THE SMALLEST INVARIANT FACTOR OF THE MULTIPLICATIVE GROUP

BEN CHANG AND GREG MARTIN

ABSTRACT. Let $\lambda_1(n)$ denote the least invariant factor in the invariant factor decomposition of the multiplicative group $M_n = (\mathbb{Z}/n\mathbb{Z})^\times$. We give an asymptotic formula, with order of magnitude $x/\sqrt{\log x}$, for the counting function of those integers n for which $\lambda_1(n) \neq 2$. We also give an asymptotic formula, for any even $q \geq 4$, for the counting function of those integers n for which $\lambda_1(n) = q$. These results require a version of the Selberg–Delange method whose dependence on certain parameters is made explicit, which we provide in an appendix. As an application, we give an asymptotic formula for the counting function of those integers n all of whose prime factors lie in an arbitrary fixed set of reduced residue classes, with implicit constants uniform over all moduli and sets of residue classes.

1. INTRODUCTION

The multiplicative group $M_n = (\mathbb{Z}/n\mathbb{Z})^\times$ of the quotient ring $\mathbb{Z}/n\mathbb{Z}$ is a finite abelian group whose structure is closely tied to functions of interest to number theorists. Most obviously, its cardinality is the Euler function $\phi(n)$, whose extreme values and distribution have been extensively studied. However, there can be many abelian groups of cardinality $\phi(n)$, which leads us to wonder which such group M_n is; for example, asking whether M_n is cyclic is precisely the same question as characterizing those moduli n that possess primitive roots.

To study the structure of this family of groups more finely, we may ask about the invariant factor decomposition of M_n, namely the unique way of writing $M_n \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \mathbb{Z}/d_\ell\mathbb{Z}$ where $d_1 \mid d_2 \mid \cdots \mid d_\ell$. For example, it is not hard to show that the length ℓ of the invariant factor decomposition of M_n is essentially the number of distinct prime factors of n (more precisely, these two quantities differ by 1, 0, or -1 depending upon the power of 2 dividing n). Moreover, the largest invariant factor d_ℓ is the exponent of the group M_n, or precisely the Carmichael function $\lambda(n)$ which has also been well studied (see [1]).

In this article, we investigate instead the distribution of the smallest invariant factor d_1 of the multiplicative group M_n, which we denote by $\lambda_1(n)$. Other than for $n = 1$ and $n = 2$, this smallest invariant factor is always even (see the proof of Proposition 5.3 below and the subsequent remark). It turns out that $\lambda_1(n) = 2$ for almost all integers n; however, we can be more precise about the exceptions, as our first theorem asserts.

Definition 1.1. Define $T(x)$ to be the number of positive integers $n \leq x$ such that the least invariant factor $\lambda_1(n)$ of M_n does not equal 2.

We prove:

Theorem 1.2. *For $x \geq 2$, we have $T(x) = (H_4 + H_6)\dfrac{x}{\sqrt{\log x}} + O\left(\dfrac{x}{(\log x)^{3/4}}\right)$, where*

$$H_4 = \frac{3}{2^{5/2}} \prod_{p \equiv 3 \;(\mathrm{mod}\; 4)} \left(1 - \frac{1}{p^2}\right)^{1/2} \approx 0.490694$$

$$H_6 = \frac{7}{2^{5/2} \cdot 3^{3/4}} \prod_{p \equiv 5 \;(\mathrm{mod}\; 6)} \left(1 - \frac{1}{p^2}\right)^{1/2} \approx 0.527129.$$

(1.1)

Indeed, our methods allow us to establish an asymptotic formula, for any fixed even number $q \geq 4$, for the counting function of those integers n for which $\lambda_1(n) = q$.

Definition 1.3. Define $E_q(x) = \#\{n \leq x \colon \lambda_1(n) = q\}$ to be the number of positive integers $n \leq x$ such that the least invariant factor of n equals q.

Theorem 1.4. *Let $q \geq 4$ be an even integer. For $x \geq e^e$,*

$$E_q(x) = \frac{H_q x}{(\log x)^{1-1/\phi(q)}} + O_q\left(\frac{x(\log\log x)^2}{(\log x)^{1-1/2\phi(q)}}\right).$$

Here the constant H_q is defined by

$$H_q = \frac{3G_q}{2} \cdot \begin{cases} 1 + \dfrac{1}{p^r(p-1)}, & \text{if there exists an odd prime power } p^r \| q \text{ such that } \dfrac{q}{p^r} \mid (p-1), \\ 1, & \text{otherwise,} \end{cases}$$

(1.2)

where

$$G_q = \frac{1}{\Gamma(1/\phi(q))} \left(\frac{\phi(q)}{q} \prod_{\substack{\chi \;(\mathrm{mod}\; q) \\ \chi \neq \chi_0}} L(1,\chi)\right)^{1/\phi(q)} \prod_{\substack{p \nmid q \\ p \not\equiv 1 \;(\mathrm{mod}\; q)}} \left(1 - \frac{1}{p^{\mathrm{ord}_q(p)}}\right)^{1/\mathrm{ord}_q(p)}.$$

(1.3)

In equation (1.3) and hereafter, we use $\mathrm{ord}_q(p)$ to denote the order of p modulo q. We show, in the proof of Proposition 5.4 below, that the odd prime power p^r (including the possibility $r = 1$) referred to in equation (1.2) is unique if it exists.

For example, if χ_{-4} and χ_{-6} denote the nonprincipal characters modulo 4 and 6, respectively, then $H_4 = \frac{3}{2}G_4$ where

$$G_4 = \frac{1}{\Gamma(1/2)}\left(\frac{2}{4}L(1,\chi_{-4})\right)^{1/2} \prod_{p \equiv 3 \;(\mathrm{mod}\; 4)}\left(1 - \frac{1}{p^2}\right)^{1/2} = \frac{1}{\sqrt{\pi}}\left(\frac{\pi}{8}\right)^{1/2} \prod_{p \equiv 3 \;(\mathrm{mod}\; 4)}\left(1 - \frac{1}{p^2}\right)^{1/2},$$

while $H_6 = \frac{3}{2}G_6 \cdot \frac{7}{6}$ where

$$G_6 = \frac{1}{\Gamma(1/2)}\left(\frac{2}{6}L(1,\chi_{-6})\right)^{1/2} \prod_{p \equiv 5 \;(\mathrm{mod}\; 6)}\left(1 - \frac{1}{p^2}\right)^{1/2} = \frac{1}{\sqrt{\pi}}\left(\frac{\pi}{6\sqrt{3}}\right)^{1/2} \prod_{p \equiv 5 \;(\mathrm{mod}\; 6)}\left(1 - \frac{1}{p^2}\right)^{1/2}.$$

Both evaluations match the expressions given in equation (1.1), which is not coincidental: the contribution to the main term for $T(x)$ in Theorem 1.2 is actually from those integers n for which $\lambda_1(n) = 4$ or $\lambda_1(n) = 6$. Indeed, Theorem 1.4 shows that any individual $q \geq 8$ leads to a counting function $E_q(x)$ with a smaller order of magnitude than either $E_4(x)$ or $E_6(x)$. We cannot directly

deduce Theorem 1.2 from Theorem 1.4, however, because of uniformity issues with the asymptotic formula in the latter theorem.

In fact, uniformity issues present the main technical obstacle to proving Theorem 1.4, for a different reason: instead of those integers n for which the smallest invariant factor is exactly q, it is more approachable to first count those integers n for which the smallest invariant factor is a multiple of q.

Definition 1.5. Define $D_q(x) = \#\{n \leq x \colon q \mid \lambda_1(n)\}$ to be the number of positive integers $n \leq x$ such that q divides the least invariant factor of n.

As it turns out, the asymptotic formula for $D_q(x)$ will be the same as the asymptotic formula in Theorem 1.4 for $E_q(x)$ (see Proposition 5.4 below). We can then recover the functions $E_q(x)$ from the functions $D_q(x)$ via inclusion–exclusion; however, this recovery step requires some quantitative statement of uniformity in q.

We will see in Proposition 5.3 that, roughly speaking, an integer is counted by $D_q(x)$ when all of its prime factors are congruent to 1 (mod q). Counting integers of this form is a standard goal in analytic number theory, going all the way back to Landau, and can be effectively done using the Selberg–Delange method. An excellent account of the Selberg–Delange method appears in the book of Tenenbaum [7, Chapter II.5]. However, that version allows implicit constants to depend on three parameters δ, c_0, and A; for our purposes, we require a version where the dependence upon the parameters δ and c_0 is explicit. Consequently, we establish such a uniform version of the Selberg–Delange method (closely following Tenenbaum's proof for the most part) in Theorem A.13; this additional uniformity might be of value in other research as well, so we have retained the generality already present.

The techniques that establish the above results could also be used to investigate the other canonical representation of the abelian group M_n, namely its primary decomposition as a direct sum of cyclic groups of prime-power order. For example, one can see that the least such primary factor of M_n equals 2 unless $4 \nmid n$ and every odd prime dividing n is congruent to 1 (mod 4). Therefore the counting function of those integers whose least primary factor does not equal 2 is precisely $D_4(x)$ (see Proposition 5.3 below), which is asymptotic to $E_4(x)$ and thus to $H_4 x / \sqrt{\log x}$ where H_4 was defined in equation (1.1). The methods of this paper would provide an asymptotic formula for the counting function of integers with any prescribed least primary factor, after carefully characterizing such integers n in terms of their prime factorizations; but we do not carry out the details of that variant herein.

After the preliminary Section 2, we give in Section 3 an asymptotic formula for the counting function of integers whose prime factors are restricted to lie in an arbitrary fixed set of reduced residue classes (see Theorem 3.4), with explicit dependence on the modulus and the number of residue classes; we hope that such a theorem might find further use elsewhere. We specialize in Section 4 to the case of counting integers all of whose prime factors are congruent to 1 (mod q); asymptotic formulas for this function can be found in the literature, but not with the uniformity we require in this application. Section 5 contains the algebra and elementary number theory necessary to give the precise relationship between this counting function and $D_q(x)$, the asymptotic formula for which is provided in Proposition 5.4. From this result, we proceed to establish Theorem 1.4 in Section 6 and finally Theorem 1.2 in Section 7. The appendix is devoted to establishing the uniform version of the Selberg–Delange method described above.

2. CLASSICAL COMPLEX ANALYTIC RESULTS

We will employ the classical "zero-free regions" for Dirichlet L-functions, with a slight wrinkle related to the fact that we need such a region to be free of even a possible exceptional zero. Using the notational convention that $s = \sigma + i\tau$, we first state the standard result (see [3, Corollary 11.8 and Theorem 11.4], although note that the τ therein is $|\tau| + 4$ in our notation):

Lemma 2.1. *There exists an effective constant $c > 0$ such that for all $q \geq 3$ and all Dirichlet characters χ (mod q), the function $L(s, \chi)$ has no zeros in the region $\sigma \geq 1 - c/\log(q(|\tau| + 4))$, except possibly for a single exceptional real zero of a single character χ (mod q). In the smaller region*

$$\sigma \geq 1 - \frac{c/2}{\log(q(|\tau| + 4))}, \tag{2.1}$$

we have

$$|\log L(s, \chi)| \leq \log\log(q(|\tau| + 4)) + O(1) \tag{2.2}$$

for every nonexceptional character χ (mod q).

