notice that

$$\sum_{\substack{p \le y/3 \\ p \ne w_1, w_2, \ldots, w_n \\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\left(\log(y/p)\right)^{\alpha}} = \sum_{\substack{p \le y/3 \\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\left(\log(y/p)\right)^{\alpha}} + O\left(\sum_{i=1}^{n} \frac{(\log\log(y/w_i))^k}{w_i\left(\log(y/w_i)\right)^{\alpha}}\right).$$

As shown in the proof of Proposition 2.3.9,

$$\sum_{i=1}^{n} \frac{1}{w_i\left(\log(y/w_i)\right)^{\alpha}} \ll_n (\log y)^{-\alpha},$$

and thus,

$$\sum_{i=1}^{n} \frac{(\log\log(y/w_i))^k}{w_i\left(\log(y/w_i)\right)^{\alpha}} \ll (\log\log y)^k \sum_{i=1}^{n} \frac{1}{w_i\left(\log(y/w_i)\right)^{\alpha}} \ll_n \frac{(\log\log y)^k}{\log^{\alpha} y}.$$

Splitting the remaining sum into two sums, we get that

$$\sum_{\substack{p\le y/3\\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\left(\log(y/p)\right)^{\alpha}} = \sum_{\substack{p\le \sqrt{y}\\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\left(\log(y/p)\right)^{\alpha}} + \sum_{\substack{\sqrt{y}<p\le y/3\\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\left(\log(y/p)\right)^{\alpha}}.$$

Starting with the second sum on the right-hand side of the equation, we can see that

$$\sum_{\substack{\sqrt{y}<p\le y/3\\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\left(\log(y/p)\right)^{\alpha}} \le \sum_{\substack{\sqrt{y}<p\le y/3\\ \nu_q(p-1)=\beta}} \frac{(\log\log y)^k}{p\left(\log(y/p)\right)^{\alpha}} = (\log\log y)^k \sum_{\substack{\sqrt{y}<p\le y/3\\ \nu_q(p-1)=\beta}} \frac{1}{p\left(\log(y/p)\right)^{\alpha}}.$$

Then, applying Proposition 2.3.8, we get that

$$\sum_{\substack{\sqrt{y}<p\le y/3\\ \nu_q(p-1)=\beta}} \frac{1}{p\left(\log(y/p)\right)^{\alpha}} \ll \frac{1}{(\log y)^{\min\{\alpha,1\}}},$$

and thus,

$$\sum_{\substack{\sqrt{y}<p\le y/3\\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\left(\log(y/p)\right)^{\alpha}} \ll \frac{(\log\log y)^k}{(\log y)^{\min\{\alpha,1\}}}.$$

Now, we will focus on the first sum on the right-hand side of the equation. By Proposition 2.3.2, since $y \ge p^2$, we have that

$$\log(y/p) = \log y + O\left(\frac{\log p}{\log^2 y}\right).$$

Furthermore, notice that

$$\frac{\log p}{\log^2 y} \le \frac{\log\sqrt{y}}{\log^2 y} \ll \frac{1}{\log y}.$$

So, it follows that

$$\begin{aligned}
(\log\log(y/p))^k &= \left(\log\left(\log y + O\left(\frac{1}{\log y}\right)\right)\right)^k \\
&= \left(\log\log y + \log\left(1 + O\left(\frac{1}{\log^2 y}\right)\right)\right)^k \\
&= \left(\log\log y + O\left(\frac{1}{\log^2 y}\right)\right)^k \\
&= \sum_{j=0}^{k} \binom{k}{j} (\log\log y)^{k-j} \left(O\left(\frac{1}{\log^2 y}\right)\right)^j \\
&= (\log\log y)^k + \sum_{j=1}^{k} \binom{k}{j} (\log\log y)^{k-j} \left(O\left(\frac{1}{\log^2 y}\right)\right)^j \\
&= (\log\log y)^k + \sum_{j=1}^{k} O\left(\binom{k}{j} \frac{(\log\log y)^{k-j}}{\log^{2j} y}\right).
\end{aligned}$$

The largest error term will occur when j is smallest, ie. when $j = 1$. Thus,

$$(\log\log(y/p))^k = (\log\log y)^k + O_k\left(\frac{(\log\log y)^{k-1}}{\log^2 y}\right).$$

Therefore, we have that

$$\sum_{\substack{p\le\sqrt{y}\\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\,(\log(y/p))^\alpha} = \left((\log\log y)^k + O_k\left(\frac{(\log\log y)^{k-1}}{\log^2 y}\right)\right)\sum_{\substack{p\le\sqrt{y}\\ \nu_q(p-1)=\beta}} \frac{1}{p\,(\log(y/p))^\alpha}.$$

Then, applying Proposition 2.3.6, we get that

$$\sum_{\substack{p\le\sqrt{y}\\ \nu_q(p-1)=\beta}} \frac{1}{p\,(\log(y/p))^\alpha} = \frac{\log\log y}{q^\beta\,(\log y)^\alpha} + O\left(\frac{1}{(\log y)^\alpha}\right).$$

Therefore, we get the following

$$\begin{aligned}
\sum_{\substack{p\le\sqrt{y}\\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\,(\log(y/p))^\alpha} &= \left((\log\log y)^k + O_k\left(\frac{(\log\log y)^{k-1}}{\log^2 y}\right)\right)\left(\frac{\log\log y}{q^\beta \log^\alpha y} + O\left(\frac{1}{\log^\alpha y}\right)\right)\\
&= \frac{(\log\log y)^{k+1}}{q^\beta \log^\alpha y} + O\left(\frac{(\log\log y)^k}{\log^\alpha y}\right) + O_{k,q}\left(\frac{(\log\log y)^k}{(\log y)^{2+\alpha}}\right)\\
&= \frac{(\log\log y)^{k+1}}{q^\beta \log^\alpha y} + O\left(\frac{(\log\log y)^k}{\log^\alpha y}\right).
\end{aligned}$$

Thus, we have shown that

$$\begin{aligned}
\sum_{\substack{p\le y/3\\ p\ne w_1,w_2,\ldots,w_n\\ \nu_q(p-1)=\beta}} \frac{(\log\log(y/p))^k}{p\,(\log(y/p))^\alpha} &= \frac{(\log\log y)^{k+1}}{q^\beta \log^\alpha y} + O\left(\frac{(\log\log y)^k}{(\log y)^{\min\{\alpha,1\}}}\right) + O_n\left(\frac{(\log\log y)^k}{\log^\alpha y}\right)\\
&= \frac{(\log\log y)^{k+1}}{q^\beta \log^\alpha y} + O_n\left(\frac{(\log\log y)^k}{(\log y)^{\min\{\alpha,1\}}}\right),
\end{aligned}$$

and thus, that

$$\begin{aligned}
\sum_{\substack{p\le y/3\\ p\ne w_1,w_2,\ldots,w_n\\ \nu_q(p-1)=\beta}} &\frac{1}{p}\left(1+O\left(\frac{1}{p}\right)\right)\left(\frac{(\log\log(y/p))^k}{(\log(y/p))^\alpha} + O\left(\frac{(\log\log y)^{k-1}}{(\log(y/p))^{\min\{\alpha,1\}}}\right)\right)\\
&= \frac{(\log\log y)^{k+1}}{q^\beta \log^\alpha y} + O_n\left(\frac{(\log\log y)^k}{(\log y)^{\min\{\alpha,1\}}}\right).
\end{aligned}$$

□

The final definitions and propositions in this section will be important in order to evaluate multiply nested sums recursively in the next section.

Definition 2.3.13. For $k, \alpha_1, \ldots, \alpha_i \in \mathbb{N}$, define

$$S_q(x;k) = \frac{(\log\log x)^k}{(\log x)^{1/(q-1)}} + O_q\left(\frac{(\log\log x)^{k-1}}{(\log x)^{1/(q-1)}}\right),$$

and define

$$\begin{aligned} &S_q(x;k;\alpha_1,\ldots,\alpha_i) \\ &\quad = \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1}\left(1+O\left(\frac{1}{p_1}\right)\right) \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2}\left(1+O\left(\frac{1}{p_2}\right)\right) \cdots \sum_{\substack{p_i \le x/3p_1\cdots p_{i-1} \\ p_i \ne p_1,\ldots,p_{i-1} \\ \nu_q(p_i-1)=\alpha_i}} \left[\frac{1}{p_i}\right. \\ &\qquad \left. \times \left(1+O\left(\frac{1}{p_i}\right)\right)\left(\frac{(\log\log(x/p_1\cdots p_i))^k}{(\log(x/p_1\cdots p_i))^{1/(q-1)}} + O_q\left(\frac{(\log\log(x/p_1\cdots p_{i-1}))^{k-1}}{(\log(x/p_1\cdots p_i))^{1/(q-1)}}\right)\right)\right]. \end{aligned}$$

Notice that the expressions $S_q(x;k)$ and $S_q(x;k;\alpha_1,\ldots,\alpha_i)$ are given by asymptotic, not explicit, formulas. For instance, when $i = 1$, applying Proposition 2.3.12, we get that

$$\begin{aligned} S_q(x;k;\alpha_1) &= \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1}\left(1+O\left(\frac{1}{p_1}\right)\right)\left(\frac{(\log\log(x/p_1))^k}{(\log(x/p_1))^{1/(q-1)}} + O_q\left(\frac{(\log\log x)^{k-1}}{(\log(x/p_1))^{1/(q-1)}}\right)\right) \\ &= \frac{(\log\log x)^k}{q^{\alpha_1}(\log x)^{1/(q-1)}} + O_q\left(\frac{(\log\log x)^{k-1}}{(\log x)^{1/(q-1)}}\right) \\ &= \frac{1}{q^{\alpha_1}} S_q(x;k). \end{aligned}$$

Here, we are not claiming that $S_q(x;k;\alpha_1)$ is exactly equal to $\frac{1}{q^{\alpha_1}} S_q(x;k)$, but rather that these two expressions have identical main terms and error terms of equal magnitude.

