

# THE TYPICAL ELASTICITY OF A QUADRATIC ORDER

KAI (STEVE) FAN AND PAUL POLLACK

ABSTRACT. For an atomic domain  $D$ , the *elasticity*  $\rho(D)$  of  $D$  is defined as  $\sup\{r/s : \pi_1 \cdots \pi_r = \rho_1 \cdots \rho_s, \text{ where each } \pi_i, \rho_j \text{ is irreducible}\}$ ; the elasticity provides a concrete measure of the failure of unique factorization in  $D$ . Fix a quadratic number field  $K$  with discriminant  $\Delta_K$ , and for each positive integer  $f$ , let  $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$  denote the order of conductor  $f$  in  $K$ . Results of Halter-Koch imply that  $\mathcal{O}_f$  has finite elasticity precisely when  $f$  is *split-free*, meaning not divisible by any rational prime  $p$  with  $(\Delta_K/p) = 1$ . When  $K$  is imaginary, we show that for almost all split-free  $f$ ,

$$\rho(\mathcal{O}_f) = f/(\log f)^{\frac{1}{2} \log \log \log f + \frac{1}{2} C_K + o(1)},$$

for a constant  $C_K$  depending on  $K$ . When  $K$  is real, we prove under the assumption of the Generalized Riemann Hypothesis that

$$\rho(\mathcal{O}_f) = (\log f)^{\frac{1}{2} + o(1)}$$

for almost all split-free  $f$ . Underlying these estimates are new statistical theorems about class groups of orders in quadratic fields, whose proofs borrow ideas from investigations of Erdős, Hooley, Li, Pomerance, Schmutz, and others into the multiplicative groups  $(\mathbb{Z}/m\mathbb{Z})^\times$ . One novelty of the argument is the development of a weighted version of the Turán–Kubilius inequality to handle a variety of sums over split-free integers.

## 1. INTRODUCTION

Let  $K$  be a number field. It was realized in the 19th century that the ring of integers  $\mathcal{O}_K$  of  $K$  may fail to be a unique factorization domain. In such cases, Dedekind showed that unique factorization is restored by looking at ideals of  $\mathcal{O}_K$  rather than elements. From this ideal-theoretic perspective, the failure of elementwise unique factorization is due to the principal ideals failing to “fill out” the space of all ideals, with the deficit captured concretely by the class group  $\text{Cl}(\mathcal{O}_K)$  of  $K$ . The finiteness of the class group can be interpreted as stating that  $\mathcal{O}_K$  is always “a finite distance away” from possessing unique factorization.

The term “distance” is used informally here, but it is reasonable to wonder whether it can be made precise. Is there a nonnegative real number we can assign to a domain  $D$  measuring the failure of unique factorization? If  $D = \mathcal{O}_K$ , one natural candidate is the class number  $h_K$  of  $K$ . But there is an alternative and in some ways more appealing candidate for such a measure, foreshadowed in work of Carlitz [2] and discussed explicitly by Valenza [30],<sup>1</sup> Steffan [28], and Narkiewicz [19]. Let  $D$  be an atomic domain, meaning an integral domain in which each nonzero nonunit possesses a factorization into irreducible elements. Following Valenza, the *elasticity*  $\rho(D)$  of  $D$  is defined by

$$\rho(D) = \sup \left\{ \frac{r}{s} : \pi_1 \cdots \pi_r = \rho_1 \cdots \rho_s, \text{ all } \pi_i, \rho_j \text{ irreducible} \right\}.$$

That is, we consider all coincidences between a product of  $r$  irreducibles and a product of  $s$  irreducibles, and we take the supremum of the ratios  $\frac{r}{s}$ . For example,  $\rho(D) = 1$  if and only if the

---

2020 *Mathematics Subject Classification*. Primary 11R27; Secondary 11N25, 11N37, 11R11, 11R65, 13A05.

<sup>1</sup>While Valenza’s paper did not appear until 1990, it was submitted in 1980!

*length* of a factorization into irreducibles (length meaning the number of factors in the product) is uniquely determined by the element being factored. In this case,  $D$  is called a *half-factorial domain* or HFD.

A beautiful theorem of Valenza, Steffan, and Narkiewicz (op. cit.) explicitly determines the elasticity of  $\rho(\mathcal{O}_K)$  for every number field  $K$ . Let  $G$  be a finite abelian group, written multiplicatively with identity element 1. Call a finite sequence  $g_1, \dots, g_n$  of elements of  $G$  a *1-product sequence* if  $g_1 \cdots g_n = 1$ . Say  $g_1, \dots, g_n$  is *1-product-free* if no nonempty subsequence of  $g_1, \dots, g_n$  is a 1-product sequence. The *Davenport constant*  $\text{Dav } G$  of  $G$  is the largest integer  $D$  for which there is a 1-product sequence  $g_1, \dots, g_D$  with no nonempty, proper 1-product subsequence. It is straightforward to show that  $\text{Dav } G$  is finite (in fact, that  $\text{Dav } G \leq \#G$ ) and that  $(\text{Dav } G) - 1$  is the length of the longest 1-product-free sequence of elements of  $G$ . (See, for instance, [8, Lemma 1.4.9].) Valenza, Narkiewicz, and Steffan's elegant result asserts that

$$\rho(\mathcal{O}_K) = \max \left\{ 1, \frac{1}{2} \text{Dav Cl}(\mathcal{O}_K) \right\}.$$

A particularly attractive corollary is that  $\mathcal{O}_K$  is half-factorial precisely when  $h_K \leq 2$ . This special case of the Valenza–Steffan–Narkiewicz theorem was already shown by Carlitz in 1960 [2].

It is of great interest to understand the extent to which unique factorization in  $\mathcal{O}_K$  fails as  $K$  varies across a family of number fields. For the collection of quadratic fields  $K$ , such questions can be seen as implicit in Gauss's *Disquisitiones* (couched in the language of binary quadratic forms). Two hundred years post-*Disquisitiones*, such problems continue to elude us. To mention one concrete instantiation of our ignorance, though it is universally believed that there are infinitely many real quadratic fields of class number 1, we cannot yet disprove that the class numbers of real quadratic fields tend to infinity with the discriminant.

In this paper we consider a natural-seeming orthogonal family of problems. Specifically, we fix a quadratic field  $K$  with discriminant  $\Delta$  and examine the factorization behavior as we range over all orders inside  $K$ . Here an *order* in  $K$  is a subring of  $\mathcal{O}_K$  strictly containing  $\mathbb{Z}$ .<sup>2</sup> Orders in a quadratic field are parametrized by the positive integers in a natural way: For each  $f \in \mathbb{N}$ , there is a unique order  $\mathcal{O}_f$  with index  $[\mathcal{O}_K : \mathcal{O}_f] = f$ , namely  $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ ; that is,

$$\mathcal{O}_f = \{ \alpha \in \mathcal{O}_K : \alpha \equiv a \pmod{f\mathcal{O}_K} \text{ for some } a \in \mathbb{Z} \}.$$

Furthermore, every order  $\mathcal{O}$  is one of the  $\mathcal{O}_f$ , with the maximal order  $\mathcal{O}_K = \mathcal{O}_1$ . The integer  $f$  is referred to as the *conductor* of  $\mathcal{O}_f$ .

In the late 1970s, Zaks [33, 34] observed that  $\mathbb{Z}[\sqrt{-3}]$  — the order of conductor 2 in  $\mathbb{Q}(\sqrt{-3})$  — is a half-factorial domain. Later, Halter-Koch [11] and Coykendall [4] wrote down necessary and sufficient algebraic conditions for an order in a quadratic field to be half-factorial. In the same paper [4] of Coykendall, it was shown that  $\mathbb{Z}[\sqrt{-3}]$  is the only half-factorial nonmaximal order in an imaginary quadratic field. The situation for real quadratic fields is more complicated. In [4] it is conjectured that (a) if one varies both the real quadratic field  $K$  and the conductor  $f$ , then  $\mathcal{O}_f$  is a half-factorial domain infinitely often, and (b) (stronger) fixing  $K = \mathbb{Q}(\sqrt{2})$  and varying only  $f$ , one still finds infinitely many half-factorial orders.

<sup>2</sup>For not-necessarily-quadratic number fields  $K$ , one needs a more complicated definition: An *order in  $K$*  is a subring of  $\mathcal{O}_K$  containing a  $\mathbb{Q}$ -basis for  $K$ .

In [22], Pollack proved form (a) of Coykendall’s conjecture. The stronger form (b) is shown subject to the assumption of the Generalized Riemann Hypothesis (GRH).<sup>3</sup> Both arguments rely on analogues of methods initially introduced to study Artin’s primitive conjecture. Some results of [22] are extended in [23]. For instance, it is proved in [23] — still assuming GRH — that every element of  $\mathcal{E} := \{1, \frac{3}{2}, 2, \frac{5}{2}, 3, \frac{7}{2}, \dots\} \cup \{\infty\}$  is the elasticity of infinitely many orders of  $\mathbb{Q}(\sqrt{2})$ . As follows from Lemma 2.2 below, an order in a quadratic field always has an elasticity belonging to  $\mathcal{E}$ , so that  $\mathbb{Z}[\sqrt{2}]$  is extremal in a natural sense.

The orders constructed in [22] and [23] are quite special. For instance, each of their conductors is composed of at most two distinct primes. In this paper we investigate elasticities corresponding to general conductors  $f$ .

Some care is needed to decide what “general” should mean. As already mentioned, the elasticity of a quadratic order may be infinite. In [12, Corollary 4], Halter-Koch shows that if  $\mathcal{O}$  is an order in a number field  $K$ , then  $\rho(\mathcal{O}) < \infty$  precisely when every nonzero prime ideal of  $\mathcal{O}$  lies below a unique prime ideal of  $\mathcal{O}_K$ . Placed in the setting of quadratic fields  $K$ , Halter-Koch’s theorem says that  $\rho(\mathcal{O}_f) < \infty$  precisely when  $f$  is *split-free*, meaning not divisible by any prime  $p$  that splits (completely) in  $K$  (cf. the proof of [23, Theorem 1.1]).

The Selberg–Delange method [29, Theorems II.5.2, II.5.4], [15, Theorem 13.2] (or a mean value theorem of the type discussed in [18]) shows that the split-free numbers have a counting function asymptotic to a certain constant multiple of  $x/\sqrt{\log x}$ . In particular, the split-free numbers  $f$  make up a set of density zero. Thus, if one fixes a quadratic field  $K$ , then  $\rho(\mathcal{O}_f) = \infty$  for asymptotically 100% of conductors  $f$ . This suggests that the proper object of study is not the arithmetic function  $\rho(\mathcal{O}_f)$ , but the corresponding function restricted to split-free  $f$ . Our main theorems address the almost-everywhere behavior of this restricted function.

First, we deal with imaginary quadratic orders. Let

$$\mathcal{D} := \{-4, \pm 8\} \cup \left\{ (-1)^{\frac{p-1}{2}} p : p > 2 \text{ is prime} \right\}. \quad (1)$$

Every discriminant of a quadratic field has a unique expression as a product of elements of  $\mathcal{D}$ .

**Theorem 1.1.** *If  $K$  is a fixed imaginary quadratic field with discriminant  $\Delta$ , then for almost all split-free  $f$ ,*

$$\rho(\mathcal{O}_f) = f / (\log f)^{\frac{1}{2} \log_3 f + \frac{1}{2} C_K + O((\log_4 f)^3 / \log_3 f)}, \quad (2)$$

where  $\log_k$  denotes the  $k$ th iterate of the natural logarithm, and

$$C_K := \sum_{p>2} \frac{\log p}{(p-1)^2} - 1 - \frac{\operatorname{sgn}(\Delta) 1_{\mathcal{D}}(\Delta) |\Delta| \log \operatorname{Rad}(|\Delta|)}{\varphi(|\Delta|)^2}.$$

“Almost all”, here and below, means that the estimate holds for all but  $o(x/\sqrt{\log x})$  split-free numbers  $f \leq x$ , as  $x \rightarrow \infty$ . (When an  $O$  appears in the estimate, as is the case here, we are asserting all of this happens for some choice of implied constant.) In what follows, in place of “almost all”, we sometimes use the term “typically” or the phrases “almost always” or “for a typical  $f$ ”. It is to be understood that  $f$  is restricted to split-free numbers.

---

<sup>3</sup>Throughout the paper, GRH refers to the Riemann Hypothesis for Dedekind zeta functions.

For real quadratic orders, we are again able to determine the typical elasticity to within a factor of  $(\log f)^{o(1)}$ , but this time we need to assume GRH. The answer is quite a bit smaller than in the imaginary case.

**Theorem 1.2** (conditional on GRH). *If  $K$  is a fixed real quadratic field, then for almost all split-free  $f$ ,*

$$\rho(\mathcal{O}_f) = (\log f)^{\frac{1}{2} + O(1/\log_4 f)}.$$

In addition to the typical size of  $\rho(\mathcal{O}_f)$ , it would seem natural to also investigate its maximal and minimal orders (restricted to split-free  $f$ ) as well as its average order. Some of these problems seem attackable by combining ideas of Erdős–Pomerance–Schmutz [5] with the technology developed in the present paper. We hope to revisit these questions on a future occasion.

We now turn to discussing the main ideas needed to establish Theorems 1.1 and 1.2. In §2, these results are shown to follow from two key propositions, whose proofs occupy §§3–7.

## 2. THEOREMS 1 AND 2: THE BIG PICTURE

For each positive integer  $f$ , let  $I_K(f)$  denote the group of fractional ideals of  $K$  generated by integral ideals comaximal with  $f\mathcal{O}_K$ . We let  $P_{K,\mathbb{Z}}(f)$  denote the subgroup of  $I_K(f)$  generated by principal ideals  $\alpha\mathcal{O}_K$ , where  $\alpha \equiv a \pmod{f\mathcal{O}_K}$  for some rational integer  $a$  with  $\gcd(a, f) = 1$ . Then the *class group*  $\text{Cl}(\mathcal{O}_f)$  of the order  $\mathcal{O}_f$  is defined to be the quotient  $I_K(f)/P_{K,\mathbb{Z}}(f)$ . When  $f = 1$ , we will write  $I_K$  instead of  $I_K(1)$  and  $P_K$  instead of  $P_{K,\mathbb{Z}}(1)$ . Then  $I_K$  (resp.  $P_K$ ) is the group of all fractional (resp. principal fractional) ideals, and the quotient  $I_K/P_K$  is the usual class group  $\text{Cl}(\mathcal{O}_K)$  of the number field  $K$ .

**2.1. Elasticity in terms of Davenport constants.** Theorems 1.1 and 1.2 are consequences of statistical theorems we establish for the associated class groups. Our starting point is the following lemma, which relates the elasticity  $\rho(\mathcal{O}_f)$  to the Davenport constant  $\text{Dav Cl}(\mathcal{O}_f)$ .

**Lemma 2.1.** *For each split-free  $f$ ,*

$$\frac{1}{2} \text{Dav Cl}(\mathcal{O}_f) \leq \rho(\mathcal{O}_f) \leq \max \left\{ \frac{1}{2} \text{Dav Cl}(\mathcal{O}_f) + \frac{3}{2} \Omega(f), 1 \right\}.$$

It will emerge from our later arguments that for any fixed quadratic field  $K$ , the quantity  $\Omega(f)$  is typically of a smaller order than  $\text{Dav Cl}(\mathcal{O}_f)$ . Hence,  $\rho(\mathcal{O}_f) \approx \frac{1}{2} \text{Dav Cl}(\mathcal{O}_f)$  most of the time.

The proof of Lemma 2.1 requires some preparation. Lemma 2.2 first appeared as [23, Lemma 2.2]. Proposition 2.3 is a classical result of Weber [32]; a modern reference is Corollary 2.11.16 on p. 159 of [8]. For the statement of the next result, recall that  $\Omega(f)$  denotes the number of prime divisors of  $f$ , counted with multiplicity. For example,  $\Omega(30) = \Omega(-27) = 3$ .