On the other hand, we have sufficient control over exceptional zeros and nearby values of L-functions (see [3, Corollary 11.12 and equations (11.9) and (11.10)] and note that $|\log L(s, \chi)| \leq \big|\log|L(s, \chi)|\big| + |\arg L(s, \chi)|$):

Lemma 2.2. *There exists an effective constant $c > 0$ such that any exceptional zero β for $L(s, \chi)$ with χ (mod q) is at most $1 - c/q^{1/2} \log^2 q$. In the region (2.1), if $|s - \beta| > 1/\log q$ then $L(s, \chi)$ satisfies the bound (2.2); on the other hand, if $|s - \beta| \leq 1/\log q$ then*

$$|\log L(s, \chi)| \leq \log|s - \beta|^{-1} + \log\log q + O(1).$$

We combine these two lemmas into the following easy-to-cite proposition:

Proposition 2.3. *There exists an effective constant $0 < \eta < \frac{1}{81}$ such that for all $q \geq 3$ and all Dirichlet characters χ (mod q), the function $L(s, \chi)$ has no zeros in the region*

$$\sigma \geq 1 - \frac{c_0}{1 + \log^+ |\tau|} \quad \text{with } c_0 = \frac{\eta}{q^{1/2} \log^2 q} \tag{2.3}$$

and satisfies the bound

$$|\log L(s, \chi)| \leq \begin{cases} \log\log^+(q\tau) + O(1), & \text{if } \chi \text{ has no exceptional zero,} \\ \frac{1}{2}\log q + 3\log\log^+(q\tau) + O(1), & \text{if } \chi \text{ has an exceptional zero } \beta \end{cases} \tag{2.4}$$

inside this region.

Proof. The derivation needs no comment other than the remark that we take $\eta < c/2$ in these lemmas, so that in particular

$$\log|s - \beta|^{-1} \leq \log \frac{q^{1/2} \log^2 q}{\eta} = \tfrac{1}{2}\log q + 2\log\log q + O(1). \qquad \square$$

We next take a moment to establish a convenient upper bound for complex logarithms and exponential functions defined by continuous variation on a domain. For fixed $z \in \mathbb{C}$, our convention will be to choose the branch of w^z (on regions to be specified) so that $1^z = 1$. Often we will set w equal to some Dirichlet series $F(s)$ with constant term 1, so that we choose the branch of $F(s)^z$ that tends to 1 as $\Re s \to \infty$. It would be easy to write down a false inequality: it is not the case, for

example, that $|w^z| \le |w|^{|z|}$, as the example $i^{-i} = e^{\pi/2}$ shows (or even the example 0.1^{-2}). But we can use a similar-looking inequality:

Lemma 2.4. *Let $w \ne 0$ and z be complex numbers, and fix any value of $\log w$. If $|\log w| \le L$, then $|w^z| \le e^{L|z|}$.*

Proof. We have $|w^z| = |e^{z \log w}| = e^{\Re(z \log w)} \le e^{|z \log w|} \le e^{|z|L}$. $\qquad\qquad\square$

3. INTEGERS WITH PRIME FACTORS FROM PRESCRIBED RESIDUE CLASSES

The following notation will be used throughout this section.

Notation 3.1. Let $q \ge 3$ be an integer. Let $\mathcal{B}$ be the union of B distinct reduced residue classes (mod q). Set $\beta = B/\phi(q)$ and $\underline{B} = \min\{B, \phi(q) - B\}$. Let $\mathcal{N}_\mathcal{B} = \{n \in \mathbb{N} \colon p \mid n \Rightarrow p \in \mathcal{B}\}$ be the set of all positive integers whose prime factors lie exclusively in $\mathcal{B}$, and define the associated Dirichlet series

$$F_\mathcal{B}(s) = \sum_{n \in \mathcal{N}_\mathcal{B}} \frac{1}{n^s} = \prod_{p \in \mathcal{B}} \left(1 - \frac{1}{p^s}\right)^{-1},$$

which converges absolutely when $\sigma > 1$. Finally, let $\zeta(s)^{-\beta}$ denote the branch of the complex exponential chosen, as discussed earlier, so that $\lim_{\Re s \to \infty} \zeta(s)^{-\beta} = 1$, and set $G_\mathcal{B}(s) = F_\mathcal{B}(s)\zeta(s)^{-\beta}$, which *a priori* is defined only when $\sigma > 1$.

Lemma 3.2. *The Dirichlet series $G_\mathcal{B}(s)$ has an analytic continuation to the region* (2.3).

Those familiar with the Selberg–Delange method, or those who refer to Definition A.4, might recognize that we are beginning to establish that $F(s)$ has the property $\mathcal{P}(\beta; c_0, \frac{1}{2}, M)$, with β as in Notation 3.1 and with c_0 as in equation (2.3).

Proof. For $\sigma > 1$, define

$$A_\mathcal{B}(s) = F_\mathcal{B}(s)^{\phi(q)} \prod_{\chi \,(\text{mod } q)} L(s, \chi)^{-\sum_{b \in \mathcal{B}} \overline{\chi}(b)}. \tag{3.1}$$

For any prime p, note that

$$\log \prod_{\chi \,(\text{mod } q)} \left(1 - \frac{\chi(p)}{p^s}\right)^{\sum_{b \in \mathcal{B}} \overline{\chi}(b)} = \sum_{\chi \,(\text{mod } q)} \sum_{b \in \mathcal{B}} \overline{\chi}(b) \log\left(1 - \frac{\chi(p)}{p^s}\right)$$

$$= \sum_{b \in \mathcal{B}} \sum_{\chi \,(\text{mod } q)} \overline{\chi}(b)\left(-\frac{\chi(p)}{p^s} + O\left(\frac{1}{p^{2\sigma}}\right)\right)$$

$$= -\frac{1}{p^s} \begin{cases} \phi(q), & \text{if } b \in \mathcal{B}, \\ 0, & \text{if } b \notin \mathcal{B} \end{cases} + O\left(\frac{\phi(q)^2}{p^{2\sigma}}\right)$$

by orthogonality, whence

$$A_\mathcal{B}(s) = \prod_{p \in \mathcal{B}} \left(1 - \frac{1}{p^s}\right)^{-\phi(q)} \prod_p \left(1 - \frac{1}{p^s} \begin{cases} \phi(q), & \text{if } b \in \mathcal{B}, \\ 0, & \text{if } b \notin \mathcal{B} \end{cases} + O\left(\frac{\phi(q)^2}{p^{2\sigma}}\right)\right)$$

$$= \prod_p \left(1 + O\left(\frac{\phi(q)^2}{p^{2\sigma}}\right)\right). \tag{3.2}$$

In particular, this infinite product has an analytic continuation to $\sigma > \frac{1}{2}$, in which it converges absolutely and therefore does not vanish. Then

$$G_{\mathcal{B}}(s)^{\phi(q)} = \zeta(s)^{-\beta\phi(q)} F_{\mathcal{B}}(s)^{\phi(q)} = \zeta(s)^{-B} A_{\mathcal{B}}(s) \prod_{\chi \,(\mathrm{mod}\, q)} L(s,\chi)^{\sum_{b\in\mathcal{B}} \overline{\chi}(b)}$$

$$= A_{\mathcal{B}}(s) \prod_{p|q}(1 - p^{-s})^B \prod_{\substack{\chi \,(\mathrm{mod}\, q) \\ \chi\neq\chi_0}} L(s,\chi)^{\sum_{b\in\mathcal{B}} \overline{\chi}(b)} \qquad (3.3)$$

can be analytically continued to the zero-free region (2.4) of these Dirichlet L-functions, which implies that $G_{\mathcal{B}}(s)$ itself can be analytically continued to this region. $\qquad\square$

The other requirement of $F(s)$ having the property $\mathcal{P}(\beta; c_0, \frac{1}{2}, M)$ is an upper bound for the related function $G_{\mathcal{B}}(s)$ inside the zero-free region (2.4), which the following lemma furnishes.

Lemma 3.3. *There exists an absolute constant $C > 0$ such that, in the region* (2.3)*, we have the bound* $|G_{\mathcal{B}}(s)| \leq M(1 + |\tau|)^{1/2}$ *with* $M \ll q^{1/2} \log^2 q \cdot (C\underline{B})^{\underline{B}}$.

Proof. The logarithm of the expression (3.2) can be bounded by

$$\log|A_{\mathcal{B}}(s)| = \sum_{p\leq q^{1/\sigma}} \log\left(1 + O\left(\frac{\phi(q)^2}{p^{2\sigma}}\right)\right) + \sum_{p>q^{1/\sigma}} \log\left(1 + O\left(\frac{\phi(q)^2}{p^{2\sigma}}\right)\right)$$

$$\ll \sum_{p\leq q^{1/\sigma}} \log\phi(q)^2 + \sum_{p>q^{1/\sigma}} \frac{\phi(q)^2}{p^{2\sigma}} \ll \pi(q^{1/\sigma})\log q + \frac{q^2}{(q^{1/\sigma})^{2\sigma-1}} \ll q^{1/\sigma}$$

uniformly for $\sigma \geq \frac{3}{4}$ say. In particular, when $\sigma \geq 1 - 1/(3\log q)$, we obtain $\log|A_{\mathcal{B}}(s)| \ll q$.

If $\chi \,(\mathrm{mod}\, q)$ is not an exceptional character, then by the first case of equation (2.4) and Lemma 2.4,

$$\log\left|L(s,\chi)^{\sum_{b\in\mathcal{B}} \overline{\chi}(b)}\right| \leq \left(\log\log^+ q|\tau| + O(1)\right)\left|\sum_{b\in\mathcal{B}} \overline{\chi}(b)\right| \leq \underline{B}\left(\log\log^+ q|\tau| + O(1)\right).$$

(Recall that $\underline{B} = \min\{B, \phi(q) - B\}$; the bound $|\sum_{b\in\mathcal{B}} \overline{\chi}(b)| \leq B$ is obvious, while the bound $|\sum_{b\in\mathcal{B}} \overline{\chi}(b)| \leq \phi(q) - B$ follows, since $\chi \neq \chi_0$, from the consequence

$$\sum_{b\in\mathcal{B}} \overline{\chi}(b) = - \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^\times \setminus \mathcal{B}} \overline{\chi}(b)$$

of orthogonality.) Similarly, if $\chi \,(\mathrm{mod}\, q)$ is an exceptional character, then by the second case of equation (2.4) and Lemma 2.4,

$$\log\left|L(s,\chi)^{\sum_{b\in\mathcal{B}} \overline{\chi}(b)}\right| \leq \underline{B}\left(\tfrac{1}{2}\log q + 3\log\log^+ q|\tau| + O(1)\right).$$

Since there can be at most one exceptional character, the product in equation (3.3) satisfies the bound

$$\log\left|\prod_{\substack{\chi \,(\mathrm{mod}\, q) \\ \chi\neq\chi_0}} L(s,\chi)^{\sum_{b\in\mathcal{B}} \overline{\chi}(b)}\right| \leq \underline{B}\left(\phi(q)\left(\log\log^+ q|\tau| + O(1)\right) + \left(\tfrac{1}{2}\log q + 3\log\log^+ q|\tau| + O(1)\right)\right),$$

and equation (3.3) becomes, for $\sigma > 1 - 1/(3\log q)$,

$$\phi(q)\log|G_{\mathcal{B}}(s)| \leq q + \underline{B}\left((\phi(q) + 3)\left(\log\log^+ q|\tau| + O(1)\right) + \tfrac{1}{2}\log q\right). \qquad (3.4)$$

6

We know that $q/\phi(q) < 2\log\log q$ when q is sufficiently large, and thus $e^{q/\phi(q)} \ll \log^2 q$. Therefore, dividing both sides of equation (3.4) by $\phi(q)$ and exponentiating yields, for some absolute constants C_1 and C_2,

$$|G_\mathcal{B}(s)| \ll e^{q/\phi(q)}\big((C_1\log^+ q|\tau|)^{(1+3/\phi(q))}e^{(\log q)/2\phi(q)}\big)^{\underline{B}}$$
$$\ll \log^2 q \cdot \big(C_2(\log^+ q|\tau|)^{(1+3/\phi(q))}\big)^{\underline{B}}. \tag{3.5}$$

A routine calculus exercise shows that the quotient of the right-hand side with $|\tau|^{1/2}$, for $|\tau| \geq e/q$, is maximized at $|\tau| = e^{2\underline{B}(1+3/\phi(q))}/q$, from which we obtain

$$|G_\mathcal{B}(s)| \ll \log^2 q \cdot \Big(C_2\big(\tfrac{2}{e}(1+\tfrac{3}{\phi(q)})\underline{B}\big)^{1+3/\phi(q)}\Big)^{\underline{B}}q^{1/2}|\tau|^{1/2} \ll q^{1/2}\log^2 q \cdot (C\underline{B})^{\underline{B}}(1+|\tau|)^{1/2}$$

for some absolute constant C. On the other hand, when $|\tau| \leq e/q$, the right-hand side of equation (3.5) simply equals $(C_2)^{\underline{B}}\log^2 q$, which justifies this final estimate for those values of τ as well. $\square$

We remark in passing that all of the constants in these proofs are effectively computable. It might seem that we could obtain a better upper bound ineffectively for M in this proposition by using Siegel's theorem on exceptional zeros in Lemma 2.2 and Proposition 2.3; this is a mirage, however, as the expression $q^{1/2}\log^2 q$ in the estimate for M actually arises by accident from completely different sources.