This observation generalizes to any natural number i, resulting in the following proposition.

Proposition 2.3.14. Let S_q be defined as in Definition 2.3.13 and let i, k and $\alpha_1, \ldots, \alpha_i$ be positive integers. Then,

$$S_q(x;k;\alpha_1,\ldots,\alpha_i) = \frac{1}{q^{\alpha_i}} S_q(x;k+1;\alpha_1,\ldots,\alpha_{i-1}),$$

where the equals sign signifies that the two expressions have the same main terms and error terms of equal magnitude.

Proof. As defined above,

$$\begin{aligned} &S_q(x;k;\alpha_1,\ldots,\alpha_i) \\ &\quad = \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1}\left(1+O\left(\frac{1}{p_1}\right)\right) \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2}\left(1+O\left(\frac{1}{p_2}\right)\right) \cdots \sum_{\substack{p_i \le x/3p_1\cdots p_{i-1} \\ p_i \ne p_1,\ldots,p_{i-1} \\ \nu_q(p_i-1)=\alpha_i}} \left[\frac{1}{p_i}\right. \\ &\qquad \left. \times \left(1+O\left(\frac{1}{p_i}\right)\right)\left(\frac{(\log\log(x/p_1\cdots p_i))^k}{(\log(x/p_1\cdots p_i))^{1/(q-1)}} + O_q\left(\frac{(\log\log(x/p_1\cdots p_{i-1}))^{k-1}}{(\log(x/p_1\cdots p_i))^{1/(q-1)}}\right)\right)\right]. \end{aligned}$$

Applying Proposition 2.3.12 to the innermost sum, we get the following:

$$\begin{aligned}
S_q(x; k;&\alpha_1, \ldots, \alpha_i) \\
&= \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1}\left(1 + O\left(\frac{1}{p_1}\right)\right) \cdots \sum_{\substack{p_{i-1} \le x/3p_1 \cdots p_{i-2} \\ p_{i-1} \ne p_1, \ldots, p_{i-2} \\ \nu_q(p_{i-1}-1)=\alpha_{i-1}}} \left[\frac{1}{p_{i-1}}\left(1 + O\left(\frac{1}{p_{i-1}}\right)\right)\right. \\
&\qquad \left. \times \left(\frac{(\log\log(x/p_1 \cdots p_{i-1}))^{k+1}}{q^{\alpha_i}(\log(x/p_1 \cdots p_{i-1}))^{1/(q-1)}} + O_q\left(\frac{(\log\log(x/p_1 \cdots p_{i-1}))^{k}}{(\log(x/p_1 \cdots p_{i-1}))^{1/(q-1)}}\right)\right)\right] \\
&= \frac{1}{q^{\alpha_i}} \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1}\left(1 + O\left(\frac{1}{p_1}\right)\right) \cdots \sum_{\substack{p_{i-1} \le x/3p_1 \cdots p_{i-2} \\ p_{i-1} \ne p_1, \ldots, p_{i-2} \\ \nu_q(p_{i-1}-1)=\alpha_{i-1}}} \left[\frac{1}{p_{i-1}}\left(1 + O\left(\frac{1}{p_{i-1}}\right)\right)\right. \\
&\qquad \left. \times \left(\frac{(\log\log(x/p_1 \cdots p_{i-1}))^{k+1}}{(\log(x/p_1 \cdots p_{i-1}))^{1/(q-1)}} + O_q\left(\frac{(\log\log(x/p_1 \cdots p_{i-2}))^{k}}{(\log(x/p_1 \cdots p_{i-1}))^{1/(q-1)}}\right)\right)\right],
\end{aligned}$$

since

$$\frac{(\log\log(x/p_1 \cdots p_{i-2}p_{i-1}))^k}{(\log(x/p_1 \cdots p_{i-1}))^{1/(q-1)}} \ll \frac{(\log\log(x/p_1 \cdots p_{i-2}))^k}{(\log(x/p_1 \cdots p_{i-1}))^{1/(q-1)}}.$$

□

Definition 2.3.15. Let γ be a positive real number and let $\alpha_1, \ldots, \alpha_i$ be positive integers. Then, define

$$E_q(x, \gamma; \alpha_1, \ldots, \alpha_i) = \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1} \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2} \cdots \sum_{\substack{p_i \le x/3p_1 \cdots p_{i-1} \\ p_i \ne p_1, \ldots, p_{i-1} \\ \nu_q(p_i-1)=\alpha_i}} \frac{1}{p_i}\left(\log \frac{x}{p_1 \cdots p_i}\right)^{-\gamma}.$$

Proposition 2.3.16. Let E_q be defined as in Definition 2.3.15. Then,

$$E_q(x; \gamma; \alpha_1, \ldots, \alpha_{i-1}, \alpha_i) \ll_q \log\log(x) E_q(x; \gamma; \alpha_1, \ldots, \alpha_{i-1}).$$

Proof. Applying Proposition 2.3.9 to the innermost sum of $E_q(x;\gamma;\alpha_1,\ldots,\alpha_{i-1},\alpha_i)$, we get:

$$\begin{aligned}
E_q(x;\gamma;&\alpha_1,\ldots,\alpha_i)\\
&= \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2}\cdots \sum_{\substack{p_i\le x/3p_1\cdots p_{i-1}\\ p_i\ne p_1,\ldots,p_{i-1}\\ \nu_q(p_i-1)=\alpha_i}} \frac{1}{p_i}\left(\log\frac{x}{p_1\cdots p_i}\right)^{-\gamma}\\
&\ll \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2}\cdots \sum_{\substack{p_{i-1}\le x/3p_1\cdots p_{i-2}\\ p_{i-1}\ne p_1,\ldots,p_{i-2}\\ \nu_q(p_{i-1}-1)=\alpha_{i-1}}} \frac{1}{p_{i-1}}\left(\frac{\log\log(x/p_1\cdots p_{i-1})}{q^{\alpha_i}(\log(x/p_1\cdots p_{i-1}))^{\gamma}}\right)\\
&\ll_q \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2}\cdots \sum_{\substack{p_{i-1}\le x/3p_1\cdots p_{i-2}\\ p_{i-1}\ne p_1,\ldots,p_{i-2}\\ \nu_q(p_{i-1}-1)=\alpha_{i-1}}} \frac{1}{p_{i-1}}\left(\frac{\log\log(x/p_1\cdots p_{i-1})}{(\log(x/p_1\cdots p_{i-1}))^{\gamma}}\right)\\
&\le \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2}\cdots \sum_{\substack{p_{i-1}\le x/3p_1\cdots p_{i-2}\\ p_{i-1}\ne p_1,\ldots,p_{i-2}\\ \nu_q(p_{i-1}-1)=\alpha_{i-1}}} \frac{1}{p_{i-1}}\left(\frac{\log\log x}{(\log(x/p_1\cdots p_{i-1}))^{\gamma}}\right)\\
&= (\log\log x)E_q(x;\gamma;\alpha_1,\ldots,\alpha_{i-1}).
\end{aligned}$$

□

2.4 Evaluating D_0

Since we can only apply Corollary 2.2.9 if $x/p_1\cdots p_j \ge 3$, we will start by splitting D_0 from equation (2.2) into two multiply nested sums such that $x/p_1\cdots p_j \ge 3$ in the first sum and $x/p_1\cdots p_j < 3$ in the second sum. Doing so, we get

$$\begin{aligned}
D_0(H,x) = C_H &\sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_j\le x/3p_1\cdots p_{j-1}\\ p_j\ne p_1,\ldots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} \sum_{\substack{m\le x/p_1\cdots p_j\\ q\nmid m\\ t\ne p_1,\ldots,p_j \text{ and } t\mid m\Rightarrow t\not\equiv 1 \ (\mathrm{mod}\ q)}} 1\\
+ C_H &\sum_{\substack{p_1\le x\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{x/3p_1\cdots p_{j-1}<p_j\le x/p_1\cdots p_{j-1}\\ p_j\ne p_1,\ldots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} \sum_{\substack{m\le x/p_1\cdots p_j\\ q\nmid m\\ t\ne p_1,\ldots,p_j \text{ and } t\mid m\Rightarrow t\not\equiv 1 \ (\mathrm{mod}\ q)}} 1. \qquad (2.9)
\end{aligned}$$

The following two propositions will evaluate the first and second sum of equation (2.9) respectively.

