MULTIPLICATIVE GROUPS AVOIDING A FIXED GROUP

MATTHIAS HANNESSON AND GREG MARTIN

ABSTRACT. We know that any finite abelian group G appears as a subgroup of *infinitely many* multiplicative groups $\mathbb{Z}_n^\times$ (the abelian groups of size $\phi(n)$ that are the multiplicative groups of units in the rings $\mathbb{Z}/n\mathbb{Z}$). It seems to be less well appeciated that G appears as a subgroup of *almost all* multiplicative groups $\mathbb{Z}_n^\times$. We exhibit an asymptotic formula for the counting function of those integers whose multiplicative group fails to contain a copy of G, for all finite abelian groups G (other than the trivial one-element group).

1. INTRODUCTION

We know that any finite abelian group G appears as a subgroup of *infinitely many* multiplicative groups $\mathbb{Z}_n^\times$ (the abelian groups of size $\phi(n)$ that are the multiplicative groups of units in the rings $\mathbb{Z}/n\mathbb{Z}$). The proof of this classic and satisfying problem, which might appear on homework sets for graduate students for example, proceeds as follows: write G as a direct sum of cyclic groups $\mathbb{Z}_{m_j}$ with orders $m_1, \dots, m_\ell$; choose primes $p_j \equiv 1 \pmod{m_j}$, so that $\mathbb{Z}_{m_j}$ is a subgroup of $\mathbb{Z}_{p-1} \cong \mathbb{Z}_p^\times$; and then $\mathbb{Z}_{p_1\cdots p_\ell}^\times \cong \mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_\ell}^\times$ contains a copy of G.

It seems to be less well appeciated that G appears as a subgroup of *almost all* multiplicative groups $\mathbb{Z}_n^\times$. In other words, if we define

$$S(x;G) = \#\{n \le x \colon G \not\leq \mathbb{Z}_n^\times\}, \tag{1.1}$$

then $S(x;G) = o(x)$ for any finite abelian group G. The essential reason, from an "anatomy of integers" standpoint, is that almost all integers are divisible by any fixed number of primes from any prescribed arithmetic progressions; in particular, almost all integers are divisible by ℓ primes p_j each congruent to 1 (mod m_j).

Whenever analytic number theorists encounter a set of integers whose counting function is $o(x)$, we are motivated to seek better quantitative information about the size of that set. The purpose of this paper is to exhibit an asymptotic formula for $S(x;G)$, the counting function of those integers whose multiplicative group fails to contain a copy of G, for all finite abelian groups G (other than the trivial one-element group).

The simplest case is when $G \cong \mathbb{Z}_2^k$, in which case estimating $S(x;G)$ essentially reduces to counting integers with at most $k-1$ distinct prime factors (as we will show in Section 3.1), which is a classical result in analytic number theory.

Theorem 1.1. *For any integer $k \ge 2$,*

$$S(x;\mathbb{Z}_2^k) = \frac{3}{2(k-2)!}\frac{x(\log\log x)^{k-2}}{\log x}\left(1 + O_k\left(\frac{1}{\log\log x}\right)\right). \tag{1.2}$$

2010 *Mathematics Subject Classification.* 11N25, 11N37, 11N45, 11N64, 20K01.

Key words and phrases. Number theory; multiplicative group; Selberg–Delange method.

For more complicated groups G, the statement of the asymptotic formula depends on some terminology related to the structure of G. Recall that the *primary decomposition* of a finite abelian group G is a representation of G as the direct sum of cyclic groups whose orders are all powers of primes; this representation is unique up to permutations of the summands. For example, if G is the multiplicative group modulo 11!, then the Chinese remainder theorem together with the fact that odd prime powers possess primitive roots (and an additional fact about the structure of $\mathbb{Z}_{2^k}^\times$) allow us to see that

$$\begin{aligned} G = \mathbb{Z}_{11!}^\times &= \mathbb{Z}_{2^8\cdot 3^4\cdot 5^2\cdot 7\cdot 11}^\times \\ &\cong \mathbb{Z}_{2^8}^\times \times \mathbb{Z}_{3^4}^\times \times \mathbb{Z}_{5^2}^\times \times \mathbb{Z}_7^\times \times \mathbb{Z}_{11}^\times \\ &\cong (\mathbb{Z}_{2^6} \oplus \mathbb{Z}_2) \oplus \mathbb{Z}_{3^3\cdot 2} \oplus \mathbb{Z}_{5^1\cdot 4} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{10} \\ &\cong (\mathbb{Z}_{64} \oplus \mathbb{Z}_2) \oplus (\mathbb{Z}_{27} \oplus \mathbb{Z}_2) \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_4) \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_2) \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_2) \end{aligned} \tag{1.3}$$

is its primary decomposition. In this example there are 10 primary summands counted with multiplicity; for our purposes, however, it turns out to be important to gather isomorphic summands together.

Definition 1.2. Let G be a finite abelian group. For any prime power p^α and any positive integer k, we say that $\mathbb{Z}_{p^\alpha}^k$ is a *gathered summand* of G if the primary decomposition of G contains exactly k copies of $\mathbb{Z}_{p^\alpha}$, or equivalently if we can write $G \cong \mathbb{Z}_{p^\alpha}^k \times H$ where $\mathbb{Z}_{p^\alpha}$ is not a primary summand of H.

We let $\Gamma(G)$ be the set of all gathered summands of G, so that

$$G \cong \prod_{\mathbb{Z}_{p^\alpha}^k \in \Gamma(G)} \mathbb{Z}_{p^\alpha}^k. \tag{1.4}$$

For example, equation (1.3) shows that $\Gamma(\mathbb{Z}_{11!}^\times) = \{\mathbb{Z}_2^4, \mathbb{Z}_3^1, \mathbb{Z}_4^1, \mathbb{Z}_5^2, \mathbb{Z}_{27}^1, \mathbb{Z}_{64}^1\}$.

We can now give an asymptotic formula for $S(x;G)$, for general finite abelian groups G, in terms of a sum over the gathered summands of G. The following theorem treats all remaining cases not already covered by Theorem 1.1.

Theorem 1.3. *For any finite abelian group $G \ncong \mathbb{Z}_2^k$,*

$$S(x;G) \sim \sum_{\mathbb{Z}_{p^\alpha}^k \in \Gamma(G)} K(p^\alpha, k) \frac{x(\log\log x)^{k-1}}{(\log x)^{1/\phi(p^\alpha)}},$$

where the constants $K(p^\alpha, k)$ are defined in Definition 3.7 below.

While the overall structure of this asymptotic formula is easy to parse, we can be even more precise with one additional piece of terminology.

Definition 1.4. The set of all possible gathered summands $\mathbb{Z}_{p^\alpha}^k$ can be endowed with a total preorder using the lexicographic ordering of the corresponding ordered pairs $(\phi(p^\alpha), k)$, that is, $\mathbb{Z}_{p^\alpha}^k \preccurlyeq \mathbb{Z}_{q^\beta}^\ell$ when either $\phi(p^\alpha) < \phi(q^\beta)$ or else $\phi(p^\alpha) = \phi(q^\beta)$ and $k \le \ell$. Equivalently, $\mathbb{Z}_{p^\alpha}^k \preccurlyeq \mathbb{Z}_{q^\beta}^\ell$ precisely when $x(\log\log x)^{k-1}/(\log x)^{1/\phi(p^\alpha)} \ll x(\log\log x)^{\ell-1}/(\log x)^{1/\phi(q^\beta)}$. Note that it is possible that simultaneously $\mathbb{Z}_{p^\alpha}^k \preccurlyeq \mathbb{Z}_{q^\beta}^\ell$ and $\mathbb{Z}_{q^\beta}^\ell \preccurlyeq \mathbb{Z}_{p^\alpha}^k$, as the example $\mathbb{Z}_3^k \preccurlyeq \mathbb{Z}_4^k$ and $\mathbb{Z}_4^k \preccurlyeq \mathbb{Z}_3^k$ demonstrates; pairs of prime powers with this property are the sole reason why this preorder is not a total order.

We then call a gathered summand of a finite abelian group G a *dominant summand* if it is a maximal element of $\Gamma(G)$ under this ordering.

Not surprisingly, the dominant summands provide the dominant contribution to the asymptotic formula for $S(x;G)$.

Theorem 1.5. *Let $G \ncong \mathbb{Z}_2^k$ be a finite abelian group. If G has a unique dominant summand $\mathbb{Z}_{p^\alpha}^k$, then*

$$S(x;G) = K(p^\alpha,k)\frac{x(\log\log x)^{k-1}}{(\log x)^{1/\phi(p^\alpha)}}\left(1+O_G\left(\frac{1}{\log\log x}\right)\right); \tag{1.5}$$

while if G has two dominant summands $\mathbb{Z}_{p^\alpha}^k$ and $\mathbb{Z}_{q^\beta}^k$, then

$$S(x;G) = \big(K(p^\alpha,k)+K(q^\beta,k)\big)\frac{x(\log\log x)^{k-1}}{(\log x)^{1/\phi(p^\alpha)}}\left(1+O_G\left(\frac{1}{\log\log x}\right)\right). \tag{1.6}$$

In both cases, the leading constants are defined in Definition 3.7 below.

Remark 1.6. It turns out (as we show in Lemma 4.4 below) that G can have at most two dominant summands, because at most two summands $\mathbb{Z}_{p^\alpha}^k$ and $\mathbb{Z}_{q^\beta}^k$ can be "equal" with respect to the total preorder $\preccurlyeq$ from Definition 1.4 (this occurs when $\phi(p^\alpha)=\phi(q^\beta)$, although the values of k must be equal in such cases). Therefore the statement of Theorem 1.5 does exhaust all possible cases (when combined with Theorem 1.1).

Remark 1.7. Note that the power of $\log x$ in equation (1.6) is the same no matter which dominant summand is chosen, since in this case $1/\phi(p^\alpha) = 1/\phi(q^\beta)$ by the definition of the ordering $\preccurlyeq$.

Remark 1.8. It might seem that we would prove Theorem 1.3 first, using some sort of divide-and-conquer strategy, and then deduce Theorem 1.5 from it. However, Theorem 1.3 is difficult to prove directly in the case where G has multiple gathered summands corresponding to the same prime p. Consequently, our actual strategy is to establish Theorem 1.5 as our main goal; it is easy to verify, using only the definitions given so far, that Theorem 1.3 does follow immediately from Theorem 1.5.