We are now able to count the integers in $\mathcal{N}_\mathcal{B}$ using the Selberg–Delange method, at least when $\mathcal{B}$ is small enough. It is crucial for our application that we can produce an asymptotic formula for this counting function that has some uniformity in q.

Theorem 3.4. *There exist positive absolute constants α, η, and C such that, uniformly for $\log x \geq \alpha q^{1/2}\log^2 q$,*

$$\#\{n \leq x\colon n \in \mathcal{N}_\mathcal{B}\}$$
$$= \frac{x}{(\log x)^{1-\beta}}\left(\frac{G_\mathcal{B}(1)}{\Gamma(\beta)} + O\Big((C\underline{B})^{\underline{B}}q^2(\log q)^8\big(e^{-\eta\sqrt{(\log x)/q^{1/2}\log^2 q}} + (\log x)^{-1}\big)\Big)\right),$$

where $G_\mathcal{B}(s) = \zeta(s)^{-\beta}\prod_{p\in\mathcal{B}}\big(1-p^{-s}\big)^{-1}$ has an analytic continuation to a neighborhood of $s = 1$. In particular, uniformly for $q \leq (\log x)^{1/3}$,

$$\#\{n \leq x\colon n \in \mathcal{N}_\mathcal{B}\} = \frac{x}{(\log x)^{1-\beta}}\left(\frac{G_\mathcal{B}(1)}{\Gamma(\beta)} + O\big((C\underline{B})^{\underline{B}}(\log x)^{-1/4}\big)\right). \tag{3.6}$$

Proof. The result is a direct application of Corollary A.14 with $F(s) = F_\mathcal{B}(s)$, which by Lemmas 3.2 and 3.3 has the property $\mathcal{P}(\beta; c_0, \tfrac{1}{2}, M)$ with the parameters $c_0 = \eta/q^{1/2}\log^2 q$ and $M \ll q^{1/2}\log^2 q \cdot (C\underline{B})^{\underline{B}}$. $\square$

Remark 3.5. If $\mathcal{B}$ and $\mathcal{B}'$ partition the reduced residue classes (mod q), then clearly $\beta + \beta' = 1$ and

$$G_\mathcal{B}(s)G_{\mathcal{B}'}(s) = \zeta(s)^{-\beta}\prod_{p\in\mathcal{B}}\left(1-\frac{1}{p^s}\right)^{-1}\zeta(s)^{-\beta'}\prod_{p\in\mathcal{B}'}\left(1-\frac{1}{p^s}\right)^{-1}$$
$$= \zeta(s)^{-1}\prod_{p\nmid q}\left(1-\frac{1}{p^s}\right)^{-1} = \prod_{p\mid q}\left(1-\frac{1}{p^s}\right);$$

in particular, $G_\mathcal{B}(1)G_{\mathcal{B}'}(1) = \phi(q)/q$. Note also that $\underline{B} = \underline{B}'$ in this situation. Consequently, one can derive the asymptotic formula for $\#\{n \le x\colon n \in \mathcal{N}_{\mathcal{B}'}\}$ directly from the asymptotic formula for $\#\{n \le x\colon n \in \mathcal{N}_\mathcal{B}\}$ from Theorem 3.4, with the same error term.

With an eye towards future applications, we exhibit one last variant of the above results, where the set $\mathcal{B}$ of primes (defined as in Notation 3.1) in modified by the removal of finitely many primes and the insertion of finitely many other primes. To fix notation, let $\mathcal{R} = \{b_1, \ldots, b_k\}$ be a finite set of primes in $\mathcal{B}$, and let $\mathcal{I} = \{p_1, \ldots, p_j\}$ be a finite set of primes that are not in $\mathcal{B}$. We will establish an asymptotic formula for the counting function of $\mathcal{N}_{\mathcal{I}\cup\mathcal{B}\setminus\mathcal{R}} = \{n \in \mathbb{N}\colon p \mid n \Rightarrow p \in \mathcal{I} \cup \mathcal{B} \setminus \mathcal{R}\}$, the set of integers all of whose prime factors lie in $\mathcal{I} \cup \mathcal{B} \setminus \mathcal{R}$. To this set of integers, define the associated Dirichlet series

$$F_{\mathcal{I}\cup\mathcal{B}\setminus\mathcal{R}}(s) = \sum_{n\in\mathcal{N}_\mathcal{B}} \frac{1}{n^s} = \prod_{p\in\mathcal{I}\cup\mathcal{B}\setminus\mathcal{R}} \left(1 - \frac{1}{p^s}\right)^{-1} = F_\mathcal{B}(s) \prod_{i=1}^{j} \left(1 - \frac{1}{p_i^s}\right)^{-1} \prod_{i=1}^{k} \left(1 - \frac{1}{b_k^s}\right). \quad (3.7)$$

As before we set $G_{\mathcal{I}\cup\mathcal{B}\setminus\mathcal{R}}(s) = F_{\mathcal{I}\cup\mathcal{B}\setminus\mathcal{R}}(s)\zeta(s)^{-\beta}$.

Each of the finitely many factors on the right-hand side of equation (3.7) is analytic for $\Re s > 0$, and so Lemma 3.2 implies that $G_{\mathcal{I}\cup\mathcal{B}\setminus\mathcal{R}}(s)$ has an analytic continuation to the region (2.3). It also easily follows from Lemma 3.3 that there exists an absolute constant $C > 0$ such that, in the region (2.3), we have the bound $|G_{\mathcal{I}\cup\mathcal{B}\setminus\mathcal{R}}(s)| \le M(1 + |\tau|)^{1/2}$ with

$$M \ll q^{1/2} \log^2 q \cdot (C\underline{B})^{\underline{B}} \prod_{i=1}^{j} \left(1 - \frac{1}{p_i^{\sigma(q)}}\right)^{-1} \prod_{i=1}^{k} \left(1 + \frac{1}{b_k^{\sigma(q)}}\right), \quad (3.8)$$

where

$$\sigma(q) = 1 - 1/(81q^{1/2}\log^2 q) \ge 0.99.$$

It follows that each factor in the products on the right-hand side of equation (3.8) is at most 2 (with a single exception if some p_i equals 2, in which case the corresponding factor is at most 3). The proof of Theorem 3.4 then yields the variant:

Theorem 3.6. *There exist positive absolute constants α, η, and C such that, uniformly for $\log x \ge \alpha q^{1/2}\log^2 q$,*

$$\#\{n \le x\colon n \in \mathcal{N}_{\mathcal{I}\cup\mathcal{B}\setminus\mathcal{R}}\} = \frac{x}{(\log x)^{1-\beta}} \left\{ \frac{G_\mathcal{B}(1)}{\Gamma(\beta)} \prod_{i=1}^{j} \left(1 - \frac{1}{p_i}\right)^{-1} \prod_{i=1}^{k} \left(1 - \frac{1}{b_k}\right) \right.$$
$$\left. + O\left((C\underline{B})^{\underline{B}} 2^{j+k} q^2 (\log q)^8 \left(e^{-\eta\sqrt{(\log x)/q^{1/2}\log^2 q}} + (\log x)^{-1}\right)\right) \right\}.$$

4. INTEGERS WITH ALL PRIME FACTORS 1 (mod q), UNIFORMLY IN q

We now apply the previous theorem to the classical counting problem for integers all of whose prime factors are congruent to 1 (mod q). Define

$$J_q(x) = \#\{n \le x\colon p \mid n \implies p \equiv 1 \ (\mathrm{mod}\ q)\}$$

Proposition 4.1. *For any positive even integer q, uniformly for $q \le (\log x)^{1/3}$,*

$$J_q(x) = \frac{G_q x}{(\log x)^{1-1/\phi(q)}} + O\left(\frac{x}{(\log x)^{5/4-1/\phi(q)}}\right),$$

where G_q is defined in equation (1.3).

Proof. We invoke the last assertion of Theorem 3.4 with $\mathcal{B}$ equal to the set of integers congruent to 1 (mod q), so that $\beta = 1/\phi(q)$ and $\underline{B} = B = 1$; for this proof we abuse notation and write simply $\mathcal{B} = \{1\}$. Our only task is to evaluate the leading constant $G_{\{1\}}(1)/\Gamma(1/\phi(q))$. By equation (3.3), we see that

$$G_{\{1\}}(s)^{\phi(q)} = A_{\{1\}}(s) \prod_{p|q} (1 - p^{-s})^1 \prod_{\substack{\chi \,(\mathrm{mod}\, q) \\ \chi \neq \chi_0}} L(s, \chi)^{\overline{\chi}(1)} = A_{\{1\}}(s) \prod_{p|q} (1 - p^{-s}) \prod_{\substack{\chi \,(\mathrm{mod}\, q) \\ \chi \neq \chi_0}} L(s, \chi),$$

(4.1)

where by equation (3.1),

$$A_{\{1\}}(s) = F_{\{1\}}(s)^{\phi(q)} \prod_{\chi \,(\mathrm{mod}\, q)} L(s, \chi)^{-\overline{\chi}(1)}$$

$$= \prod_{p \equiv 1 \,(\mathrm{mod}\, q)} \left(1 - \frac{1}{p^s}\right)^{-\phi(q)} \prod_{\chi \,(\mathrm{mod}\, q)} \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)$$

$$= \prod_{\chi \,(\mathrm{mod}\, q)} \prod_{p \not\equiv 1 \,(\mathrm{mod}\, q)} \left(1 - \frac{\chi(p)}{p^s}\right).$$

For each prime p not dividing q in the product, there are exactly $\phi(q)/\operatorname{ord}_q(p)$ characters that send p to any given $\operatorname{ord}_q(p)$th root of unity. Hence

$$\prod_{\chi \,(\mathrm{mod}\, q)} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{k=1}^{\operatorname{ord}_q(p)} \left(1 - \frac{e^{2\pi i k/\operatorname{ord}_q(p)}}{p^s}\right)^{\phi(q)/\operatorname{ord}_q(p)} = \left(1 - \frac{1}{(p^s)^{\operatorname{ord}_q(p)}}\right)^{\phi(q)/\operatorname{ord}_q(p)},$$

so that

$$A_{\{1\}}(s) = \prod_{\substack{p \nmid q \\ p \not\equiv 1 \,(\mathrm{mod}\, q)}} \left(1 - \frac{1}{p^{s \operatorname{ord}_q(p)}}\right)^{\phi(q)/\operatorname{ord}_q(p)}$$