Proposition 2.4.1.

$$C_H \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_j \le x/3p_1\cdots p_{j-1} \\ p_j \ne p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \sum_{\substack{m \le x/p_1\cdots p_j \\ q \nmid m \\ t \ne p_1,\ldots,p_j \text{ and } t|m \Rightarrow t \not\equiv 1 \ (\mathrm{mod}\ q)}} 1$$

$$= B_q C_H \left(\frac{q-1}{q^{1+\sum_{i=1}^{j} \alpha_i}} \right) \frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} + O_q\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}} \right).$$

Proof. Throughout this proof, let

$$J := C_H \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_j \le x/3p_1\cdots p_{j-1} \\ p_j \ne p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \sum_{\substack{m \le x/p_1\cdots p_j \\ q \nmid m \\ t \ne p_1,\ldots,p_j \text{ and } t|m \Rightarrow t \not\equiv 1 \ (\mathrm{mod}\ q)}} 1.$$

By Corollary 2.2.9, we get that

$$J = C_H \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_j \le x/3p_1\cdots p_{j-1} \\ p_j \ne p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \Bigg[B_q \frac{x}{p_1\cdots p_j} \left(\log \frac{x}{p_1 \cdots p_j} \right)^{-1/(q-1)}$$

$$\times \left(1 - \frac{1}{q}\right) \prod_{i=1}^{j} \left(1 - \frac{1}{p_i}\right)^{-1} + O\left(\frac{x}{p_1\cdots p_j} \left(\log \frac{x}{p_1\cdots p_j} \right)^{-1-1/(q-1)} \right) \Bigg]$$

$$= B_q C_H x \left(1 - \frac{1}{q}\right) \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \cdots \sum_{\substack{p_j \le x/3p_1\cdots p_{j-1} \\ p_j \ne p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \frac{1}{p_1\cdots p_j} \left(\log \frac{x}{p_1\cdots p_j} \right)^{-1/(q-1)} \prod_{i=1}^{j} \left(1 - \frac{1}{p_i}\right)^{-1}$$

$$+ O\Bigg(x \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_j \le x/3p_1\cdots p_{j-1} \\ p_j \ne p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \frac{1}{p_1\cdots p_j} \left(\log \frac{x}{p_1\cdots p_j} \right)^{-1-1/(q-1)} \Bigg)$$

Now, since

$$\left(1 - \frac{1}{p_i}\right)^{-1} = 1 + O\left(\frac{1}{p_i}\right),$$

we have that,

$$
\begin{aligned}
J &= B_q C_H x \left(1 - \frac{1}{q}\right) \\
&\quad \times \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_j \le x/3p_1\cdots p_{j-1} \\ p_j \ne p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \frac{1}{p_1 \cdots p_j} \left(\log \frac{x}{p_1 \cdots p_j}\right)^{-1/(q-1)} \prod_{i=1}^{j} \left(1 + O\left(\frac{1}{p_i}\right)\right) \\
&\qquad + O\Bigg(x \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_j \le x/3p_1\cdots p_{j-1} \\ p_j \ne p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \frac{1}{p_1 \cdots p_j} \left(\log \frac{x}{p_1 \cdots p_j}\right)^{-1-1/(q-1)} \Bigg) \\
&= B_q C_H x \left(1 - \frac{1}{q}\right) \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1} \left(1 + O\left(\frac{1}{p_1}\right)\right) \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2} \left(1 + O\left(\frac{1}{p_2}\right)\right) \cdots \\
&\sum_{\substack{p_j \le x/3p_1\cdots p_{j-1} \\ p_j \ne p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \frac{1}{p_j} \left(\log \frac{x}{p_1 \cdots p_j}\right)^{-1/(q-1)} \left(1 + O\left(\frac{1}{p_j}\right)\right) \\
&\qquad + O\Bigg(x \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1} \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2} \cdots \sum_{\substack{p_j \le x/3p_1\cdots p_{j-1} \\ p_j \ne p_1,\ldots,p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \frac{1}{p_j} \left(\log \frac{x}{p_1 \cdots p_j}\right)^{-1-1/(q-1)} \Bigg).
\end{aligned}
\tag{2.10}
$$

We will start by focusing on the nested sum in the main term. Applying Proposition 2.3.11 to the innermost sum, we get that:

$$\begin{aligned}
&\sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1}\left(1+O\left(\frac{1}{p_1}\right)\right)\cdots \sum_{\substack{p_j\le x/3p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} \frac{1}{p_j}\left(\log\frac{x}{p_1\cdots p_j}\right)^{-1/(q-1)}\left(1+O\left(\frac{1}{p_j}\right)\right)\\
&\quad= \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1}\left(1+O\left(\frac{1}{p_1}\right)\right)\cdots \sum_{\substack{p_{j-1}\le x/3p_1\cdots p_{j-2}\\ p_{j-1}\ne p_1,\dots,p_{j-2}\\ \nu_q(p_{j-1}-1)=\alpha_{j-1}}} \left[\frac{1}{p_{j-1}}\left(1+O\left(\frac{1}{p_{j-1}}\right)\right)\right.\\
&\qquad\left.\times\left(\frac{\log\log(x/p_1\cdots p_{j-1})}{q^{\alpha_j}(\log(x/p_1\cdots p_{j-1}))^{1/(q-1)}}+O_q\left(\frac{1}{(\log(x/p_1\cdots p_{j-1}))^{1/(q-1)}}\right)\right)\right]\\
&\quad=\frac{1}{q^{\alpha_j}} \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1}\left(1+O\left(\frac{1}{p_1}\right)\right)\cdots \sum_{\substack{p_{j-1}\le x/3p_1\cdots p_{j-2}\\ p_{j-1}\ne p_1,\dots,p_{j-2}\\ \nu_q(p_{j-1}-1)=\alpha_{j-1}}} \left[\frac{1}{p_{j-1}}\left(1+O\left(\frac{1}{p_{j-1}}\right)\right)\right.\\
&\qquad\left.\times\left(\frac{\log\log(x/p_1\cdots p_{j-1})}{(\log(x/p_1\cdots p_{j-1}))^{1/(q-1)}}+O_q\left(\frac{1}{(\log(x/p_1\cdots p_{j-1}))^{1/(q-1)}}\right)\right)\right]. \qquad (2.11)
\end{aligned}$$

Now, it follows that if we apply Proposition 2.3.14 to the nested sum in equation (2.11) $j-1$ times, we will get that

$$\begin{aligned}
&\sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1}\left(1+O\left(\frac{1}{p_1}\right)\right)\cdots \sum_{\substack{p_j\le x/3p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} \frac{1}{p_j}\left(\log\frac{x}{p_1\cdots p_j}\right)^{-1/(q-1)}\left(1+O\left(\frac{1}{p_j}\right)\right)\\
&\quad=\frac{1}{q^{\sum_{i=1}^j\alpha_i}}\frac{(\log\log x)^j}{(\log x)^{1/(q-1)}}+O_q\left(\frac{(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right).
\end{aligned}$$

Thus, from equation (2.10), we have that

$$\begin{aligned}
J&=B_qC_Hx\left(1-\frac{1}{q}\right)\left(\frac{1}{q^{\sum_{i=1}^j\alpha_i}}\frac{(\log\log x)^j}{(\log x)^{1/(q-1)}}+O_q\left(\frac{(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right)\right)\\
&\quad+O\Bigg(x\sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}}\frac{1}{p_1}\sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}}\frac{1}{p_2}\cdots\sum_{\substack{p_j\le x/3p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}}\frac{1}{p_j}\left(\log\frac{x}{p_1\cdots p_j}\right)^{-1-1/(q-1)}\Bigg)\\
&=B_qC_H\left(\frac{q-1}{q^{1+\sum_{i=1}^j\alpha_i}}\right)\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}}+O_q\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right)\\
&\quad+O\Bigg(x\sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}}\frac{1}{p_1}\sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}}\frac{1}{p_2}\cdots\sum_{\substack{p_j\le x/3p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}}\frac{1}{p_j}\left(\log\frac{x}{p_1\cdots p_j}\right)^{-1-1/(q-1)}\Bigg).
\end{aligned}$$

Now, we will evaluate the error term. Applying Proposition 2.3.16 to the error term j times, we get that

$$x \sum_{\substack{p_1 \le x/3 \\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1} \sum_{\substack{p_2 \le x/3p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2} \cdots \sum_{\substack{p_j \le x/3p_1 \cdots p_{j-1} \\ p_j \ne p_1, \ldots, p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \frac{1}{p_j} \left(\log \frac{x}{p_1 \cdots p_j} \right)^{-1-1/(q-1)} \ll_q \frac{x(\log\log x)^j}{(\log x)^{1+1/(q-1)}}.$$

Therefore, we have that

$$J = B_q C_H \left(\frac{q-1}{q^{1+\sum_{i=1}^j \alpha_i}} \right) \frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} + O_q \left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}} \right) + O_q \left(\frac{x(\log\log x)^j}{(\log x)^{1+1/(q-1)}} \right).$$

Now, since $\log\log x \ll \log x$, we have that

$$\frac{(\log\log x)^j}{(\log\log x)^{j-1}} \ll \frac{(\log x)^{1+1/(q-1)}}{(\log x)^{1/(q-1)}},$$

and thus,

$$\frac{x(\log\log x)^j}{(\log x)^{1+1/(q-1)}} \ll \frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}.$$

So,

$$J = B_q C_H \left(\frac{q-1}{q^{1+\sum_{i=1}^j \alpha_i}} \right) \frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} + O_q \left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}} \right).$$

□

Proposition 2.4.2.

$$C_H \sum_{\substack{p_1 \le x \\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2 \le x/p_1 \\ p_2 \ne p_1 \\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{x/3p_1 \cdots p_{j-1} < p_j \le x/p_1 \cdots p_{j-1} \\ p_j \ne p_1, \ldots, p_{j-1} \\ \nu_q(p_j-1)=\alpha_j}} \sum_{\substack{m \le x/p_1 \cdots p_j \\ q \nmid m \\ t \ne p_1, \ldots, p_j \text{ and } t \mid m \Rightarrow t \not\equiv 1 \pmod{q}}} 1 \ll_q \frac{x(\log\log x)^{j-1}}{\log x}.$$

Proof. First, notice that, in this sum, $x/p_1 p_2 \cdots p_j < 3$ and thus,

$$\sum_{\substack{m \le x/p_1 \cdots p_j \\ q \nmid m \\ t \ne p_1, \ldots, p_j \text{ and } t \mid m \Rightarrow t \not\equiv 1 \pmod{q}}} 1 \le 2.$$

So, we get that

$$
\begin{aligned}
C_H \sum_{\substack{p_1\le x\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{x/3p_1\cdots p_{j-1}<p_j\le x/p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} \sum_{\substack{m\le x/p_1\cdots p_j\\ q\nmid m\\ t\ne p_1,\dots,p_j \text{ and } t|m\Rightarrow t\not\equiv 1 \text{ (mod } q)}} 1 \\
\le C_H \sum_{\substack{p_1\le x\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{x/3p_1\cdots p_{j-1}<p_j\le x/p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} 2 \\
= 2C_H \sum_{\substack{p_1\le x\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{x/3p_1\cdots p_{j-1}<p_j\le x/p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} 1
\end{aligned}
$$