The methods used in this paper are extensions of the methods used by Chang and the second author [1] and by Downey and the second author [2] when counting the number of multiplicative groups with a particular least invariant factor or a particular p-Sylow subgroup, respectively. Section 2, which contains many technical lemmas about weighted sums over primes and related counting functions, has the most in common with these prior papers. In Section 3 we establish an asymptotic formula for the counting function $S(x;G)$ from equation (1.1) in the important special case when G is a single gathered summand $\mathbb{Z}_{p^\alpha}^k$, in particular proving Theorem 1.1 therein. Finally, in Section 4 we complete the proof of Theorem 1.5 in full generality.

Throughout this paper, p and q are used exclusively to denote primes. Furthermore, G always denotes a finite abelian group, while H always denotes a finite abelian p-group (a group whose cardinality is a power of p). Furthermore, if G has the decomposition (1.4) as a direct product of its gathered summands, then an implied constant depending on G means that it may depend on some or all of the quantities p^α and k appearing in those gathered summands, as well as on the number of gathered summands.

2. Technical lemmas

In this section we invest in some technical results to prepare ourselves for the main proofs to come, beginning with two preliminary estimates for general functions. In Section 2.1 we treat several sums over primes in arithmetic progressions that are closely parallel to the methods of [2]; in Section 2.2 we import and apply an asymptotic formula from [1] for the counting function of integers with prime factors satisfying certain constraints.

To avoid annoying technicalities when x is small, we use throughout the notation

$$\log_2 x = \log\log\bigl(\max\{x, 3\}\bigr). \tag{2.1}$$

Lemma 2.1. *Let $k \geq 0$ and $\gamma > 0$ be real numbers. For any real numbers $n \geq 2$ and $x \geq n^2$,*

$$\frac{(\log_2(x/n))^k}{(\log(x/n))^\gamma} = \frac{(\log_2 x)^k}{(\log x)^\gamma}\left(1 + O_{k,\gamma}\left(\frac{\log n}{\log x}\right)\right) \ll_{k,\gamma} \frac{(\log_2 x)^k}{(\log x)^\gamma}.$$

Proof. Since $(\log n)/\log x \leq \frac{1}{2}$, the lemma follows immediately from the approximations

$$\begin{aligned}
\log(x/n) &= \log x \cdot \left(1 - \frac{\log n}{\log x}\right) \\
\log\log(x/n) &= \log\log x + \log\left(1 - \frac{\log n}{\log x}\right) \\
&= \log\log x + O\left(\frac{\log n}{\log x}\right) = \log\log x \cdot \left(1 + O\left(\frac{\log n}{\log x \log\log x}\right)\right)
\end{aligned}$$

when $\frac{x}{n} \geq 3$ (and the lemma is trivial otherwise since all expressions are bounded). □

Lemma 2.2. *Let $k \geq 0$ and $\gamma > 0$ be real numbers. Let $f(t)$ be a function satisfying $0 \leq f(t) \leq t$ for $t \geq 0$. Suppose further that $f(t) \ll_{k,\gamma} t(\log_2 t)^k/(\log t)^\gamma$ for $t \geq 3$. Then for any real numbers $x \geq 2$ and $m \geq 2$,*

$$\sum_{\ell=0}^{\infty} f(x/m^\ell) \ll_{k,\gamma} \frac{x(\log_2 x)^k}{(\log x)^\gamma}.$$

Proof. We split the sum into two ranges depending on the relative sizes of x/m^ℓ and $\sqrt{x}$. In the first range, $x/m^\ell \geq m^\ell \geq 2$ and thus

$$\begin{aligned}
\sum_{0 \leq \ell \leq (\log\sqrt{x})/\log m} f(x/m^\ell) &\ll_{k,\gamma} \sum_{0 \leq \ell \leq (\log\sqrt{x})/\log m} \frac{x(\log_2(x/m^\ell))^k}{m^\ell(\log(x/m^\ell))^\gamma} \\
&\ll_{k,\gamma} \frac{x(\log_2 x)^k}{(\log x)^\gamma} \sum_{0 \leq \ell \leq (\log\sqrt{x})/\log m} \frac{1}{m^\ell}
\end{aligned}$$

by Lemma 2.1, and this last geometric series is at most 2. In the second range,

$$\sum_{\ell > (\log\sqrt{x})/\log m} f(x/m^\ell) \leq \sum_{\ell > (\log\sqrt{x})/\log m} \frac{x}{m^\ell} \ll \frac{x}{m^{(\log\sqrt{x})/\log m}} = \sqrt{x},$$

which completes the proof. □

2.1. **Sums over primes in arithmetic progressions.** The results in this section are direct adaptations of the methods used in the paper [2] by Downey and the second author. We give a full proof of the first such lemma, after which we describe the precise relationship between our lemma and the analogous result in [2]. For the remaining lemmas, we simply indicate which result in [2] is analogous without reproducing the proofs.

We use the notation $\mathbb{N} = \{1, 2, \dots\}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; in this section $\alpha \in \mathbb{N}_0$ will always be a nonnegative integer. We also use $p^\alpha \parallel n$ to mean that $p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$. Note that when $\alpha = 0$, the condition $q \equiv 1 \pmod{p^0}$ is true for all primes q.

Lemma 2.3. *Let $\gamma > 0$ such that $\gamma \notin \mathbb{N}$, let p be prime, and let $\alpha \in \mathbb{N}_0$. Then for $y \geq 2$,*

$$\sum_{\substack{q \leq \sqrt{y} \\ q \equiv 1 \pmod{p^\alpha}}} \frac{1}{q(\log(y/q))^\gamma} = \frac{\log_2 y}{\phi(p^\alpha)(\log y)^\gamma} + O_\gamma\biggl(\frac{1}{(\log y)^\gamma}\biggr).$$

Proof. We may assume $y \geq 9$ since the lemma is trivial for smaller y. We may also absorb the $q = 2$ summand (which is relevant in the case $\alpha = 0$) into the error term. If we define

$$M(x) = \sum_{\substack{q \leq x \\ q \equiv 1 \pmod{p^\alpha}}} \frac{1}{q}, \tag{2.2}$$

it then follows by a well-known result (see for example [3, Corollary 4.12]) that there exists a constant c_{p^α} such that $M(x) = (\log_2 x)/\phi(p^\alpha) + c_{p^\alpha} + O(1/\log x)$ for $x \geq 3$ (note that $\log_2 x$ and $\log\log x$ are synonymous in this range). We can then define

$$R(x) = M(x) - (\log_2 x)/\phi(p^\alpha) - c_{p^\alpha}, \tag{2.3}$$

so that $R(x) \ll 1/\log x$. It then follows that

$$\begin{aligned}
\sum_{\substack{3 \leq q \leq \sqrt{y} \\ q \equiv 1 \pmod{p^\alpha}}} \frac{1}{q(\log(y/q))^\gamma} &= \int_3^{\sqrt{y}} \frac{1}{(\log(y/u))^\gamma}\, dM(u) \\
&= \int_3^{\sqrt{y}} \frac{1}{(\log(y/u))^\gamma}\, d\bigl((\log_2 u)/\phi(p^\alpha) + c_{p^\alpha} + R(u)\bigr) \\
&= \frac{1}{\phi(p^\alpha)} \int_3^{\sqrt{y}} \frac{1}{(\log(y/u))^\gamma} \frac{du}{u \log u} + \int_3^{\sqrt{y}} \frac{1}{(\log(y/u))^\gamma}\, dR(u) \\
&= \frac{1}{\phi(p^\alpha)} \biggl(\frac{\log_2 y}{(\log y)^\gamma} + O_\gamma\biggl(\frac{1}{(\log y)^\gamma}\biggr)\biggr) + \int_3^{\sqrt{y}} \frac{1}{(\log(y/u))^\gamma}\, dR(u),
\end{aligned}$$

where we used [2, Lemma 2.11] to estimate the first integral in the second-to-last line. Applying integration by parts to the remaining integral yields

$$\begin{aligned}\int_3^{\sqrt{y}} \frac{1}{(\log(y/u))^\gamma}\,dR(u) &= \frac{R(u)}{(\log(y/u))^\gamma}\bigg|_3^{\sqrt{y}} - \int_3^{\sqrt{y}} R(u)\frac{d}{du}\left(\frac{1}{(\log(y/u))^\gamma}\right)du \\ &= \frac{R(\sqrt{y})}{(\log(\sqrt{y}))^\gamma} - \frac{R(3)}{(\log(y/3))^\gamma} - \int_3^{\sqrt{y}} \frac{\gamma R(u)}{u(\log(y/u))^{\gamma+1}}\,du \\ &\ll_\gamma \frac{1/\log y}{(\log y)^\gamma} + \frac{1}{(\log y)^\gamma} + \int_3^{\sqrt{y}} \frac{1/\log u}{u(\log(y/u))^{\gamma+1}}\,du \\ &\ll_\gamma \frac{1}{(\log y)^\gamma} + \frac{1}{(\log y)^{\gamma+1}}\int_3^{\sqrt{y}} \frac{1}{u\log u}\,du \\ &\ll \frac{1}{(\log y)^\gamma} + \frac{\log_2 y}{(\log y)^{\gamma+1}},\end{aligned}$$

which completes the proof. □

Remark 2.4. Lemma 2.3 is virtually the same as [2, Lemma 2.12], except that our sum runs over primes q with $q \equiv 1 \pmod{p^\alpha}$ whereas their sum runs over primes q with $p^\alpha \parallel (q-1)$. Note that our constant $1/\phi(p^\alpha)$ is the relative density of $\{q\colon q \equiv 1 \pmod{p^\alpha}\}$ within the primes, while their constant $1/p^\alpha$ is the relative density of $\{q\colon p^\alpha \parallel (q-1)\}$. Indeed, we can recover their result immediately from ours, since

$$\{q\colon p^\alpha \parallel (q-1)\} = \{q\colon q \equiv 1 \pmod{p^\alpha}\} \setminus \{q\colon q \equiv 1 \pmod{p^{\alpha+1}}\}.$$

Unfortunately, we cannot directly prove our result from theirs, since

$$\{q\colon q \equiv 1 \pmod{p^\alpha}\} = \{q\colon p^\alpha \parallel (q-1)\} \cup \{q\colon p^{\alpha+1} \parallel (q-1)\} \cup \{q\colon p^{\alpha+2} \parallel (q-1)\} \cup \cdots,$$

and handling the resulting infinite sum leads to worse error terms. Nevertheless, other than the fact that we start from equation (2.3) while they start from [2, equation (2.6)], the two proofs are identical (up to notational choices).