**Lemma 2.2.** *For each natural number  $f$ ,*

$$\rho(\mathcal{O}_f) = \frac{1}{2} \sup \{ \Omega(\text{Nm}_{K/\mathbb{Q}} \pi) : \pi \text{ an irreducible element of } \mathcal{O}_f \}.$$

**Proposition 2.3.** *Let  $f \in \mathbb{N}$ . Every class in  $\text{Cl}(\mathcal{O}_f)$  is represented by infinitely many prime ideals of  $\mathcal{O}_K$ .*

Our argument for Lemma 2.1 also depends on the following simple but useful observation: Suppose  $\alpha, \beta \in \mathcal{O}_f$  and that  $\alpha$  divides  $\beta$  in the ring  $\mathcal{O}_K$ . Choose  $a \in \mathbb{Z}$  with  $\alpha \equiv a \pmod{f\mathcal{O}_K}$ , and suppose that  $\gcd(a, f) = 1$ . (This coprimality condition is equivalent to the comaximality of  $\alpha\mathcal{O}_K$  and  $f\mathcal{O}_K$ .) Then  $\alpha$  divides  $\beta$  in  $\mathcal{O}_f$ . To see this, say that  $\beta \equiv b \pmod{f\mathcal{O}_K}$ . Write  $\beta = \alpha\gamma$ , where  $\gamma \in \mathcal{O}_K$ . Then  $b \equiv a\gamma \pmod{f\mathcal{O}_K}$ . Multiplying both sides by an integer  $\bar{a}$  that inverts  $a \pmod{f}$  shows that  $\gamma \equiv b\bar{a} \pmod{f\mathcal{O}_K}$ , so that  $\gamma \in \mathcal{O}_f$ .

*Proof of Lemma 2.1.* For notational convenience, let  $D = \text{Dav Cl}(\mathcal{O}_f)$ .

We begin with the lower bound half of Lemma 2.1. Using Proposition 2.3, choose prime ideals  $P_1, P_2, \dots, P_D$ , comaximal with  $f\mathcal{O}_K$ , such that the product  $P_1 \cdots P_D$  represents the identity in  $\text{Cl}(\mathcal{O}_f)$  and no nonempty, proper subproduct of  $P_1, \dots, P_D$  represents the identity. Write  $P_1 \cdots P_D = \pi\mathcal{O}_K$ , where  $\pi \in \mathcal{O}_f$ . Then  $\pi$  is irreducible in  $\mathcal{O}_f$ . Otherwise,  $\pi = \alpha\beta$  for  $\alpha, \beta$  nonunits in  $\mathcal{O}_f$  and, after rearranging the  $P_i$ , we have  $\alpha\mathcal{O}_K = P_1 \cdots P_d$  for some  $1 \leq d < D$ . But then  $P_1 \cdots P_d$  represents the identity in  $\text{Cl}(\mathcal{O}_f)$ , contrary to the choice of  $D$ . Invoking Lemma 2.1,

$$\rho(\mathcal{O}_f) \geq \frac{1}{2}\Omega(\text{Nm}_{K/\mathbb{Q}} \pi) = \frac{1}{2}\Omega\left(\prod_{i=1}^D \text{Nm}(P_i)\right) \geq \frac{1}{2}D.$$

For the upper bound, we let  $\pi$  be an arbitrary irreducible element of  $\mathcal{O}_f$  and proceed to bound  $\Omega(\text{Nm} \pi)$ . Write

$$\pi\mathcal{O}_K = \prod_{i=1}^g P_i \prod_{j=1}^h Q_j^{e_j}, \quad (3)$$

where the  $P_i$  are prime ideals of  $\mathcal{O}_K$  comaximal with  $f\mathcal{O}_K$  and  $Q_1, \dots, Q_h$  are prime ideals containing  $f\mathcal{O}_K$ .

Suppose to start with that some  $P_i$  has degree 2. Then  $P_i = p_i\mathcal{O}_K$  for an inert prime  $p_i$  not dividing  $f$ . Since  $p_i$  divides  $\pi$  in  $\mathcal{O}_K$ , the observation preceding the proof shows that  $p_i$  divides  $\pi$  in  $\mathcal{O}_f$ . Hence,  $\pi$  is a unit multiple of  $p_i$ , we have  $\text{Nm}_{K/\mathbb{Q}}(\pi) = p_i^2$ , and

$$\frac{1}{2}\Omega(\text{Nm}_{K/\mathbb{Q}} \pi) = 1. \quad (4)$$

For the rest of the proof, we suppose that each  $P_i$  has degree 1. We proceed to bound  $g$  and the exponents  $e_1, \dots, e_h$  appearing in (3).

We must have  $g \leq D$ : If  $g > D$ , select a subsequence of  $P_1, \dots, P_D$  multiplying to  $\alpha\mathcal{O}_K$  for some  $\alpha \in \mathcal{O}_f$ . Then  $\alpha$  divides  $\pi$  in  $\mathcal{O}_K$  and  $\alpha\mathcal{O}_K$  and  $f\mathcal{O}_K$  are comaximal. Hence,  $\alpha$  divides  $\pi$  in  $\mathcal{O}_f$ . Since  $\pi$  is irreducible,  $\pi$  is a unit multiple of  $\alpha$ , contradicting that  $\frac{\pi}{\alpha}$  is contained in  $P_g$ .

Now let  $Q$  be one of the  $Q_j$ , and let  $e$  be the corresponding  $e_j$ . Let  $q$  be the rational prime lying below  $Q$ . Since  $f$  is split-free,  $Q$  is the *unique* prime of  $\mathcal{O}_K$  lying above  $q$ .

We consider first the case that  $q$  is inert, so that  $q\mathcal{O}_K = Q$ . If  $e \geq v_q(f) + 1$ , we argue that the equation

$$\pi = q \cdot \frac{\pi}{q} \quad (5)$$

exhibits a nontrivial factorization of  $\pi$  over  $\mathcal{O}_f$ , contradicting the irreducibility of  $\pi$ . Both right-hand factors in (5) are nonunits in  $\mathcal{O}_K$ , so it suffices to show that  $\frac{\pi}{q} \in \mathcal{O}_f$ . Write  $f = q^v f'$ , where  $v = v_q(f)$  and  $q \nmid f'$ . Since  $\pi \in \mathcal{O}_f$ , there is a rational integer  $u$  with  $\pi \equiv u \pmod{f\mathcal{O}_K}$ .

Then  $q \frac{\pi}{q} = \pi \equiv u \pmod{f'}$ . Hence, if  $\bar{q} \in \mathbb{Z}$  inverts  $q \pmod{f}$ , we have  $\frac{\pi}{q} \equiv u\bar{q} \pmod{f'\mathcal{O}_K}$ . It follows that  $\frac{\pi}{q} \in \mathcal{O}_{f'}$ . If  $e \geq v + 1$ , we also have  $\frac{\pi}{q} \equiv 0 \pmod{q^v\mathcal{O}_K}$ , so that  $\frac{\pi}{q} \in \mathcal{O}_{q^v}$ . Therefore,  $\frac{\pi}{q} \in \mathcal{O}_{f'} \cap \mathcal{O}_{q^v} = \mathcal{O}_f$ .

If  $q$  is ramified, then  $q\mathcal{O}_K = Q^2$ . In this case, an entirely analogous argument to that of the last paragraph shows that (5) contradicts the irreducibility of  $\pi$  if  $e \geq 2(v_q(f) + 1)$ .

Collecting our bounds,

$$\begin{aligned} \Omega(N\pi) &= \sum_{i=1}^g \Omega(\text{Nm } P_i) + \sum_{\substack{1 \leq j \leq h \\ Q_j \text{ inert}}} e_j \cdot \Omega(\text{Nm } Q_j) + \sum_{\substack{1 \leq j \leq h \\ Q_j \text{ ramified}}} e_j \cdot \Omega(\text{Nm } Q_j) \\ &\leq g + \sum_{\substack{1 \leq j \leq h \\ Q_j \text{ inert}}} 2v_{q_j}(f) + \sum_{\substack{1 \leq j \leq h \\ Q_j \text{ ramified}}} (2v_{q_j}(f) + 1) \\ &\leq \text{Dav } \mathcal{O}_f + 3 \sum_{1 \leq j \leq h} v_{q_j}(f) \\ &= \text{Dav } \mathcal{O}_f + 3\Omega(f). \end{aligned}$$

(Here and below,  $v_q$  is the usual  $q$ -adic valuation.) Hence,

$$\frac{1}{2}\Omega(\text{Nm}_{K/\mathbb{Q}} \pi) \leq \frac{1}{2}\text{Dav}(\mathcal{O}_f) + \frac{3}{2}\Omega(f). \quad (6)$$

Lemma 2.1 follows from (4), (6), and Lemma 2.2.  $\square$

**2.2. The principal subgroup  $\text{PrinCl}(\mathcal{O}_f)$  as a proxy for  $\text{Cl}(\mathcal{O}_f)$ .** For our purposes, rather than directly analyze  $\text{Cl}(\mathcal{O}_f)$  it is more convenient to work with the group

$$\text{PrinCl}(\mathcal{O}_f) := (\mathcal{O}_K/f\mathcal{O}_K)^\times / \langle \text{images of integers prime to } f, \text{ units of } \mathcal{O}_K \rangle.$$

We can, and will, identify  $\text{PrinCl}(\mathcal{O}_f)$  with the subgroup  $(I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f)$  of  $I_K(f)/P_{K,\mathbb{Z}}(f) = \text{Cl}(\mathcal{O}_f)$ , with the identification prescribed by the exact sequence

$$(\mathbb{Z}/f\mathbb{Z})^\times \times \mathcal{O}_K^\times \xrightarrow{\mu} (\mathcal{O}_K/f\mathcal{O}_K)^\times \xrightarrow{\iota} (I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f) \longrightarrow 1;$$

here  $\mu((a \bmod f\mathbb{Z}, \eta)) := a\eta \bmod f\mathcal{O}_K$  and  $\iota(\alpha \bmod f\mathcal{O}_K) := [\alpha\mathcal{O}_K]$ . We think of  $\text{PrinCl}(\mathcal{O}_f)$  as the ‘‘principal subgroup’’ of the class group of  $\mathcal{O}_f$ .

$\text{PrinCl}(\mathcal{O}_f)$  fits into the exact sequence

$$\begin{array}{ccccccc} 1 & \longrightarrow & (I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f) & \longrightarrow & I_K(f)/P_{K,\mathbb{Z}}(f) & \longrightarrow & I_K/P_K \longrightarrow 1. \\ & & \parallel & & \parallel & & \parallel \\ & & \text{PrinCl}(\mathcal{O}_f) & & \text{Cl}(\mathcal{O}_f) & & \text{Cl}(\mathcal{O}_K) \end{array}$$

(The maps here are the obvious ones. To show exactness at the last position, one needs that every ideal class in  $\mathcal{O}_K$  has a representative comaximal with  $f\mathcal{O}_K$ ; this is immediate from Proposition 2.3, although easier arguments are also possible.) Hence,  $\text{PrinCl}(\mathcal{O}_f)$  has index  $h_K := \#\text{Cl}(\mathcal{O}_K)$  when viewed as a subgroup of  $\text{Cl}(\mathcal{O}_f)$ . Now we are always working with a fixed quadratic field  $K$ . The following easy lemma will guarantee that, at the level of precision we are aiming for, there is no harm in working with  $\text{PrinCl}(\mathcal{O}_f)$  in place of  $\text{Cl}(\mathcal{O}_f)$ .

**Lemma 2.4.** *Let  $G$  be a finite abelian group, and let  $H$  be a subgroup of  $G$ . Then*

$$\max\{\text{Dav}(H), \text{Dav}(G/H)\} \leq \text{Dav}(G) \leq \text{Dav}(H) \text{Dav}(G/H). \quad (7)$$

As a consequence of Lemma 2.4,

$$\text{Dav PrinCl}(\mathcal{O}_f) \leq \text{Dav Cl}(\mathcal{O}_f) \leq h_K \text{Dav PrinCl}(\mathcal{O}_f). \quad (8)$$

*Proof of Lemma 2.4.* The first inequality in (7) is clear, as a 1-product-free sequence in  $H$  or in  $G/H$  corresponds to a 1-product-free sequence in  $G$  of the same length. Turning to the second inequality, we argue that a sequence  $g_1, \dots, g_{\text{Dav}(H)\text{Dav}(G/H)}$  in  $G$  is never 1-product-free. Split the sequence into  $\text{Dav}(H)$  blocks of  $\text{Dav}(G/H)$  terms. Each block contains a nonempty subsequence multiplying to the identity in  $G/H$  — that is, a subsequence whose product belongs to  $H$ . List these products as  $h_1, \dots, h_{\text{Dav}(H)}$ . Then some subsequence of  $h_1, \dots, h_{\text{Dav}(H)}$  multiplies to 1. Rewriting each  $h_j$  as a product of terms from a certain block of the  $g_i$  yields a 1-product subsequence of  $g_1, \dots, g_{\text{Dav}(H)\text{Dav}(G/H)}$ .  $\square$

**2.3. The pre-class group and two key propositions.** We will study  $\text{PrinCl}(\mathcal{O}_f)$  by viewing it as a quotient of a yet-simpler object, termed the *pre-class group*, defined by

$$\text{PreCl}(\mathcal{O}_f) = (\mathcal{O}_K/f\mathcal{O}_K)^\times / \langle \text{images of integers prime to } f \rangle.$$

Comparing the definitions of  $\text{PrinCl}(\mathcal{O}_f)$  and  $\text{PreCl}(\mathcal{O}_f)$ , we see that the former is obtained from the latter upon quotienting by the images of units of  $\mathcal{O}_K$ . Our arguments ultimately depend on the groups  $\text{PreCl}(\mathcal{O}_f)$  being close cousins of the more familiar multiplicative groups  $(\mathbb{Z}/m\mathbb{Z})^\times$ .

To set up the analogy, we begin by computing the order of  $\text{PreCl}(\mathcal{O}_f)$  for split-free  $f$ . By the Chinese Remainder Theorem,  $\text{PreCl}(\mathcal{O}_f) \cong \prod_{p^k \parallel f} \text{PreCl}(\mathcal{O}_{p^k})$ . If  $p$  is inert, then

$$\#\text{PreCl}(\mathcal{O}_{p^k}) = \frac{(\#\mathcal{O}_K/(p\mathcal{O}_K)^k)^\times}{\#(\mathbb{Z}/p^k\mathbb{Z})^\times} = \frac{\text{Nm}((p\mathcal{O}_K)^k) - \text{Nm}((p\mathcal{O}_K)^{k-1})}{p^k - p^{k-1}} = p^k + p^{k-1}.$$

If  $p$  is ramified, with  $p\mathcal{O}_K = P^2$ , then

$$\#\text{PreCl}(\mathcal{O}_{p^k}) = \frac{(\#\mathcal{O}_K/P^{2k})^\times}{\#(\mathbb{Z}/p^k\mathbb{Z})^\times} = \frac{\text{Nm}(P^{2k}) - \text{Nm}(P^{2k-1})}{p^k - p^{k-1}} = p^k.$$

Hence,  $\#\text{PreCl}(\mathcal{O}_f) = \psi(f)$ , where  $\psi$  is the multiplicative function whose values at prime powers are given by  $\psi(p^k) = p^k(1 - \frac{1}{p}(\frac{\Delta}{p}))$ . This is of course reminiscent of Euler's classical formula  $\varphi(m) = \prod_{p^k \parallel m} p^k(1 - \frac{1}{p})$  for the order of  $(\mathbb{Z}/m\mathbb{Z})^\times$ .