(4.2)

Inserting this identity into equation (4.1) and taking $s = 1$ yields

$$G_{\{1\}}(1) = \left\{ \prod_{\substack{p \nmid q \\ p \not\equiv 1 \,(\mathrm{mod}\, q)}} \left(1 - \frac{1}{p^{\operatorname{ord}_q(p)}}\right)^{\phi(q)/\operatorname{ord}_q(p)} \prod_{p|q}(1 - p^{-1}) \prod_{\substack{\chi \,(\mathrm{mod}\, q) \\ \chi \neq \chi_0}} L(1, \chi) \right\}^{1/\phi(q)}$$

$$= \prod_{\substack{p \nmid q \\ p \not\equiv 1 \,(\mathrm{mod}\, q)}} \left(1 - \frac{1}{p^{\operatorname{ord}_q(p)}}\right)^{1/\operatorname{ord}_q(p)} \left\{ \frac{\phi(q)}{q} \prod_{\substack{\chi \,(\mathrm{mod}\, q) \\ \chi \neq \chi_0}} L(1, \chi) \right\}^{1/\phi(q)};$$

together with the factor $1/\Gamma(1/\phi(q))$ from equation (3.6), this comprises the constant G_q defined in equation (1.3) as required. $\qquad\square$

Remark 4.2. There are many equivalent ways to write the constant G_q defined in equation (1.3); we note, for example, that the first parenthetical factor is actually equal to a residue of a Dedekind zeta-function, which can be evaluated using the analytic class number formula (see [5, Chapter VII, Corollary 5.11] for example) and the formula for the discriminant of a cyclotomic field (see [8,

Proposition 2.7] for example):

$$\frac{\phi(q)}{q} \prod_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} L(1,\chi) = \operatorname*{Res}_{s=1} \zeta_{\mathbb{Q}(e^{2\pi i/q})}(s)$$

$$= \frac{(2\pi)^{\phi(q)/2} \gcd(q,2) \operatorname{Reg}_{\mathbb{Q}(e^{2\pi i/q})} h(\mathbb{Q}(e^{2\pi i/q})) \prod_{p|q} p^{\phi(q)/2(p-1)}}{2q^{\phi(q)/2+1}}$$

where $\operatorname{Reg}(K)$ and $h(K)$ denote the regulator and class number of K. The form we have chosen has the advantage of being easy to estimate, as the following proposition will show.

A very similar constant appears in the counting function of those integers n for which $\phi(n)$ is not divisible by a given prime q (see [6, 2], and in particular note that our calculation (4.2) has a close counterpart in [2]). This is to be expected, as such integers are essentially those free of prime factors $p \equiv 1 \pmod{q}$, which is the case $\mathcal{B}' \equiv \{2, \ldots, q-1\}$ of Theorem 3.4; and by Remark 3.5, the leading constant in that asymptotic formula is closely related to the leading constant (1.3) for $\mathcal{B} = \{1\}$ (in the notation of the proof of Proposition 4.1).

Proposition 4.3. *The constant G_q defined in equation* (1.3) *satisfies $G_q \ll \dfrac{\log q}{\phi(q)}$.*

Proof. The factor $\phi(q)/q$ is at most 1, as is the second product over primes. Since $\Gamma(s)$ has a pole at $s = 0$, we have $1/\Gamma(s) \ll |s|$ for $|s| \leq \frac{1}{2}$, say, and in particular $1/\Gamma(1/\phi(q)) \ll 1/\phi(q)$. Finally, it is well known (see [3, Theorem 11.4] for example) that $L(1,\chi) \ll \log q$. Combining these estimates establishes the proposition. $\square$

5. COUNTING n FOR WHICH $q \mid \lambda_1(n)$

We return now to invariant factors, beginning with characterizations of the least invariant factor $\lambda_1(n)$ in terms of the prime factorization of n.

Lemma 5.1. *Let q and $m_1, \ldots, m_\ell$ be positive integers. Suppose that $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_\ell\mathbb{Z}$, where $\gcd(m_1, \ldots, m_\ell) > 1$. Then $q \mid \lambda_1(G)$ if and only if $q \mid m_j$ for each $1 \leq j \leq \ell$.*

Note that the greatest common divisor condition is necessary, as shown by the example $G = \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ for which $\lambda_1(G) = 30$.

Proof. It suffices to prove the lemma when q is a prime power. Note that the assertion $q \mid \lambda_1(G)$ is equivalent to the existence of a subgroup of G of the form $(\mathbb{Z}/q\mathbb{Z})^m$, where m is the length of the invariant factor decomposition of G; on the other hand, the assertion that $q \mid m_j$ for each $1 \leq j \leq \ell$ is equivalent to the existence of a subgroup of G of the form $(\mathbb{Z}/q\mathbb{Z})^\ell$. Therefore it suffices to show that the length of the invariant factor decomposition of G equals ℓ.

By hypothesis, there exists a prime p dividing $\gcd(m_1, \ldots, m_\ell)$, which implies that $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_\ell\mathbb{Z}$ has a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\ell$. In particular, the length of the invariant factor decomposition of G is at least ℓ.

On the other hand, for any finite abelian group H, the length of the invariant factor decomposition of H is the maximum, over all primes p dividing the cardinality of H, of the length of the p-Sylow subgroup of H. But the p-Sylow subgroup of $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_\ell\mathbb{Z}$ is simply $\mathbb{Z}/p^{\nu_1} \times \cdots \times \mathbb{Z}/p^{\nu_\ell}$ where each ν_j is the power of p in the prime factorization of m_j; in particular, this length is at most ℓ. $\square$

The following useful corollary is an immediate consequence of Lemma 5.1:

Corollary 5.2. *If $m_1, \ldots, m_\ell$ are even integers, then the least invariant factor of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_\ell\mathbb{Z}$ equals* 2.

The next proposition completely characterizes the integers n counted by $D_q(x)$. We define $q_{(p)}$ to be the largest divisor of q that is not divisible by p, or equivalently $q_{(p)} = q/p^r$ where p^r is the exact power of p dividing q.

Proposition 5.3. *Fix an even integer $q \geq 4$. For any positive integer n, the least invariant factor of M_n is a multiple of q if and only if all of the following conditions hold:*

(1) *for primes $p \nmid q$: if $p \mid n$ then we must have $p \equiv 1 \pmod{q}$;*
(2) *for odd primes $p \mid q$ such that $q_{(p)} \mid (p-1)$: either $p \nmid n$ or $p^{r+1} \mid n$;*
(3) *for odd primes $p \mid q$ such that $q_{(p)} \nmid (p-1)$: we must have $p \nmid n$;*
(4) *$4 \nmid n$.*

Note that there can be at most one prime p satisfying the assumptions of condition (2) (see the proof of Proposition 5.4 below). The reader is invited to form the intuition that (1) is the most important condition, so that the order of magnitude of $D_q(x)$ is the same as the order of magnitude of $J_q(x)$ from the previous section, while the conditions (2)–(4) at the finitely many primes dividing q are more minor and affect merely the leading constant in the asymptotic formula.

Proof. First, assume that n is odd. Write the factorization $n = p_1^{\nu_1} \cdots p_m^{\nu_m}$. Since n is odd, each $\phi(p_j^{\nu_j})$ is even, and each $\mathbb{Z}/p_j^{\nu_j}\mathbb{Z}$ is isomorphic to $\mathbb{Z}/\phi(p_j^{\nu_j})\mathbb{Z}$. By the Chinese remainder theorem, $M_n \cong \mathbb{Z}/\phi(p_1^{\nu_1})\mathbb{Z} \times \cdots \times \mathbb{Z}/\phi(p_m^{\nu_m})\mathbb{Z}$ where $2 \mid \gcd\big(\phi(p_1^{\nu_1}), \ldots, \phi(p_m^{\nu_m})\big)$. Therefore, by Lemma 5.1, the least invariant factor of M_n is a multiple of q if and only if $q \mid \phi(p^\nu) = p^{\nu-1}(p-1)$ for all $p^\nu \| n$. The lemma now follows for odd n upon examining the three given cases for the relationship between p and q.

Next, assume that n is twice an odd number; then $M_n \cong M_{n/2}$, and the lemma follows for these n by the argument above applied to $n/2$.

Finally, assume that $4 \mid n$. Write the factorization $n = 2^r p_1^{\nu_1} \cdots p_m^{\nu_m}$. By the Chinese remainder theorem, M_n is isomorphic to $\mathbb{Z}/2Z \times \mathbb{Z}/\phi(p_1^{\nu_1})\mathbb{Z} \times \cdots \times \mathbb{Z}/\phi(p_m^{\nu_m})\mathbb{Z}$ if $r = 2$ and isomorphic to $\mathbb{Z}/2Z \times \mathbb{Z}/2^{r-2}\mathbb{Z} \times \mathbb{Z}/\phi(p_1^{\nu_1})\mathbb{Z} \times \cdots \times \mathbb{Z}/\phi(p_m^{\nu_m})\mathbb{Z}$ if $r \geq 3$; in either case, Corollary 5.2 implies that the least invariant factor of M_n equals 2. In other words, if the least invariant factor of M_n is a multiple of q then $4 \nmid n$, completing the proof of the proposition. $\square$

We remark that an examination of the proof confirms that $\lambda_1(n)$ is even for all $n \geq 3$.

We are now ready to establish an asymptotic formula for the counting function $D_q(x)$ from Definition 1.5.

Proposition 5.4. *Uniformly for even integers $4 \leq q \leq (\log x)^{1/3}$,*

$$D_q(x) = \frac{H_q x}{(\log x)^{1-1/\phi(q)}} + O\left(\frac{x}{(\log x)^{5/4-1/\phi(q)}}\right),$$

where H_q is defined in equation (1.2). In particular, when $q \ll (\log x)^{1/4}$,

$$D_q(x) \ll \frac{\log q}{\phi(q)} \frac{x}{(\log x)^{1-1/\phi(q)}}. \tag{5.1}$$

Proof. Define $D_q^1(x)$ to be the number of odd positive integers $n \le x$ such that q divides the least invariant factor of n. By condition (4) of Lemma 5.3, every even integer counted by $D_q(x)$ is of the form $2m$ where m is counted by $D_q^1(\frac{x}{2})$. Therefore $D_q(x) = D_q^1(x) + D_q^1(\frac{x}{2})$, and so it suffices to show that

$$D_q^1(x) = \frac{G_q x}{(\log x)^{1-1/\phi(q)}} \begin{cases} 1 + 1/p^r(p-1), & \text{if there exists an odd prime power} \\ & \qquad\qquad p^r \| q \text{ such that } q/p^r \mid (p-1), \\ 1, & \text{otherwise} \end{cases}$$
$$+ O\left(\frac{x}{(\log x)^{5/4-1/\phi(q)}}\right). \quad (5.2)$$

If there is no prime power p^r satisfying the condition on the right-hand side of equation (5.2), then by conditions (1) and (3) of Lemma 5.3 the integers counted by $D_q^1(x)$ are precisely those integers all of whose prime factors are congruent to 1 (mod q), the number of which is $J_q(x)$ by definition; hence the asymptotic formula (5.2) is exactly Proposition 4.1 in this case.

Next we argue why there can be at most one prime power p^r satisfying the condition on the right-hand side of equation (5.2): if $p_1^{r_1}$ and $p_2^{r_2}$ were to satisfy these conditions (with $p_1 \ne p_2$), then

$$p_1 p_2 \mid q = p_2^{r_2}(q/p_2^{r_2}) \mid (q/p_1^{r_1})(q/p_2^{r_2}) \mid (p_1-1)(p_2-1) < p_1 p_2, \quad (5.3)$$

a contradiction.