Lemma 2.5. *Let $\gamma > 0$ such that $\gamma \notin \mathbb{N}$, let p be prime, and let $\alpha \in \mathbb{N}_0$. Then for $y \geq 9$,*

$$\sum_{\substack{\sqrt{y} < q \leq y/2 \\ q \equiv 1 \pmod{p^\alpha}}} \frac{1}{q(\log(y/q))^\gamma} \ll_\gamma \frac{1}{(\log y)^{\min\{1,\gamma\}}}.$$

Proof. This formula is directly analogous to [2, Lemma 2.14], except that our sum runs over primes q with $q \equiv 1 \pmod{p^\alpha}$ whereas their sum runs over primes q with $p^\alpha \parallel (q-1)$. (We have also chosen to let q range up to $\frac{y}{2}$ in this paper, while they used an upper bound of $\frac{y}{3}$.) The proof is again essentially identical, other than starting from equation (2.3) and using Lemma 2.3 while they start from [2, equation (2.6)] and use [2, Lemma 2.12]. □

Lemma 2.6. *Let $k \geq 0$ and $\gamma > 0$ such that $\gamma \notin \mathbb{N}$, let p be prime, and let $\alpha \in \mathbb{N}_0$. Then for $y \geq 2$,*

$$\sum_{\substack{q \leq y/2 \\ q \equiv 1 \pmod{p^\alpha}}} \frac{(\log_2(y/q))^k}{q(\log(y/q))^\gamma} = \frac{(\log_2 y)^{k+1}}{\phi(p^\alpha)(\log y)^\gamma} + O_{k,\gamma}\left(\frac{(\log_2 y)^k}{(\log y)^{\min\{1,\gamma\}}}\right).$$

Proof. This formula is directly analogous to [2, Lemma 2.18], except that again our sum runs over primes q with $q \equiv 1 \pmod{p^\alpha}$ whereas their sum runs over primes q with $p^\alpha \parallel (q-1)$. The proof is again otherwise identical. □

Lemma 2.7. *Let $k \geq 0$ and $\gamma > 0$ such that $\gamma \notin \mathbb{N}$. Then for $y \geq 2$,*

$$\sum_{q \leq y/2} \frac{(\log_2(y/q))^k}{q(\log(y/q))^\gamma} \ll_{k,\gamma} \frac{(\log_2 y)^{k+1}}{(\log y)^{\min\{\gamma,1\}}}.$$

Proof. This bound is an immediate consequence of the $\alpha = 0$ case of Lemma 2.6. □

Lemma 2.8. *Let $k \geq 0$. Then for $y \geq 2$,*

$$\sum_{q \leq y/2} \frac{(\log_2(y/q))^k}{q(\log(y/q))} \ll_k \frac{(\log_2 y)^{k+1}}{\log y}.$$

Proof. The lemma follows by splitting the range of summation and noting that

$$\sum_{q \leq \sqrt{y}} \frac{(\log_2(y/q))^k}{q(\log(y/q))} \ll \frac{(\log_2 y)^k}{\log y} \sum_{q \leq \sqrt{y}} \frac{1}{q} \ll \frac{(\log_2 y)^{k+1}}{\log y}$$

$$\sum_{\sqrt{y} < q \leq y/2} \frac{(\log_2(y/q))^k}{q(\log(y/q))} \ll (\log_2 y)^k \sum_{\sqrt{y} < q \leq y/2} \frac{1}{q \log(y/q)} \ll \frac{(\log_2 y)^{k+1}}{\log y},$$

where this last sum is bounded using [2, Lemma 2.15]. □

Lemma 2.9. *Let $j \in \mathbb{N}$ and $0 < \gamma < 2$. Then for $y \geq 2$,*

$$\sum_{p_1 \leq y/2} \frac{1}{p_1} \cdots \sum_{p_j \leq y/2p_1 \cdots p_{j-1}} \frac{1}{p_j} \frac{1}{(\log(y/p_1 \cdots p_j))^\gamma} \ll_{j,\gamma} \frac{(\log_2 y)^j}{(\log y)^{\min\{\gamma,1\}}}.$$

Proof. The lemma follows by an inductive application of Lemma 2.7, or Lemma 2.8 in the case that $\gamma = 1$, since for any $i \leq j$ we have

$$\sum_{p_i \leq y/2p_1 \cdots p_{i-1}} \frac{1}{p_i} \frac{(\log_2(y/p_1 \cdots p_i))^{j-i}}{(\log(y/p_1 \cdots p_i))^\gamma} \ll_{j,\gamma} \frac{(\log_2(y/p_1 \cdots p_{i-1}))^{j-(i-1)}}{(\log(y/p_1 \cdots p_{i-1}))^{\min\{\gamma,1\}}}.$$

□

Lemma 2.10. *Let $j \in \mathbb{N}$. Then for $y \geq 3$,*

$$\sum_{p_1 \leq y/2} \cdots \sum_{p_{j-1} \leq y/2p_1 \cdots p_{j-2}} \sum_{y/2p_1 \cdots p_{j-1} < p_j \leq y/p_1 \cdots p_{j-1}} \sum_{n \leq y/p_1 \cdots p_j} 1 \ll_j \frac{y(\log_2 y)^{j-1}}{\log y}.$$

Proof. Since $y/2p_1 \cdots p_{j-1} < p_j$, it follows that the inner sum can have at most one term. Therefore

$$\sum_{p_1 \leq y/2} \cdots \sum_{y/2p_1 \cdots p_{j-1} < p_j \leq y/p_1 \cdots p_{j-1}} \sum_{n \leq y/p_1 \cdots p_j} 1 \leq \sum_{p_1 \leq y/2} \cdots \sum_{p_{j-1} \leq y/2p_1 \cdots p_{j-2}} \sum_{y/2p_1 \cdots p_{j-1} < p_j \leq y/p_1 \cdots p_{j-1}} 1$$

$$\leq \sum_{p_1 \leq y/2} \cdots \sum_{p_{j-1} \leq y/2p_1 \cdots p_{j-2}} \pi(y/p_1 \cdots p_{j-1}) \ll \sum_{p_1 \leq y/2} \cdots \sum_{p_{j-1} \leq y/2p_1 \cdots p_{j-2}} \frac{y/p_1 \cdots p_{j-1}}{\log(y/p_1 \cdots p_{j-1})},$$

so the lemma follows by Lemma 2.9. □

Lemma 2.11. *Let $k \geq 0$ and $\gamma > 0$ such that $\gamma \notin \mathbb{N}$, let $p_1, \dots, p_j$ be distinct primes, let p be prime and let $\alpha \in \mathbb{N}$. Then for $y \geq 2$,*

$$\sum_{\substack{q \leq y/2 \\ q \equiv 1 \pmod{p^\alpha} \\ q \nmid p_1 \cdots p_j}} \frac{q + O(1)}{q^2} \left(\frac{(\log_2(y/q))^k}{(\log(y/q))^\gamma} + O\left(\frac{(\log_2(y/q))^{k-1}}{(\log(y/q))^{\min\{\gamma,1\}}} \right) \right)$$

$$= \frac{(\log_2 y)^{k+1}}{\phi(p^\alpha)(\log y)^\gamma} + O_{j,k,\gamma}\left(\frac{(\log_2 y)^k}{(\log y))^{\min\{\gamma,1\}}} \right).$$

Proof. This formula is again directly analogous to [2, Proposition 2.20], except that our sum runs over primes q with $q \equiv 1 \pmod{p^\alpha}$ whereas their sum runs over primes q with $p^\alpha \parallel (q-1)$. □

2.2. **Integers with constrained prime factors.** We will need asymptotic formulas and estimates for the number of integers with particular constraints (most notably congruence restrictions) on their prime factors. We begin by defining a complicated constant occurring in the main term of such asymptotic formulas.

Definition 2.12. Let $\mathcal{B}$ be a set of τ distinct reduced residue classes modulo d, and define

$$\delta(\mathcal{B}) = \lim_{s \to 1^+} \zeta(s)^{-\tau/\phi(d)} \prod_{q \in \mathcal{B}} \left(1 - \frac{1}{q^s}\right)^{-1}.$$

The limit exists because the function on the right-hand side has an analytic continuation to a neighbourhood of $s = 1$ (see for example [1, Lemma 3.2]).

Lemma 2.13. *Let $\mathcal{B}$ be a set of τ distinct reduced residue classes modulo d, and let $p_1, \dots, p_m$ be distinct primes not belonging to $\mathcal{B}$. Then for $x \geq 2$,*

$$\sum_{\substack{n \leq x \\ (q \mid n \text{ and } q \notin \mathcal{B}) \implies q \mid p_1 \cdots p_m}} 1 = \frac{\delta(\mathcal{B})}{\Gamma(\tau/\phi(d))} \frac{p_1 \cdots p_m}{\phi(p_1 \cdots p_m)} \frac{x}{(\log x)^{1-\tau/\phi(d)}} + O_{d,m}\left(\frac{x}{(\log x)^{2-\tau/\phi(d)}} \right).$$

Proof. Let $\mathcal{I} = \{p_1, \dots, p_m\}$ and $\mathcal{R} = \varnothing$, so that we are counting integers all of whose prime factors belong to $\mathcal{B} \cup \mathcal{I} \backslash \mathcal{R}$. Since we are allowing our error term depend on d and m, the statement of [1, Theorem 3.6] simplifies to

$$\sum_{\substack{n \leq x \\ (q \mid n \text{ and } q \notin \mathcal{B}) \implies q \mid p_1 \cdots p_m}} 1 = \#\{n \leq x \colon q \mid n \implies q \in \mathcal{B} \cup \mathcal{I} \backslash \mathcal{R}\}$$

$$= \frac{x}{(\log x)^{1-\tau/\phi(d)}} \left(\frac{\delta(\mathcal{B})}{\Gamma(\tau/\phi(d))} \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)^{-1} + O_{d,m}\left(\frac{1}{\log x} \right) \right),$$

which is equivalent to the statement of the lemma. (Their Theorem 3.6 includes the constraint $\log x \gg d^{1/2} \log^2 d$; however, since we allow our O-constant to depend on d, we may extend that range all the way down to $x \geq 3$.) □