An important invariant of the group  $(\mathbb{Z}/m\mathbb{Z})^\times$  is its exponent, denoted  $\lambda(m)$ . While typically referred to as *Carmichael's lambda-function*, the study of  $\lambda(m)$  goes back to Gauss. In fact, already in the *Disquisitiones*, one can read the result that  $\lambda(m)$  is the least common multiple of the numbers  $\varphi(p^k)$  for the prime powers  $p^k \parallel m$ , with the caveat that if  $p = 2$  and  $k \geq 3$  one should replace  $\varphi(2^k)$  with  $\frac{1}{2}\varphi(2^k)$ .

To prove Theorems 1.1 and 1.2, we will need to understand how the exponents of  $\text{Cl}(\mathcal{O}_f)$  are distributed. We begin by establishing a (partial) analogue of Gauss's formula. We get this going with the observation that  $\text{Exp PreCl}(\mathcal{O}_f) = \text{lcm}\{\text{Exp PreCl}\mathcal{O}_{p^k} : p^k \parallel f\}$ . The next lemma, due essentially to Halter-Koch, determines almost all of the exponents  $\text{Exp PreCl}(\mathcal{O}_{p^k})$ .

**Lemma 2.5.** *If  $p > 3$ , and  $p$  is inert or ramified in  $K$ , then  $\text{PreCl}(\mathcal{O}_{p^k})$  is cyclic.*

*Proof.* Write  $K = \mathbb{Q}(\sqrt{D})$ , where  $D$  is a squarefree integer.

Suppose first that  $p$  is inert in  $K$ . By results of Halter-Koch, summarized in the table on p. 77 of [10],  $(\mathcal{O}_K/p^k\mathcal{O}_K)^\times$  is generated by (the images of)  $w$ ,  $1 + p$ , and  $1 + p\sqrt{D}$ , of respective orders  $p^2 - 1$ ,  $p^{k-1}$ , and  $p^{k-1}$ . Here  $w$  (denoted  $w_s$  in [10]) is an element of  $\mathcal{O}_K$  comaximal with  $p\mathcal{O}_K$  whose precise definition does not concern us here (see [10, p. 75]). Since  $\text{PreCl}(\mathcal{O}_{p^k})$  is a quotient of  $(\mathcal{O}_K/p^k\mathcal{O}_K)^\times$  in which  $1 + p$  becomes trivial,  $\text{PreCl}(\mathcal{O}_{p^k})$  is generated by  $w$  and  $1 + p\sqrt{D}$ , of respective orders dividing  $p^2 - 1$  and  $p^{k-1}$ . But  $p^2 - 1$  and  $p^{k-1}$  are relatively prime. Hence,  $w(1 + p\sqrt{D})$  generates  $\text{PreCl}(\mathcal{O}_{p^k})$ .

The ramified case is similar. Here  $(\mathcal{O}_K/p^k\mathcal{O}_K)^\times$  is generated by three elements  $w$ ,  $1 + p$ , and  $1 + \sqrt{D}$  (same table in [10]). In this case,  $w$  can be chosen as a rational integer that generates  $(\mathbb{Z}/p\mathbb{Z})^\times$ . So both  $w$  and  $1 + p$  become trivial in the quotient defining  $\text{PreCl}(\mathcal{O}_{p^k})$ , implying that  $\text{PreCl}(\mathcal{O}_{p^k})$  is generated by the image of  $1 + \sqrt{D}$ .  $\square$

From Lemma 2.5 and the preceding remarks, if we define  $L(f) := \text{lcm}\{\psi(p^k) : p^k \parallel f\}$  and  $L'(f) := \text{lcm}\{\psi(p^k) : p^k \parallel f, p > 3\}$ , then

$$L'(f) \mid \text{Exp PreCl}(\mathcal{O}_f) \mid L(f) \tag{9}$$

for all split-free numbers  $f$ . The typical behavior of  $\text{Exp PreCl}(\mathcal{O}_f)$  for split-free  $f$  is now determined by our next result, which is the analogue of a theorem proved for Carmichael's  $\lambda$ -function by Erdős, Pomerance, and Schmutz [5, Theorem 2].

**Proposition 2.6.** *For almost all split-free  $f$ ,*

$$L(f) = f / (\log f)^{\frac{1}{2} \log_3 f + \frac{1}{2} C_K + O((\log_4 f)^3 / \log_3 f)}.$$

*The same estimate holds with  $L'(f)$  replacing  $L(f)$ .*

As we explain in the next subsection, our Theorem 1.1 (typical elasticity for imaginary quadratic orders) can be quickly deduced from Proposition 2.6. To prove Theorem 1.2 (concerning real quadratic orders) we must work a bit harder.

Recall that when  $K$  is a real quadratic field, we are using  $\varepsilon$  to denote the fundamental unit of  $K$ , normalized so that  $\varepsilon > 1$ . Then  $\text{PrinCl}(\mathcal{O}_f) \cong \text{PreCl}(\mathcal{O}_f) / \langle \text{image of } \varepsilon \rangle$ . We let  $\ell(f)$  denote the order of  $\varepsilon$  viewed inside  $\text{PreCl}(\mathcal{O}_f)$ , so that

$$\ell(f) = \frac{\#\text{PreCl}(\mathcal{O}_f)}{\#\text{PrinCl}(\mathcal{O}_f)}.$$

Concretely,  $\ell(f)$  can be described as the least positive integer  $\ell$  for which  $\varepsilon^\ell \in \mathcal{O}_f$ .

The next proposition collects various estimates needed in our proof of Theorem 1.2.

**Proposition 2.7** (conditional on GRH). *Let  $K$  be a real quadratic field. For almost all split-free  $f$ ,*

- (a)  $\text{RadExp PrinCl}(\mathcal{O}_f) = (\log f)^{\frac{1}{2} + O(1/\log_4 f)}$ ,
- (b)  $\text{Exp PrinCl}(\mathcal{O}_f) = (\text{RadExp PrinCl}(\mathcal{O}_f)) \cdot (\log f)^{O(1/\log_4 f)}$ ,
- (c)  $L(f)/\ell(f) = (\log f)^{O(1/\log_4 f)}$ .



As with Proposition 2.6, the estimates of Proposition 2.7 take their inspiration from research into the multiplicative groups  $(\mathbb{Z}/m\mathbb{Z})^\times$ . Specifically, we adapt ideas introduced by Pollack in [21] to show that  $\frac{\varphi(m)}{\lambda(m)}$  typically has about  $\frac{\log_2 m}{\log_3 m}$  distinct prime factors. We also draw heavily on methods introduced by Li and Pomerance [16], who do a statistical comparison of  $\lambda(m)$  with  $\ell_a(m)$ , the order of  $a$  (a fixed integer) in  $(\mathbb{Z}/m\mathbb{Z})^\times$ .

**2.4. Proofs of Theorems 1.1 and 1.2, modulo Propositions 2.6 and 2.7.** We now describe how to complete the proofs of Theorems 1.1 and 1.2, taking for granted Propositions 2.6 and 2.7. In addition to the tools already introduced, we rely on known results relating the Davenport constant and the exponent.

**Proposition 2.8.** *For every finite abelian group  $G$ ,*

$$1 \leq \frac{\text{Dav } G}{\text{Exp } G} \leq 1 + \log \frac{\#G}{\text{Exp } G}.$$

The lower bound in Proposition 2.8 is trivial: If  $g$  has order  $\text{Exp } G$ , then  $g, g, \dots, g$  (repeated  $(\text{Exp } G) - 1$  times) is 1-product-free. The nontrivial and elegant upper bound is due to Van Emde Boas and Kruyswijk [31]. A simplified proof can be found in [1].

Now let  $K$  be an imaginary quadratic field. The image  $H$  (say) of  $\mathcal{O}_K^\times$  in  $\text{PreCl}(\mathcal{O}_f)$  has size at most  $\#\mathcal{O}_K^\times \leq 6$ . Identifying  $\text{PrinCl}(\mathcal{O}_f)$  with  $\text{PreCl}(\mathcal{O}_f)/H$ , Lemma 2.4 implies that

$$\frac{\text{Dav PreCl}(\mathcal{O}_f)}{\text{Dav}(H)} \leq \text{Dav PrinCl}(\mathcal{O}_f) \leq \text{Dav PreCl}(\mathcal{O}_f).$$

It is well-known and simple-to-show that the Davenport constant of a group is bounded by the size of the group. Hence,  $\text{Dav } H \leq 6$ , and  $\text{Dav PrinCl}(\mathcal{O}_f)$  is within a factor of 6 of  $\text{Dav PreCl}(\mathcal{O}_f)$ .

Applying Proposition 2.8,

$$1 \leq \frac{\text{Dav PreCl}(\mathcal{O}_f)}{\text{Exp PreCl}(\mathcal{O}_f)} \leq 1 + \log \frac{\psi(f)}{\text{Exp PreCl}(\mathcal{O}_f)}. \quad (10)$$

Notice that  $\psi(f) \leq f \prod_{p|f} (1 + \frac{1}{p}) \ll f \log \log(3f)$ , for all split-free  $f$ . Furthermore, from (9) and Proposition 2.6, we typically have

$$\text{Exp PreCl}(\mathcal{O}_f) = f / (\log f)^{\frac{1}{2} \log_3 f + \frac{1}{2} C_K + O((\log_4 f)^3 / \log_3 f)} \quad (11)$$

Hence,  $\psi(f) / \text{Exp PreCl}(\mathcal{O}_f)$  is typically at most  $(\log f)^{\log_3 f}$ , and  $1 + \log(\psi(f) / \text{Exp PreCl}(\mathcal{O}_f)) \ll \log_2 f \log_3 f$ . Referring back to (10),

$$\text{Dav PreCl}(\mathcal{O}_f) = (\text{Exp PreCl}(\mathcal{O}_f)) \exp(O(\log_3 f)),$$

typically. Plugging in the estimate (11),

$$\text{Dav PreCl}(\mathcal{O}_f) = f / (\log f)^{\frac{1}{2} \log_3 f + \frac{1}{2} C_K + O((\log_4 f)^3 / \log_3 f)},$$

for almost all split-free  $f$ . Our discussion in the last paragraph permits replacing  $\text{PreCl}$  with  $\text{PrinCl}$ , and (8) allows us to replace  $\text{PrinCl}$  with  $\text{Cl}$ . Theorem 1.1 then follows from Lemma 2.1, in view of the trivial upper bound  $\Omega(f) \leq \frac{\log f}{\log 2}$ .

Turning to Theorem 1.2, suppose that  $K$  is real quadratic. By Proposition 2.7(a,b),

$$\text{Exp PrinCl}(\mathcal{O}_f) = (\log f)^{\frac{1}{2} + O(1/\log_4 f)} \quad (12)$$

for almost all split-free  $f$ . Furthermore,

$$\frac{\#\text{PrinCl}(\mathcal{O}_f)}{\text{Exp PrinCl}(\mathcal{O}_f)} \leq \#\text{PrinCl}(\mathcal{O}_f) = \frac{\psi(f)}{\ell(f)} = \frac{\psi(f)}{L(f)} \frac{L(f)}{\ell(f)} \leq (\log f)^{\log_3 f},$$

typically. For the final inequality we used Proposition 2.6 and Proposition 2.7(c). Invoking Proposition 2.8,

$$\text{Dav PrinCl}(\mathcal{O}_f) = (\text{Exp PrinCl}(\mathcal{O}_f)) \exp(O(\log_3 f)),$$

almost always. Substituting in the estimate of (12), we see that typically

$$\text{Dav PrinCl}(\mathcal{O}_f) = (\log f)^{\frac{1}{2} + O(1/\log_4 f)}.$$

Owing to (8), the same estimate holds with PrinCl replaced by Cl. Theorem 1.2 now follows from Lemma 2.1, since the count of all positive integers  $f \leq x$  with  $\Omega(f) > 10 \log \log f$  (say) is  $\ll x/\log x = o(S_\alpha(x))$ . (This last estimate follows from well-known results on the distribution of numbers with many prime factors; see for instance [9, Exercise 08] or [17, Lemma 13]. To apply the estimates as stated there, treat separately the cases when  $f \leq \sqrt{x}$  and  $\sqrt{x} < f \leq x$ .)

**What lies ahead.** The rest of the paper is organized as follows. In §3, we establish a variant of the Turán–Kubilius inequality result for additive functions appearing with multiplicative weights. In §4 we prove the key Proposition 2.6. There our weighted Turán–Kubilius inequality, with weight function  $1_{\text{split-free}}$ , plays an important role. Section 5 is something of a waypoint. There we show that  $\text{Rad} \frac{\psi(f)}{L(f)}$  is typically of size  $\approx (\log f)^{1/2}$ . It will turn out that  $\text{Rad} \frac{\psi(f)}{L(f)}$  is a reasonable approximation to  $\text{Exp PreCl}(\mathcal{O}_f)$  (typically, and assuming GRH). To connect those two quantities requires us to relate  $L(f)$  and  $\ell(f)$ , for typical  $f$ . In §6 we set up the algebraic framework needed to carry out this comparison. In §7 we present the details; this work, supplemented by various ‘anatomical’ arguments, allows us to complete the proof of the key Proposition 2.7.

### 3. A WEIGHTED TURÁN–KUBILIUS INEQUALITY

An important tool for studying the normal order of an additive function is the Turán–Kubilius inequality. Let  $f: \mathbb{N} \rightarrow \mathbb{C}$  be an additive function. It is often reasonable to think of the mean value of  $f$  as a good candidate for its normal order. Since the mean value of  $f$  over  $[1, x]$  is

$$\frac{1}{x} \sum_{n \leq x} f(n) = \frac{1}{x} \sum_{p^k \leq x} f(p^k) \sum_{\substack{n \leq x \\ p^k \parallel n}} 1 = \frac{1}{x} \sum_{p^k \leq x} f(p^k) \left( \left\lfloor \frac{x}{p^k} \right\rfloor - \left\lfloor \frac{x}{p^{k+1}} \right\rfloor \right) = A_f(x) + O \left( \frac{1}{x} \sum_{p^k \leq x} |f(p^k)| \right),$$

where

$$A_f(x) := \sum_{p^k \leq x} \frac{f(p^k)}{p^k} \left( 1 - \frac{1}{p} \right),$$

in many situations we may think of  $A_f(x)$  as an approximation to the mean value of  $f$  over  $[1, x]$ . The Turán–Kubilius inequality furnishes an upper bound for the mean square of  $f(n) - A_f(x)$ , which may be thought of as the ‘variance’ of  $f$  over  $[1, x]$ . In its simplest form, the Turán–Kubilius inequality asserts that

$$\frac{1}{x} \sum_{n \leq x} |f(n) - A_f(x)|^2 \ll B_f(x),$$

where

$$B_f(x) := \sum_{p^k \leq x} \frac{|f(p^k)|^2}{p^k}.$$

An immediate corollary of this inequality is that if  $B_f(x) = o(|A_f(x)|^2)$  as  $x \rightarrow \infty$ , then for every fixed  $\varepsilon > 0$ , we have  $|f(n) - A_f(x)| < \varepsilon |A_f(x)|$  for all but  $o(x)$  values of  $n \in \mathbb{N} \cap [1, x]$ . Moreover, if one can show that  $A_f(n)$  is close to  $A_f(x)$  on average, then  $A_f(n)$  serves as a normal order of  $f(n)$ .

For our applications, we will need a version of the Turán–Kubilius inequality in which all the means involved are taken over the set of split-free positive integers. From a probabilistic point of view, we think of  $n \in \mathbb{N} \cap [1, x]$  as a discrete random variable with probability distribution given by  $\mathbb{P}(n = m) = 1_{\text{split-free}}(m) / \sum_{k \leq x} 1_{\text{split-free}}(k)$  for all  $m \in \mathbb{N} \cap [1, x]$ , rather than as a discrete random variable with uniform distribution given by  $\mathbb{P}(n = m) = 1/[x]$  for all  $m \in \mathbb{N} \cap [1, x]$ . More generally, one may replace  $1_{\text{split-free}}$  by an arbitrary nonnegative multiplicative function  $\alpha$ . In this direction, we prove the following weighted version of the Turán–Kubilius inequality inspired by Remark 3.11.1 in Fan’s PhD thesis on weighted Erdős–Kac theorems [7].