Notice that if $x/p_1\cdots p_{j-1}<3$, then

$$\sum_{\substack{x/3p_1\cdots p_{j-1}<p_j\le x/p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} 1 = 0.$$

Therefore, we can assume that $x/p_1\cdots p_{j-1}\ge 3$. Similarly, if $x/p_1\cdots p_{i-1}<3$ for any i, then

$$\sum_{\substack{p_i\le x/p_1\cdots p_{i-1}\\ p_i\ne p_1,\dots,p_{i-1}\\ \nu_q(p_i-1)=\alpha_i}} 1 = 0.$$

Thus, we have the following equality:

$$
\begin{aligned}
2C_H \sum_{\substack{p_1\le x\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{x/3p_1\cdots p_{j-1}<p_j\le x/p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} 1 \\
= 2C_H \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{x/3p_1\cdots p_{j-1}<p_j\le x/p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} 1.
\end{aligned}
$$

Applying the prime number theorem to the innermost sum, we get that

$$
\begin{aligned}
&2C_H \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{x/3p_1\cdots p_{j-1}<p_j\le x/p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} 1\\
&\le 2C_H \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_{j-1}\le x/3p_1\cdots p_{j-2}\\ p_{j-1}\ne p_1,\dots,p_{j-2}\\ \nu_q(p_{j-1}-1)=\alpha_{j-1}}} \pi(x/p_1p_2\cdots p_{j-1})\\
&\ll \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{p_{j-1}\le x/3p_1\cdots p_{j-2}\\ p_{j-1}\ne p_1,\dots,p_{j-2}\\ \nu_q(p_{j-1}-1)=\alpha_{j-1}}} \frac{x/p_1\cdots p_{j-1}}{\log(x/p_1\cdots p_{j-1})}\\
&= x \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \frac{1}{p_1} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \frac{1}{p_2} \cdots \sum_{\substack{p_{j-1}\le x/3p_1\cdots p_{j-2}\\ p_{j-1}\ne p_1,\dots,p_{j-2}\\ \nu_q(p_{j-1}-1)=\alpha_{j-1}}} \frac{1}{p_{j-1}\log(x/p_1\cdots p_{j-1})}.
\end{aligned}
$$

Next, we can apply Proposition 2.3.16 $j-1$ times, to get that,

$$
\begin{aligned}
2C_H \sum_{\substack{p_1\le x/3\\ \nu_q(p_1-1)=\alpha_1}} \sum_{\substack{p_2\le x/3p_1\\ p_2\ne p_1\\ \nu_q(p_2-1)=\alpha_2}} \cdots \sum_{\substack{x/3p_1\cdots p_{j-1}<p_j\le x/p_1\cdots p_{j-1}\\ p_j\ne p_1,\dots,p_{j-1}\\ \nu_q(p_j-1)=\alpha_j}} 1 &\ll_q \frac{x(\log\log x)^{j-1}}{\log x}\\
&\ll_q \frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}.
\end{aligned}
$$

□

Therefore, combining Propositions 2.4.1 and 2.4.2, we have shown that,

$$
D_0(H,x) = B_q C_H \left(\frac{q-1}{q^{1+\sum_{i=1}^{j}\alpha_i}}\right)\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} + O_q\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right).
$$

2.5 Evaluating $D_1(H,x)$

First, by definition of D_1, we have that

$$
\begin{aligned}
D_1((q;\alpha_1,\dots,\alpha_j),x) &= \#\{n\le x\colon q \parallel n, G_q(n)=(q;\alpha_1,\dots,\alpha_j)\}\\
&= \#\{n\le x/q\colon q\nmid n, G_q(n)=(q;\alpha_1,\dots,\alpha_j)\}\\
&= D_0((q;\alpha_1,\dots,\alpha_j),x/q)
\end{aligned}
$$

So, applying our results from the previous section, we get that

$$\begin{aligned}
D_0(H,x/q) &= B_qC_H\left(\frac{q-1}{q^{1+\sum_{i=1}^{j}\alpha_i}}\right)\frac{x(\log\log x/q)^j}{q(\log x/q)^{1/(q-1)}} + O_q\left(\frac{x(\log\log x/q)^{j-1}}{q(\log x/q)^{1/(q-1)}}\right)\\
&= B_qC_H\left(\frac{q-1}{q^{2+\sum_{i=1}^{j}\alpha_i}}\right)\frac{x(\log\log x/q)^j}{(\log x/q)^{1/(q-1)}} + O_q\left(\frac{x(\log\log x)^{j-1}}{(\log x/q)^{1/(q-1)}}\right).
\end{aligned}$$

As shown in the proof of Proposition 2.3.12,

$$(\log\log(x/q))^j = (\log\log x)^j + O_j\left(\frac{(\log\log x)^{j-1}}{\log^2 x}\right).$$

Also, by Proposition 2.3.2, if we suppose that $x > q^2$, then

$$(\log x/q)^{-1/(q-1)} = (\log x)^{-1/(q-1)} + O_q\left((\log x)^{-1-1/(q-1)}\right).$$

Therefore,

$$\begin{aligned}
\frac{x(\log\log x/q)^j}{(\log x/q)^{1/(q-1)}} &= x\left((\log\log x)^j + O_j\left(\frac{(\log\log x)^{j-1}}{\log^2 x}\right)\right)\left((\log x)^{-1/(q-1)} + O_q\left((\log x)^{-1-1/(q-1)}\right)\right)\\
&= \frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} + O_q\left(\frac{x(\log\log x)^j}{(\log x)^{1+1/(q-1)}}\right) + O_j\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{2+1/(q-1)}}\right)\\
&= \frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} + O_q\left(\frac{x(\log\log x)^j}{(\log x)^{1+1/(q-1)}}\right).
\end{aligned}$$

Now, since we are assuming that $x > q^2$, we can apply Lemma 2.3.1 to get that

$$\frac{x(\log\log x)^{j-1}}{(\log x/q)^{1/(q-1)}} \ll \frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}.$$

Thus, we have that

$$\begin{aligned}
D_0(H,x/q) &= B_qC_H\left(\frac{q-1}{q^{2+\sum_{i=1}^{j}\alpha_i}}\right)\left(\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} + O_q\left(\frac{x(\log\log x)^j}{(\log x)^{1+1/(q-1)}}\right)\right)\\
&\quad + O_q\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right)\\
&= B_qC_H\left(\frac{q-1}{q^{2+\sum_{i=1}^{j}\alpha_i}}\right)\left(\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}}\right) + O_q\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right),
\end{aligned}$$

since

$$\frac{x(\log\log x)^j}{(\log x)^{1+1/(q-1)}} \ll \frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}.$$

2.6 Evaluating $D_k(H, x)$ for $k \geq 2$

In this section, we show that for all $k \geq 2$, $D_k(H, x)$ will contribute to the error term of $D(H, x)$.

Proposition 2.6.1. Let $H = (q; \alpha_1, \ldots, \alpha_j)$. Then, for $k \geq 2$,

$$D_k(H, x) \ll_H \frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}.$$

Proof. Let $k \geq 2$. Recall, from Section 2.1, that by definition, $D_k(H, x) = \#\{n \leq x \colon q^k \parallel n, G_q(n) = H\}$. Notice that we can rewrite the above set as $D_k(H, x) = \#\{n \leq x/q^k \colon q \nmid n, G_q(q^k n) = H\}$. Now, by the Chinese Remainder Theorem, since q is an odd prime and $q \nmid n$,

$$\mathbb{Z}_{q^k n}^\times \cong \mathbb{Z}_{q^k}^\times \times \mathbb{Z}_n^\times \cong \mathbb{Z}_{\phi(q^k)} \times \mathbb{Z}_{\phi(n)} \cong \mathbb{Z}_{q^{k-1}} \times \mathbb{Z}_{q-1} \times \mathbb{Z}_{\phi(n)}.$$

If $k - 1 \notin \{\alpha_1, \alpha_2, \ldots, \alpha_j\}$, it follows that $D_k(H, x) = 0$, and thus, our proposition will be trivially true. So, assume that $\alpha_i = k - 1$ for some $i \in \{\alpha_1, \ldots, \alpha_j\}$. Then, it follows that

$$\begin{aligned} D_k((q; \alpha_1, \ldots, \alpha_j), x) &= \#\{n \leq x/q^k \colon q \nmid n, G_q(n) = (q; \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_j)\} \\ &= D_0((q; \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_j), x/q^k). \end{aligned}$$

Since

$$D_0((q; \alpha_1, \ldots, \alpha_j), x) = B_q C_H \left(\frac{q-1}{q^{1+\sum_{i=1}^{j} \alpha_i}} \right) \frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} + O_q \left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}} \right),$$

we have that

$$D_0((q; \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_j), x/q^k) \ll_H \frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}.$$

$\square$

So, by the above proposition, we can see that

$$\sum_{k=2}^{\alpha_1+1} D_k((q; \alpha_1, \ldots, \alpha_j), x) \ll_H \frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}.$$

2.7 Evaluating $D(H, x)$

Theorem 2.7.1. Let q be an odd prime, let $H = (q; \alpha_1, \alpha_2, \ldots, \alpha_j)$, and for a prime number p, let k_p be the order of p modulo q. Then,

$$D(H, x) = K_H \left(\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} \right) + O_H \left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}} \right),$$

where

$$K_H = B_q C_H E_q,$$

where

$$B_q = \frac{1}{\Gamma(1-1/(q-1))}\left((1-1/q)^{-1/(q-1)} \prod_{\substack{p\neq q \\ p\not\equiv 1 \ (\mathrm{mod}\ q)}} (1-1/p^{k_p})^{-1/k_p} \prod_{\chi\neq\chi_0} L(1,\chi)^{-1/(q-1)}\right),$$

$$C_H = \prod_{k=1}^{\alpha_1-1} \frac{1}{(a_k - a_{k+1})!},$$

and

$$E_q = \frac{q^2-1}{q^{2+\sum_{i=1}^{j}\alpha_i}}.$$

Proof. Recall from equation (2.1) that

$$D((q;\alpha_1,\ldots,\alpha_j),x) = \sum_{k=0}^{\alpha_1+1} D_k(q;\alpha_1,\ldots,\alpha_j).$$