Definition 2.14. Let $\mathcal{B}$ be any set of positive integers. For any $m \in \mathbb{N}_0$, define

$$D_m(x; \mathcal{B}) = \#\big\{N \leq x \colon N \text{ has exactly } m \text{ distinct prime factors that are not in } \mathcal{B}\big\}.$$

Note that in particular

$$D_0(x;\mathcal{B}) = \sum_{\substack{n\le x\\ q\mid n \implies q\in\mathcal{B}}} 1. \tag{2.4}$$

Lemma 2.15. *Let $\mathcal{B}$ be the union of τ distinct reduced residue classes modulo d. Then*

$$D_m(x;\mathcal{B}) = \frac{1}{m!}\sum_{\substack{p_1\le x/2\\ p_1\notin\mathcal{B}}}\sum_{\substack{p_2\le x/2p_1\\ p_2\notin\mathcal{B}\\ p_2\neq p_1}}\cdots\sum_{\substack{p_m\le x/2p_1\cdots p_{m-1}\\ p_m\notin\mathcal{B}\\ p_m\nmid p_1\cdots p_{m-1}}}\sum_{\substack{n\le x/p_1\cdots p_m\\ (q\mid n \text{ and } q\notin\mathcal{B})\implies q\mid p_1\cdots p_m}} 1 + O_{d,m}\left(\frac{x(\log_2 x)^{m-1}}{(\log x)^{1-\tau/\phi(d)}}\right). \tag{2.5}$$

Proof. When $m=0$ the claim is immediate from equation (2.4), so we may assume $m\ge 1$. We first claim that

$$D_m(x;\mathcal{B}) = \frac{1}{m!}\sum_{\substack{p_1\le x\\ p_1\notin\mathcal{B}}}\sum_{\substack{p_2\le x/p_1\\ p_2\notin\mathcal{B}\\ p_2\neq p_1}}\cdots\sum_{\substack{p_j\le x/p_1\cdots p_{j-1}\\ p_j\notin\mathcal{B}\\ p_j\nmid p_1\cdots p_{j-1}}}\sum_{\substack{n\le x/p_1\cdots p_j\\ (q\mid n \text{ and } q\notin\mathcal{B})\implies q\mid p_1\cdots p_j}} 1. \tag{2.6}$$

To see this, for any N counted by $D_m(x;\mathcal{B})$, let $p_1,\dots,p_m$ be the distinct prime factors outside $\mathcal{B}$ that divide N, and set $n = N/p_1\cdots p_m$; then n is counted by the innermost sum in equation (2.6), while the factor of $1/m!$ comes from the fact that each distinct set of primes $\{p_1,\dots,p_m\}$ outside of $\mathcal{B}$ will be counted $m!$ times by the multiple sum.

In equation (2.6), if $p_j > x/2p_1\cdots p_{j-1}$ for any $1\le j\le m-1$ then the the sum over $p_{j+1}\le x/p_1\cdots p_i$ will be empty; consequently we may adjust those ranges of summation to $p_j\le x/2p_1\cdots p_{j-1}$. We also split the sum over p_m into two ranges at $x/2p_1\cdots p_{m-1}$, which yields $D_m(x;\mathcal{B}) = \frac{1}{m!}(J_1+J_2)$ where we have defined

$$J_1 = \sum_{\substack{p_1\le x/2\\ p_1\notin\mathcal{B}}}\sum_{\substack{p_2\le x/2p_1\\ p_2\notin\mathcal{B}\\ p_2\neq p_1}}\cdots\sum_{\substack{p_m\le x/2p_1\cdots p_{m-1}\\ p_m\equiv\notin\mathcal{B}\\ p_m\nmid p_1\cdots p_{m-1}}}\sum_{\substack{n\le x/p_1\cdots p_m\\ (q\mid n \text{ and } q\nmid p_1\cdots p_m)\implies q\in\mathcal{B}}} 1$$

$$J_2 = \sum_{\substack{p_1\le x/2\\ p_1\notin\mathcal{B}}}\sum_{\substack{p_2\le x/2p_1\\ p_2\notin\mathcal{B}\\ p_2\neq p_1}}\cdots\sum_{\substack{x/2p_1\cdots p_{m-1}<p_m\le x/p_1\cdots p_{m-1}\\ p_m\notin\mathcal{B}\\ p_m\nmid p_1\cdots p_{m-1}}}\sum_{\substack{n\le x/p_1\cdots p_m\\ (q\mid n \text{ and } q\nmid p_1\cdots p_m)\implies q\in\mathcal{B}}} 1.$$

For J_2, we may simply ignore the congruence and divisibility restrictions on the p_j and on n so as to apply Lemma 2.10, yielding the estimate $J_2 \ll_m x(\log_2 x)^{m-1}/\log x$ that establishes the lemma. □

Lemma 2.16. *Let $\mathcal{B}$ be the union of τ distinct reduced residue classes modulo d. For any $k\in\mathbb{N}_0$, the number of integers up to x that have at most k distinct prime factors that are not in $\mathcal{B}$ is $\ll_{d,k} x(\log_2 x)^k/(\log x)^{1-\tau/\phi(d)}$.*

Proof. For any $0 \le m \le k$, we invoke Lemma 2.15 and then apply Lemma 2.13 to the innermost sum in equation (2.5) to obtain

$$D_m(x;\mathcal{B}) \ll_{d,m} \sum_{\substack{p_1 \le x/2 \\ p_1 \notin \mathcal{B}}} \cdots \sum_{\substack{p_m \le x/2p_1\cdots p_{m-1} \\ p_m \notin \mathcal{B} \\ p_m \nmid p_1\cdots p_{m-1}}} \frac{x/p_1\cdots p_m}{(\log(x/p_1\cdots p_m))^{1-\tau/\phi(d)}} + \frac{x(\log_2 x)^{m-1}}{(\log x)^{1-\tau/\phi(d)}}.$$

We may now ignore the restrictions that the p_i are distinct and not in $\mathcal{B}$ so as to apply Lemma 2.9, from which we deduce that $D_m(x;\mathcal{B}) \ll_{d,m} x(\log_2 x)^j/(\log x)^{1-c/\phi(d)}$; the lemma follows upon summing over $0 \le m \le k$. □

Definition 2.17. For any $m \in \mathbb{N}_0$, define

$$D_m(x;p^\alpha) = \#\big\{N \le x : p \nmid N, \\ N \text{ has exactly } m \text{ distinct prime factors congruent to 1 modulo } p^\alpha\big\}.$$

Note that this is almost the same quantity as $D_m(x;\mathcal{B}_{p^\alpha})$, where

$$\mathcal{B}_{p^\alpha} = \{c \in \mathbb{Z}_{p^\alpha}^\times : c \not\equiv 1 \pmod{p^\alpha}\} \tag{2.7}$$

is the union of $\phi(p^\alpha)-1$ reduced residue classes modulo p^α; however, $D_m(x;\mathcal{B}_{p^\alpha})$ counts some integers divisible by p while $D_m(x;p^\alpha)$ does not. Nevertheless, the proof of Lemma 2.15 goes through virtually unchanged to show that

$$D_m(x;p^\alpha) = \frac{1}{m!} \sum_{\substack{p_1 \le x/2 \\ p_1 \equiv 1 \pmod{p^\alpha}}} \sum_{\substack{p_2 \le x/2p_1 \\ p_2 \equiv 1 \pmod{p^\alpha} \\ p_2 \ne p_1}} \cdots \sum_{\substack{p_m \le x/2p_1\cdots p_{m-1} \\ p_m \equiv 1 \pmod{p^\alpha} \\ p_m \nmid p_1\cdots p_{m-1}}} \sum_{\substack{n \le x/p_1\cdots p_m \\ (q\mid n \text{ and } q \notin \mathcal{B}_{p^\alpha}) \Longrightarrow q \mid p_1\cdots p_m}} 1 \\ + O_{d,m}\left(\frac{x(\log_2 x)^{m-1}}{(\log x)^{1-\tau/\phi(d)}}\right). \tag{2.8}$$

Lemma 2.18. *For any prime power $p^\alpha \ge 3$ and any $m \in \mathbb{N}_0$,*

$$D_m(x;p^\alpha) = \frac{\delta(\mathcal{B}_{p^\alpha})/m!}{\Gamma(1-1/\phi(p^\alpha))} \frac{x(\log_2 x)^m}{\phi(p^\alpha)^m(\log x)^{1/\phi(p^\alpha)}} + O_{p,\alpha,m}\left(\frac{x(\log_2 x)^{m-1}}{(\log x)^{1/\phi(p^\alpha)}}\right).$$

In particular, $D_m(x;p^\alpha) \ll_{p,\alpha,m} x(\log_2 x)^m/(\log x)^{1/\phi(p^\alpha)}$.

Proof. Let J_1 equal the multiple sum in equation (2.8). We apply Lemma 2.13 with $d = p^\alpha$ and $\mathcal{B} = \mathcal{B}_{p^\alpha}$ from equation (2.7), so that $\tau = \phi(p^\alpha) - 1$, to the innermost sum to obtain

$$\begin{aligned} J_1 &= \frac{1}{m!} \sum_{\substack{p_1 \le x/2 \\ p_1 \equiv 1 \pmod{p^\alpha}}} \cdots \sum_{\substack{p_m \le x/2p_1\cdots p_{m-1} \\ p_m \equiv 1 \pmod{p^\alpha} \\ p_m \nmid p_1\cdots p_{m-1}}} \left(\frac{\delta(\mathcal{B}_{p^\alpha})}{\Gamma(1-1/\phi(p^\alpha))} \frac{x/p_1\cdots p_m}{(\log(x/p_1\cdots p_m))^{1/\phi(p^\alpha)}} \frac{p_1\cdots p_m}{\phi(p_1\cdots p_m)} \right. \\ &\qquad \left. + O_{p,\alpha,m}\left(\frac{x/p_1\cdots p_m}{(\log(x/p_1\cdots p_m))^{1+1/\phi(p^\alpha)}} \right) \right) \\ &= \frac{\delta(\mathcal{B}_{p^\alpha})x/m!}{\Gamma(1-1/\phi(p^\alpha))} \sum_{\substack{p_1 \le x/2 \\ p_1 \equiv 1 \pmod{p^\alpha}}} \frac{p_1 + O(1)}{p_1^2} \cdots \sum_{\substack{p_m \le x/2p_1\cdots p_{m-1} \\ p_m \equiv 1 \pmod{p^\alpha} \\ p_m \nmid p_1\cdots p_{m-1}}} \frac{p_m + O(1)}{p_m^2} \frac{1}{(\log(x/p_1\cdots p_m))^{1/\phi(p^\alpha)}} \\ &\qquad + O_{p,\alpha,m}\left(\sum_{\substack{p_1 \le x/2 \\ p_1 \equiv 1 \pmod{p^\alpha}}} \cdots \sum_{\substack{p_m \le x/2p_1\cdots p_{m-1} \\ p_m \equiv 1 \pmod{p^\alpha} \\ p_m \nmid p_1\cdots p_{m-1}}} \frac{x/p_1\cdots p_m}{(\log(x/p_1\cdots p_m))^{1+1/\phi(p^\alpha)}} \right). \end{aligned} \tag{2.9}$$

In the error term, we may again ignore the congruence and distinctness conditions on the p_j so as to apply Lemma 2.9, which yields the acceptable error $\ll_{p,\alpha,m} x(\log_2 x)^{m-1}/\log x$.