**Theorem 3.1.** *Let  $f: \mathbb{N} \rightarrow \mathbb{C}$  be an additive function, and let  $\alpha: \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$  be a multiplicative function with partial sums*

$$S_\alpha(x) := \sum_{n \leq x} \alpha(n).$$

*Suppose that there exist  $c_\alpha, \delta > 0$ ,  $\sigma \geq 0$  and  $\kappa \in \mathbb{R}$ , such that*

$$\sum_{\substack{n \leq x \\ (n, a) = 1}} \alpha(n) = c_\alpha x^\sigma (\log 3x)^{\kappa-1} \left( F_\alpha(a)^{-1} + O\left(\frac{1}{\log \log 3x}\right) \right) \quad (13)$$

*uniformly for all  $x \geq 1$  and all squarefree  $a \in \mathbb{N} \cap [1, x^\delta]$  with at most two prime factors, where*

$$F_\alpha(a) := \prod_{p|a} \sum_{k \geq 0} \frac{\alpha(p^k)}{p^{k\sigma}} < \infty.$$

*Furthermore, suppose that*

$$\sum_{p^k \leq x} \frac{\alpha(p^k)}{p^{k\sigma}} \log p^k \ll \log x \quad (14)$$

*for all  $x \geq 2$ . Then we have*

$$S_\alpha(x)^{-1} \sum_{n \leq x} \alpha(n) |f(n) - A_{\alpha, f}(x)|^2 \ll B_{\alpha, f}(x) \quad (15)$$

*for all  $x \geq 1$ , where*

$$A_{\alpha, f}(x) := \sum_{p^k \leq x} \alpha(p^k) F_\alpha(p)^{-1} \frac{f(p^k)}{p^{k\sigma}},$$

$$B_{\alpha, f}(x) := \sum_{p^k \leq x} \alpha(p^k) \frac{|f(p^k)|^2}{p^{k\sigma}} \left( 1 - \frac{\log p^k}{\log 3x} \right)^{\min(\kappa-1, 0)}.$$

*The implied constant in (15) depends at most on the parameters  $\delta, \kappa$  and the implied constants in (13) and (14).*

*Proof.* We may suppose  $x \geq 2$ , since (15) holds trivially when  $x \in [1, 2)$ . For technical reasons, we first prove (15) for the additive function  $f_\eta$  defined by  $f_\eta(p^k) = f(p^k)1_{p^k \leq x^\eta}$ , where  $\eta = \delta/(2 + 2\delta)$ . For convenience, we adopt the shorthand notation  $1_{p^k}(n) := 1_{p^k \parallel n}(n)$  and the notation

$$\mathbb{E}_{\leq x}^\alpha[g] := S_\alpha(x)^{-1} \sum_{\substack{n \leq x \\ p^k \parallel n}} \alpha(n)g(n)$$

for any arithmetic function  $g: \mathbb{N} \rightarrow \mathbb{C}$ . We start by computing the expectation of  $f_\eta$ . For  $p^k \leq x^\eta$ , we have by (13) that

$$\begin{aligned} \mathbb{E}_{\leq x}^\alpha[1_{p^k}] &= S_\alpha(x)^{-1} \sum_{\substack{n \leq x \\ p^k \parallel n}} \alpha(n) \\ &= S_\alpha(x)^{-1} \alpha(p^k) \sum_{\substack{n \leq x/p^k \\ (n,p)=1}} \alpha(n) \\ &= \frac{\alpha(p^k)}{p^{k\sigma}} \left(1 - \frac{\log p^k}{\log x}\right)^{\kappa-1} \left(F_\alpha(p)^{-1} + O\left(\frac{1}{\log \log 3x}\right)\right) \\ &= \frac{\alpha(p^k)}{p^{k\sigma}} \left(F_\alpha(p)^{-1} + O\left(\frac{\log p^k}{\log x} + \frac{1}{\log \log 3x}\right)\right). \end{aligned}$$

Hence, the expectation of  $f_\eta$  is

$$\mathbb{E}_{\leq x}^\alpha[f_\eta] = \sum_{p^k \leq x^\eta} f(p^k) \mathbb{E}_{\leq x}^\alpha[1_{p^k}] = A_{\alpha, f_\eta}(x) + O\left(\sum_{p^k \leq x^\eta} \alpha(p^k) \frac{|f(p^k)|}{p^{k\sigma}} \left(\frac{\log p^k}{\log x} + \frac{1}{\log \log 3x}\right)\right).$$

By Cauchy–Schwarz and (14), the error term on the previous line is

$$\ll \left(\sum_{p^k \leq x^\eta} \alpha(p^k) \frac{|f(p^k)|^2}{p^{k\sigma}}\right)^{1/2} \left(\sum_{p^k \leq x^\eta} \frac{\alpha(p^k)}{p^{k\sigma}} \left(\left(\frac{\log p^k}{\log x}\right)^2 + \frac{1}{(\log \log 3x)^2}\right)\right)^{1/2} \ll \sqrt{B_{\alpha, f_\eta}(x)},$$

whence

$$\mathbb{E}_{\leq x}^\alpha[f_\eta] = A_{\alpha, f_\eta}(x) + O\left(\sqrt{B_{\alpha, f_\eta}(x)}\right). \quad (16)$$

Next, we compute the variance of  $f_\eta$ . It is clear that

$$\text{Var}_{\leq x}^\alpha[1_{p^k}] := \mathbb{E}_{\leq x}^\alpha \left[ |1_{p^k} - \mathbb{E}_{\leq x}^\alpha[1_{p^k}]|^2 \right] = \mathbb{E}_{\leq x}^\alpha[1_{p^k}^2] - (\mathbb{E}_{\leq x}^\alpha[1_{p^k}])^2 \ll \frac{\alpha(p^k)}{p^{k\sigma}}.$$

For  $p^k, q^l \leq x^\eta$  with  $p \neq q$ , we have by (13) that

$$\begin{aligned} \mathbb{E}_{\leq x}^\alpha[1_{p^k} 1_{q^l}] &= S_\alpha(x)^{-1} \alpha(p^k) \alpha(q^l) \sum_{\substack{n \leq x/p^k q^l \\ (n, pq)=1}} \alpha(n) \\ &= \frac{\alpha(p^k) \alpha(q^l)}{p^{k\sigma} q^{l\sigma}} \left(1 - \frac{\log p^k q^l}{\log x}\right)^{\kappa-1} \left(F_\alpha(pq)^{-1} + O\left(\frac{1}{\log \log 3x}\right)\right). \end{aligned}$$

It follows that

$$\begin{aligned}
\text{Cov}_{\leq x}^{\alpha}[1_{p^k}, 1_{q^l}] &:= \mathbb{E}_{\leq x}^{\alpha}[1_{p^k} 1_{q^l}] - \mathbb{E}_{\leq x}^{\alpha}[1_{p^k}] \mathbb{E}_{\leq x}^{\alpha}[1_{q^l}] \\
&= \frac{\alpha(p^k) \alpha(q^l)}{p^{k\sigma} q^{l\sigma}} \left(1 - \frac{\log p^k q^l}{\log x}\right)^{\kappa-1} \left(F_{\alpha}(pq)^{-1} + O\left(\frac{1}{\log \log 3x}\right)\right) \\
&\quad - \frac{\alpha(p^k) \alpha(q^l)}{p^{k\sigma} q^{l\sigma}} \left(1 - \frac{\log p^k}{\log x}\right)^{\kappa-1} \left(1 - \frac{\log q^l}{\log x}\right)^{\kappa-1} \left(F_{\alpha}(pq)^{-1} + O\left(\frac{1}{\log \log 3x}\right)\right) \\
&\ll \frac{\alpha(p^k) \alpha(q^l)}{p^{k\sigma} q^{l\sigma}} \left(\frac{\log p^k}{\log x} \cdot \frac{\log q^l}{\log x} + \frac{1}{\log \log 3x}\right),
\end{aligned}$$

where we have used the inequality  $|a^{\kappa-1} - b^{\kappa-1}| \ll |a - b|$  for any  $a, b \in [(1 - \eta)^2, 1]$ , which is a direct consequence of the mean value theorem in calculus. Thus, the variance of  $f_{\eta}$  is

$$\begin{aligned}
\text{Var}_{\leq x}^{\alpha}[f_{\eta}] &= \mathbb{E}_{\leq x}^{\alpha} \left[ |f_{\eta} - \mathbb{E}_{\leq x}^{\alpha}[f_{\eta}]|^2 \right] = \sum_{p^k \leq x^{\eta}} |f(p^k)|^2 \text{Var}_{\leq x}^{\alpha}[1_{p^k}] + \sum_{\substack{p^k, q^l \leq x^{\eta} \\ p \neq q}} f(p^k) \overline{f(q^l)} \text{Cov}_{\leq x}^{\alpha}[1_{p^k}, 1_{q^l}] \\
&\ll B_{\alpha, f_{\eta}}(x) + \left( \sum_{p^k \leq x^{\eta}} \alpha(p^k) \frac{|f(p^k)|}{p^{k\sigma}} \left( \frac{\log p^k}{\log x} + \frac{1}{\sqrt{\log \log 3x}} \right) \right)^2 \\
&\ll B_{\alpha, f_{\eta}}(x)
\end{aligned}$$

by Cauchy–Schwarz and (14) as before. Combining this with (16), we find that

$$\mathbb{E}_{\leq x}^{\alpha} [|f_{\eta} - A_{\alpha, f_{\eta}}(x)|^2] \leq 2 \text{Var}_{\leq x}^{\alpha}[f_{\eta}] + 2 |\mathbb{E}_{\leq x}^{\alpha}[f_{\eta}] - A_{\alpha, f_{\eta}}(x)|^2 \ll B_{\alpha, f_{\eta}}(x),$$

which is exactly (15) with  $f_{\eta}$  in place of  $f$ .

Now it is an easy matter to deduce (15) for a general additive function  $f$ . Since

$$|f - A_{\alpha, f}(x)|^2 \leq 3 (|f - f_{\eta}|^2 + |f_{\eta} - A_{\alpha, f_{\eta}}(x)|^2 + |A_{\alpha, f_{\eta}}(x) - A_{\alpha, f}(x)|^2),$$

applying  $\mathbb{E}_{\leq x}^{\alpha}$  to both sides yields

$$\mathbb{E}_{\leq x}^{\alpha} [|f - A_{\alpha, f}(x)|^2] \ll \mathbb{E}_{\leq x}^{\alpha} [|f - f_{\eta}|^2] + B_{\alpha, f_{\eta}}(x) + |A_{\alpha, f_{\eta}}(x) - A_{\alpha, f}(x)|^2.$$

Clearly,  $B_{\alpha, f_{\eta}}(x) \ll B_{\alpha, f}(x)$ . To estimate  $\mathbb{E}_{\leq x}^{\alpha} [|f - f_{\eta}|^2]$ , we observe that for any  $n \in \mathbb{N} \cap [1, x]$ , the number of prime powers  $p^k > x^{\eta}$  exactly dividing  $n$  is at most  $1/\eta$ . Hence, we have by (13) that

$$\begin{aligned}
\mathbb{E}_{\leq x}^{\alpha} [|f - f_{\eta}|^2] &= S_{\alpha}(x)^{-1} \sum_{n \leq x} \alpha(n) \left| \sum_{p^k \parallel n, p^k > x^{\eta}} f(p^k) \right|^2 \\
&\ll S_{\alpha}(x)^{-1} \sum_{n \leq x} \alpha(n) \sum_{p^k \parallel n, p^k > x^{\eta}} |f(p^k)|^2 \\
&\leq S_{\alpha}(x)^{-1} \sum_{p^k \leq x} |f(p^k)|^2 \sum_{\substack{n \leq x \\ p^k \parallel n}} \alpha(n) \\
&\leq S_{\alpha}(x)^{-1} \sum_{p^k \leq x} \alpha(p^k) |f(p^k)|^2 \sum_{n \leq x/p^k} \alpha(n) \\
&\ll B_{\alpha, f}(x).
\end{aligned}$$

Finally, Cauchy–Schwarz together with (14) yields the upper bound

$$\begin{aligned}
|A_{\alpha, f_\eta}(x) - A_{\alpha, f}(x)|^2 &= \left| \sum_{x^\eta < p^k \leq x} \alpha(p^k) F_\alpha(p)^{-1} \frac{f(p^k)}{p^{k\sigma}} \right|^2 \\
&\ll B_{\alpha, f}(x) \sum_{x^\eta < p^k \leq x} \frac{\alpha(p^k)}{p^{k\sigma}} \\
&\ll \frac{B_{\alpha, f}(x)}{\log x} \sum_{p^k \leq x} \frac{\alpha(p^k)}{p^{k\sigma}} \log p^k \\
&\ll B_{\alpha, f}(x).
\end{aligned}$$

Putting everything together, we obtain  $\mathbb{E}_{\leq x}^\alpha [|f - A_{\alpha, f}(x)|^2] \ll B_{\alpha, f}(x)$  as desired.  $\square$

Examining the proof, one sees readily that Theorem 3.1 remains valid if  $F_\alpha$  is replaced by any positive multiplicative function whose restriction on primes is bounded away from 0. Nevertheless, the definition of  $F_\alpha$  given in Theorem 3.1 is intuitive and follows heuristically from (13). With this definition, (13) holds true for a myriad of multiplicative functions  $\alpha$ ; see [6, Lemma 3.2], for instance. In the sequel, we shall always take  $\alpha$  to be the characteristic function of the set of split-free integers. For this particular choice of  $\alpha$  we have

$$S_\alpha(x) = c_\alpha x (\log 3x)^{-1/2} \left( 1 + O\left(\frac{1}{\log 3x}\right) \right) \quad (17)$$

and

$$\sum_{p^k \leq x} \frac{\alpha(p^k)}{p^{k\sigma}} \log p^k = \frac{1}{2} \log x + O(1)$$

for all  $x \geq 1$ , where

$$\begin{aligned}
c_\alpha &= \frac{1}{\sqrt{\pi}} \prod_p \left( 1 - \frac{1}{p} \right)^{1/2} \sum_{k \geq 0} \frac{\alpha(p^k)}{p^k} \\
&= \sqrt{\frac{1}{\pi L(1, \chi)} \cdot \frac{|\Delta|}{\varphi(|\Delta|)}} \prod_{p \text{ inert}} \left( 1 - \frac{1}{p^2} \right)^{-1/2},
\end{aligned}$$

with  $\chi := (\Delta/\cdot)$ . We remind the reader that the value  $L(1, \chi)$  can be expressed in terms of the arithmetic invariants of  $K$  via Dirichlet’s class number formula [25, Ch. 26]:

$$h_K = \begin{cases} \frac{\sqrt{\Delta}}{2 \log \varepsilon} L(1, \chi), & \text{if } K \text{ is real,} \\ \frac{w \sqrt{-\Delta}}{2\pi} L(1, \chi), & \text{if } K \text{ is imaginary,} \end{cases}$$

where  $\varepsilon > 1$  is the normalized fundamental unit of  $K$ , and

$$w = \begin{cases} 2, & \text{if } \Delta < -4, \\ 4, & \text{if } \Delta = -4, \\ 6, & \text{if } \Delta = -3, \end{cases}$$

is the number of roots of unity in  $K$ . Moreover, it can be shown [6, Lemma 3.2] that

$$\sum_{\substack{n \leq x \\ (n,a)=1}} \alpha(n) = c_\alpha x (\log 3x)^{-1/2} \left( F_\alpha(a)^{-1} + O\left(\frac{1}{\log 3x}\right) \right)$$

uniformly for all  $x \geq 1$  and all  $a \in \mathbb{N} \cap [1, x]$ , where  $F_\alpha(a)$  is given by

$$F_\alpha(a) = \prod_{p|a} \sum_{k \geq 0} \frac{\alpha(p^k)}{p^k} = \prod_{\substack{p|a \\ \chi(p) \neq 1}} \left(1 - \frac{1}{p}\right)^{-1}.$$

Hence,  $\alpha$  satisfies the conditions of Theorem 3.1. We will apply our weighted Turán–Kubilius inequality to prove Proposition 2.6.