Inputting the values of D_k found in Sections 2.4, 2.5 and 2.6, we get that

$$\begin{aligned}
D(H,x) &= B_q C_H \left(\frac{q-1}{q^{1+\sum_{i=1}^{j}\alpha_i}}\right)\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} + B_q C_H \left(\frac{q-1}{q^{2+\sum_{i=1}^{j}\alpha_i}}\right)\left(\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}}\right) \\
&\quad + O_H\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right) \\
&= B_q C_H \left(\frac{q-1}{q^{1+\sum_{i=1}^{j}\alpha_i}}\right)\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}}\left(1+\frac{1}{q}\right) + O_H\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right) \\
&= B_q C_H \left(\frac{q^2-1}{q^{2+\sum_{i=1}^{j}\alpha_i}}\right)\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}} + O_H\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right) \\
&= K_H\left(\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}}\right) + O_H\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right).
\end{aligned}$$

$\square$

Chapter 3

Counting Function for Maximally Non-cyclic Multiplicative Groups

3.1 Setup

Rather than focusing on local Sylow subgroups, we now wish to focus on the global structure of a group, and in particular, whether or not a group is cyclic. While not directly related to the problem we have spent the first part of the thesis solving, the problem that we are about to introduce is of a similar nature. Counting functions of the number of integers n up to x such that $\mathbb{Z}_n^\times$ is cyclic is a topic that has been well studied in number theory. Consider, for instance, the following proposition, which can easily be proved using well known results.

Proposition 3.1.1.

$$\#\{n \leq x \colon \mathbb{Z}_n^\times \text{ is cyclic}\} \sim \frac{3}{2}\frac{x}{\log x}.$$

Proof. First, we know that $\mathbb{Z}_n^\times$ is cyclic if and only if $n = 1, 2, 4, p^r$ or $2p^r$, where p is an odd prime and r is a positive integer. Then,

$$\begin{aligned}\#\{n \leq x \colon \mathbb{Z}_n^\times \text{ is cyclic}\} &= 3 + \sum_{\substack{p^r \leq x \\ \text{p odd}}} 1 + \sum_{\substack{2p^r \leq x \\ \text{p odd}}} 1 \\ &= 3 + \sum_{\substack{p^r \leq x \\ \text{p odd}}} 1 + \sum_{\substack{p^r \leq x/2 \\ \text{p odd}}} 1.\end{aligned}$$

Since $2^r \le x$ if and only if $r \le \log x/\log 2$, we have that

$$\sum_{\substack{p^r \le x \\ \text{p odd}}} 1 = \sum_{p^r \le x} 1 + O(\log x),$$

and thus,

$$\#\{n \le x \colon \mathbb{Z}_n^\times \text{ is cyclic}\} = 3 + \sum_{p^r \le x} 1 + \sum_{p^r \le x/2} 1 + O(\log x).$$

Now, notice that we can rewrite the sum of prime powers up to x as follows,

$$\begin{aligned}\sum_{p^r \le x} 1 &= \sum_{p \le x} 1 + \sum_{p^2 \le x} 1 + \sum_{p^3 \le x} 1 + \cdots \\ &= \sum_{p \le x} 1 + \sum_{p \le x^{1/2}} 1 + \sum_{p \le x^{1/3}} 1 + \cdots \\ &= \pi(x) + \pi(x^{1/2}) + \pi(x^{1/3}) + \cdots \\ &= \pi(x) + O(x^{1/2}) + O(x^{1/2}) + \cdots,\end{aligned}$$

and similarly, we can rewrite the sum of prime powers up to $x/2$ as follows,

$$\begin{aligned}\sum_{p^r \le x/2} 1 &= \sum_{p \le x/2} 1 + \sum_{p^2 \le x/2} 1 + \sum_{p^3 \le x/2} 1 + \cdots \\ &= \sum_{p \le x/2} 1 + \sum_{p \le (x/2)^{1/2}} 1 + \sum_{p \le (x/2)^{1/3}} 1 + \cdots \\ &= \pi(x/2) + \pi((x/2)^{1/2}) + \pi((x/2)^{1/3}) + \cdots \\ &= \pi(x/2) + O(x^{1/2}) + O(x^{1/2}) + \cdots.\end{aligned}$$

If $r > \log x/\log 2$, then for any prime p, $p^r \ge 2^r > 2^{\log x/\log 2} = x$, and thus, we get

$$\sum_{p^r \le x} 1 = \pi(x) + \frac{\log x}{\log 2} O(x^{1/2}) = \pi(x) + O(x^{1/2}\log x)$$

and

$$\sum_{p^r \le x/2} 1 = \pi(x/2) + \frac{\log x}{\log 2} O(x^{1/2}) = \pi(x/2) + O(x^{1/2}\log x).$$

Now, by the Prime Number Theorem, we have that

$$\sum_{p^r \le x} 1 = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right) + O(x^{1/2}\log x)$$

and

$$\sum_{p^r \le x/2} 1 = \frac{x/2}{\log(x/2)} + O\left(\frac{x/2}{\log^2(x/2)}\right) + O(x^{1/2}\log x).$$

If we assume that $x > 4$, we can apply Lemma 2.3.1 and Proposition 2.3.2 to get that

$$\begin{aligned}\sum_{p^r \leq x/2} 1 &= \frac{x}{2}\left((\log x)^{-1} + O\left(\frac{\log 2}{\log^2 x}\right)\right) + O\left(\frac{x}{\log^2 x}\right) + O(x^{1/2}\log x)\\ &= \frac{x}{2\log x} + O\left(\frac{x}{\log^2 x}\right) + O(x^{1/2}\log x).\end{aligned}$$

Thus, so far, we have shown that

$$\#\{n \leq x \colon \mathbb{Z}_n^\times \text{ is cyclic}\} = 3 + \frac{x}{\log x} + \frac{x}{2\log x} + O\left(\frac{x}{\log^2 x}\right) + O(x^{1/2}\log x).$$

Since $\log^3 x \ll x^{1/2}$ implies that $x^{1/2}\log^3 x \ll x$, and thus, $x^{1/2}\log x \ll x/\log^2 x$, we have that

$$\#\{n \leq x \colon \mathbb{Z}_n^\times \text{ is cyclic}\} = \frac{3}{2}\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Thus, from here, it follows that

$$\#\{n \leq x \colon \mathbb{Z}_n^\times \text{ is cyclic}\} \sim \frac{3}{2}\frac{x}{\log x}.$$

□

This has led us to ask, what would make a group as non-cyclic as possible? Before we can define this, we need to define the primary decomposition and invariant factor decomposition of a group.

Definition 3.1.2 (Primary Decomposition)**.** The primary decomposition of a finite abelian group G is the unique decomposition

$$G \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_t}$$

such that $k_1, k_2, \ldots, k_t$ are powers of primes.

Definition 3.1.3 (Invariant Factor Decomposition)**.** The invariant factor decomposition of a finite abelian group G is the unique decomposition

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_\ell}$$

such that $d_1 \mid d_2 \mid \cdots \mid d_\ell$.

Now, we can give the definition of a maximally non-cyclic group.

Definition 3.1.4. Let G be a finite abelian group of order m, for some positive integer m. Let the following be its invariant factor decomposition:

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_\ell},$$

where $d_1 \mid d_2 \mid \cdots \mid d_\ell$. Then, we call G *maximally non-cyclic* if any of the four following equivalent conditions hold:

(1) for any prime q, its Sylow q-subgroup is of the form

$$\mathbb{Z}_q \times \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q;$$

(2) d_ℓ is minimal among all finite abelian groups of order m;

(3) d_j is squarefree for every $1 \leq j \leq \ell$;

(4) each factor of the primary decomposition of G is of the form $\mathbb{Z}_p$ for some prime p.

Below is a proof that the four conditions are indeed equivalent.

Proof. Let G be a group of order m with invariant factor decomposition,

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_\ell},$$

where $d_1 \mid d_2 \mid \cdots \mid d_\ell$. Also, let $\{p_1, p_2, \ldots, p_s\}$ be the set of all primes which divide m.

$(1) \implies (4)$: First, we can write G as

$$G = \bigoplus_{i=1}^{s} G_{p_i}$$

where, for each i, G_{p_i} is the Sylow p_i-subgroup of G. By condition (1), G_{p_i} is of the form $\mathbb{Z}_{p_i} \times \cdots \times \mathbb{Z}_{p_i}$ for every i. Thus, it follows that

$$G = \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{m_i} \mathbb{Z}_{p_i},$$

for some positive integers $m_1, \ldots, m_s$. Notice that this must be the primary decomposition of G by definition of primary decomposition, and thus, condition (4) holds.

$(4) \implies (3)$: Assume condition (4) holds. Then, since we construct the invariant factor decomposition of G by combining factors from the primary decomposition whose orders are relatively prime, and every factor from the primary decomposition is, by assumption, of the form $\mathbb{Z}_p$ for some prime p, it follows that each d_j is squarefree.