Regarding the main term on the right-hand side of equation (2.9), Lemma 2.11 tells us that for any $i \le m$,

$$\begin{aligned} &\frac{1}{\phi(p^\alpha)^{m-i}} \sum_{\substack{p_i \le x/2p_1\cdots p_{i-1} \\ p_i \equiv 1 \pmod{p^\alpha}}} \frac{p_i + O(1)}{p_i^2} \left(\frac{(\log_2(x/p_1\cdots p_i))^{m-i}}{(\log(x/p_1\cdots p_i)^{1/\phi(p^\alpha)}} \right. \\ &\qquad \left. + O_{p,\alpha,m}\left(\frac{(\log_2(x/p_1\cdots p_i))^{m-i-1}}{(\log(x/p_1\cdots p_i)^{1/\phi(p^\alpha)}} \right) \right) \\ &= \frac{1}{\phi(p^\alpha)^{m-(i-1)}} \frac{(\log_2(x/p_1\cdots p_{i-1}))^{m-(i-1)}}{(\log(x/p_1\cdots p_{i-1})^{1/\phi(p^\alpha)}} + O_{p,\alpha,m}\left(\frac{(\log_2(x/p_1\cdots p_{i-1}))^{m-i}}{(\log(x/p_1\cdots p_{i-1})^{1/\phi(p^\alpha)}} \right). \end{aligned}$$

This observation allows us to iteratively evaluate the innermost sum one at a time, and it follows inductively in this way that

$$\begin{aligned} &\sum_{\substack{p_1 \le x/2 \\ p_1 \equiv 1 \pmod{p^\alpha}}} \frac{p_1 + O(1)}{p_1^2} \cdots \sum_{\substack{p_m \le x/2p_1\cdots p_{m-1} \\ p_m \equiv 1 \pmod{p^\alpha} \\ p_m \nmid p_1\cdots p_{m-1}}} \frac{p_m + O(1)}{p_m^2} \frac{1}{(\log(x/p_1\cdots p_m))^{1/\phi(p^\alpha)}} \\ &\qquad = \frac{(\log_2 x)^m}{\phi(p^\alpha)^m (\log x)^{1/\phi(p^\alpha)}} + O_{p,\alpha,m}\left(\frac{(\log_2 x)^{m-1}}{(\log x)^{1/\phi(p^\alpha)}} \right), \end{aligned}$$

which completes the proof of the lemma when inserted back into equation (2.9). □

3. Individual gathered summands

The estimation of $S(x;\mathbb{Z}_{p^\alpha}^k)$ will be crucial to the estimation of $S(x;G)$ for general finite abelian groups G. It will be helpful to group the integers counted by $S(x;\mathbb{Z}_{p^\alpha}^k)$ according to the power of p dividing them.

Definition 3.1. For any prime power p^α and any integers $k \geq 1$ and $\ell \geq 0$, define

$$S_\ell(x;\mathbb{Z}_{p^\alpha}^k) = \#\big\{n \leq x \colon \mathbb{Z}_{p^\alpha}^k \not\leq \mathbb{Z}_n^\times,\, p^\ell \parallel n\big\}.$$

This quantity refines $S(x;\mathbb{Z}_{p^\alpha}^k)$, and indeed a comparison to Definition 1.1 reveals that

$$S(x;\mathbb{Z}_{p^\alpha}^k) = \sum_{\ell=0}^{\infty} S_\ell(x;\mathbb{Z}_{p^\alpha}^k). \tag{3.1}$$

Fortunately, every quantity $S_\ell(x;\mathbb{Z}_{p^\alpha}^k)$ can be expressed in terms of $S_0(y;\mathbb{Z}_{p^\alpha}^j)$ for various values of y and j, as we now demonstrate.

Lemma 3.2. *For any prime power $p^\alpha \geq 3$ and any integers $k \geq 1$ and $\ell \geq 0$,*

$$S_\ell(x;\mathbb{Z}_{p^\alpha}^k) = \begin{cases} S_0(x/p^\ell;\mathbb{Z}_{p^\alpha}^k), & \text{if } p \text{ is odd and } \ell \leq \alpha, \\ S_0(x/p^\ell;\mathbb{Z}_{p^\alpha}^{k-1}), & \text{if } p \text{ is odd and } \ell \geq \alpha+1, \\ S_0(x/2^\ell;\mathbb{Z}_{2^\alpha}^k), & \text{if } p=2 \text{ and } \alpha \geq 2 \text{ and } \ell \leq \alpha+1, \\ S_0(x/2^\ell;\mathbb{Z}_{2^\alpha}^{k-1}), & \text{if } p=2 \text{ and } \alpha \geq 2 \text{ and } \ell \geq \alpha+2. \end{cases}$$

Furthermore, $S_1(x;\mathbb{Z}_2^k) = S_0(x/2;\mathbb{Z}_2^k)$ and $S_2(x;\mathbb{Z}_2^k) = S_0(x/4,\mathbb{Z}_2^{k-1})$, while $S_\ell(x;\mathbb{Z}_2^k) = S_0(x/2^\ell,\mathbb{Z}_2^{k-2})$ for $\ell \geq 3$.

Proof. Every integer counted by $S_\ell(x;\mathbb{Z}_{p^\alpha}^k)$ can be written as $n = p^\ell r$ where $r \leq x/p^\ell$ and $p \nmid r$; as a result, $\mathbb{Z}_n^\times \cong \mathbb{Z}_{p^\ell}^\times \times \mathbb{Z}_r^\times$.

If p is odd, then $\mathbb{Z}_{p^\ell}^\times \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{\ell-1}}$, which contains a copy of $\mathbb{Z}_{p^\alpha}$ if and only if $\ell \geq \alpha+1$. Therefore $\mathbb{Z}_r^\times$ cannot contain k copies of $\mathbb{Z}_{p^\alpha}$ if $\ell \leq \alpha$, and cannot contain $k-1$ copies of $\mathbb{Z}_{p^\alpha}$ if $\ell \geq \alpha+1$.

If $p=2$, then $\mathbb{Z}_{2^1}^\times \cong \mathbb{Z}_1$ and $\mathbb{Z}_{2^2}^\times \cong \mathbb{Z}_2$, while $\mathbb{Z}_{2^\ell}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\ell-2}}$ for $\ell \geq 3$. When $\alpha \geq 2$, these groups contain a copy of $\mathbb{Z}_{2^\alpha}$ if and only if $\ell \geq \alpha+2$. Therefore $\mathbb{Z}_r^\times$ cannot contain k copies of $\mathbb{Z}_{2^\alpha}$ if $\ell \leq \alpha+1$, and cannot contain $k-1$ copies of $\mathbb{Z}_{2^\alpha}$ if $\ell \geq \alpha+2$. The identities for $S_\ell(x;\mathbb{Z}_2^k)$ follow similarly by noting that $\mathbb{Z}_{2^\ell}^\times$ contains 0, 1, or 2 copies of $\mathbb{Z}_2$ depending on whether $\ell=1$, $\ell=2$, or $\ell \geq 3$. □

Thanks to Lemma 3.2, we can concentrate solely on $S_0(x;\mathbb{Z}_{p^\alpha}^k)$ to understand the behaviour of $S(x;\mathbb{Z}_{p^\alpha}^k)$. It turns out that the case $p^\alpha = 2$ is special, but also straightforward, so we handle that case first.

3.1. The special case of $\mathbb{Z}_2^k$.

In this section, we prove Theorem 1.1. The reason that the case $p^\alpha = 2$ is different from other cases is that *every* odd prime dividing n produces a primary factor $\mathbb{Z}_2$ in the multiplicative group $\mathbb{Z}_n^\times$, and more such factors are produced if $4 \mid n$. In particular, it follows immediately that if $\mathbb{Z}_2 \not\leq \mathbb{Z}_n^\times$ then either $n=1$ or $n=2$, and therefore $S(x;\mathbb{Z}_2) = 2$ for all $x \geq 2$.

In general, the number of copies of $\mathbb{Z}_2$ present in the primary decomposition of the multiplicative group $\mathbb{Z}_n^\times$ is nearly the same as the number of prime factors of n. Indeed, we will

be able to derive our asymptotic formula for $S(x;\mathbb{Z}_2^k)$ quickly from the classical counting function of integers with a given number of prime factors.