The only remaining case to consider is if there is a (unique) odd prime power p^r satisfying the condition on the right-hand side of equation (1.2). In this case, conditions (1)–(3) of Lemma 5.3 imply that

$$D_q^1(x) = D_{q,0}^1(x) + \sum_{\ell \ge r+1} D_{q,\ell}^1(x),$$

where $D_{q,\ell}^1(x)$ denotes the number of odd integers $n \le x$ of the form $n = p^\ell m$ where all prime factors of m are congruent to 1 (mod q); this quantity is exactly $J_q(x/p^\ell)$. Since the number of integers up to x that are divisible by p^L is trivially at most x/p^L for any positive integer L, we may truncate the above sum and apply Proposition 4.1 to obtain

$$D_q^1(x) = J_q(x) + \sum_{\ell=r+1}^{L-1} J_q\left(\frac{x}{p^\ell}\right) + O\left(\frac{x}{p^L}\right)$$
$$= \frac{G_q x}{(\log x)^{1-1/\phi(q)}} + O\left(\frac{x}{(\log x)^{5/4-1/\phi(q)}}\right)$$
$$+ \sum_{\ell=r+1}^{L-1}\left(\frac{G_q x/p^\ell}{(\log(x/p^\ell))^{1-1/\phi(q)}} + O\left(\frac{x/p^\ell}{(\log(x/p^\ell))^{5/4-1/\phi(q)}}\right)\right) + O\left(\frac{x}{p^L}\right).$$

If we choose L so that $p^{L-1} < \exp(\sqrt{\log x}) \le p^L$, then $\log(x/p^\ell) = (\log x)(1 + O(1/\sqrt{\log x}))$ for each ℓ in the sum, and hence the above expression can be simplified to

$$
\begin{aligned}
D_q^1(x) &= \left(G_q + O\left(\frac{1}{(\log x)^{1/4}} \right) \right) \frac{x}{(\log x)^{1-1/\phi(q)}} \left(1 + \sum_{\ell=r+1}^{L-1} \frac{1}{p^\ell} \right) + O\left(\frac{x}{p^L} \right) \\
&= \left(G_q + O\left(\frac{1}{(\log x)^{1/4}} \right) \right) \frac{x}{(\log x)^{1-1/\phi(q)}} \left(1 + \frac{1}{p^r(p-1)} - \frac{1}{p^{L-1}(p-1)} \right) + O\left(\frac{x}{p^L} \right) \\
&= \left(G_q + O\left(\frac{1}{(\log x)^{1/4}} \right) \right) \frac{x}{(\log x)^{1-1/\phi(q)}} \left(1 + \frac{1}{p^r(p-1)} \right) + O\left(\frac{x}{\exp(\sqrt{\log x})} \right)
\end{aligned}
$$

(since $G_q \ll 1$ by Proposition 4.3), which is enough to establish equation (5.2) in this final case. $\qquad \square$

It is also possible to prove Proposition 5.4 directly using the Selberg–Delange method, inserting relevant Euler factors at the primes dividing q. However, we have chosen our proof to proceed via Theorem 3.4 in the hopes that developing this general infrastructure will have value beyond this paper.

6. COUNTING n FOR WHICH $\lambda_1(n) = q$

The goal of this section is to obtain an asymptotic formula for $E_q(x)$, the counting function of those integers n for which $\lambda_1(n) = q$ (and thereby establish Theorem 1.4), from the asymptotic formula established in the previous section for $D_q(x)$, the counting function of those integers n for which $q \mid \lambda_1(n)$. We proceed essentially by inclusion–exclusion (encoded, as usual, by the Möbius mu-function). For technical reasons, however, we work with slight variants of the functions $E_q(x)$ and $D_q(x)$ in which we insist that the integers being counted do not have few prime factors. The following definition, in which $\omega(n)$ as usual denotes the number of distinct prime factors of n, can be compared with Definitions 1.3 and 1.5:

Definition 6.1. Given an integer parameter $b \ge 4$, define

$$
\begin{aligned}
E_q^*(x; b) &= \#\{n \le x \colon \lambda_1(n) = q \text{ and } \omega(n) > b\} \\
D_q^*(x; b) &= \#\{n \le x \colon q \mid \lambda_1(n) \text{ and } \omega(n) > b\}
\end{aligned}
$$

Lemma 6.2. *For all integers $q, M, b \ge 4$ and all real numbers $x \ge e^e$,*

$$
E_q(x) = D_q(x) + O_b\left(\sum_{1 < m < M} D_{mq}(x) + \sum_{m \ge M} D_{mq}^*(x; b) + \frac{Mx(\log\log x)^{b-1}}{\log x} \right).
$$

Proof. It is obvious from the definitions of D_q^* and E_q^* that $D_q^*(x; b) = \sum_{m=1}^\infty E_{mq}^*(x; b)$; a version of Möbius inversion then implies that $E_q^*(x; b) = \sum_{m=1}^\infty \mu(m) D_{mq}^*(x; b)$. (Both series are actually finite sums for any given value of x, so there are no issues of convergence. We note that these identities hold even for $q = 2$.) We write

$$
E_q^*(x; b) = D_q^*(x; b) + O\left(\sum_{1 < m < M} D_{mq}^*(x; b) + \sum_{m \ge M} D_{mq}^*(x; b) \right). \tag{6.1}
$$

13

Using known estimates for the number of integers with a constant number of prime factors (see [3, Section 7.4] for example),

$$0 \le E_q(x) - E_q^*(x; b) = \#\{n \le x \colon \lambda_1(n) = q \text{ and } \omega(n) \le b\}$$
$$\le \#\{n \le x \colon \omega(n) \le b\}$$
$$\ll_b \sum_{k \le b} \frac{x}{\log x} \frac{(\log \log x)^{k-1}}{(k-1)!} \ll_b \frac{x(\log \log x)^{b-1}}{\log x}.$$

The same argument gives $0 \le D_{mq}(x) - D_{mq}^*(x; b) \ll_b x(\log \log x)^{b-1}/\log x$ uniformly in mq, and thus the formula (6.1) becomes

$$E_q(x) = E_q^*(x; b) + O_b\left(\frac{x(\log \log x)^{b-1}}{\log x}\right)$$
$$= D_q^*(x) + O_b\left(\sum_{1 < m < M} D_{mq}^*(x; b) + \sum_{m \ge M} D_{mq}^*(x; b) + \frac{x(\log \log x)^{b-1}}{\log x}\right)$$
$$= D_q(x) + O_b\left(\sum_{1 < m < M} D_{mq}(x) + \sum_{m \ge M} D_{mq}^*(x; b) + \frac{Mx(\log \log x)^{b-1}}{\log x}\right)$$

as desired. (A more careful argument could remove the factor of M from the last error term, but this version suffices for our purposes.) $\qquad\square$

We already have the upper bound (5.1) that can be applied to $D_{mq}(x)$ for small m; we now complement that with an upper bound for $D_{mq}^*(x; b)$ that improves as m increases.

Lemma 6.3. *For $b \ge 3$ and $x \ge e^e$,*

$$D_{mq}^*(x; b) \ll_b \frac{x(\log \log x)^{b-1}}{m^{b-2}}.$$

Proof. First note that by the argument surrounding equation (5.3), with q replaced by mq, there can be at most one prime p_0 such that $(mq)_{(p_0)} \mid (p_0 - 1)$. Suppose that n is counted by $D_{mq}^*(x; b)$. We know that $\omega(n) \ge b+1$, and so we can choose $b-1$ distinct odd primes $p_1, \ldots, p_{b-1}$ dividing n (and hence not exceeding x), none of which is equal to p_0 if it exists. Of course the number of $n \le x$ divisible by these $b-1$ primes is at most $x/p_1 \cdots p_{b-1}$.

We also know that mq divides $\lambda_1(n)$; by Proposition 5.3 with q replaced by mq, we must have $p_1 \equiv \cdots \equiv p_{b-1} \equiv 1 \pmod{mq}$. Sorting all such integers n by the primes $p_1, \ldots, p_{b-1}$ (and ignoring the possibility of double-counting), we conclude that

$$D_{mq}^*(x; b) \le \sum_{\substack{p_1 \le x \\ p_1 \equiv 1 \,(\mathrm{mod}\ mq)}} \cdots \sum_{\substack{p_{b-1} \le x \\ p_{b-1} \equiv 1 \,(\mathrm{mod}\ mq)}} \frac{x}{p_1 \cdots p_{b-1}} \le x \left(\sum_{\substack{p \le x \\ p \equiv 1 \,(\mathrm{mod}\ mq)}} \frac{1}{p} \right)^{b-1}.$$

It follows quickly from the Brun–Titchmarsh theorem and partial summation that for $x \ge e^e$,

$$\sum_{\substack{p \le x \\ p \equiv 1 \,(\mathrm{mod}\ mq)}} \frac{1}{p} \ll \frac{\log \log x}{\phi(mq)};$$

14

therefore

$$D^*_{mq}(x; b) \ll_b x \left(\frac{\log\log x}{\phi(mq)} \right)^{b-1} \le x \left(\frac{\log\log x}{\phi(m)} \right)^{b-1}.$$

The lemma follows since $\phi(m) \gg_b m^{(b-2)/(b-1)}$. $\qquad\square$

We now have the tools we need to assemble our asymptotic formula for $E_q(x)$ for all even integers $q \ge 4$.

Proof of Theorem 1.4. Beginning with Lemma 6.2, we input the upper bound (5.1) for the terms in the first error-term sum (valid as long as $M \le (\log x)^{1/4}$) and Lemma 6.3 for the terms in the second error-term sum, obtaining

$$E_q(x) = D_q(x) + O_b \left(\sum_{1 < m < M} \frac{\log mq}{\phi(mq)} \frac{x}{(\log x)^{1-1/\phi(mq)}} + \sum_{m \ge M} \frac{x(\log\log x)^{b-1}}{m^{b-2}} + \frac{Mx(\log\log x)^{b-1}}{\log x} \right)$$

$$= D_q(x) + O_{q,b} \left(\frac{x}{(\log x)^{1-1/\phi(2q)}} \sum_{1 < m < M} \frac{\log m}{\phi(m)} + \frac{x(\log\log x)^{b-1}}{M^{b-3}} + \frac{Mx(\log\log x)^{b-1}}{\log x} \right)$$

$$= D_q(x) + O_{q,b} \left(\frac{x(\log M)^2}{(\log x)^{1-1/2\phi(q)}} + \frac{x(\log\log x)^{b-1}}{M^{b-3}} + \frac{Mx(\log\log x)^{b-1}}{\log x} \right).$$

Choosing $M = \lfloor (\log x)^{1/3\phi(q)} \rfloor$ and $b = 3\phi(q) + 2$, we conclude that

$$E_q(x) = D_q(x) + O_q \left(\frac{x(\log\log x)^2}{(\log x)^{1-1/2\phi(q)}} + \frac{x(\log\log x)^{3\phi(q)+1}}{(\log x)^{1-1/3\phi(q)}} \right) = D_q(x) + O_q \left(\frac{x(\log\log x)^2}{(\log x)^{1-1/2\phi(q)}} \right),$$

which suffices to establish the theorem in light of Proposition 5.4. $\qquad\square$

7. COUNTING n FOR WHICH $\lambda_1(n) \ne 2$

We adapt the method of the previous section to assemble our asymptotic formula for $T(x)$.