#### 4. THE TYPICAL SIZE OF $L(f)$ : PROOF OF PROPOSITION 2.6

Our proof of Proposition 2.6 builds on that of [5, Theorem 2] on the normal order of Carmichael’s  $\lambda$ -function. Due to the introduction of the weight  $\alpha$  used to capture only the split-free integers  $f$ , some special care needs to be taken of the estimation of various weighted sums in our proof. For this reason, our argument is more delicate than its counterpart in [5]. We shall only prove Proposition 2.6 for  $L(f)$ , as one sees readily from the proof that primes in any bounded interval which divide a typical  $f$  contribute a negligible amount and can thus be left out.

To begin with, we write

$$\begin{aligned} \log \psi(f) &= \sum_q v_q(\psi(f)) \log q, \\ \log L(f) &= \sum_q v_q(L(f)) \log q, \end{aligned}$$

where the sums run over all primes  $q$ . Since  $f/\log_2 f \ll \psi(f) \ll f \log_2 f$  for all  $f \geq 3$ , it suffices to show

$$\log \psi(f) - \log L(f) = \frac{1}{2} y \log y + \frac{1}{2} C_K y + O\left(\frac{y(\log_2 y)^3}{\log y}\right) \quad (18)$$

for all but  $o(x/\sqrt{\log x})$  split-free  $f \leq x$ , where  $y = \log_2 x$ . As in [5], we divide the primes  $q$  into the following four ranges:

$$\begin{aligned} I_1: q \leq y/\log y, & & I_2: y/\log y < q \leq y \log y, \\ I_3: y \log y < q \leq y^2, & & I_4: q > y^2. \end{aligned}$$

We estimate the contribution to the left-hand side of (18) from the primes in each of these four intervals separately. In the proof, we shall frequently resort to (17) without further notice. Note that  $q^2 \nmid f$  for any  $q \notin I_1$  for all but  $o(S_\alpha(x)) = o(x/\sqrt{\log x})$  split-free  $f \leq x$ . This follows from

the estimate

$$\begin{aligned}
S_\alpha(x)^{-1} \sum_{q \notin I_1} \sum_{\substack{f \leq x \\ q^2 | f}} \alpha(f) &= S_\alpha(x)^{-1} \sum_{q > y/\log y} \alpha(q^2) \sum_{f \leq x/q^2} \alpha(f) \\
&\ll \sum_{y/\log y < q \leq \sqrt{x}} \frac{1}{q^2} \left(1 - \frac{\log q^2}{\log 3x}\right)^{-1/2} \\
&\ll \sum_{y/\log y < q \leq x^{1/3}} \frac{1}{q^2} + (\log x)^{1/2} \sum_{x^{1/3} < q \leq x} \frac{1}{q^2} \ll \frac{1}{y}.
\end{aligned}$$

We will make use of this fact when examining the contributions from  $q \in I_3 \cup I_4$ . Finally, we set  $\mathcal{R}_i := \{a \in \mathbb{Z}/\Delta\mathbb{Z} : \chi(a) = i\}$  and  $\mathcal{P}_i := \{p \text{ prime} : \chi(p) = i\}$  for  $i \in \{0, \pm 1\}$ .

**4.1. A cutoff of  $\log \psi$ .** Before estimating the contribution from primes in  $I_1 \cup I_2$ , we define a cutoff of  $\log \psi$  by

$$h(f) := \sum_{q \leq y \log y} v_q(\psi(f)) \log q.$$

We wish to determine the typical size of the additive function  $h$  by applying Theorem 3.1 to  $h$  and the multiplicative weight  $\alpha$ . It boils down to estimating

$$\begin{aligned}
A_{\alpha, h}(x) &= \sum_{p^k \leq x} \alpha(p^k) \frac{h(p^k)}{p^k} \left(1 - \frac{1}{p}\right), \\
B_{\alpha, h}(x) &= \sum_{p^k \leq x} \alpha(p^k) \frac{h(p^k)^2}{p^k} \left(1 - \frac{\log p^k}{\log 3x}\right)^{-1/2}.
\end{aligned}$$

Using the trivial bound  $h(p^k) \leq \log \psi(p^k) \ll \log p^k$ , we find that

$$\sum_{p^k \leq x} \alpha(p^k) \frac{h(p^k)}{p^{k+1}} \ll \sum_{p^k \leq x} \frac{\log p^k}{p^{k+1}} \ll \sum_{p \leq x} \frac{\log p}{p^2} \ll 1$$

and that

$$\begin{aligned}
\sum_{\substack{p^k \leq x \\ k \geq 2}} \alpha(p^k) \frac{h(p^k)^j}{p^k} \left(1 - \frac{\log p^k}{\log 3x}\right)^{-1/2} &\ll \sum_{\substack{p^k \leq \sqrt{x} \\ k \geq 2}} \frac{(\log p^k)^j}{p^k} + (\log x)^{j+1/2} \sum_{\substack{\sqrt{x} < p^k \leq x \\ k \geq 2}} \frac{1}{p^k} \\
&\ll 1 + (\log x)^{j+1/2} \sum_{\substack{\sqrt{x} < p^k \leq x \\ p \leq x^{1/4}}} \frac{1}{p^k} + (\log x)^{j+1/2} \sum_{\substack{p > x^{1/4} \\ k \geq 2}} \frac{1}{p^k} \\
&\ll 1 + \frac{(\log x)^{j+1/2}}{x^{1/2}} \sum_{p \leq x^{1/4}} 1 + (\log x)^{j+1/2} \sum_{p > x^{1/4}} \frac{1}{p^2} \ll 1,
\end{aligned}$$



where  $j \in \{1, 2\}$ . It follows that

$$A_{\alpha, h}(x) = \sum_{p \leq x} \alpha(p) \frac{h(p)}{p} + O(1),$$

$$B_{\alpha, h}(x) = \sum_{p \leq x} \alpha(p) \frac{h(p)^2}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} + O(1).$$

Let us estimate  $A_{\alpha, h}(x)$  first. By definition of  $h$ , we have

$$\begin{aligned} A_{\alpha, h}(x) &= \sum_{q \leq y \log y} \log q \sum_{\substack{p \leq x \\ p \notin \mathcal{P}_1}} \frac{v_q(p - \chi(p))}{p} + O(1) \\ &= \sum_{q \leq y \log y} \log q \sum_{i \geq 1} \sum_{\substack{p \leq x \\ p \notin \mathcal{P}_1 \\ p \equiv \chi(p) \pmod{q^i}}} \frac{1}{p} + O(1) \\ &= \sum_{q \leq y \log y} \log q \sum_{i \geq 1} \sum_{\substack{p \leq x \\ p \in \mathcal{P}_{-1} \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} + O(1). \end{aligned}$$

For each  $n \in \mathbb{N}$ , let  $\beta(n) := \#\{a \in \mathcal{R}_{-1} : a \equiv -1 \pmod{(n, \Delta)}\}$ . The contribution to  $A_{\alpha, h}(x)$  from the primes  $q \mid \Delta$  is

$$\sum_{q \mid \Delta} \log q \sum_{i \geq 1} \sum_{\substack{p \leq x \\ p \in \mathcal{P}_{-1} \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} = \sum_{q \mid \Delta} \log q \sum_{i \geq 1} \sum_{\substack{a \in \mathcal{R}_{-1} \\ a \equiv -1 \pmod{(q^i, \Delta)}}} \sum_{\substack{p \leq x \\ p \equiv a \pmod{|\Delta|} \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p}.$$

To estimate the innermost sum, we appeal to the following estimate due independently to Norton [20] and Pomerance [24]:

$$\sum_{\substack{m < p \leq x \\ p \equiv a \pmod{m}}} \frac{1}{p} = \frac{\log_2 x}{\varphi(m)} + O\left(\frac{\log 3m}{\varphi(m)}\right) \quad (19)$$

uniformly for all  $x \geq 3$ , all  $m \in \mathbb{N}$ , and all  $a \in \mathbb{Z}$  coprime to  $m$ . If  $q$  is odd, then the Chinese remainder theorem and (19) imply that

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{|\Delta|} \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} = \frac{y}{\varphi(|\Delta|q^{i-1})} + O\left(\frac{\log q^i}{\varphi(q^i)}\right) = \frac{y + O(\log q^i)}{\varphi(|\Delta|)q^{i-1}},$$

where one observes that the contribution from the only possible prime  $< |\Delta|q^{i-1}$  appearing in the sum gets subsumed into the error. If  $2^j \parallel \Delta$  for some  $1 \leq j \leq 3$ , then the Chinese remainder theorem and (19) yield

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{|\Delta|} \\ p \equiv -1 \pmod{2^i}}} \frac{1}{p} = \frac{y + O(1)}{\varphi(|\Delta|)},$$

for  $1 \leq i \leq j$ , and

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{|\Delta|} \\ p \equiv -1 \pmod{2^i}}} \frac{1}{p} = \frac{y}{\varphi(|\Delta|2^{i-j})} + O\left(\frac{\log 2^i}{\varphi(2^i)}\right) = \frac{y + O(\log 2^i)}{\varphi(|\Delta|)2^{i-j}}$$

for  $i > j$ , where  $2^i - 1 \leq a'' < |\Delta|2^{i-j}$  is some positive integer. Hence, the contribution to  $A_{\alpha,h}(x)$  from the primes  $q \mid \Delta$  is

$$\frac{1}{\varphi(|\Delta|)} \left( \sum_{\substack{q \mid \Delta \\ q > 2}} \beta(q) \log q \sum_{i \geq 1} \frac{1}{q^{i-1}} + 1_{2 \mid \Delta} \log 2 \left( \sum_{i=1}^j \beta(2^i) + \sum_{i>j} \frac{\beta(2^i)}{2^{i-j}} \right) \right) y + O(1) = c_1 y + O(1),$$

where

$$c_1 := \frac{1}{\varphi(|\Delta|)} \left( \sum_{q \mid \Delta} \frac{\beta(q) q \log q}{q-1} + (1_{4 \mid \Delta} (2\beta(4) - \beta(2)) + 1_{8 \mid \Delta} (2\beta(8) - \beta(4))) \log 2 \right).$$

Using the orthogonality relations between Dirichlet characters and the fact that  $\chi \pmod{|\Delta|}$  is primitive, one can show that

$$\beta(d) = \frac{\varphi(|\Delta|)(1 - \chi(-1)1_{d=|\Delta|})}{2\varphi(d)}$$

for any positive integer  $d \mid \Delta$ . As a consequence, since  $\chi(-1) = \text{sgn}(\Delta)$ , we have

$$c_1 = \frac{1}{2} \left( \sum_{q \mid \Delta} \frac{q \log q}{(q-1)^2} - \frac{\text{sgn}(\Delta) 1_{\mathcal{D}}(\Delta) |\Delta| \log \text{Rad}(|\Delta|)}{\varphi(|\Delta|)^2} \right),$$

where  $\mathcal{D}$  is defined by (1). On the other hand, the contribution to  $A_{\alpha,h}(x)$  from the primes  $q \nmid \Delta$  is

$$\begin{aligned} \sum_{\substack{q \leq y \log y \\ q \nmid \Delta}} \log q \sum_{i \geq 1} \sum_{\substack{p \leq x \\ p \in \mathcal{P}_{-1} \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} &= \sum_{\substack{q \leq y \log y \\ q \nmid \Delta}} \log q \sum_{i \geq 1} \sum_{a \in \mathcal{R}_{-1}} \sum_{\substack{p \leq x \\ p \equiv a \pmod{|\Delta|} \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} \\ &= \frac{1}{2} \sum_{\substack{q \leq y \log y \\ q \nmid \Delta}} \log q \sum_{i \geq 1} \frac{y + O(\log q^i)}{\varphi(q^i)} \\ &= \frac{y}{2} \sum_{q \leq y \log y} \frac{q \log q}{(q-1)^2} - \frac{y}{2} \sum_{q \mid \Delta} \frac{q \log q}{(q-1)^2} + O\left((\log y)^2 \sum_{q \leq y \log y} \frac{1}{q}\right) \\ &= \frac{y}{2} \sum_{q \leq y \log y} \frac{q \log q}{(q-1)^2} - \frac{y}{2} \sum_{q \mid \Delta} \frac{q \log q}{(q-1)^2} + O((\log y)^2 \log_2 y), \end{aligned}$$

by (19) and the fact that  $\#\mathcal{R}_{-1} = \varphi(|\Delta|)/2$ . It is shown in [5] that

$$\sum_{q \leq y \log y} \frac{q \log q}{(q-1)^2} = \log y + \log_2 y + \left( -\gamma + \sum_p \frac{\log p}{(p-1)^2} \right) + O\left(e^{-\sqrt{\log y}}\right),$$

where  $\gamma = 0.57721\dots$  is the Euler–Mascheroni constant. Hence, the contribution to  $A_{\alpha,h}(x)$  from the primes  $q \nmid \Delta$  is

$$\frac{1}{2}y \log y + \frac{1}{2}y \log_2 y + \frac{1}{2} \left( -\gamma + \sum_p \frac{\log p}{(p-1)^2} - \sum_{q|\Delta} \frac{q \log q}{(q-1)^2} \right) y + O\left(ye^{-\sqrt{\log y}}\right).$$

We conclude that

$$A_{\alpha,h}(x) = \frac{1}{2}y \log y + \frac{1}{2}y \log_2 y + \frac{c_2}{2}y + O\left(ye^{-\sqrt{\log y}}\right), \quad (20)$$

where

$$c_2 := \sum_p \frac{\log p}{(p-1)^2} - \frac{\operatorname{sgn}(\Delta) 1_{\mathcal{D}}(\Delta) |\Delta| \log \operatorname{Rad}(|\Delta|)}{\varphi(|\Delta|)^2} - \gamma.$$

Next, we estimate  $B_{\alpha,h}(x)$ . Since the primes  $p \in \mathcal{P}_0$  contribute  $O(1)$ , we have

$$\begin{aligned} B_{\alpha,h}(x) &= \sum_{\substack{p \leq x \\ p \in \mathcal{P}_{-1}}} \frac{h(p)^2}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} + O(1) \\ &= \sum_{q_1, q_2 \leq y \log y} \log q_1 \log q_2 \sum_{\substack{p \leq x \\ p \in \mathcal{P}_{-1}}} \frac{v_{q_1}(p - \chi(p)) v_{q_2}(p - \chi(p))}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} + O(1) \\ &= \sum_{q_1, q_2 \leq y \log y} \log q_1 \log q_2 \sum_{i,j \geq 1} \sum_{\substack{p \leq x \\ p \in \mathcal{P}_{-1} \\ p \equiv \chi(p) \pmod{[q_1^i, q_2^j]}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} + O(1) \\ &\leq \sum_{q_1, q_2 \leq y \log y} \log q_1 \log q_2 \sum_{i,j \geq 1} \sum_{\substack{p \leq x \\ p \equiv -1 \pmod{[q_1^i, q_2^j]}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} + O(1), \end{aligned}$$

where  $[q_1^i, q_2^j]$  denotes the least common multiple of  $q_1^i$  and  $q_2^j$ . Since  $(1 - \log p / \log 3x)^{-1/2} \ll 1$  when  $p \leq \sqrt{x}$ , the estimates for  $H_1$  and  $H_2$  from [5, p. 367] lead to

$$\sum_{q_1, q_2 \leq y \log y} \log q_1 \log q_2 \sum_{i,j \geq 1} \sum_{\substack{p \leq \sqrt{x} \\ p \equiv -1 \pmod{[q_1^i, q_2^j]}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \ll y(\log y)^2.$$