Definition 3.3. For all nonnegative integers m, define

$$\pi_m(x) = \#\{n \le x : \omega(n) = m\} \quad \text{and} \quad \pi_m^\star(x) = \#\{n \le x : 2 \nmid n,\, \omega(n) = m\}$$

The estimation of $\pi_m(x)$ is classical:

Lemma 3.4. *For all positive integers m,*

$$\pi_m(x) = \frac{1}{(m-1)!}\frac{x(\log_2 x)^{m-1}}{\log x} + O_m\left(\frac{x(\log_2 x)^{m-2}}{\log x}\right).$$

Proof. While this statement can be proved by induction on m, we instead use the Selberg–Sathe asymptotic formula (see for example [4, Theorem 6.4]), which asserts that

$$\pi_m(x) = \frac{1}{(m-1)!}\frac{x(\log_2 x)^{m-1}}{\log x}\left(\lambda\left(\frac{m-1}{\log_2 x}\right) + O_m\left(\frac{1}{(\log_2 x)^2}\right)\right),$$

where

$$\lambda(z) = \frac{1}{\Gamma(1+z)}\prod_p \left(1 + \frac{z}{p-1}\right)\left(1 - \frac{1}{p}\right)^z. \tag{3.2}$$

Since λ is analytic on some neighbourhood of 0, it follows that $\lambda(z) = \lambda(0) + O(z)$ for sufficiently small z. Therefore,

$$\lambda\left(\frac{m-1}{\log_2 x}\right) = 1 + O\left(\frac{m-1}{\log_2 x}\right),$$

which completes the proof. □

It turns out that the same asymptotic formula holds when we count only odd integers:

Lemma 3.5. *For all positive integers m,*

$$\pi_m^\star(x) = \frac{1}{(m-1)!}\frac{x(\log_2 x)^{m-1}}{\log x} + O_m\left(\frac{x(\log_2 x)^{m-2}}{\log x}\right).$$

Proof. Every integer counted by $\pi_m(x)$ but not by $\pi_m^\star(x)$ can be written as $n = 2^\ell r$ where $r \le x/2^\ell$ and $2 \nmid r$ and $\omega(r) = m-1$; consequently,

$$\pi_m(x) - \pi_m^\star(x) = \sum_{\ell=1}^{\infty} \pi_{m-1}^\star(x/2^\ell) \le \sum_{\ell=1}^{\infty} \pi_{m-1}(x/2^\ell).$$

The claimed asymptotic formula follows since Lemmas 2.2 and 3.4 imply that

$$\sum_{\ell=1}^{\infty} \pi_{m-1}(x/2^\ell) \ll_m \frac{x(\log_2 x)^{m-2}}{\log x}.$$ □

With the estimation of $\pi_m^\star(x)$ complete, we are ready to establish the asymptotic formula for $S(x;\mathbb{Z}_2^k)$.

Proof of Theorem 1.1. Since every odd prime dividing n produces a primary factor $\mathbb{Z}_2$ in the multiplicative group $\mathbb{Z}_n^\times$, we see that $S_0(x;\mathbb{Z}_2^k)$ is exactly equal to the number of odd integers up to x with at most $k-1$ distinct (odd) prime factors, which is to say that

$$S_0(x;\mathbb{Z}_2^k) = \sum_{m=0}^{k-1} \pi_m^\star(x).$$

It follows directly from Lemma 3.5 that

$$S_0(x;\mathbb{Z}_2^k) = \frac{1}{(k-2)!}\frac{x(\log_2 x)^{k-2}}{\log x} + O_k\left(\frac{x(\log_2 x)^{k-3}}{\log x}\right). \tag{3.3}$$

Then by equation (3.1) and Lemma 3.2,

$$\begin{aligned} S(x;\mathbb{Z}_2^k) &= \sum_{\ell=0}^{\infty} S_\ell(x;\mathbb{Z}_2^k) \\ &= S_0(x,\mathbb{Z}_2^k) + S_0(x/2,\mathbb{Z}_2^k) + S_0(x/4,\mathbb{Z}_2^{k-1}) + \sum_{\ell=3}^{\infty} S_0(x/2^\ell,\mathbb{Z}_2^{k-2}). \end{aligned} \tag{3.4}$$

By equation (3.3), the first two terms contribute

$$\begin{aligned} &S_0(x,\mathbb{Z}_2^k) + S_0(x/2,\mathbb{Z}_2^k) \\ &\quad= \frac{1}{(k-2)!}\frac{x(\log_2 x)^{k-2}}{\log x} + \frac{1}{(k-2)!}\frac{(x/2)(\log_2(x/2))^{k-2}}{\log(x/2)} + O_k\left(\frac{x(\log_2 x)^{k-3}}{\log x}\right) \\ &\quad= \frac{3}{2(k-2)!}\frac{x(\log_2 x)^{k-2}}{\log x} + O_k\left(\frac{x(\log_2 x)^{k-3}}{\log x}\right) \end{aligned}$$

using Lemma 2.1, while the remaining terms contribute

$$S_0(x/4,\mathbb{Z}_2^{k-1}) + \sum_{\ell=3}^{\infty} S_0(x/2^\ell,\mathbb{Z}_2^{k-2}) \ll_k \frac{x(\log_2 x)^{k-3}}{\log x} + \frac{x(\log_2 x)^{k-4}}{\log x}$$

by equation (3.3) again and Lemma 2.2. Inserting these last two estimates into equation (3.4) completes the proof of the theorem. □

3.2. **Estimation of $S_0(x;\mathbb{Z}_{p^\alpha}^k)$ and $S(x;\mathbb{Z}_{p^\alpha}^k)$.** We now return to the goal of asymptotically evaluating $S_0(x;\mathbb{Z}_{p^\alpha}^k)$ when p^α is a prime power exceeding 2, which is the main technical task of this paper (although we have done much of the technical work already in Section 2.1). Afterwards we will derive an asymptotic formula for $S(x;\mathbb{Z}_{p^\alpha}^k)$ itself.

Lemma 3.6. *For any prime power $p^\alpha \geq 3$ and any $k \in \mathbb{N}$,*

$$S_0(x;\mathbb{Z}_{p^\alpha}^k) = \sum_{m=0}^{k-1} D_m(x;p^\alpha), \tag{3.5}$$

where $D_m(x;p^\alpha)$ is as in Definition 2.17.

Proof. By definition, $S_0(x;\mathbb{Z}_{p^\alpha}^k)$ is the number of integers $N \le x$ not divisible by p such that $\mathbb{Z}_{p^\alpha}^k \not\leq \mathbb{Z}_N^\times$. Given $N = 2^\beta p_1^{\beta_1}...p_\ell^{\beta_\ell}$ with $p \nmid N$, we have

$$\begin{aligned}\mathbb{Z}_N^\times &\cong \mathbb{Z}_{2^\beta}^\times \times \mathbb{Z}_{p_1^{\beta_1}}^\times \times \cdots \times \mathbb{Z}_{p_\ell^{\beta_\ell}}^\times \\ &\cong \mathbb{Z}_{2^\beta}^\times \times (\mathbb{Z}_{p_1^{\beta_1-1}} \times \mathbb{Z}_{p_1-1}) \times \cdots \times (\mathbb{Z}_{p_\ell^{\beta_\ell-1}} \times \mathbb{Z}_{p_\ell-1}) \\ &\cong (\mathbb{Z}_{2^\beta}^\times \times \mathbb{Z}_{p_1^{\beta_1-1}} \times \cdots \times \mathbb{Z}_{p_\ell^{\beta_\ell-1}}) \times (\mathbb{Z}_{p_1-1} \times \cdots \times \mathbb{Z}_{p_\ell-1}).\end{aligned}$$

Note that we can disregard the $\mathbb{Z}_{2^\beta}^\times$ factor completely, since $\beta = 0$ if $p = 2$, while $\mathbb{Z}_{p^\alpha}$ cannot be a subgroup of the 2-group $\mathbb{Z}_{2^\beta}^\times$ if p is odd. Similarly, we can disregard each factor $\mathbb{Z}_{p_j}^{\beta_j-1}$ since p does not equal any of the p_j; therefore $\mathbb{Z}_{p^\alpha}^k \not\leq \mathbb{Z}_N^\times$ if and only if $\mathbb{Z}_{p^\alpha}^k \not\leq \mathbb{Z}_{p_1-1} \times \cdots \times \mathbb{Z}_{p_m-1}$. Finally, each cyclic group $\mathbb{Z}_{p_j-1}$ contains a copy of $\mathbb{Z}_{p^\alpha}$ precisely when $p_j \equiv 1 \pmod{p^\alpha}$. Consequently, $\mathbb{Z}_{p^\alpha}^k \not\leq \mathbb{Z}_N^\times$ if and only if n has fewer than k prime factors $p_j \equiv 1 \pmod{p^\alpha}$, which completes the proof. □

We are now in a position to complete the asymptotic evaluation of $S(x;\mathbb{Z}_{p^\alpha}^k)$, once we define the leading constant $K(p^\alpha, k)$ that appears.

Definition 3.7. Given a prime p and positive integers α and k, define

$$K(p^\alpha,k) = \begin{cases} \dfrac{\delta(\mathcal{B}_{p^\alpha})/(k-1)!}{\Gamma\big(1-1/\phi(p^\alpha)\big)} \dfrac{p^{\alpha+1}-1}{p^{k(\alpha-1)+1}(p-1)^k}, & \text{if } p \ge 3, \\ \dfrac{\delta(\mathcal{B}_{2^\alpha})/(k-1)!}{\Gamma\big(1-1/\phi(2^\alpha)\big)} \dfrac{2^{\alpha+2}-1}{2^{k(\alpha-1)+2}}, & \text{if } p = 2 \text{ and } \alpha \ge 2, \\ 1, & \text{if } p^\alpha = 2, \end{cases}$$

where $\mathcal{B}_{p^\alpha}$ is as in Definition 2.7.

Remark 3.8. The quantity $K(2,k)$ in the last case needs to be given some positive value for Theorem 1.3 to make sense in all possible cases. Its exact value is actually irrelevant, however: the corresponding summand will never be a main term in the sum in equation (1.2) (equivalently, $\mathbb{Z}_2^k$ is never a dominant summand of a finite abelian group that is not simply isomorphic to $\mathbb{Z}_2^k$ itself), and thus the value of $K(2,k)$ never appears in Theorem 1.5—the earlier Theorem 1.1 handles those cases explicitly.

Remark 3.9. It is possible to write down an exact formula for $\delta(\mathcal{B}_{p^\alpha})$, in terms of either an absolutely convergent infinite product such as [1, equation (1.3)], or algebraic invariants of the field $\mathbb{Q}(e^{2\pi i/p^\alpha})$ as in [1, Remark 4.2]. Indeed, the special case $\alpha = 1$ already appears as [2, Proposition 2.6], the proof of wihch uses [1, Proposition 4.1 and Remark 3.5].