Proof of Theorem 1.2. Because of the identity

$$T(x) = \lfloor x \rfloor - E_2(x) = D_2(x) + 2 - E_2(x),$$

we begin by examining the function $E_2(x)$ using the method of the proof of Lemma 6.2, whose deductions we will use here without specific comment. We write

$$E^*_2(x; b) = \sum_{m=1}^{\infty} \mu(m) D^*_{2m}(x; b)$$

$$= D^*_2(x; b) - D^*_4(x; b) - D^*_6(x; b) + O \left(D^*_{10}(x; b) + \sum_{7 \le m < M} D^*_{2m}(x; b) + \sum_{m \ge M} D^*_{2m}(x; b) \right)$$

$$= D_2(x) - D_4(x) - D_6(x)$$

$$+ O \left(D_{10}(x) + \sum_{7 \le m < M} D_{2m}(x) + \sum_{m \ge M} D^*_{2m}(x; b) + \frac{Mx(\log\log x)^{b-1}}{\log x} \right).$$

Again we input the upper bound (5.1) for the terms in the first error-term sum (valid as long as $M \le (\log x)^{1/4}$) and Lemma 6.3 for the terms in the second error-term sum, obtaining

$$T(x) = D_2(x) + 2 - E_2(x)$$

$$= D_4(x) + D_6(x) + O\left(\frac{x}{(\log x)^{1-1/\phi(10)}}\right.$$

$$+ \sum_{7 \le m < M} \frac{\log 2m}{\phi(2m)} \frac{x}{(\log x)^{1-1/\phi(mq)}} + \frac{x(\log\log x)^{b-1}}{M^{b-3}} + \left.\frac{Mx(\log\log x)^{b-1}}{\log x}\right)$$

$$= D_4(x) + D_6(x) + O\left(\frac{x}{(\log x)^{3/4}}\right.$$

$$+ \frac{x}{(\log x)^{5/6}} \sum_{m < M} \frac{\log m}{\phi(m)} + \frac{x(\log\log x)^{b-1}}{M^{b-3}} + \left.\frac{Mx(\log\log x)^{b-1}}{\log x}\right),$$

where in the last line we have used the fact that $\phi(mq) \ge 6$ for $mq \ge 14$. Choosing $M = \lfloor (\log x)^{1/5} \rfloor$ and $b = 7$, we conclude that

$$T(x) = D_4(x) + D_6(x) + O\left(\frac{x}{(\log x)^{3/4}} + \frac{x(\log\log x)^2}{(\log x)^{5/6}} + \frac{x(\log\log x)^6}{(\log x)^{4/5}}\right)$$

$$= D_4(x) + D_6(x) + O\left(\frac{x}{(\log x)^{3/4}}\right),$$

which again suffices to establish the theorem in light of Proposition 5.4. $\qquad\square$

APPENDIX: THE SELBERG–DELANGE METHOD WITH ADDITIONAL UNIFORMITY

The goal of this appendix is to establish a version of the Selberg–Delange formula where the dependence on certain parameters has been made explicit. More precisely, Tenenbaum [7, Chapter II.5] has a statement of the Selberg–Delange formula for Dirichlet series $F(s)$ satisfying certain hypotheses (see Definitions A.4 and A.6 below) that involve two parameters in particular: c_0, a constant involved in the definition of a zero-free-region-shaped domain of analytic continuation for $F(s)$, and δ, a constant involved in the rate of growth of $F(s)$ within that domain. In Tenenbaum's work, implicit constants in the formulas are allowed to depend upon c_0 and δ. Here, we give a version of the theorem that is uniform in those two parameters; see Theorem A.13 for our most general statement and Corollary A.14 for an important special case.

We recommend that the reader have Tenenbaum's book available for reference; however, our proof herein is largely self-contained once we quote relevant results from that source. We are essentially following Tenenbaum's proof (except for rendering one error term, in Lemma A.11 below, in a form more convenient for our present purposes), although we have reorganized the order of the steps for clarity in this context.

A.1. **Definitions and preliminaries.** All of the definitions in this section are taken directly fom Tenenbaum's book; we also record several simple consequences of those definitions for later use. All of this notation will be used throughout this appendix.

Definition A.1. For any complex number z, the function $Z(s; z) = \left((s - 1)\zeta(s)\right)^z / s$ is defined on any simply connected domain not containing a zero of $\zeta(s)$. We always assume that its domain

of definition contains $[1, \infty)$, and we choose the branch of the complex exponential satisfying $Z(1; z) = 1$.

As stated in [7, Part II, Theorem 5.1], there exist entire functions $\gamma_j(z)$ such that the function $Z(s; z)$ has the Taylor expansion $Z(s; z) = \sum_{j=0}^{\infty} \frac{1}{j!} \gamma_j(z)(s-1)^j$, and moreover, on the disk $\{|z| \le A\}$, we have $\frac{1}{j!} \gamma_j(z) \ll_{A,\varepsilon} (1 + \varepsilon)^j$ for any $\varepsilon > 0$.

Lemma A.2. *For any $0 < r < 1$, we have $Z(s; z) \ll_{A,r} 1$ uniformly for $|s - 1| \le r$ and $|z| \le A$.*

Proof. Choosing $\varepsilon = \frac{1-r}{2r}$ in the estimate in Definition A.1, we deduce from the Taylor expansion of $Z(s; z)$ that

$$|Z(s; z)| \le \sum_{j=0}^{\infty} \left| \frac{\gamma_j(z)}{j!} \right| |s - 1|^j \ll_{A,r} \sum_{j=0}^{\infty} \left(1 + \frac{1-r}{2r} \right)^j r^j = \frac{2}{1-r} \ll_r 1$$

under the hypotheses of the lemma, as desired. $\qquad \square$

We define $\log^+(y) = \max\{0, \log y\}$; the following calculus inequality will be helpful later.

Lemma A.3. *Given real numbers $A > 0$ and $0 < \delta \le 1$, we have $(1 + \log^+ y)^A \ll_A \delta^{-A}(1+y)^{\delta/2}$ for all $y \ge 0$.*

Proof. Since the assertion is trivial for $0 \le y \le e^{-1}$, we may assume that $y \ge e^{-1}$. The function $(1 + \log t)^A / t^{\delta/2}$ is increasing for $e^{-1} \le t \le e^{2A/\delta - 1}$ and decreasing thereafter, and its value at $t = e^{2A/\delta - 1}$ equals $2^A e^{\delta/2 - A} (\frac{A}{\delta})^A \le 2^A e^{1/2 - A}(\frac{A}{\delta})^A$; this global maximum value shows that $(1 + \log y)^A \ll_A \delta^{-A} y^{\delta/2}$ for all $y \ge e^{-1}$, which is enough to establish the lemma. $\qquad \square$

We continue to follow the same convention as Tenenbaum of writing the real and imaginary parts of complex numbers as $s = \sigma + i\tau$.

Definition A.4. Let z be a complex number, and let c_0, δ, and M be positive real numbers with $\delta \le 1$. A Dirichlet series $F(s)$ *has the property* $\mathcal{P}(z; c_0, \delta, M)$ if the Dirichlet series $G(s; z) = F(s)\zeta(s)^{-z}$ has an analytic continuation to the region $\sigma \ge 1 - c_0/(1 + \log^+ |\tau|)$, wherein it satisfies the bound $|G(s; z)| \le M(1 + |\tau|)^{1-\delta}$. Note that this inequality implies that $G(s; z) \ll M$ uniformly for $|s - 1| \le \min\{1, c_0\}$.

Define a simply connected domain $\mathcal{D}$ and parameters c_0 and c associated to it by

$$\mathcal{D} = \left\{ 1 - c/(1 + \log^+ |\tau|) \le \sigma \le 2 \right\} \setminus (-\infty, 1], \quad \text{where } c = c(c_0) = \tfrac{47}{48} c_0. \qquad (A.1)$$

(The fraction $\frac{47}{48}$ is convenient in one step of the proof of Lemma A.11 below and is otherwise insignificant, other than being less than 1.) Notice that if $c_0 \le \frac{2}{11}$, then $c^{-1} > 5.573412$, which implies [4, Theorem 1] that $\zeta(s) \ne 0$ for $s \in \mathcal{D}$.

Lemma A.5. *Suppose that $F(s)$ has the property $\mathcal{P}(z; c_0, \delta, M)$, where $|z| \le A$ and $c_0 \le \frac{2}{11}$. Then $F(s)$ has an analytic continuation to $\mathcal{D}$ which satisfies*

$$F(s) \ll_A \begin{cases} \delta^{-A} M (1 + |\tau|)^{1 - \delta/2}, & \text{if } |\tau| \ge 3, \\ M|s - 1|^{-A}, & \text{if } |\tau| \le 3. \end{cases}$$

Proof. The analytic continuation follows from the identity $F(s) = G(s; z)\zeta(s)^z$ and the assumed analytic continuation of $G(s; z)$.

17

In $\{s \in \mathcal{D} \colon |\tau| \geq 3\}$, we have the upper bound $\zeta(s)^z \ll_A (1 + \log^+ |\tau|)^A$ [7, Part II, equation (5.10)], which by our assumption on $G(s; z)$ implies

$$F(s) = G(s; z)\zeta(s)^z \ll_A M(1 + |\tau|)^{1-\delta}(1 + \log^+ |\tau|)^A \ll_A \delta^{-A} M(1 + |\tau|)^{1-\delta/2}$$

by Lemma A.3.

On the other hand, the fact that $\zeta(s) = 1/(s-1) + O(1)$ in any compact neighborhood of $s = 1$ implies that $|\zeta(s)^z| \ll_A |\zeta(s)|^A \ll_A |s - 1|^{-A}$ in $\{s \in \mathcal{D} \colon |\tau| \leq 3\}$ (as can be derived from Lemma 2.4). Again by assumption, $G(s; z) \ll M(1 + |\tau|)^{1-\delta} \ll M$ when $|\tau| \leq 3$ (since $\delta > 0$). These bounds establish the second case of the lemma. $\square$

Definition A.6. Let z and w be complex numbers, and let c_0, δ, and M be positive real numbers with $\delta \leq 1$. A Dirichlet series $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ *has type* $\mathcal{T}(z, w; c_0, \delta, M)$ if it has the property $\mathcal{P}(z; c_0, \delta, M)$ and there exist nonnegative real numbers b_n, with $|a_n| \leq b_n$ for all $n \geq 1$, such that the Dirichlet series $\sum_{n=1}^{\infty} b_n n^{-s}$ has the property $\mathcal{P}(w; c_0, \delta, M)$ as in Definition A.4.

Note that when the a_n are nonnegative real numbers, if $F(s)$ has the property $\mathcal{P}(z; c_0, \delta, M)$ then it automatically has type $\mathcal{T}(z, z; c_0, \delta, M)$. (We remark that Tenenbaum has "positive" in place of "nonnegative" in both places in this definition, but strict positivity is never used.)

Definition A.7. For $x > e^{1/c} = e^{48/(47c_0)}$, we define

$$\Phi(x) = \frac{1}{2\pi i} \int_{\Gamma} F(s) x^{s+1} \frac{ds}{s(s+1)} \tag{A.2}$$

where Γ is a truncated Hankel contour (see Figure 1), consisting of a circle around $s = 1$ with radius $1/(2 \log x)$ and two line segments, above and below the branch cut, joining $1 - c/2$ to $1 - 1/(2 \log x)$; note that Γ is entirely contained in the domain $\mathcal{D}$ defined in equation (A.1).