$(3) \implies (2)$: Suppose that condition (3) holds. By construction of the invariant factor decomposition, we know that d_ℓ divides m and that p_i divides d_ℓ for each $1 \leq i \leq s$. Then, since d_ℓ is squarefree, it follows that each p_i must divide d_ℓ exactly once. Therefore, we must have that $d_\ell = p_1 p_2 \cdots p_s$. Now, suppose that G' is another finite abelian group of order m with invariant factor decomposition, $\mathbb{Z}_{d'_1} \times \mathbb{Z}_{d'_2} \times \cdots \times \mathbb{Z}_{d'_{\ell'}}$, where $d'_1 \mid d'_2 \mid \cdots \mid d'_{\ell'}$. Then, $d'_{\ell'}$ must also be divisible by p_i for each i in $\{1, 2, \ldots, s\}$. So, $p_1 p_2 \cdots p_s \mid d'_{\ell'}$, and thus, $d_\ell \mid d'_{\ell'}$, which implies that $d_\ell \leq d'_{\ell'}$. Since G' was chosen arbitrarily, it follows that d_ℓ must be minimal among all finite abelian groups of order m.

$(2) \implies (1)$: We will argue this implication by contrapositive. Suppose that there exists some prime p_j, $1 \leq j \leq s$, such that the Sylow p_j-subgroup of G is of the form $\mathbb{Z}_{p_j^{\alpha_1}} \times \mathbb{Z}_{p_j^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_j^{\alpha_k}}$ where

$1 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$ and $\alpha_k > 1$. Without loss of generality, we can assume that $j = 1$. Then, $p_1^{\alpha_k}$ must divide d_i for some $1 \leq i \leq \ell$. Since $d_1 \mid d_2 \mid \cdots \mid d_\ell$, it follows that $p_1^{\alpha_k}$ divides d_ℓ. So, $p_1^{\alpha_k} p_2 \cdots p_s \mid d_\ell$ since p_i divides d_ℓ for each $1 \leq i \leq s$. However, from our previous cases, we can see that it is possible to find a finite abelian group of order m such that $d_\ell = p_1 p_2 \cdots p_s$ which is clearly a smaller d_ℓ than $p_1^{\alpha_k} p_2 \cdots p_s$ since $\alpha_k > 1$. Thus, in this case, d_ℓ is not minimal among all finite abelian groups of order m.

$\square$

We remark that these four equivalent conditions imply that l is maximal among all finite abelian groups of order m, however this implication doesn't go both ways. For instance, consider the following two finite abelian groups of order 36: $G_1 \cong \mathbb{Z}_2 \times \mathbb{Z}_{18}$ and $G_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_6$. Here, $l = 2$ for both groups. From their invariant factor decompositions, we can see that their primary factor decompositions are $G_1 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$ and $G_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Here, it is easy to see that G_2 satisfies condition (1) of our definition, but that G_1 does not, since its Sylow 3-subgroup is $\mathbb{Z}_9$.

Lemma 3.1.5. Let $G \cong G_1 \times G_2 \times \cdots \times G_j$, where $G, G_1, \ldots, G_j$ are finite abelian groups. Then, G is maximally non-cyclic if and only if $G_1, \ldots, G_j$ are maximally non-cyclic.

Proof. By condition (4) of Definition 3.1.4, G is maximally non-cyclic if and only if each factor of its primary decomposition is of the form $\mathbb{Z}_p$ for some prime p. Since G and $G_1 \times G_2 \times \cdots \times G_j$ are isomorphic, their primary decompositions will be identical. So, each factor of the primary decomposition of $G_1 \times G_2 \times \cdots \times G_j$ will be of the form $\mathbb{Z}_p$, and thus, for each $1 \leq i \leq j$, the primary decomposition of G_i can only have factors of the form $\mathbb{Z}_p$. By condition (4) of Definition 3.1.4, each G_i must be maximally non-cyclic. $\square$

Our goal throughout the remainder of this chapter is to estimate the counting function for the number of n up to x such that $\mathbb{Z}_n^\times$ is maximally non-cyclic. First, applying Chinese Remainder Theorem to $\mathbb{Z}_n^\times$, we get that

$$\begin{aligned} \mathbb{Z}_n^\times &\cong \mathbb{Z}_{2^\alpha}^\times \oplus \bigoplus_{\substack{p^\beta \| n \\ p \text{ odd}}} \mathbb{Z}_{p^\beta}^\times \\ &\cong \mathbb{Z}_{2^\alpha}^\times \oplus \bigoplus_{\substack{p^\beta \| n \\ p \text{ odd}}} \mathbb{Z}_{\phi(p^\beta)}, \end{aligned}$$

where $\alpha \geq 0$ is an integer. Note that by Lemma 3.1.5, $\mathbb{Z}_n^\times$ will be maximally non-cyclic if and only if $\mathbb{Z}_{2^\alpha}^\times$ and $\mathbb{Z}_{\phi(p^\beta)}$ for each odd prime p with $p^\beta \parallel n$ are all maximally non-cyclic.

We will start by focusing on the factor corresponding to 2. If α is 0 or 1, then $\mathbb{Z}_{2^\alpha}^\times$ will be the trivial group. Otherwise,

$$\mathbb{Z}_{2^\alpha}^\times \cong \begin{cases} \mathbb{Z}_2, & \text{if } \alpha = 2 \\ \mathbb{Z}_2 \times \mathbb{Z}_2, & \text{if } \alpha = 3 \\ \mathbb{Z}_{2^{\alpha-2}} \times \mathbb{Z}_2, & \text{if } \alpha \geq 4. \end{cases}$$

Notice that condition (1) from Definition 3.1.4 will not be satisfied if α is greater than 3. Thus, it follows that in order for $\mathbb{Z}_n^\times$ to be maximally non-cyclic, we require that 2^4 does not divide n. Now, let p be an odd prime divisor of n and suppose that $p^\beta \parallel n$. Then,

$$\mathbb{Z}_{\phi(p^\beta)} \cong \begin{cases} \mathbb{Z}_{p-1}, & \text{if } \beta = 1 \\ \mathbb{Z}_p \times \mathbb{Z}_{p-1}, & \text{if } \beta = 2 \\ \mathbb{Z}_{p^{\beta-1}} \times \mathbb{Z}_{p-1}, & \text{if } \beta \geq 3. \end{cases}$$

Here, we can see that condition (1) from Definition 3.1.4 will not be satisfied if α is greater than 2 or if $p-1$ is divisible by a square. Thus, it follows that in order for $\mathbb{Z}_n^\times$ to be maximally non-cyclic, we require that if p is an odd divisor n, then p^3 does not divide n and $p-1$ is squarefree. Therefore, we have that

$$\begin{aligned} &\#\{n \leq x \colon \mathbb{Z}_n^\times \text{ is maximally non-cyclic}\} \\ &\qquad = \#\{n \leq x \colon 2^4 \nmid n, p^3 \nmid n \text{ for any odd prime p, and } p \mid n \Rightarrow p-1 \text{ is squarefree}\}. \end{aligned}$$

So, we can see that this is another case of counting integers with restrictions on their prime factors.

3.2 Useful Propositions

In order to find a counting function for the number of n up to x such that $\mathbb{Z}_n^\times$ is maximally non-cyclic, we first need to state and prove some useful propositions.

Proposition 3.2.1. For any positive integer n,

$$\frac{n}{\phi(n)} = \sum_{d \mid n} \frac{\mu(d)^2}{\phi(d)}.$$

Proof. First, since $\phi(n) = n \prod_{p \mid n}(1 - 1/p)$, we have that

$$\frac{n}{\phi(n)} = \frac{n}{n \prod_{p \mid n}(1 - 1/p)} = \prod_{p \mid n}(1 - 1/p)^{-1}.$$

Notice that $n/\phi(n)$ is a multiplicative function since both n and $\phi(n)$ are multiplicative functions. Also, we can see that $\sum_{d \mid n} \frac{\mu(d)^2}{\phi(d)}$ is a multiplicative function since it is the divisor sum of a multiplicative function.

Since both $n/\phi(n)$ and $\sum_{d|n} \frac{\mu(d)^2}{\phi(d)}$ are multiplicative functions, showing that they are equal is equivalent to checking that they agree on powers of primes. So, let q be a prime and let α be a positive integer. Then,

$$\frac{q^\alpha}{\phi(q^\alpha)} = \prod_{p|q^\alpha}(1-1/p)^{-1} = (1-1/q)^{-1} = \frac{q}{q-1},$$

and

$$\sum_{d|q^\alpha} \frac{\mu(d)^2}{\phi(d)} = 1 + \frac{1}{q-1} = \frac{q}{q-1}.$$

Therefore, from this, it follows that $\frac{n}{\phi(n)} = \sum_{d|n} \frac{\mu(d)^2}{\phi(d)}$ for any positive integer n. □

Proposition 3.2.2. For any real number x,

$$\sum_{n\le x} \frac{n}{\phi(n)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)}x + O(x^{1/2}).$$

Proof. First, by Proposition 3.2.1, we have that

$$\sum_{n\le x} \frac{n}{\phi(n)} = \sum_{n\le x}\sum_{d|n} \frac{\mu(d)^2}{\phi(d)}.$$

So, by switching the order of summation, we get

$$\sum_{n\le x} \frac{n}{\phi(n)} = \sum_{d\le x} \frac{\mu(d)^2}{\phi(d)} \sum_{\substack{n\le x\\ d|n}} 1 = \sum_{d\le x} \frac{\mu(d)^2}{\phi(d)} \left\lfloor \frac{x}{d} \right\rfloor.$$

Now, since $\lfloor x/d \rfloor = x/d + O(1)$, we have that

$$\begin{aligned}
\sum_{n\le x} \frac{n}{\phi(n)} &= \sum_{d\le x} \frac{\mu(d)^2}{\phi(d)} \left(\frac{x}{d} + O(1)\right) \\
&= x\sum_{d\le x} \frac{\mu(d)^2}{d\phi(d)} + O\Bigg(\sum_{d\le x} \frac{1}{\phi(d)}\Bigg) \\
&= x\sum_{d=1}^{\infty} \frac{\mu(d)^2}{d\phi(d)} + O\Bigg(x\sum_{d>x} \frac{1}{d\phi(d)} + \sum_{d\le x} \frac{1}{\phi(d)}\Bigg). \qquad (3.1)
\end{aligned}$$