Proposition 3.10. *For any prime power $p^\alpha \ge 3$, any $k \in \mathbb{N}$, and any $x \ge 3$,*

$$S(x;\mathbb{Z}_{p^\alpha}^k) = K(p^\alpha,k)\frac{x(\log_2 x)^{k-1}}{(\log x)^{1/\phi(p^\alpha)}} + O_{p,\alpha,k}\left(\frac{x(\log_2 x)^{k-2}}{(\log x)^{1/\phi(p^\alpha)}}\right).$$

Proof. We first note that if we set $\alpha^* = \alpha$ when p is odd and $\alpha^* = \alpha + 1$ when $p = 2$, it follows from equation (3.1) and Lemma 3.2 that

$$S(x;\mathbb{Z}_{p^\alpha}^k) = \sum_{\ell=0}^{\infty} S_\ell(x;\mathbb{Z}_{p^\alpha}^k) = \sum_{\ell=0}^{\alpha^*} S_0(x/p^\ell;\mathbb{Z}_{p^\alpha}^k) + \sum_{\ell=\alpha^*+1}^{\infty} S_0(x/p^\ell;\mathbb{Z}_{p^\alpha}^{k-1}). \tag{3.6}$$

By Lemma 2.18, we can rewrite Lemma 3.6 as

$$\begin{aligned} S_0(x;\mathbb{Z}^k_{p^\alpha}) &= \sum_{m=0}^{k-1} D_m(x;p^\alpha) \\ &= \frac{\delta(\mathcal{B}_{p^\alpha})/(k-1)!}{\Gamma(1-1/\phi(p^\alpha))}\frac{x(\log_2 x)^{k-1}}{\phi(p^\alpha)^{k-1}(\log x)^{1/\phi(p^\alpha)}} + O_{p,\alpha,k}\left(\frac{x(\log_2 x)^{k-2}}{(\log x)^{1/\phi(p^\alpha)}}\right). \end{aligned} \tag{3.7}$$

In particular, $S_0(x;\mathbb{Z}^{k-1}_{p^\alpha}) \ll_{p,\alpha,k} x(\log_2 x)^{k-2}/(\log x)^{1/\phi(p^\alpha)}$, and therefore Lemma 2.2 implies

$$\sum_{\ell=\alpha^*+1}^{\infty} S_0(x/p^\ell;\mathbb{Z}^{k-1}_{p^\alpha}) \ll_{p,\alpha,k} \frac{x(\log_2 x)^{k-2}}{(\log x)^{1/\phi(p^\alpha)}}.$$

It therefore remains to evaluate the first sum on the right-hand side of equation (3.6). By equation (3.7) and Lemma 2.1,

$$\begin{aligned} &\sum_{\ell=0}^{\alpha^*} S_0(x/p^\ell;\mathbb{Z}^k_{p^\alpha}) \\ &\quad= \frac{x\delta(\mathcal{B}_{p^\alpha})/(k-1)!}{\phi(p^\alpha)^{k-1}\Gamma(1-1/\phi(p^\alpha))}\sum_{\ell=0}^{\alpha^*}\left(\frac{(\log_2(x/p^\ell))^{k-1}}{p^\ell(\log(x/p^\ell))^{1/\phi(p^\alpha)}} + O_{p,\alpha,k}\left(\frac{(\log_2(x/p^\ell))^{k-2}}{(\log(x/p^\ell))^{1/\phi(p^\alpha)}}\right)\right) \\ &\quad= \frac{x\delta(\mathcal{B}_{p^\alpha})/(k-1)!}{\phi(p^\alpha)^{k-1}\Gamma(1-1/\phi(p^\alpha))}\sum_{\ell=0}^{\alpha^*}\left(\frac{(\log_2 x)^{k-1}}{p^\ell(\log x)^{1/\phi(p^\alpha)}} + O_{p,\alpha,k}\left(\frac{(\log_2 x)^{k-2}}{(\log x)^{1/\phi(p^\alpha)}}\right)\right) \\ &\quad= \frac{x\delta(\mathcal{B}_{p^\alpha})/(k-1)!}{\phi(p^\alpha)^{k-1}\Gamma(1-1/\phi(p^\alpha))}\frac{(\log_2 x)^{k-1}}{(\log x)^{1/\phi(p^\alpha)}}\sum_{\ell=0}^{\alpha^*}\frac{1}{p^\ell} + O_{p,\alpha,k}\left(\frac{x(\log_2 x)^{k-2}}{(\log x)^{1/\phi(p^\alpha)}}\right). \end{aligned}$$

The application of Lemma 2.1 requires that $\sqrt{x} \geq p^{\alpha^*}$, but because the implicit constant in the error term is allowed to depend on p and α, the resulting asymptotic formula is valid for all $x \geq 3$. Since

$$\frac{1}{\phi(p^\alpha)^{k-1}}\sum_{\ell=0}^{\alpha^*}\frac{1}{p^\ell} = \frac{1}{p^{(\alpha-1)(k-1)}(p-1)^{k-1}}\frac{p^{\alpha^*+1}-1}{p^{\alpha^*}(p-1)} = \begin{cases} \dfrac{p^{\alpha+1}-1}{p^{k(\alpha-1)+1}(p-1)^k}, & \text{if } p \geq 3, \\ \dfrac{2^{\alpha+2}-1}{2^{k(\alpha-1)+2}}, & \text{if } p = 2, \end{cases}$$

the proposition now follows by Definition 3.7. □

Between Theorem 1.1 and Proposition 3.10, we have now found asymptotic formulas for $S(x;\mathbb{Z}^k_{p^\alpha})$ for all gathered summands $\mathbb{Z}^k_{p^\alpha}$. To complete the proof of Theorem 1.5 itself which concerns the general counting function $S(x;G)$, we need to understand how the various gathered summands of G interact.

4. General finite abelian groups

If the cardinalities of two finite abelian groups G_1 and G_2 are relatively prime, then an abelian group contains a copy of $G_1 \times G_2$ if and only if it contains a copy of G_1 and a copy of G_2. Consequently, $S(x;G_1 \times G_2) \leq S(x;G_1) + S(x;G_2)$ when $(\#G_1, \#G_2) = 1$, and the only reason this inequality is not an equality is because the right-hand side double-counts

multiplicative groups that contain neither G_1 nor G_2. This inequality extends immediately to any number of factors with relatively prime cardinalities.

In general, however, a finite abelian group can have subgroups isomorphic to both G_1 and G_2 without having a subgroup isomorphic to $G_1 \times G_2$. For example, $\mathbb{Z}_{16}^\times \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ has subgroups isomorphic to $\mathbb{Z}_4$ and $\mathbb{Z}_2^2$, but does not have a subgroup isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2^2$. It follows that $S(x; G_1 \times G_2)$ is not directly comparable to $S(x, G_1) + S(x; G_2)$ in general. However, this difficulty can be overcome with a bit of deliberate attention.

In the next section, we estimate $S(x; H_1)$ and $S(x; H_1 \times H_2)$ when H_1 and H_2 are both finite abelian p-groups. These are the last analytic tools we need to prove our main result, Theorem 1.5, in the final section.

4.1. **Finite abelian p-groups.** Our first lemma uses a convenient group-theoretic observation to show that the main contribution to $S(x; H)$, where H is a finite abelian p-group, comes from the dominant summand of H (which in this case is the gathered summand of H corresponding to the largest power of p).

Lemma 4.1. *Let $H \cong \mathbb{Z}_{p^{\alpha_1}}^{k_1} \times \cdots \times \mathbb{Z}_{p^{\alpha_\ell}}^{k_\ell}$ be a finite abelian p-group with $\alpha_1 < \cdots < \alpha_\ell$, and set $m = k_1 + k_2 + \cdots + k_\ell$. Then*

$$S(x; H) = S(x; \mathbb{Z}_{p^{\alpha_\ell}}^{k_\ell}) + O_H\left(\frac{x(\log_2 x)^{m-1}}{(\log x)^{1/\phi(p^{\alpha_\ell - 1})}}\right).$$

Proof. Note that $S(x; \mathbb{Z}_{p^{\alpha_\ell}}^{k_\ell}) \le S(x; H)$ since $\mathbb{Z}_{p^{\alpha_\ell}}^{k_\ell} \le H$. Additionally, $H \le \mathbb{Z}_{p^{\alpha_\ell - 1}}^{m-k_\ell} \times \mathbb{Z}_{p^{\alpha_\ell}}^{k_\ell}$, and if an abelian group contains both $\mathbb{Z}_{p^{\alpha_\ell - 1}}^{m}$ and $\mathbb{Z}_{p^{\alpha_\ell}}^{k_\ell}$ then it also contains $\mathbb{Z}_{p^{\alpha_\ell - 1}}^{m-k_\ell} \times \mathbb{Z}_{p^{\alpha_\ell}}^{k_\ell}$. Therefore $S(x; H) \le S(x; \mathbb{Z}_{p^{\alpha_\ell - 1}}^{m-k_\ell} \times \mathbb{Z}_{p^{\alpha_\ell}}^{k_\ell}) \le S(x; \mathbb{Z}_{p^{\alpha_\ell - 1}}^{m}) + S(x; \mathbb{Z}_{p^{\alpha_\ell}}^{k_\ell})$. Hence $S(x; H) = S(x; \mathbb{Z}_{p^{\alpha_\ell}}^{k_\ell}) + O\big(S(x; \mathbb{Z}_{p^{\alpha_\ell - 1}}^{m})\big)$, which completes the proof by Proposition 3.10. □

Corollary 4.2. *Let G be a finite abelian group. If $\mathbb{Z}_{p^\alpha}^k$ is a dominant summand of G, and $H \le G$ is a q-group with $\mathbb{Z}_{p^\alpha}^k \not\le H$, then*

$$S(x; H) \ll_G \frac{x(\log_2 x)^{k-2}}{(\log x)^{1/\phi(p^\alpha)}}. \tag{4.1}$$

Proof. If $\mathbb{Z}_{q^\beta}^\ell$ is the dominant summand of H, then Lemma 4.1 implies that for some integer m depending on H,

$$S(x; H) = S(x; \mathbb{Z}_{q^\beta}^\ell) + O_H\left(\frac{x(\log_2 x)^{m-1}}{(\log x)^{1/\phi(q^{\beta-1})}}\right) \ll_G \frac{x(\log_2 x)^{\ell-1}}{(\log x)^{1/\phi(q^\beta)}} \tag{4.2}$$

by Proposition 3.10 (or Theorem 1.1 if $q^\beta = 2$). Note that $\mathbb{Z}_{q^\beta}^\ell$ is a gathered summand, but not a dominant summand, of G. By Definition (1.4), either $\phi(q^\beta) < \phi(p^\alpha)$, or else $\phi(q^\beta) = \phi(p^\alpha)$ but $\ell < k$. In the second case, the bound (4.2) implies the bound (4.1) immediately since $\ell \le k - 1$; in the first case, the bound (4.2) implies the bound (4.1), regardless of the values of k and ℓ, because $(\log x)^{1/\phi(p^\alpha)} \ll (\log x)^{1/\phi(q^\beta)}$. □