Lemma A.8. *Suppose that $F(s)$ has the property $\mathcal{P}(z; c_0, \delta, M)$, where $|z| \leq A$ and $c_0 \leq \frac{2}{11}$. Then $\Phi''(x) \ll_A M(\log x)^A$ uniformly for $x > e^{48/(47c_0)}$.*

Proof. Differentiating equation (A.2) under the integral sign yields

$$\Phi'(x) = \frac{1}{2\pi i} \int_{\Gamma} F(s) x^s \frac{ds}{s} \quad \text{and} \quad \Phi''(x) = \frac{1}{2\pi i} \int_{\Gamma} F(s) x^{s-1} \, ds \tag{A.3}$$

for $x > 0$. The length of the contour Γ is $O(1)$, and for $s \in \Gamma$ we have $|x^{s-1}| \leq e^{1/2}$ and $F(s) \ll M|s - 1|^A$ by Lemma A.5, so that

$$\Phi''(x) \ll |F(s)| \ll_A M|s - 1|^{-A} \ll_A M(\log x)^A$$

since $|s - 1| \leq 2 \log x$. $\square$

Lemma A.9. *Suppose that $F(s)$ has the property $\mathcal{P}(z; c_0, \delta, M)$, where $|z| \leq A$ and $c_0 \leq \frac{2}{11}$. Then uniformly for $x \geq e^{2/c_0}$ and $|h| \leq \frac{x}{2}$,*

$$\Phi(x + h) - \Phi(x) = h\Phi'(x) + O_A(Mh^2(\log x)^A).$$

Proof. The assertion follows immediately from the integration-by-parts formula $\Phi(x+h) - \Phi(x) = h\Phi'(x) + h^2 \int_0^1 (1-t)\Phi''(x + ht) \, dt$ and Lemma A.8 (noting that the assumption $x \geq e^{2/c_0}$ implies that $x + h \geq \frac{x}{2} > e^{48/(47c_0)}$ since $c_0 \leq \frac{2}{11}$). $\square$
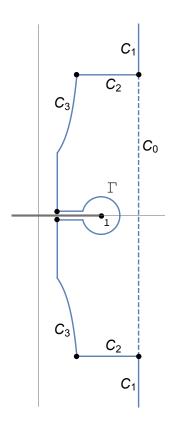
18

FIGURE 1. The truncated Hankel contour Γ, and the contour of integration in Lemma A.10

A.2. **Derivation of the Selberg–Delange formula.** Throughout this section, we write a_n for the coefficients of the Dirichlet series $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, and we define the summatory function $A(t) = \sum_{n \leq t} a_n$. The next three lemmas contain the majority of the work in establishing our version of the Selberg–Delange formula at the end of this section.

Lemma A.10. *Suppose that $F(s)$ has the property $\mathcal{P}(z; c_0, \delta, M)$, where $|z| \leq A$ and $c_0 \leq \frac{2}{11}$. Then for $x > e^{1/c}$,*

$$\int_0^x A(t)\, dt = \Phi(x) + O_A\big((\delta^{-A-1} + c_0^{-A})Mx^2 e^{-\frac{1}{2}\sqrt{c\delta \log x}}\big).$$

Proof. By Perron's formula, we know that

$$\int_0^x A(t)\, dt = \int_{(1+1/\log x)} F(s) x^{s+1} \frac{ds}{s(s+1)},$$

where the contour integral is over the vertical line $\Re s = 1 + 1/\log x$ (the union of the segment C_0 and the two rays C_1 in Figure 1). Define $\sigma(t) = 1 - \frac{c}{2}/(1 + \log^+ t)$. By Cauchy's theorem, for any $T \geq 3$ we may modify the path of integration into the union of:

- the vertical ray extending upward from $1 + 1/\log x + iT$ and its reflection in the real axis (labeled C_1 in Figure 1);
- the horizontal segment from $\sigma(T) + iT$ to $1 + 1/\log x + iT$ and its reflection (labeled C_2);
- the parametric curve $\sigma(\tau) + i\tau$ for $0^+ \leq \tau \leq T$ and its reflection (labeled C_3);
- the truncated Hankel contour Γ from Definition A.7.

19

Note that this modified contour is entirely contained within the domain $\mathcal{D}$ defined in equation (A.1).

When the first case of Lemma A.5, which makes explicit the dependence of the upper bound on δ, is used in Tenenbaum's argument in place of [7, Part II, equation (5.19)], the resulting estimate for the contributions of C_1 and C_2 to the modified contour integral is $O_A(\delta^{-A}Mx^2T^{-\delta/2})$.

Tenenbaum's argument for the contribution of C_3 to the modified contour integral may be used for $|\tau| \geq 3$, yielding an upper bound of $O_A(\delta^{-A-1}Mx^{1+\sigma(T)})$. However, to make explicit the dependence upon c and hence c_0, we must use the second case of Lemma A.5 for the portion of C_3 with $|\tau| \leq 3$: we obtain

$$\ll_A \int M|s-1|^{-A}|x^{s+1}|\frac{|ds|}{|s^2|} \ll Mx^{2-c/5}\int_0^3 \frac{(c/2+\tau)^{-A}}{(1+\tau)^2}\,d\tau$$

$$\ll_A Mx^{2-c/5}\left(\int_0^c \frac{c^{-A}}{(1+\tau)^2}\,d\tau + \int_c^3 \frac{(1+\tau)^{-A}}{(1+\tau)^2}\,d\tau\right)$$

$$\ll_A Mx^{2-c/5}c^{-A} \ll_A Mx^{2-c/5}c_0^{-A}.$$

Summarizing the proof thus far, we have shown that

$$\int_0^x A(t)\,dt = \int_\Gamma \frac{F(s)x^{s+1}\,ds}{s(s+1)} + \int_{C_1\cup C_2}\frac{F(s)x^{s+1}\,ds}{s(s+1)} + \int_{C_3}\frac{F(s)x^{s+1}\,ds}{s(s+1)}$$

$$= \Phi(x) + O_A\big(\delta^{-A}Mx^2T^{-\delta/2} + (\delta^{-A-1}Mx^{1+\sigma(T)} + Mx^{2-c/5}c_0^{-A})\big). \tag{A.4}$$

As Tenenbaum does, we choose $T = e^{\sqrt{(c/\delta)\log x}}$, so that

$$\sigma(T) = 1 - \frac{c/2}{1+\sqrt{(c/\delta)\log x}} \leq \begin{cases} 1, & \text{if } x < e^{7\delta/c}, \\ 1 - \frac{1}{2}\sqrt{\frac{c\delta}{\log x}} + \frac{\delta}{2\log x}, & \text{if } x \geq e^{7\delta/c} \end{cases}$$

(where the second case of the inequality is an easy calculus exercise). In the case $x \geq e^{7\delta/c}$, the error term in equation (A.4) becomes

$$O_A(\delta^{-A}Mx^2e^{-\frac{1}{2}\sqrt{c\delta\log x}} + \delta^{-A-1}Mx^2e^{-\frac{1}{2}\sqrt{c\delta\log x}}e^{\delta/2} + Mx^{2-c/5}c_0^{-A}). \tag{A.5}$$

Since $\delta \leq 1$ we have $e^{\delta/2} \ll 1$, and we also have $x^{-c/5} \leq e^{-\frac{1}{2}\sqrt{c\delta\log x}}$ for $x \geq e^{7\delta/c}$; thus the above expression simplifies to

$$O_A\big((\delta^{-A-1} + c_0^{-A})Mx^2e^{-\frac{1}{2}\sqrt{c\delta\log x}}\big).$$

But this bound for the expression (A.5) also holds for $x < e^{7\delta/c}$, as $x^{-c/5} < 1 \ll e^{-\frac{1}{2}\sqrt{c\delta\log x}}$ in this range. $\qquad\square$

We continue to follow the structure of Tenenbaum's proof; however, in the next proposition we give a somewhat different form for the error term, to simplify the dependence upon c_0.

Lemma A.11. *Suppose that $F(s)$ has the property $\mathcal{P}(z; c_0, \delta, M)$, where $|z| \leq A$ and $c_0 \leq \frac{2}{11}$. For $x > e^{48/(47c_0)}$ and for any $N \in \mathbb{N}$,*

$$\Phi'(x) = x(\log x)^{z-1}\left(\sum_{k=0}^N \frac{\lambda_k(z)}{(\log x)^k} + O_A\left(M\Gamma(N+A+2)\left(\frac{48}{c_0\log x}\right)^{N+1}\right)\right),$$

where the functions $\lambda_k(z)$ are defined in equation (A.9) below.

Proof. Since $F(s) = G(s; z)\zeta(s)^z$ by assumption, Definition A.1 and equation (A.3) imply that

$$\Phi'(x) = \frac{1}{2\pi i} \int_\Gamma \frac{G(s; z)Z(s; z)x^s}{(s-1)^z} \, ds.$$

Lemma A.2 and the last remark of Definition A.4 imply that $G(s; z)Z(s; z) \ll_A M$ uniformly for $|s - 1| \le \frac{2}{11}$ and thus for $|s - 1| \le c$. If we define $\mu_k(z) = \Gamma(z - k)\lambda_k(z)$ (compare to [7, Part II, equation (5.24)] and the preceding equation), it follows immediately that $\mu_k(z) \ll_A Mc^{-k}$ for all $k \ge 0$. The derivation of [7, Part II, equation (5.25)] and the following display proceeds with no changes other than clarifying the dependence on the parameters, yielding

$$\Phi'(x) = \sum_{k=0}^N \mu_k(z)\frac{1}{2\pi i} \int_\Gamma x^s(s-1)^{k-z} \, ds + O_A\big(Mc^{-N}x(\log x)^{\Re z - N - 2}\Gamma(N + A + 2)\big). \quad \text{(A.6)}$$

The subsequent change of variables $w = (s - 1)\log x$ leads, using [7, Part II, Corollary 0.18], to

$$\frac{1}{2\pi i} \int_\Gamma x^s(s-1)^{k-z} \, ds = \frac{x}{2\pi i}(\log x)^{z-1-k} \int_{\mathcal{H}(\frac{1}{2}c\log x)} w^{k-z}e^w \, dw$$

$$= x(\log x)^{z-1-k}\left(\frac{1}{\Gamma(z-k)} + O\big(47^{|z-k|}\Gamma(1 + |z - k|)e^{-\frac{1}{4}c\log x}\big)\right).$$

Using this identity in equation (A.6) gives

$$\Phi'(x) = \sum_{k=0}^N \mu_k(z)x(\log x)^{z-1-k}\left(\frac{1}{\Gamma(z-k)} + O\big(x^{-c/4}47^{|z-k|}\Gamma(1 + |z - k|)\big)\right)$$
$$\quad + O_A\big(Mc^{-N}x(\log x)^{\Re z - N - 2}\Gamma(N + A + 2)\big)$$
$$= x(\log x)^{z-1}\left(\sum_{k=0}^N \frac{\lambda_k(z)}{(\log x)^k} + O\left(x^{-c/4}\sum_{k=0}^N \frac{|\mu_k(z)|}{(\log x)^k}47^{|z-k|}\Gamma(1 + |z - k|)\right)\right)$$
$$\quad + O_A\big(Mc^{-N}x(\log x)^{\Re z - N - 2}\Gamma(N + A + 2)\big)$$
$$= x(\log x)^{z-1}\left\{\sum_{k=0}^N \frac{\lambda_k(z)}{(\log x)^k} + O_A\left(Mx^{-c/4}\sum_{k=0}^N \left(\frac{47}{c\log x}\right)^k\Gamma(k + A + 1)\right)\right.$$
$$\left. + O_A\big(Mc^{-N}(\log x)^{-N-1}\Gamma(N + A + 2)\big)\right\}. \quad \text{(A.7)}$$