It remains to bound the tail

$$\sum_{q_1, q_2 \leq y \log y} \log q_1 \log q_2 \sum_{i,j \geq 1} \sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{[q_1^i, q_2^j]}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2}.$$

When  $[q_1^i, q_2^j] \leq x^{1/3}$ , we have by Brun–Titchmarsh and partial summation that

$$\sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{[q_1^i, q_2^j]}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \ll \frac{1}{\varphi([q_1^i, q_2^j])}.$$

Borrowing the relevant estimates from [5, p. 367], we see that the contribution to the tail from  $q_1^i$  and  $q_2^j$  with  $[q_1^i, q_2^j] \leq x^{1/3}$  is

$$\ll \sum_{q_1, q_2 \leq y \log y} \log q_1 \log q_2 \sum_{i, j \geq 1} \frac{1}{\varphi([q_1^i, q_2^j])} \ll y(\log y)^2.$$

On the other hand, the contribution to the tail from  $q_1^i$  and  $q_2^j$  with  $[q_1^i, q_2^j] > x^{1/3}$  is trivially

$$(\log x)^{1/2} \sum_{q_1, q_2 \leq y \log y} \log q_1 \log q_2 \sum_{\substack{i, j \geq 1 \\ x^{1/3} < [q_1^i, q_2^j] \leq x+1}} \sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{[q_1^i, q_2^j]}}} \frac{1}{p}.$$

Note that

$$\sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{[q_1^i, q_2^j]}}} \frac{1}{p} \leq \sum_{\substack{n \leq x \\ n \equiv -1 \pmod{[q_1^i, q_2^j]}}} \frac{1}{n} \ll \frac{\log x}{[q_1^i, q_2^j]}.$$

Thus, the contribution to the tail from  $q_1^i$  and  $q_2^j$  with  $[q_1^i, q_2^j] > x^{1/3}$  is

$$\ll (\log x)^{3/2} \sum_{q_1, q_2 \leq y \log y} \log q_1 \log q_2 \sum_{\substack{i, j \geq 1 \\ x^{1/3} < [q_1^i, q_2^j] \leq x+1}} \frac{1}{[q_1^i, q_2^j]}.$$

The contribution to the last line from the diagonal terms with  $q_1 = q_2$  is

$$\begin{aligned} &\leq 2(\log x)^{3/2} \sum_{q \leq y \log y} (\log q)^2 \sum_{\substack{i, j \geq 1 \\ x^{1/3} < q^i \leq x+1}} \frac{1}{q^i} \\ &\leq 2(\log x)^{3/2} \sum_{q \leq y \log y} (\log q)^2 \sum_{\substack{i \geq 1 \\ q^i > x^{1/3}}} \frac{i}{q^i} \\ &\ll \frac{(\log x)^{5/2}}{x^{1/3}} \sum_{q \leq y \log y} \log q \\ &\ll \frac{(\log x)^{5/2} y \log y}{x^{1/3}}, \end{aligned}$$

while the contribution from the off-diagonal terms with  $q_1 \neq q_2$  is

$$\begin{aligned}
&\leq 2(\log x)^{3/2} \sum_{q_1 < q_2 \leq y \log y} \log q_1 \log q_2 \sum_{\substack{i, j \geq 1 \\ x^{1/3} < q_1^i q_2^j \leq x+1}} \frac{1}{q_1^i q_2^j} \\
&\leq 2(\log x)^{3/2} \sum_{q_1 < q_2 \leq y \log y} \log q_1 \log q_2 \sum_{q_1^i \leq x} \frac{1}{q_1^i} \sum_{q_2^j > x^{1/3}/q_1^i} \frac{1}{q_2^j} \\
&\ll \frac{(\log x)^{3/2}}{x^{1/3}} \sum_{q_1 < q_2 \leq y \log y} \log q_1 \log q_2 \sum_{q_1^i \leq x} 1 \\
&\leq \frac{(\log x)^{5/2}}{x^{1/3}} \sum_{q_1, q_2 \leq y \log y} \log q_2 \\
&\ll \frac{(\log x)^{5/2} y^2 \log y}{x^{1/3}}.
\end{aligned}$$

Collecting all the contributions to the tail shows that the tail is  $\ll y(\log y)^2$ , whence  $B_{\alpha, h}(x) \ll y(\log y)^2$ . Combining this estimate with (20) and invoking Theorem 3.1, we conclude that

$$\left| h(f) - \frac{1}{2}y \log y - \frac{1}{2}y \log_2 y - \frac{c_2}{2}y \right| < \frac{y}{\log y} \quad (21)$$

holds for all but  $o(S_\alpha(x))$  split-free positive integers  $f \leq x$ .

**4.2. The contribution from  $I_1$ .** With (21) in hand, we proceed to estimate the contribution to  $\log L(f)$  from the primes in  $I_1$ . To this end, we show that

$$\sum_{\substack{q^i > y^2 / \log^2 y \\ i > 1, q^i \parallel L(f)}} \log q^i < (\log y)^2 \quad (22)$$

for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ . Once we have this, we can conclude that the contribution to  $\log L(f)$  from the primes  $q \in I_1$  is at most

$$\sum_{\substack{q \in I_1, q^i \parallel L(f) \\ q^i \leq y^2 / \log^2 y}} \log q^i + (\log y)^2 \ll \sum_{q \in I_1} \log y + (\log y)^2 \ll \frac{y}{\log y} \quad (23)$$

for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ . Now we prove (22) by averaging the left-hand side over split-free  $f \leq x$ . More precisely, we show

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \sum_{\substack{q^i > y^2 / \log^2 y \\ i > 1, q^i \parallel L(f)}} \log q^i \ll \log y, \quad (24)$$

from which (22) follows at once. Note that if  $q^i \mid L(f)$ , then  $q^i \mid f$  with  $q$  ramified, or  $q^{i+1} \mid f$  with  $q$  unramified, or  $f$  has a prime factor  $p$  with  $p \equiv \chi(p) \pmod{q^i}$ . The first case contributes at most

$$\begin{aligned}
S_\alpha(x)^{-1} \sum_{\substack{q^i > y^2 / \log^2 y \\ q \mid \Delta, i > 1}} \log q^i \sum_{\substack{f \leq x \\ q^i \mid f}} \alpha(f) &\ll \sum_{\substack{y^2 / \log^2 y < q^i \leq x \\ q \mid \Delta, i > 1}} \frac{\log q^i}{q^i} \left(1 - \frac{\log q^i}{\log 3x}\right)^{-1/2} \\
&\ll \sum_{\substack{y^2 / \log^2 y < q^i \leq \sqrt{x} \\ q \mid \Delta, i > 1}} \frac{\log q^i}{q^i} + (\log x)^{1/2} \sum_{\substack{q^i > \sqrt{x} \\ q \mid \Delta}} \frac{\log q^i}{q^i} \\
&\ll \sum_{q \mid \Delta} \sum_{i > 1} \frac{\log q^i}{q^i} + \frac{(\log x)^{3/2}}{\sqrt{x}} \ll 1,
\end{aligned}$$

Similarly, the contribution to the left-hand side of (24) from the second case is

$$\begin{aligned}
&\leq S_\alpha(x)^{-1} \sum_{\substack{q^i > y^2 / \log^2 y \\ i > 1}} \log q^i \sum_{\substack{f \leq x \\ q^{i+1} \mid f}} \alpha(f) \\
&\ll \sum_{\substack{y^2 / \log^2 y < q^i \leq x/q \\ i > 1}} \frac{\log q^i}{q^{i+1}} \left(1 - \frac{\log q^{i+1}}{\log 3x}\right)^{-1/2} \\
&\ll \sum_{\substack{y^2 / \log^2 y < q^i \leq \sqrt{x}/q \\ i > 1}} \frac{\log q^i}{q^{i+1}} + (\log x)^{1/2} \sum_{\substack{\sqrt{x} < q^{i+1} \leq x \\ i > 1}} \frac{\log q^i}{q^{i+1}} \\
&\ll \sum_q \sum_{i > 1} \frac{\log q^i}{q^{i+1}} + \frac{(\log x)^{3/2}}{\sqrt{x}} \sum_{q \leq x^{1/3}} 1 \ll 1.
\end{aligned}$$

Finally, the contribution to the left-hand side of (24) from the last case is

$$\begin{aligned}
&\leq S_\alpha(x)^{-1} \sum_{\substack{q^i > y^2 / \log^2 y \\ i > 1}} \log q^i \sum_{\substack{p \leq x \\ p \equiv \chi(p) \pmod{q^i} \\ p \notin \mathcal{P}_1}} \sum_{\substack{f \leq x \\ p \mid f}} \alpha(f) \\
&= S_\alpha(x)^{-1} \sum_{\substack{y^2 / \log^2 y < q^i \leq x+1 \\ i > 1}} \log q^i \sum_{\substack{p \leq x \\ p \equiv \chi(p) \pmod{q^i}}} \alpha(p) \sum_{f \leq x/p} \alpha(f) \\
&\ll \sum_{\substack{q^i > y^2 / \log^2 y \\ i > 1}} \log q^i \sum_{\substack{p \leq x \\ p \equiv \chi(p) \pmod{q^i}}} \frac{\alpha(p)}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \\
&\leq \sum_{\substack{y^2 / \log^2 y < q^i \leq x+1 \\ i > 1}} \log q^i \sum_{\substack{p \leq x \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \\
&\ll \sum_{\substack{y^2 / \log^2 y < q^i \leq x+1 \\ i > 1}} \log q^i \sum_{\substack{p \leq \sqrt{x} \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} + \sum_{\substack{y^2 / \log^2 y < q^i \leq x+1 \\ i > 1}} \log q^i \sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2}.
\end{aligned}$$

The first double sum on the last line follows easily from Brun–Titchmarsh and partial summation. Indeed, the first double sum is

$$\begin{aligned} \ll y \sum_{\substack{q^i > y^2/\log^2 y \\ i > 1}} \frac{\log q^i}{\varphi(q^i)} &\leq y \sum_{\substack{q^i > y^2/\log^2 y \\ q \leq y/\log y}} \frac{\log q^i}{\varphi(q^i)} + y \sum_{\substack{q > y/\log y \\ i > 1}} \frac{\log q^i}{\varphi(q^i)} \\ &\ll \frac{y \log y}{y^2/\log^2 y} \sum_{q \leq y/\log y} 1 + y \sum_{q > y/\log y} \frac{\log q}{q^2} \\ &\ll \log y. \end{aligned}$$

We split the second double sum into the two following subsums

$$\begin{aligned} &\sum_{\substack{y^2/\log^2 y < q^i \leq x^{1/3} \\ i > 1}} \log q^i \sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2}, \\ &\sum_{\substack{x^{1/3} < q^i \leq x+1 \\ i > 1}} \log q^i \sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2}. \end{aligned}$$

By Brun–Titchmarsh and partial summation, we have

$$\sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \ll \frac{1}{\varphi(q^i)}$$

whenever  $q^i \leq x^{1/3}$ , the first subsum above is

$$\ll \sum_{\substack{q^i > y^2/\log^2 y \\ i > 1}} \frac{\log q^i}{\varphi(q^i)} \ll \frac{\log y}{y}.$$

Similarly, the second subsum is

$$\begin{aligned} &\ll (\log x)^{1/2} \sum_{\substack{x^{1/3} < q^i \leq x+1 \\ i > 1}} \log q^i \sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{q^i}}} \frac{1}{p} \\ &\ll y(\log x)^{1/2} \sum_{\substack{q^i > x^{1/3} \\ i > 1}} \frac{\log q^i}{\varphi(q^i)} \\ &\leq y(\log x)^{1/2} \sum_{\substack{q \leq x^{1/6} \\ q^i > x^{1/3}}} \frac{\log q^i}{\varphi(q^i)} + y(\log x)^{1/2} \sum_{\substack{q > x^{1/6} \\ i > 1}} \frac{\log q^i}{\varphi(q^i)} \\ &\ll \frac{y(\log x)^{3/2}}{x^{1/3}} \sum_{q \leq x^{1/6}} 1 + y(\log x)^{1/2} \sum_{q > x^{1/6}} \frac{\log q}{q^2} \\ &\ll \frac{y(\log x)^{1/2}}{x^{1/6}}. \end{aligned}$$

Gathering the estimates above completes the proof of (24).

**4.3. The contribution from  $I_2$ .** We now turn to the most elaborate part of the proof: estimating the contribution to  $\log L(f)$  from the primes in  $I_2$ . Following the argument in [5], we define analogously

$$\begin{aligned}\mathcal{Q}(q) &:= \{p \leq x : p \notin \mathcal{P}_1 \text{ and } p \equiv \chi(p) \pmod{q}\}, \\ \mathcal{Q}_1(q) &:= \{p \in \mathcal{Q}(q) \cap [2, x^{1/y}] : p \not\equiv \chi(p) \pmod{qq'} \text{ for any } q' \in I_2\}, \\ \mathcal{Q}_2(q) &:= \{p \in \mathcal{Q}(q) : p \equiv \chi(p) \pmod{qq'} \text{ for some } q' \in I_2\}, \\ \mathcal{Q}_3(q) &:= \{p \in \mathcal{Q}(q) \cap (x^{1/y}, x] : p \not\equiv \chi(p) \pmod{qq'} \text{ for any } q' \in I_2\},\end{aligned}$$

for each prime  $q \in I_2$ , so that  $\mathcal{Q}(q) = \mathcal{Q}_1(q) \cup \mathcal{Q}_2(q) \cup \mathcal{Q}_3(q)$ . Moreover, for every  $p \in \mathcal{Q}(q)$  we have  $p \equiv -1 \pmod{q}$ , and in particular,  $p > q - 1 > y/\log y - 1$ . In view of (22), we know that the contribution to  $\log L(f)$  from the primes  $q \in I_2$  is

$$\sum_{\substack{q \in I_2 \\ (f, \mathcal{Q}_1(q)) > 1}} \log q + O\left(\sum_{q \in I_2} \sum_{\substack{p|f \\ p \in \mathcal{Q}_2(q)}} \log q + \sum_{q \in I_2} \sum_{\substack{p|f \\ p \in \mathcal{Q}_3(q)}} \log q\right) + O((\log y)^2) \quad (25)$$

for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ .

We first show that the second big  $O$  term is negligible by averaging. We start by proving

$$\sum_{q \in I_2} \sum_{\substack{p|f \\ p \in \mathcal{Q}_2(q)}} \log q < \frac{y(\log_2 y)^3}{\log y} \quad (26)$$

for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ . The proof is straightforward. We have

$$\begin{aligned}& S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \sum_{q \in I_2} \sum_{\substack{p|f \\ p \in \mathcal{Q}_2(q)}} \log q \\ &= S_\alpha(x)^{-1} \sum_{q \in I_2} \log q \sum_{p \in \mathcal{Q}_2(q)} \sum_{\substack{f \leq x \\ p|f}} \alpha(f) \\ &\ll \sum_{q, q' \in I_2} \log q \sum_{\substack{p \leq x \\ p \notin \mathcal{P}_1 \\ p \equiv \chi(p) \pmod{qq'}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \\ &\leq \sum_{q, q' \in I_2} \log q \sum_{\substack{p \leq x \\ p \equiv -1 \pmod{qq'}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \\ &\ll \sum_{q, q' \in I_2} \log q \sum_{\substack{p \leq \sqrt{x} \\ p \equiv -1 \pmod{qq'}}} \frac{1}{p} + \sum_{q, q' \in I_2} \log q \sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{qq'}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2}.\end{aligned}$$

It follows from Brun–Titchmarsh and partial summation that the first double sum is

$$\ll y \sum_{q, q' \in I_2} \frac{\log q}{\varphi(qq')} \ll y \log y \left(\sum_{q \in I_2} \frac{1}{q}\right)^2 \ll \frac{y(\log_2 y)^2}{\log y},$$



and the second double sum is

$$\ll \sum_{q, q' \in I_2} \frac{\log q}{\varphi(qq')} \ll \frac{(\log_2 y)^2}{\log y}.$$

Hence, we obtain

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(n) \sum_{q \in I_2} \sum_{\substack{p|f \\ p \in \mathcal{Q}_2(q)}} \log q \ll \frac{y(\log_2 y)^2}{\log y},$$

of which (26) is an immediate consequence.