Note that the convergence of the sum in the main term of (3.1) follows from (3.2). Then, since $\mu(d)^2/d\phi(d)$ is a multiplicative function, we can rewrite the coefficients of the main term of (3.1) as an Euler product as follows,

$$\sum_{d=1}^{\infty} \frac{\mu(d)^2}{\phi(d)} \cdot d^{-1} = \prod_p \left(1 + \frac{\mu(p)^2}{\phi(p)} p^{-1} + \frac{\mu(p^2)^2}{\phi(p^2)} p^{-2} + \cdots\right)$$
$$= \prod_p \left(1 + \frac{1}{p-1} p^{-1} + 0 + 0 + \cdots\right)$$
$$= \prod_p \left(1 + \frac{1}{p(p-1)}\right)$$
$$= \prod_p \left(\frac{p^2 - p + 1}{p(p-1)}\right).$$

Now multiplying the numerator and denominator by $(p+1)(p^3-1)$ and then dividing the numerator and denominator by p^6, we get the following chain of equalities:

$$\sum_{d=1}^{\infty} \frac{\mu(d)^2}{d\phi(d)} = \prod_p \left(\frac{p^6 - 1}{p(p^2-1)(p^3-1)}\right)$$
$$= \prod_p \left(\frac{1 - 1/p^6}{(1-1/p^2)(1-1/p^3)}\right)$$
$$= \frac{\prod_p (1-p^{-2})^{-1} \prod_p (1-p^{-3})^{-1}}{\prod_p (1-p^{-6})^{-1}}.$$

Since the Euler product representation of Riemann's zeta function is $\zeta(s) = \prod_p (1-p^{-s})^{-1}$, we can see that

$$\sum_{d=1}^{\infty} \frac{\mu(d)^2}{d\phi(d)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)}.$$

Now, we will simplify the error term of (3.1). First, since $\phi(d) \gg_\epsilon d^{1-\epsilon}$ for any positive ϵ, taking $\epsilon = 1/2$, we get that

$$x \sum_{d>x} \frac{1}{d\phi(d)} \ll x \sum_{d>x} \frac{1}{d^{3/2}} \ll x \int_x^\infty \frac{1}{t^{3/2}} dt = x \left(-\frac{2}{t^{1/2}}\right)\Big|_x^\infty = x \cdot \frac{2}{x^{1/2}} \ll x^{1/2} \tag{3.2}$$

and

$$\sum_{d \le x} \frac{1}{\phi(d)} \ll \sum_{d \le x} \frac{1}{d^{1/2}} \ll \int_1^x \frac{1}{t^{1/2}} dt = 2t^{1/2}\Big|_1^x = 2x^{1/2} - 2 \ll x^{1/2}.$$

Substituting our revised main term and our simplified error term back into (3.1), we get that

$$\sum_{n \le x} \frac{n}{\phi(n)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} x + O(x^{1/2}).$$

□

Proposition 3.2.3. For any real number y,

$$\sum_{n>y} \frac{1}{n\phi(n)} \ll \frac{1}{y}.$$

Proof. First, notice that we can rewrite the above sum as follows,

$$\sum_{n>y} \frac{1}{n\phi(n)} = \sum_{n>y} \frac{n}{\phi(n)} \cdot \frac{1}{n^2}.$$

Then, since $f(t) = 1/t^2$ is a continuous function, we can use a Riemann-Stieltjes integral to evaluate the above sum:

$$\begin{aligned}
\sum_{n>y} \frac{1}{n\phi(n)} &= \int_y^\infty \frac{1}{t^2} d\biggl(\sum_{n\le t} \frac{n}{\phi(n)}\biggr) \\
&= \frac{1}{t^2} \sum_{n\le t} \frac{n}{\phi(n)}\bigg|_y^\infty - \int_y^\infty \sum_{n\le t} \frac{n}{\phi(n)} d\left(\frac{1}{t^2}\right) \\
&= -\frac{1}{y^2} \sum_{n\le y} \frac{n}{\phi(n)} + 2\int_y^\infty \frac{1}{t^3} \sum_{n\le t} \frac{n}{\phi(n)} dt.
\end{aligned}$$

Now, since $\sum_{n\le x} \frac{n}{\phi(n)} \ll x$ by Proposition 3.2.2, we have that

$$\begin{aligned}
\sum_{n>y} \frac{1}{n\phi(n)} &\ll \frac{1}{y^2} \cdot y + 2\int_y^\infty \frac{1}{t^3} \cdot t dt \\
&= \frac{1}{y} + 2\left(-\frac{1}{t}\right)\bigg|_y^\infty \\
&\ll \frac{1}{y}.
\end{aligned}$$

□

Definition 3.2.4. Let ξ be Artin's constant, that is,

$$\xi = \prod_p \left(1 - \frac{1}{p(p-1)}\right).$$

Proposition 3.2.5. Let C be any positive real constant. Then,

$$\#\{p \le x \colon p-1 \text{ is squarefree}\} = \mathrm{li}(x)\xi + O\left(\frac{x}{(\log x)^{C/2}}\right),$$

where ξ is defined as in Definition 3.2.4 and

$$\mathrm{li}(x) = \int_0^x \frac{dt}{\ln t}.$$

Proof. First, notice that,

$$\#\{p \leq x \colon p-1 \text{ is squarefree }\} = \sum_{p \leq x} (\mu(p-1))^2.$$

Then, since $(\mu(p-1))^2 = \sum_{d^2 | p-1} \mu(d)$ (equation (2.4) on p.36 of [4]), we have that

$$\begin{aligned}
\#\{p \leq x \colon p-1 \text{ is squarefree }\} &= \sum_{p \leq x} \sum_{d^2 | p-1} \mu(d) \\
&= \sum_{d^2 \leq x} \sum_{\substack{p \leq x \\ d^2 | p-1}} \mu(d) \\
&= \sum_{d^2 \leq x} \mu(d) \sum_{\substack{p \leq x \\ d^2 | p-1}} 1 \\
&= \sum_{d \leq \sqrt{x}} \mu(d) \pi(x; d^2, 1).
\end{aligned}$$

By Corollary 11.21 from [4], for $d^2 < (\log x)^C$,

$$\pi(x; d^2, 1) = \frac{\mathrm{li}(x)}{\varphi(d^2)} + O_C(x e^{-c_1 \sqrt{\log x}}),$$

where c_1 is a positive constant. So,

$$\begin{aligned}
\sum_{d \leq (\log x)^{C/2}} \mu(d) \pi(x; d^2, 1) &= \sum_{d \leq (\log x)^{C/2}} \mu(d) \left(\frac{\mathrm{li}(x)}{\varphi(d^2)} + O_C(x e^{-c_1 \sqrt{\log x}}) \right) \\
&= \mathrm{li}(x) \sum_{d \leq (\log x)^{C/2}} \frac{\mu(d)}{\varphi(d^2)} + O_C\left((\log x)^{C/2} x e^{-c_1 \sqrt{\log x}} \right).
\end{aligned}$$

Since $\phi(d^2) = d\phi(d)$, we can see that

$$\begin{aligned}
\sum_{d \leq (\log x)^{C/2}} \frac{\mu(d)}{\varphi(d^2)} &= \sum_{d \geq 1} \frac{\mu(d)}{d\phi(d)} + O\Bigg(\sum_{d > (\log x)^{C/2}} \frac{1}{d\phi(d)} \Bigg) \\
&= \prod_p \left(1 - \frac{1}{p(p-1)} \right) + O\left(\frac{1}{(\log x)^{C/2}} \right) \\
&= \xi + O\left(\frac{1}{(\log x)^{C/2}} \right).
\end{aligned}$$

The second equality above is valid due to Proposition 3.2.3. Thus, so far, we have that

$$\sum_{d \leq (\log x)^{C/2}} \mu(d) \pi(x; d^2, 1) = \mathrm{li}(x)\xi + O\left(\frac{\mathrm{li}(x)}{(\log x)^{C/2}} \right) + O_C\left((\log x)^{C/2} x e^{-c_1 \sqrt{\log x}} \right).$$

Now, we can use the trivial estimate $\pi(x; d^2, 1) \ll 1 + x/d^2$, to get that

$$\begin{aligned}\sum_{(\log x)^{C/2} < d \leq \sqrt{x}} \mu(d)\pi(x; d^2, 1) &\ll \sum_{(\log x)^{C/2} < d \leq \sqrt{x}} \left(1 + \frac{x}{d^2}\right) \\ &\ll \sum_{(\log x)^{C/2} < d \leq \sqrt{x}} \left(\frac{x}{d^2}\right), \text{ since } d > \sqrt{x} \\ &< x \sum_{(\log x)^{C/2} < d} \left(\frac{1}{d^2}\right) \\ &< x \int_{(\log x)^{C/2}-1}^{\infty} \frac{1}{t^2} dt \\ &\ll \frac{x}{(\log x)^{C/2}}.\end{aligned}$$

Thus,

$$\begin{aligned}&\sum_{d \leq \sqrt{x}} \mu(d)\pi(x; d^2, 1) \\ &\qquad = \mathrm{li}(x)\xi + O\left(\frac{\mathrm{li}(x)}{(\log x)^{C/2}}\right) + O_C\left((\log x)^{C/2} x e^{-c_1\sqrt{\log x}}\right) + O\left(\frac{x}{(\log x)^{C/2}}\right).\end{aligned}$$

Now, since $\mathrm{li}\, x \ll x/\log x$, we have that

$$\begin{aligned}&\sum_{d \leq \sqrt{x}} \mu(d)\pi(x; d^2, 1) \\ &= \mathrm{li}(x)\xi + O\left(\frac{x}{(\log x)^{1+C/2}}\right) + O_C\left((\log x)^{C/2} x e^{-c_1\sqrt{\log x}}\right) + O\left(\frac{x}{(\log x)^{C/2}}\right) \\ &= \mathrm{li}(x)\xi + O\left(\frac{x}{(\log x)^{C/2}}\right) + O_C\left((\log x)^{C/2} x e^{-c_1\sqrt{\log x}}\right).\end{aligned}$$

Now, since

$$\lim_{x\to\infty} \frac{(\log x)^C}{e^{c_1\sqrt{\log x}}} = 0,$$

we have that $(\log x)^C = o(e^{c_1\sqrt{\log x}})$, and thus $(\log x)^C \ll e^{c_1\sqrt{\log x}}$. From here, it follows that

$$\frac{x(\log x)^{C/2}}{e^{c_1\sqrt{\log x}}} \ll \frac{x}{(\log x)^{C/2}},$$

and thus,

$$\sum_{d \leq \sqrt{x}} \mu(d)\pi(x; d^2, 1) = \mathrm{li}(x)\xi + O\left(\frac{x}{(\log x)^{C/2}}\right).$$

$\square$

Let $A = \{p \colon p-1 \text{ is squarefree}\}$. Then, we can calculate the density $d(A)$ of A as follows:

$$d(A) = \lim_{x\to\infty} \frac{\#\{p \leq x \colon p-1 \text{ is squarefree }\}}{\pi(x)}$$

Notice that, as stated in the next proposition, $d(A)$ turns out to be Artin's constant.