Since $\Gamma(N + A + 1) = (N + A)(N + A - 1) \cdots (k + A + 1)\Gamma(k + A + 1)$, the sum in the error term above can be estimated (changing indices $j = N - k$) by

$$\sum_{k=0}^{N} \left(\frac{47}{c\log x}\right)^k \Gamma(k + A + 1) = \Gamma(N + A + 1)\left(\frac{47}{c\log x}\right)^N \sum_{j=0}^{N} \left(\frac{c\log x}{47}\right)^j \prod_{i=1}^{j} \frac{1}{N - j + A + i}$$

$$\leq \Gamma(N + A + 1)\left(\frac{47}{c\log x}\right)^N \sum_{j=0}^{\infty} \left(\frac{c\log x}{47}\right)^j \prod_{i=1}^{j} \frac{1}{i}$$

$$= \Gamma(N + A + 1)\left(\frac{47}{c\log x}\right)^N e^{(c\log x)/47}$$

$$< \Gamma(N + A + 1)\left(\frac{47}{c\log x}\right)^{N+1} x^{c/4},$$

where the last inequality is equivalent to $x^{c/47} < 47x^{c/4}/(c\log x)$ which can be verified for $x > e^{48/(47c_0)} = e^{1/c}$ by an easy calculus exercise. Therefore equation (A.7) becomes

$$\Phi'(x) = x(\log x)^{z-1}\left\{\sum_{k=0}^{N} \frac{\lambda_k(z)}{(\log x)^k} + O_A\left(M\Gamma(N + A + 1)\left(\frac{47}{c\log x}\right)^{N+1}\right)\right.$$

$$\left. + O_A\big(Mc^{-N}(\log x)^{-N-1}\Gamma(N + A + 2)\big)\right\},$$

which implies the statement of the lemma. $\qquad\square$

Lemma A.12. *Suppose that the Dirichlet series $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ has type $\mathcal{T}(z, w; c_0, \delta, M)$, where $|z| \leq A$ and $|w| \leq A$ and $c_0 \leq \frac{2}{11}$. For any $x \geq e^{2/c_0}$ and $0 \leq h \leq \frac{x}{2}$,*

$$\int_{x}^{x+h} |A(t) - A(x)| \, dt \ll_A Mh^2(\log x)^A + (\delta^{-A-1} + c_0^{-A})Mx^2 e^{-\frac{1}{2}\sqrt{c\delta\log x}}.$$

Proof. By assumption, there exist nonnegative real numbers b_n, with $|a_n| \leq b_n$ for all $n \geq 1$, such that the Dirichlet series $\sum_{n=1}^{\infty} b_n n^{-s}$ has the property $\mathcal{P}(w; c_0, \delta, M)$. If we let $B(t) = \sum_{n \leq t} b_n$, which is an increasing function, then the triangle inequality implies that $|A(t) - A(x)| \leq B(t) - B(x)$ for all $t \geq x$, and thus

$$\int_{x}^{x+h} |A(t) - A(x)| \, dt \leq \int_{x}^{x+h} (B(t) - B(x)) \, dt \leq \int_{x}^{x+h} B(t) \, dt - \int_{x-h}^{x} B(t) \, dt. \quad (A.8)$$

By Lemmas A.9 and A.10, applied to $G(s) = \sum_{n=1}^{\infty} b_n n^{-s}$ in place of $F(s)$ and $B(t)$ in place of $A(t)$ and w in place of z, there exists a function Φ_1 such that

$$\Phi_1(x \pm h) - \Phi_1(x) = \pm h\Phi_1'(x) + O_A(Mh^2(\log x)^A)$$

and

$$\int_{0}^{x} B(t) \, dt = \Phi_1(x) + O_A\big((\delta^{-A-1} + c_0^{-A})Mx^2 e^{-\frac{1}{2}\sqrt{c\delta\log x}}\big),$$

which implies that

$$\int_x^{x+h} B(t)\, dt - \int_{x-h}^x B(t)\, dt = \big(\Phi_1(x+h) - \Phi_1(x)\big) + \big(\Phi_1(x-h) - \Phi_1(x)\big)$$
$$+ O_A\big((\delta^{-A-1} + c_0^{-A})Mx^2 e^{-\frac{1}{2}\sqrt{c\delta \log x}}\big)$$
$$= h\Phi_1'(x) + (-h)\Phi_1'(x)$$
$$+ O_A\big(Mh^2(\log x)^A + (\delta^{-A-1} + c_0^{-A})Mx^2 e^{-\frac{1}{2}\sqrt{c\delta \log x}}\big).$$

Combining this estimate with equation (A.8) establishes the lemma. $\qquad\square$

With these tools in hand, we are ready to establish our version of the Selberg–Delange formula, which can be compared with [7, Part II, Theorem 5.2].

Theorem A.13. *Let $A \geq 1$ be a real number and N a nonnegative integer. Let z and w be complex numbers with $|z| \leq A$ and $|w| \leq A$, and let c_0, δ, and M be positive real numbers with $c_0 \leq \frac{2}{11}$ and $\delta \leq 1$. Let $F(s) = \sum_{n=1}^\infty a_n n^{-s}$ be a Dirichlet series that has type $\mathcal{T}(z, w; c_0, \delta, M)$ as in Definition A.6. Then, uniformly for $x \geq \exp\big(8^{1/A} \max\{\delta^{-1-1/A}, 2/c_0\}\big)$,*

$$\sum_{n \leq x} a_n = x(\log x)^{z-1}\bigg(\sum_{k=0}^N \frac{\lambda_k(z)}{(\log x)^k} + O_A(MR_N(x))\bigg),$$

where

$$\lambda_k(z) = \frac{1}{\Gamma(z-k)} \sum_{h=0}^k \frac{1}{h!(k-h)!} \frac{\partial^h G}{\partial s^h}(1; z)\gamma_{k-h}(z) \tag{A.9}$$

with $G(s; z) = F(s)\zeta(s)^{-z}$ and with $\gamma_j(z)$ as in Definition A.1, and where

$$R_N(x) = (\delta^{-2A-3/2} + c_0^{-2A-1})Mx e^{-\frac{1}{6}\sqrt{c_0\delta \log x}} + M\Gamma(N + A + 2)\bigg(\frac{48}{c_0 \log x}\bigg)^{N+1}.$$

Proof. Note that the assumed lower bound on x implies that $x \geq e^{2/c_0} > e^{1/c}$. Using Lemma A.10, for any $0 \leq h \leq \frac{x}{2}$ we have

$$A(x) = \frac{1}{h}\int_x^{x+h} A(t)\, dt - \frac{1}{h}\int_x^{x+h}(A(t) - A(x))\, dt$$
$$= \frac{1}{h}\big(\Phi(x+h) - \Phi(x) + O_A\big((\delta^{-A-1} + c_0^{-A})Mx^2 e^{-\frac{1}{2}\sqrt{c\delta \log x}}\big)\big)$$
$$+ O\bigg(\frac{1}{h}\int_x^{x+h}|A(t) - A(x)|\, dt\bigg).$$

Applying Lemmas A.9 and A.12 converts this expression into

$$A(x) = \Phi'(x) + O_A\big(Mh(\log x)^A + (\delta^{-A-1} + c_0^{-A})Mx^2 h^{-1} e^{-\frac{1}{2}\sqrt{c\delta \log x}}\big).$$

With the assumed lower bound on x, each of the quantities $\delta^{-A-1}(\log x)^{-A}$ and $c_0^{-A}(\log x)^{-A}$ is at most $\frac{1}{8}$, which implies that $(\delta^{-A-1} + c_0^{-A})(\log x)^{-A} \leq \frac{1}{4}$. In particular, we may take $h =$

$(\delta^{-A-1} + c_0^{-A})^{1/2} x (\log x)^{-A/2} e^{-\frac{1}{4}\sqrt{c\delta \log x}}$, which is less than $\frac{x}{2}$; we obtain

$$A(x) = \Phi'(x) + O_A\left((\delta^{-A-1} + c_0^{-A})^{1/2} M x (\log x)^{A/2} e^{-\frac{1}{4}\sqrt{c\delta \log x}}\right)$$

$$= x(\log x)^{z-1}\left\{\sum_{k=0}^{N} \frac{\lambda_k(z)}{(\log x)^k} + O_A\left(M\Gamma(N+A+2)\left(\frac{48}{c_0 \log x}\right)^{N+1}\right)\right.$$

$$\left. + O_A\left((\delta^{-A-1} + c_0^{-A})^{1/2} M (\log x)^{3A/2+1} e^{-\frac{1}{4}\sqrt{c\delta \log x}}\right)\right\}$$

$$= x(\log x)^{z-1}\left\{\sum_{k=0}^{N} \frac{\lambda_k(z)}{(\log x)^k} + O_A\left(M\Gamma(N+A+2)\left(\frac{48}{c_0 \log x}\right)^{N+1}\right)\right.$$

$$\left. + O_A\left((\delta^{-A-1} + c_0^{-A})^{1/2} M (c\delta)^{-3A/2-1} e^{-\frac{1}{5}\sqrt{c\delta \log x}}\right)\right\},$$

where the middle equality is from Lemma A.11 and the last equality is a simple calculus exercise. The theorem now follows from the fact that $\frac{1}{5}\sqrt{c} = \frac{1}{5}\sqrt{\frac{47}{48}c_0} > \frac{1}{6}\sqrt{c_0}$. □

Corollary A.14. *Let z be a complex number with $|z| \leq 1$, and let c_0 and M be positive real numbers with $c_0 \leq \frac{2}{11}$. Let $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ be a Dirichlet series with nonnegative coefficients that has the property $\mathcal{P}(z; c_0, \frac{1}{2}, M)$ as in Definition A.4. Then, uniformly for $x \geq e^{16/c_0}$,*

$$\sum_{n \leq x} a_n = x(\log x)^{z-1}\left(\lambda_0(z) + O(MR_0(x))\right),$$

where

$$\lambda_0(z) = \frac{G(1;z)}{\Gamma(z)} = \frac{1}{\Gamma(z)} \lim_{s \to 1} F(s)\zeta(s)^{-z}$$

and

$$R_0(x) = c_0^{-3}\left(e^{-\frac{1}{9}\sqrt{c_0 \log x}} + (\log x)^{-1}\right).$$

Proof. The fact that the a_n are nonnegative means that $F(s)$ automatically has type $\mathcal{T}(z, z; c_0, \frac{1}{2}, M)$ as per Definition A.6. We take $\delta = \frac{1}{2}$ and $A = 1$ in Theorem A.13, applying it directly with $N = 0$. By equation (A.9), we have simply $\lambda_0(z) = G(1;z)\gamma_0(z)/\Gamma(z)$; but by Definition A.1, $\gamma_0(z) = G(1;z) = 1$ identically, since the residue of the simple pole of $\zeta(s)$ at $s = 1$ equals 1. □

REFERENCES

[1] P. Erdős, C. Pomerance, and E Schmutz. Carmichael's lambda function. *Acta Arith.*, 58(4):363–385, 1991.
[2] K. Ford, F. Luca, and P. 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] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.
[4] M. J. Mossinghoff and T. S. Trudgian. Nonnegative trigonometric polynomials and a zero-free region for the Riemann zeta-function. *J. Number Theory*, 157:329–349, 2015.

[5] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[6] B. K. Spearman and K. S. Williams. Values of the Euler phi function not divisible by a given odd prime. *Ark. Mat.*, 44(1):166–181, 2006.

[7] G. 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.

[8] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, BAHEN CENTRE, 40 ST. GEORGE ST., ROOM 6290, TORONTO, ONTARIO, CANADA M5S 2E4

E-mail address: bchang@math.toronto.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, ROOM 121, 1984 MATHEMATICS ROAD, VANCOUVER, BC, CANADA V6T 1Z2

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