The inequality in the first paragraph of Section 4 is useful, but in one circumstance we will need not just an inequality but an asymptotic formula. We accomplish this, when $(\#H_1, \#H_2) = 1$, by writing

$$S(x; G) = S(x; H_1) + S(x; H_2) - S(x; H_1, H_2), \tag{4.3}$$

where (to compensate for the aforementioned double-counting) we have defined

$$S(x; H_1, H_2) = \sum_{\substack{n \le x \\ H_1 \not\leq \mathbb{Z}_n^\times \\ H_2 \not\leq \mathbb{Z}_n^\times}} 1.$$

Lemma 4.3. *Let H_1 be a finite abelian p_1-group and H_2 a finite abelian p_2-group with $p_1 \neq p_2$, and set $H = H_1 \times H_2$. For $i = 1, 2$ write*

$$H_i \cong \mathbb{Z}_{p_i^{\alpha_{1,i}}}^{k_{1,i}} \times \mathbb{Z}_{p_i^{\alpha_{2,i}}}^{k_{2,i}} \times \cdots \times \mathbb{Z}_{p_i^{\alpha_{\ell_i,i}}}^{k_{\ell_i,i}}$$

with $\alpha_{1,i} < \cdots < \alpha_{\ell_i,i}$, and set $\beta_i = \alpha_{\ell_i,i}$. Then

$$S(x; H) = S(x; H_1) + S(x; H_2) + O_H\left(\frac{x(\log_2 x)^{m_1+m_2-2}}{(\log x)^\rho}\right), \tag{4.4}$$

where $m_i = k_{1,i} + \cdots + k_{\ell_i,i}$ and $\rho = 1/\phi(p_1^{\beta_1}) + 1/\phi(p_2^{\beta_2}) - 1/\phi(p_1^{\beta_1} p_2^{\beta_2})$. In particular, if $p_1^{\beta_1} \geq 3$ then

$$S(x; H) = S(x; H_1) + S(x; H_2) + O_H\left(\frac{x(\log_2 x)^{-1}}{(\log x)^{1/\phi(p_1^{\beta_1})}}\right). \tag{4.5}$$

Proof. By the inclusion–exclusion formula (4.3), for the first claim it suffices to show that $S(x; H_1, H_2)$ is bounded by the error term in equation (4.4). Moreover, since $H_i \leq \mathbb{Z}_{p_i^{\beta_i}}^{m_i}$, it suffices to establish such a bound for $S(x; \mathbb{Z}_{p_1^{\beta_1}}^{m_1}, \mathbb{Z}_{p_2^{\beta_2}}^{m_2})$.

Let $\mathcal{B}_H$ be the set of reduced residue classes modulo $p_1^{\beta_1} p_2^{\beta_2}$ such that $c \in \mathcal{B}_H$ precisely when $c \not\equiv 1 \pmod{p_1^{\beta_1}}$ and $c \not\equiv 1 \pmod{p_2^{\beta_2}}$. By an argument similar to the proof of Lemma 3.6, no prime in $\mathcal{B}_H$ can contribute any factors of $\mathbb{Z}_{p_1^{\beta_1}}$ or $\mathbb{Z}_{p_2^{\beta_2}}$ to a multiplicative group. It follows that if both $\mathbb{Z}_{p_1^{\beta_1}}^{m_1} \not\leq \mathbb{Z}_n^\times$ and $\mathbb{Z}_{p_2^{\beta_2}}^{m_2} \not\leq \mathbb{Z}_n^\times$, then n has at most $m_1 + m_2 - 2$ prime factors $q \notin \mathcal{B}_H$. Since $\mathcal{B}_H$ is the union of $\tau = \phi(p_1^{\beta_1} p_2^{\beta_2}) - \phi(p_1^{\beta_1}) - \phi(p_2^{\beta_2}) + 1$ distinct reduced residue classes modulo $p_1^{\beta_1} p_2^{\beta_2}$, Lemma 2.16 implies that

$$S(x; \mathbb{Z}_{p_1^{\beta_1}}^{m_1}, \mathbb{Z}_{p_2^{\beta_2}}^{m_2}) \ll_H \frac{x(\log_2 x)^{m_1+m_2-2}}{(\log x)^{1-\tau/\phi(p_1^{\beta_1} p_2^{\beta_2})}},$$

which is the same as the error expression in equation (4.4).

In addition, $\rho - 1/\phi(p_1^{\beta_1}) = (1 - 1/\phi(p_1^{\beta_1}))/\phi(p_2^{\beta_2}) > 0$ when $p_1^{\beta_1} \geq 3$, which means that equation (4.4) implies equation (4.5). □

4.2. **The general case.** We now have all the tools needed to complete our estimation of $S(x; G)$ and thereby establish Theorem 1.5. The statement of that theorem, however, includes the assumption (as mentioned in Remark 1.6) that a finite abelian group can have at most two dominant summands; we now justify that assumption with the following simple elementary number theory argument.

Lemma 4.4. *There can be at most two prime powers that share the same ϕ-value. Furthermore, when this occurs, one of the prime powers must be an actual prime.*

Proof. Suppose there exist prime powers $p_1^{\alpha_1} \neq p_2^{\alpha_2}$ such that $\phi(p_1^{\alpha_1}) = \phi(p_2^{\alpha_2})$. Then $p_1 \neq p_2$, and we may assume without loss of generality that $p_1 > p_2$. It thus follows that $\alpha_1 = 1$ as p_1 divides neither p_2 nor $p_2 - 1$. Then for any p^α such that $\phi(p^\alpha) = \phi(p_1^{\alpha_1}) = \phi(p_2^{\alpha_2})$, either $p^\alpha = p_2^{\alpha_2}$, or it again follows that $\alpha = 1$ and thus that $p = p_1$. □

Proof of Theorem 1.5. For any way of writing

$$G \cong G_1 \times G_2 \times \cdots \times G_\ell$$

where the $\#G_i$ are pairwise relatively prime, we have

$$S(x; G_1) \leq S(x; G) \leq S(x; G_1) + \cdots + S(x; G_\ell)$$

(the first inequality holds because $G_1 \leq G$, while the second inequality holds by the union bound described in the first paragraph of Section 4); in particular,

$$S(x; G) = S(x; G_1) + O\big(S(x; G_2) + \cdots + S(x; G_\ell)\big). \tag{4.6}$$

Suppose first that G has a unique dominant summand $\mathbb{Z}_{p^\alpha}^k$. We take G_1 to be the p-Sylow subgroup of G (the largest p-group contained in G) and $G_2, \ldots, G_\ell$ to be the Sylow subgroups of G corresponding to the other prime factors of $\#G$. Using Lemma 4.1 for the main term and Corollary 4.2 for the error terms, equation (4.6) becomes

$$\begin{aligned} S(x; G) &= \left(S(x; \mathbb{Z}_{p^\alpha}^k) + O_{G_1}\left(\frac{x(\log_2 x)^m}{(\log x)^{1/\phi(p^{\alpha-1})}}\right)\right) + O_G\left(\sum_{j=2}^{\ell} \frac{x(\log_2 x)^{k-2}}{(\log x)^{1/\phi(p^\alpha)}}\right) \\ &= K(p^\alpha, k)\frac{x(\log_2 x)^{k-1}}{(\log x)^{1/\phi(p^\alpha)}} + O_G\left(\frac{x(\log_2 x)^{k-2}}{(\log x)^{1/\phi(p^\alpha)}}\right) \end{aligned}$$

by Proposition 3.10 (note that $p^\alpha \geq 3$ since $G \ncong \mathbb{Z}_2^k$ by assumption), which establishes the theorem in this case.

Suppose now that G has two dominant summands $\mathbb{Z}_{p^\alpha}^k$ and $\mathbb{Z}_{q^\beta}^k$. We take $G_1 \cong H_1 \times H_2$, where H_1 is the p-Sylow subgroup of G and H_2 is the q-Sylow subgroup of G, and $G_2, \ldots, G_\ell$ to be the Sylow subgroups of G corresponding to the other prime factors of $\#G$. Using Lemma 4.3 for the main term and Corollary 4.2 for the error terms, equation (4.6) becomes

$$\begin{aligned} S(x; G_1) &= S(x; H_1) + S(x; H_2) + O_G\left(\frac{x(\log_2 x)^{-1}}{(\log x)^{1/\phi(p^\alpha)}}\right) + O_G\left(\sum_{j=2}^{\ell} \frac{x(\log_2 x)^{k-2}}{(\log x)^{1/\phi(p^\alpha)}}\right) \\ &= K(p^\alpha, k)\frac{x(\log_2 x)^{k-1}}{(\log x)^{1/\phi(p^\alpha)}} + K(q^\beta, k)\frac{x(\log_2 x)^{k-1}}{(\log x)^{1/\phi(q^\beta)}} + O_G\left(\frac{x(\log_2 x)^{k-2}}{(\log x)^{1/\phi(p^\alpha)}}\right) \end{aligned}$$

again by Proposition 3.10, which establishes the theorem in this case since $\phi(p^\alpha) = \phi(q^\beta)$. □

Acknowledgments

The second author was supported in part by a Natural Sciences and Engineering Council of Canada Discovery Grant.

References

[1] B. Chang and G. Martin. The smallest invariant factor of the multiplicative group. *Int. J. Number Theory*, 16(6):1377–1405, 2020.

[2] J. Downey and G. Martin. Counting multiplicative groups with prescribed subgroups. *Int. J. Number Theory*, 17(9):2087–2112, 2021.

[3] H. Montgomery and R. Vaughan. *Multiplicative Number Theory. I. Classical Theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[4] G. Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015.

Department of Mathematics, Vancouver Island University, 900 Fifth Street, Nanaimo, BC, Canada V9R 5S5

Email address: matthiashannesson@gmail.com

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

Email address: gerg@math.ubc.ca