Proposition 3.2.6. $d(A) = \xi$, where ξ is as defined in Definition 3.2.4.

Proof. First, by Proposition 3.2.5,

$$\begin{aligned} d(A) &= \lim_{x\to\infty} \frac{\mathrm{li}(x)\xi + O\left(\frac{x}{(\log x)^{C/2}}\right)}{\pi(x)} \\ &= \lim_{x\to\infty} \left(\frac{\mathrm{li}(x)}{\pi(x)}\xi + O\left(\frac{x}{\pi(x)(\log x)^{C/2}}\right)\right). \end{aligned}$$

Now, by the Prime Number Theorem, we have that

$$\frac{x}{\pi(x)(\log x)^{C/2}} \ll \frac{x \log x}{x(\log x)^{C/2}} = (\log x)^{1-C/2}.$$

Let $C > 2$. Then, $1 - C/2 < 0$, and so, as x goes to infinity, the above error term goes to 0.

Also, by the Prime Number Theorem, we know that

$$\lim_{x\to\infty} \frac{\mathrm{li}(x)}{\pi(x)} = 1.$$

Therefore, it follows that, $d(A) = \xi$. □

3.3 Counting integers n such that $\mathbb{Z}_n^\times$ is maximally non-cyclic

In order to prove Proposition 3.3.2, we will need to use the Wirsing-Odoni Method. Below is a statement of the method taken directly from [1]:

Proposition 3.3.1 (Wirsing Odoni Method)**.** Let f be a multiplicative function. Suppose that there exist constants u and v such that $0 \leq f(p^r) \leq ur^v$ for all primes p and all positive integers r. Suppose also that there exist real numbers $\omega > 0$ and $0 < \beta < 1$ such that

$$\sum_{p<P} f(p) = \omega \frac{P}{\log P} + O\left(\frac{P}{(\log P)^{1+\beta}}\right)$$

as $P \to \infty$. Then the product over all primes

$$C_f = \frac{1}{\Gamma(\omega)} \prod_p \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \frac{f(p^3)}{p^3} + \cdots\right)\left(1 - \frac{1}{p}\right)^\xi$$

converges (hence is positive), and

$$\sum_{n<N} f(n) = C_f N(\log N)^{\omega-1} + O_f(N(\log N)^{\omega-1-\beta})$$

as $N \to \infty$.

Proposition 3.3.2.

$$\#\{n \leq x \colon \mathbb{Z}_n^\times \text{ is maximally non-cyclic}\} \sim C_f \frac{x}{(\log x)^{1-\xi}},$$

where ξ is as defined in Definition 3.2.4 and C_f is the convergent product,

$$C_f = \frac{15}{14\Gamma(\xi)} \lim_{x\to\infty}\Bigg(\prod_{\substack{p\leq x\\ p-1 \text{ squarefree}}}\left(1+\frac{1}{p}+\frac{1}{p^2}\right)\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{\xi}\Bigg).$$

Proof. Recall that, as shown in Section 3.1,

$$\begin{aligned}\#\{n \leq x \colon &\mathbb{Z}_n^\times \text{ is maximally non-cyclic}\}\\ &= \#\{n \leq x \colon 2^4 \nmid n, p^3 \nmid n \text{ for any odd prime p, and } p \mid n \Rightarrow p-1 \text{ is squarefree}\}.\end{aligned}$$

Let

$$f(n) = \begin{cases} 1, & \text{if } 2^4 \nmid n, p^3 \nmid n \text{ for any odd prime p and } p \mid n \Rightarrow p-1 \text{ is squarefree},\\ 0, & \text{otherwise.}\end{cases}$$

Then, f is multiplicative and for any prime p and natural number r, $0 \leq f(p^r) \leq 1 \leq 2\cdot r^1$. Also, by Proposition 3.2.5, we have that

$$\begin{aligned}\sum_{p\leq x} f(p) &= \#\{p \leq x \colon p-1 \text{ is squarefree}\}\\ &= \mathrm{li}(x)\xi + O\left(\frac{x}{(\log x)^{C/2}}\right).\end{aligned}$$

Since

$$\mathrm{li}(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

we get that

$$\begin{aligned}\sum_{p\leq x} f(p) &= \left[\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right)\right]\xi + O\left(\frac{x}{(\log x)^{C/2}}\right)\\ &= \frac{x}{\log x}\xi + O\left(\frac{x}{(\log x)^{\min(2,C/2)}}\right).\end{aligned}$$

Choosing $C > 4$, we get that,

$$\begin{aligned}\sum_{p\le x} f(p) &= \xi \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right)\\ &= \xi \frac{x}{\log x} + O\left(\frac{x}{(\log x)^{1+\beta}}\right),\end{aligned}$$

where $0 < \beta < 1$. Then, applying Proposition 3.3.1, we get that

$$\begin{aligned}C_f &= \frac{1}{\Gamma(\xi)} \prod_p \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \frac{f(p^3)}{p^3} + \cdots\right)\left(1 - \frac{1}{p}\right)^{\xi}\\ &= \frac{1}{\Gamma(\xi)} \cdot \frac{\left(1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8}\right)}{\left(1 + \frac{1}{2} + \frac{1}{4}\right)} \lim_{x\to\infty}\left(\prod_{\substack{p \\ p-1 \text{ squarefree}}} \left(1 + \frac{1}{p} + \frac{1}{p^2}\right) \prod_p \left(1 - \frac{1}{p}\right)^{\xi}\right)\\ &= \frac{15}{14\Gamma(\xi)} \lim_{x\to\infty}\left(\prod_{\substack{p \\ p-1 \text{ squarefree}}} \left(1 + \frac{1}{p} + \frac{1}{p^2}\right) \prod_p \left(1 - \frac{1}{p}\right)^{\xi}\right)\end{aligned}$$

converges and

$$\sum_{n\le x} f(n) = C_f x(\log x)^{\xi-1} + O_f\left(x(\log x)^{\xi-1-\beta}\right).$$

The statement of the proposition follows directly from this. $\square$

Chapter 4

Conclusion

To conclude, throughout this thesis, we have examined multiple counting functions of integers with restrictions on their prime factors. First, in Chapter 2, we proved that for a fixed odd prime q and a fixed q-group $H = \mathbb{Z}_{q^{\alpha_1}} \times \mathbb{Z}_{q^{\alpha_2}} \times \cdots \times \mathbb{Z}_{q^{\alpha_j}}$, the counting function for the number of n up to x for which H is the Sylow q-subgroup of $\mathbb{Z}_n^\times$ is

$$D(H,x) = K_H\left(\frac{x(\log\log x)^j}{(\log x)^{1/(q-1)}}\right) + O_H\left(\frac{x(\log\log x)^{j-1}}{(\log x)^{1/(q-1)}}\right),$$

where K_H is a constant that depends on H. Then, in Chapter 3, we proved that the number of n up to x such that $\mathbb{Z}_n^\times$ is cyclic is asymptotic to $\frac{3}{2}x/\log x$ and that the number of n up to x such that $\mathbb{Z}_n^\times$ is maximally non-cyclic is asymptotic to $C_f x/(\log x)^{1-\xi}$, where ξ is Artin's constant and C_f is the convergent product,

$$C_f = \frac{15}{14\Gamma(\xi)} \lim_{x\to\infty}\left(\prod_{\substack{p\le x \\ p-1 \text{ squarefree}}} \left(1+\frac{1}{p}+\frac{1}{p^2}\right) \prod_{p\le x}\left(1-\frac{1}{p}\right)^{\xi}\right).$$

As a next step, given a fixed finite abelian group G of order m, it might be interesting to consider the problem of finding an asymptotic formula for the number of n up to x such that G is not contained in $\mathbb{Z}_n^\times$.

Bibliography

[1] Steven Finch, Greg Martin, and Pascal Sebah. Roots of unity and nullity modulo n. Proc. Amer. Math. Soc., 138(8):2729–2743, 2010.

[2] Kevin Ford, Florian Luca, and Pieter Moree. Values of the Euler ϕ-function not divisible by a given odd prime, and the distribution of Euler-Kronecker constants for cyclotomic fields. Math. Comp., 83(287):1447–1476, 2014.

[3] Edmund Landau. Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung enforderlichen Quadrate. Arch. der Math. und Phys., 13(3):305–312, 1908.

[4] Hugh L. Montgomery and Robert C. Vaughan. Multiplicative number theory. I. Classical theory, volume 97 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2007.

[5] Gérald Tenenbaum. Introduction to analytic and probabilistic number theory, volume 163 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.