In a similar fashion, we show that

$$\sum_{q \in I_2} \sum_{\substack{p|f \\ p \in \mathcal{Q}_3(q)}} \log q < (\log y)^2. \quad (27)$$

for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ . Indeed, we have

$$\begin{aligned} & S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \sum_{q \in I_2} \sum_{\substack{p|f \\ p \in \mathcal{Q}_3(q)}} \log q \\ &= S_\alpha(x)^{-1} \sum_{q \in I_2} \log q \sum_{p \in \mathcal{Q}_3(q)} \sum_{\substack{f \leq x \\ p|f}} \alpha(f) \\ &\ll \sum_{q \in I_2} \log q \sum_{\substack{x^{1/y} < p \leq x \\ p \equiv -1 \pmod{q}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \\ &\ll \sum_{q \in I_2} \log q \sum_{\substack{x^{1/y} < p \leq \sqrt{x} \\ p \equiv -1 \pmod{q}}} \frac{1}{p} + \sum_{q \in I_2} \log q \sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{q}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \\ &\ll \log y \sum_{q \in I_2} \frac{\log q}{\varphi(q)} + \sum_{q \in I_2} \frac{\log q}{\varphi(q)} \\ &\ll (\log y) \log_2 y, \end{aligned}$$

which implies (27).

Inserting (26) and (27) into (25), we see that the contribution to  $\log L(f)$  from the primes  $q \in I_2$  is

$$\sum_{\substack{q \in I_2 \\ (f, \mathcal{Q}_1(q)) > 1}} \log q + O\left(\frac{y(\log_2 y)^3}{\log y}\right) \quad (28)$$

for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ . Now we estimate the sum in (28). Let

$$g(f) := \sum_{\substack{q \in I_2 \\ (f, \mathcal{Q}_1(q)) = 1}} 1.$$

Although  $g$  is not additive, we can still determine its typical size by computing its first and second moments weighted by  $\alpha$ . We begin with its first moment

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f)g(f) = S_\alpha(x)^{-1} \sum_{q \in I_2} \sum_{\substack{f \leq x \\ (f, \mathcal{Q}_1(q))=1}} \alpha(f).$$

The fundamental lemma of sieve theory [15, Theorem 19.1] ensures that there exist upper and lower bound sieve weights  $\lambda^\pm$  (not to be confused with Carmichael's  $\lambda$ -function) of level  $D = x^{u/y}$  with  $u = \log y$ , which are 1-bounded and supported on positive integers  $n \leq D$  composed entirely of primes factors from  $\mathcal{Q}_1(q)$ , such that  $1 * \lambda^- \leq 1_{(n, \mathcal{Q}_1(q))=1} \leq 1 * \lambda^+$  and

$$\sum_{d \leq D} \frac{\lambda^\pm(d)\alpha(d)}{d} = (1 + O(u^{-u/2})) \prod_{p \in \mathcal{Q}_1(q)} \left(1 - \frac{1}{p}\right), \quad (29)$$

where  $*$  denotes the Dirichlet convolution. Then we have

$$\sum_{\substack{f \leq x \\ (f, \mathcal{Q}_1(q))=1}} \alpha(f) = \sum_{f \leq x} \alpha(f) 1_{(f, \mathcal{Q}_1(q))=1} \leq \sum_{f \leq x} \alpha(f) \sum_{d|f} \lambda^+(d) = \sum_{d \leq D} \lambda^+(d) \sum_{\substack{f \leq x \\ d|f}} \alpha(f). \quad (30)$$

Note that

$$\begin{aligned} \sum_{d \leq D} \lambda^+(d) \sum_{\substack{f \leq x \\ d|f}} \alpha(f) &= \sum_{d \leq D} \lambda^+(d) \alpha(d) c_\alpha \frac{x}{d} \left(\log \frac{x}{d}\right)^{-1/2} \left(1 + O\left(\left(\log \frac{x}{d}\right)^{-1}\right)\right) \\ &= c_\alpha x (\log x)^{-1/2} \sum_{d \leq D} \frac{\lambda^+(d) \alpha(d)}{d} \left(1 + O\left(\frac{\log D}{\log x}\right)\right) \left(1 + O\left(\frac{1}{\log x}\right)\right) \\ &= c_\alpha x (\log x)^{-1/2} \sum_{d \leq D} \frac{\lambda^+(d) \alpha(d)}{d} \left(1 + O\left(\frac{\log y}{y}\right)\right) \\ &= c_\alpha x (\log x)^{-1/2} \left(\sum_{d \leq D} \frac{\lambda^+(d) \alpha(d)}{d} + O\left(\frac{\log y}{y} \sum_{d \leq D} \frac{|\lambda^+(d)| \alpha(d)}{d}\right)\right). \end{aligned}$$

For each  $q \in I_2$ , we have by (19) that

$$\sum_{p \in \mathcal{Q}_1(q)} \frac{1}{p} \leq \sum_{p \in \mathcal{Q}(q)} \frac{1}{p} \leq \sum_{\substack{p \leq x \\ p \in \mathcal{P}_{-1} \\ p \equiv -1 \pmod{q}}} \frac{1}{p} = \frac{\varphi(|\Delta|)}{2} \cdot \frac{y + O(\log q)}{\varphi(|\Delta|)\varphi(q)} = \frac{y + O(\log y)}{2\varphi(q)} = \frac{y + O(\log y)}{2q},$$

where the last equality results from the inequality  $y/(q\varphi(q)) < 2(\log y)/q$ . It follows that

$$\sum_{d \leq D} \frac{|\lambda^+(d)| \alpha(d)}{d} \leq \sum_{\substack{d \geq 1 \\ p|d \Rightarrow p \in \mathcal{Q}_1(q)}} \frac{1}{d} \leq \prod_{p \in \mathcal{Q}_1(q)} \left(1 - \frac{1}{p}\right)^{-1} \ll \exp\left(\sum_{p \in \mathcal{Q}_1(q)} \frac{1}{p}\right) \ll e^{\frac{y}{2q}},$$

whence

$$\sum_{d \leq D} \lambda^+(d) \sum_{\substack{f \leq x \\ d|f}} \alpha(f) = c_\alpha x (\log x)^{-1/2} \left(\sum_{d \leq D} \frac{\lambda^+(d) \alpha(d)}{d} + O\left(\frac{\log y}{y} e^{\frac{y}{2q}}\right)\right).$$

Inserting this into (30) and applying (29), we have

$$\sum_{\substack{f \leq x \\ (f, \mathcal{Q}_1(q))=1}} \alpha(f) \leq S_\alpha(x) (1 + O(u^{-u/2})) \prod_{p \in \mathcal{Q}_1(q)} \left(1 - \frac{1}{p}\right) + O\left(\frac{S_\alpha(x) \log y}{y} e^{\frac{y}{2q}}\right).$$

Arguing with  $\lambda^-$  in place of  $\lambda^+$  leads to the reversed inequality. Therefore, we obtain

$$\sum_{\substack{f \leq x \\ (f, \mathcal{Q}_1(q))=1}} \alpha(f) = S_\alpha(x) (1 + O(u^{-u/2})) \prod_{p \in \mathcal{Q}_1(q)} \left(1 - \frac{1}{p}\right) + O\left(\frac{S_\alpha(x) \log y}{y} e^{\frac{y}{2q}}\right),$$

Summing on  $q \in I_2$ , we conclude that

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f) = (1 + O(u^{-u/2})) \sum_{q \in I_2} \prod_{p \in \mathcal{Q}_1(q)} \left(1 - \frac{1}{p}\right) + O\left(\frac{\sqrt{y}}{\log y}\right), \quad (31)$$

since

$$\sum_{q \in I_2} e^{\frac{y}{2q}} \leq \sum_{y/\log y < q \leq 2y/\log y} e^{\frac{\log y}{2}} + \sum_{2y/\log y < q \leq y \log y} e^{\frac{\log y}{4}} \ll \frac{y^{3/2}}{(\log y)^2}. \quad (32)$$

To complete the estimation of the first weighted moment of  $g$ , it suffices to estimate

$$\sum_{q \in I_2} \prod_{p \in \mathcal{Q}_1(q)} \left(1 - \frac{1}{p}\right).$$

A similar sum is handled in [5], and the method there can be easily adapted to treat our sum above. So we will be brief. We start by observing that

$$\begin{aligned} \sum_{p \in \mathcal{Q}_1(q)} \frac{1}{p} &= \sum_{\substack{p \leq x^{1/y} \\ p \notin \mathcal{P}_1 \\ p \equiv \chi(p) \pmod{q}}} \frac{1}{p} - \sum_{\substack{p \leq x^{1/y} \\ p \in \mathcal{Q}_2(q)}} \frac{1}{p} \\ &= \sum_{\substack{p \leq x^{1/y} \\ p \in \mathcal{P}_{-1} \\ p \equiv -1 \pmod{q}}} \frac{1}{p} + O\left(\sum_{q' \in I_2} \sum_{\substack{p \leq x \\ p \equiv -1 \pmod{qq'}}} \frac{1}{p}\right) \\ &= \frac{\varphi(|\Delta|)}{2} \cdot \frac{\log \log x^{1/y} + O(\log q)}{\varphi(|\Delta|)\varphi(q)} + O\left(y \sum_{q' \in I_2} \frac{1}{\varphi(qq')}\right) \\ &= \frac{y}{2q} + O\left(\frac{y \log_2 y}{q \log y}\right). \end{aligned}$$

Thus, following [5, pp. 369–370], we have

$$\begin{aligned}
\sum_{q \in I_2} \prod_{p \in \mathcal{Q}_1(q)} \left(1 - \frac{1}{p}\right) &= \sum_{q \in I_2} \exp\left(-\frac{y}{2q} + O\left(\frac{y \log_2 y}{q \log y}\right)\right) \\
&= \sum_{q \in I_2} e^{-\frac{y}{2q}} \left(1 + O\left(\frac{y \log_2 y}{q \log y}\right)\right) + O\left(\sum_{q \leq y/4 \log_2 y} \frac{1}{(\log y)^2}\right) \\
&= \sum_{q \in I_2} e^{-\frac{y}{2q}} + O\left(\frac{y(\log_2 y)^2}{(\log y)^2}\right). \tag{33}
\end{aligned}$$

By partial summation, we see that

$$\sum_{q \in I_2} e^{-\frac{y}{2q}} = \left(\pi(y \log y) - \pi\left(\frac{y}{\log y}\right)\right) e^{-\frac{1}{2 \log y}} - \int_{y/\log y}^{y \log y} e^{-\frac{y}{2t}} \frac{y}{2t^2} \left(\pi(t) - \pi\left(\frac{y}{\log y}\right)\right) dt. \tag{34}$$

By the Prime Number Theorem, we have

$$\left(\pi(y \log y) - \pi\left(\frac{y}{\log y}\right)\right) e^{-\frac{1}{2 \log y}} = y - \frac{y \log_2 y}{\log y} + \frac{y}{2 \log y} + O\left(\frac{y(\log_2 y)^2}{(\log y)^2}\right).$$

Following [5, p 371], the integral in (34) equals

$$\begin{aligned}
&\int_{y/\log y}^{y \log y} e^{-\frac{y}{2t}} \frac{y}{2t^2} \left(\frac{t}{\log t} + O\left(\frac{t}{(\log t)^2}\right)\right) dt - \pi\left(\frac{y}{\log y}\right) \left(e^{-\frac{1}{2 \log y}} - e^{-\frac{\log y}{2}}\right) \\
&= \int_{y/\log y}^{y \log y} e^{-\frac{y}{2t}} \frac{y}{2t} \left(\frac{1}{\log y} + O\left(\frac{\log_2 y}{(\log y)^2}\right)\right) dt + O\left(\frac{y}{(\log y)^2}\right) \\
&= \frac{y}{2 \log y} \int_{2/\log y}^{2 \log y} e^{-\frac{1}{v}} \frac{dv}{v} + O\left(\frac{y(\log_2 y)^2}{(\log y)^2}\right) \\
&= \frac{y}{2 \log y} \left(e^{-\frac{1}{2 \log y}} \log(2 \log y) + e^{-\frac{\log y}{2}} \log \frac{\log y}{2} - \int_{2/\log y}^{2 \log y} e^{-\frac{1}{v}} \frac{\log v}{v^2} dv\right) + O\left(\frac{y(\log_2 y)^2}{(\log y)^2}\right) \\
&= \frac{y}{2 \log y} \left(\log_2 y + \log 2 - \int_0^\infty e^{-\frac{1}{v}} \frac{\log v}{v^2} dv\right) + O\left(\frac{y(\log_2 y)^2}{(\log y)^2}\right) \\
&= \frac{y \log_2 y}{2 \log y} + \frac{1}{2}(\log 2 - \gamma) \frac{y}{\log y} + O\left(\frac{y(\log_2 y)^2}{(\log y)^2}\right),
\end{aligned}$$

by partial integration and the Prime Number Theorem, where we have exploited the identity

$$\gamma = -\Gamma'(1) = -\int_0^\infty e^{-t} \log t dt = \int_0^\infty e^{-\frac{1}{v}} \frac{\log v}{v^2} dv,$$

with  $\Gamma$  being the Gamma function. Combining these estimates with (33) and (34) yields

$$\sum_{q \in I_2} \prod_{p \in \mathcal{Q}_1(q)} \left(1 - \frac{1}{p}\right) = y - \frac{3y \log_2 y}{2 \log y} + \frac{1}{2}(1 - \log 2 + \gamma) \frac{y}{\log y} + O\left(\frac{y(\log_2 y)^2}{(\log y)^2}\right).$$

Carrying this back into (31), we conclude that the first weighted moment of  $g$  is

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f) = y - \frac{3y \log_2 y}{2 \log y} + \frac{1}{2}(1 - \log 2 + \gamma) \frac{y}{\log y} + O\left(\frac{y(\log_2 y)^2}{(\log y)^2}\right). \tag{35}$$

Next, we estimate the second weighted moment of  $g$  defined by

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f)^2 = S_\alpha(x)^{-1} \sum_{q_1, q_2 \in I_2} \sum_{\substack{f \leq x \\ (f, \mathcal{Q}_1(q_1) \cup \mathcal{Q}_1(q_2))=1}} \alpha(f).$$

The contribution from the diagonal terms with  $q_1 = q_2$  is exactly the first weighted moment of  $g$  whose estimate is provided by (35). On the other hand, a similar application of the fundamental lemma of sieve theory to  $\mathcal{Q}_1(q_1) \cup \mathcal{Q}_1(q_2)$ , but with  $D = x^{u/y}$  and  $u = \log_2 y$  this time, implies that the contribution from the off-diagonal terms with  $q_1 \neq q_2$  is

$$(1 + O(u^{-u/2})) \sum_{\substack{q_1, q_2 \in I_2 \\ q_1 \neq q_2}} \prod_{p \in \mathcal{Q}_1(q_1) \cup \mathcal{Q}_1(q_2)} \left(1 - \frac{1}{p}\right) + O\left(\frac{\log_2 y}{y} \sum_{\substack{q_1, q_2 \in I_2 \\ q_1 \neq q_2}} e^{\frac{y}{2q_1} + \frac{y}{2q_2}}\right),$$

where the second error term is evidently  $O(y^2 \log_2 y / (\log y)^4)$  by (32). Since  $\mathcal{Q}_1(q_1) \cap \mathcal{Q}_1(q_2) = \emptyset$  for  $q_1 \neq q_2$ , we have

$$\begin{aligned} & (1 + O(u^{-u/2})) \sum_{\substack{q_1, q_2 \in I_2 \\ q_1 \neq q_2}} \prod_{p \in \mathcal{Q}_1(q_1) \cup \mathcal{Q}_1(q_2)} \left(1 - \frac{1}{p}\right) \\ &= (1 + O(u^{-u/2})) \left( \sum_{q \in I_2} \prod_{p \in \mathcal{Q}_1(q)} \left(1 - \frac{1}{p}\right) \right)^2 - (1 + O(u^{-u/2})) \sum_{q \in I_2} \prod_{p \in \mathcal{Q}_1(q)} \left(1 - \frac{1}{p}\right)^2 \\ &= (1 + O(u^{-u/2})) \left( S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f) + O\left(\frac{\sqrt{y}}{\log y}\right) \right)^2 + O(\pi(y \log y)) \\ &= \left( S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f) \right)^2 + O(y^2 u^{-u/2}), \end{aligned}$$

by (31) and (35). Thus, the contribution from the off-diagonal terms with  $q_1 \neq q_2$  is

$$\left( S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f) \right)^2 + O\left(\frac{y^2 \log_2 y}{(\log y)^4}\right).$$

It follows that the second weighted moment of  $g$  is

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f)^2 = \left( S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f) \right)^2 + O\left(\frac{y^2 \log_2 y}{(\log y)^4}\right).$$

Therefore,

$$\begin{aligned} & S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \left( g(f) - S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f) \right)^2 \\ &= S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f)^2 - \left( S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) g(f) \right)^2 \ll \frac{y^2 \log_2 y}{(\log y)^4}, \end{aligned}$$

which in conjunction with (35) allows us to deduce that

$$\left| g(f) - \left( y - \frac{3y \log_2 y}{2 \log y} + \frac{1}{2}(1 - \log 2 + \gamma) \frac{y}{\log y} \right) \right| < \frac{y(\log_2 y)^3}{(\log y)^2} \quad (36)$$

holds for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ .

Combining (28) with (36), we find, as in [5], that the contribution to  $\log L(f)$  from the primes  $q \in I_2$  is

$$\begin{aligned} & (\log y + O(\log_2 y)) \sum_{\substack{q \in I_2 \\ (f, \mathcal{Q}_1(q)) > 1}} 1 + O\left(\frac{y(\log_2 y)^3}{\log y}\right) \\ &= (\log y + O(\log_2 y)) \left( \pi(y \log y) - \pi\left(\frac{y}{\log y}\right) - g(f) \right) + O\left(\frac{y(\log_2 y)^3}{\log y}\right) \\ &= (\log y + O(\log_2 y)) \left( \frac{y \log_2 y}{2 \log y} + \frac{1}{2}(1 + \log 2 - \gamma) \frac{y}{\log y} + O\left(\frac{y(\log_2 y)^3}{(\log y)^2}\right) \right) + O\left(\frac{y(\log_2 y)^3}{\log y}\right) \\ &= \frac{1}{2} y \log_2 y + \frac{1}{2}(1 + \log 2 - \gamma)y + O\left(\frac{y(\log_2 y)^3}{\log y}\right). \end{aligned} \quad (37)$$

**4.4. Contribution from  $I_3$ .** Now we estimate the contribution to the left-hand side of (18) from the primes  $q \in I_3$ . As remarked at the beginning of Section 4, we have that  $q^2 \nmid f$  for any  $q \notin I_1$  for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ . So we may assume  $q^2 \nmid f$  for any  $q \in I_3$ . We may assume further that  $q^2 \nmid L(f)$  for any  $q \in I_3$ , thanks to the estimate

$$\begin{aligned} & S_\alpha(x)^{-1} \sum_{q \in I_3} \sum_{\substack{p \leq x \\ p \equiv \chi(p) \pmod{q^2}}} \sum_{\substack{f \leq x \\ p \mid f}} \alpha(f) \\ &\ll \sum_{q \in I_3} \sum_{\substack{p \leq x \\ p \equiv \chi(p) \pmod{q^2}}} \frac{\alpha(p)}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \\ &\leq \sum_{q \in I_3} \sum_{\substack{p \leq x \\ p \equiv -1 \pmod{q^2}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \\ &\ll \sum_{q \in I_3} \sum_{\substack{p \leq \sqrt{x} \\ p \equiv -1 \pmod{q^2}}} \frac{1}{p} + \sum_{q \in I_3} \sum_{\substack{\sqrt{x} < p \leq x \\ p \equiv -1 \pmod{q^2}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \\ &\ll y \sum_{q > y \log y} \frac{1}{\varphi(q^2)} + \sum_{q > y \log y} \frac{1}{\varphi(q^2)} \\ &\ll \frac{1}{(\log y)^2}. \end{aligned}$$

If  $q^2 \nmid f$  and  $v_q(L(f)) = 1$ , then  $p \not\equiv \chi(p) \pmod{q^2}$  for any  $p \mid f$ , and the number  $\omega(f, \mathcal{Q}(q))$  of primes  $p \in \mathcal{Q}(q)$  dividing  $f$  is  $v_q(\psi(f))$ . Thus, setting

$$G(f) := \sum_{\substack{q \in I_3 \\ \omega(f, \mathcal{Q}(q)) > 1}} \omega(f, \mathcal{Q}(q)) \log q,$$

we have

$$\sum_{q \in I_3} (v_q(\psi(f)) - v_q(L(f))) \log q = \sum_{\substack{q \in I_3 \\ v_q(L(f))=1}} (v_q(\psi(f)) - 1) \log q \leq G(f)$$

for those  $f$  with  $q^2 \nmid f$  and  $q^2 \nmid L(f)$  for any  $q \in I_3$ . We show that the mean value of  $G$  over split-free  $f \leq x$  is

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) G(f) \ll \frac{y}{\log y}. \quad (38)$$

From this it follows that  $G(f) < y \log_2 y / \log y$  for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ . Hence, the contribution to the left-hand side of (18) from the primes  $q \in I_3$  is

$$\sum_{q \in I_3} (v_q(\psi(f)) - v_q(L(f))) \log q < \frac{y \log_2 y}{\log y} \quad (39)$$

for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ . We now prove (38). We have

$$\begin{aligned} S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) G(f) &= S_\alpha(x)^{-1} \sum_{q \in I_3} \log q \sum_{k \geq 2} k \sum_{\substack{f \leq x \\ \omega(f, \mathcal{Q}(q))=k}} \alpha(f) \\ &\leq S_\alpha(x)^{-1} \sum_{q \in I_3} \log q \sum_{k \geq 2} k \sum_{p_1 < \dots < p_k \in \mathcal{Q}(q)} \sum_{\substack{f \leq x \\ p_1 \dots p_k \mid f}} \alpha(f) \\ &\ll \sum_{q \in I_3} \log q \sum_{k \geq 2} k \sum_{\substack{p_1 \dots p_k \leq x \\ p_1 < \dots < p_k \\ \forall i, p_i \equiv -1 \pmod{q}}} \frac{1}{p_1 \dots p_k} \left( 1 - \frac{\log(p_1 \dots p_k)}{\log 3x} \right)^{-1/2}. \end{aligned}$$

By (19), we have

$$\begin{aligned} &\sum_{q \in I_3} \log q \sum_{k \geq 2} k \sum_{\substack{p_1 \dots p_k \leq \sqrt{x} \\ p_1 < \dots < p_k \\ \forall i, p_i \equiv -1 \pmod{q}}} \frac{1}{p_1 \dots p_k} \left( 1 - \frac{\log(p_1 \dots p_k)}{\log 3x} \right)^{-1/2} \\ &\ll \sum_{q \in I_3} \log q \sum_{k \geq 2} \frac{1}{(k-1)!} \left( \sum_{\substack{p \leq x \\ p \equiv -1 \pmod{q}}} \frac{1}{p} \right)^k \\ &= \sum_{q \in I_3} \log q \sum_{k \geq 2} \frac{1}{(k-1)!} \left( \frac{y + O(\log q)}{\varphi(q)} \right)^k \ll \frac{y}{\log y}, \end{aligned}$$

where the last inequality follows from  $y/\varphi(q) \ll 1/\log y = o(1)$ , as in [5]. We still have to estimate

$$\sum_{q \in I_3} \log q \sum_{k \geq 2} k \sum_{\substack{\sqrt{x} < p_1 \cdots p_k \leq x \\ p_1 < \cdots < p_k \\ \forall i, p_i \equiv -1 \pmod{q}}} \frac{1}{p_1 \cdots p_k} \left(1 - \frac{\log(p_1 \cdots p_k)}{\log 3x}\right)^{-1/2}.$$

Put  $m = \lceil y/\log y \rceil$ . Stirling's formula implies that

$$m! \gg m^{m+1/2} e^{-m} = e^{y+O(y/\log y)} \geq (\log x)^{1/2}.$$

Since  $y/\varphi(q) = o(1)$ , we have

$$\begin{aligned} & \sum_{q \in I_3} \log q \sum_{k \geq m+1} k \sum_{\substack{\sqrt{x} < p_1 \cdots p_k \leq x \\ p_1 < \cdots < p_k \\ \forall i, p_i \equiv -1 \pmod{q}}} \frac{1}{p_1 \cdots p_k} \left(1 - \frac{\log(p_1 \cdots p_k)}{\log 3x}\right)^{-1/2} \\ & \ll (\log x)^{1/2} \sum_{q \in I_3} \log q \sum_{k \geq m+1} k \sum_{\substack{\sqrt{x} < p_1 \cdots p_k \leq x \\ p_1 < \cdots < p_k \\ \forall i, p_i \equiv -1 \pmod{q}}} \frac{1}{p_1 \cdots p_k} \\ & \leq (\log x)^{1/2} \sum_{q \in I_3} \log q \sum_{k \geq m+1} \frac{1}{(k-1)!} \left( \sum_{\substack{p \leq x \\ p \equiv -1 \pmod{q}}} \frac{1}{p} \right)^k \\ & \ll \sum_{q \in I_3} \log q \sum_{k \geq m+1} \frac{m!}{(k-1)!} \left( \frac{y + O(\log y)}{\varphi(q)} \right)^k \\ & \leq e \sum_{q \in I_3} \log q \left( \frac{y + O(\log y)}{\varphi(q)} \right)^2 \\ & \ll y^2 \sum_{q > y \log y} \frac{\log q}{q^2} \ll \frac{y}{\log y}. \end{aligned}$$

Thus, it remains to estimate

$$\sum_{q \in I_3} \log q \sum_{k=2}^m k \sum_{\substack{\sqrt{x} < p_1 \cdots p_k \leq x \\ p_1 < \cdots < p_k \\ \forall i, p_i \equiv -1 \pmod{q}}} \frac{1}{p_1 \cdots p_k} \left(1 - \frac{\log(p_1 \cdots p_k)}{\log 3x}\right)^{-1/2} \quad (40)$$

Thanks to the constraint  $k \leq m$ , we have  $x^{1/2k}/q = x^{(1/2-o(1))/k}$ . Besides, the constraints  $p_1 \cdots p_k > \sqrt{x}$  and  $p_1 < \cdots < p_k$  imply that  $p_k > (p_1 \cdots p_k)^{1/k} > x^{1/2k}$ . Let  $m_k := p_1 \cdots p_{k-1}$ ,  $a_k := \max(x^{1/2k}, \sqrt{x}/m_k)$  and  $b_k := x/m_k \in (x^{1/2k}, x]$ . Since

$$-\frac{d}{dt} \left( \frac{1}{t} \left(1 - \frac{\log(m_k t)}{\log 3x}\right)^{-1/2} \right) \leq \frac{1}{t^2} \left(1 - \frac{\log(m_k t)}{\log 3x}\right)^{-1/2}$$



for any  $t \in (0, b_k]$ , it follows from Brun–Titchmarsh and partial summation that

$$\begin{aligned}
& \sum_{\substack{a_k < p_k \leq b_k \\ p_k \equiv -1 \pmod{q}}} \frac{1}{p_k} \left( 1 - \frac{\log(p_1 \cdots p_k)}{\log 3x} \right)^{-1/2} \\
& \ll \frac{(\log x)^{1/2} \pi(b_k; q, -1)}{b_k} - \int_{a_k}^{b_k} \pi(t; q, -1) \frac{d}{dt} \left( \frac{1}{t} \left( 1 - \frac{\log(m_k t)}{\log 3x} \right)^{-1/2} \right) dt \\
& \leq \frac{(\log x)^{1/2} \pi(b_k; q, -1)}{b_k} + \int_{a_k}^{b_k} \frac{\pi(t; q, -1)}{t^2} \left( 1 - \frac{\log(m_k t)}{\log 3x} \right)^{-1/2} dt \\
& \ll \frac{k}{\varphi(q) \sqrt{\log x}} + \frac{1}{\varphi(q)} \int_{a_k}^{b_k} \frac{1}{t \log t} \left( 1 - \frac{\log(m_k t)}{\log 3x} \right)^{-1/2} dt \\
& \ll \frac{k}{\varphi(q) \sqrt{\log x}} + \frac{k}{\varphi(q) \log x} \int_{\sqrt{x}}^x \frac{1}{t} \left( 1 - \frac{\log t}{\log 3x} \right)^{-1/2} dt \\
& \ll \frac{k}{\varphi(q) \sqrt{\log x}} + \frac{k}{\varphi(q)} \int_{\frac{\log \sqrt{x}}{\log 3x}}^{\frac{\log x}{\log 3x}} (1-t)^{-1/2} dt \\
& \ll \frac{k}{\varphi(q)}.
\end{aligned}$$

Hence, we have

$$\begin{aligned}
& \sum_{q \in I_3} \log q \sum_{k=2}^m k \sum_{\substack{\sqrt{x} < p_1 \cdots p_k \leq x \\ p_1 < \cdots < p_k \\ \forall i, p_i \equiv -1 \pmod{q}}} \frac{1}{p_1 \cdots p_k} \left( 1 - \frac{\log(p_1 \cdots p_k)}{\log 3x} \right)^{-1/2} \\
& \ll \sum_{q \in I_3} \frac{\log q}{\varphi(q)} \sum_{k \geq 2} k^2 \sum_{\substack{p_1 < \cdots < p_{k-1} \leq x \\ \forall i, p_i \equiv -1 \pmod{q}}} \frac{1}{p_1 \cdots p_{k-1}} \\
& \ll \sum_{q \in I_3} \frac{\log q}{\varphi(q)} \sum_{k \geq 2} \frac{k}{(k-2)!} \left( \frac{y + O(\log y)}{\varphi(q)} \right)^{k-1} \\
& \ll \sum_{q \in I_3} \frac{\log q}{\varphi(q)} \left( \frac{y + O(\log y)}{\varphi(q)} \right) \ll \frac{1}{\log y}.
\end{aligned}$$

Collecting the estimates above yields (38).

**4.5. Contribution from  $I_4$  and completion of the proof.** Finally, we estimate the contribution to the left-hand side of (18) from the primes  $q \in I_4$ . We show that

$$\sum_{q \in I_4} (v_q(\psi(f)) - v_q(L(f))) \log q = 0 \tag{41}$$

for all but  $o(S_\alpha(x))$  split-free  $f \leq x$ . Since we may assume  $q^2 \nmid f$  for any  $q \in I_4$ , it suffices to show that all but  $o(S_\alpha(x))$  split-free  $f \leq x$  are divisible by at most one prime in  $\mathcal{Q}(q)$  for any  $q \in I_4$ .

This follows quickly from an averaging argument. We have

$$S_\alpha(x)^{-1} \sum_{q \in I_4} \sum_{p_1 < p_2 \in \mathcal{Q}(q)} \sum_{\substack{f \leq x \\ p_1 p_2 | f}} \alpha(f) \ll \sum_{y^2 < q \leq \sqrt{x}+1} \sum_{\substack{p_1 p_2 \leq x \\ p_1 < p_2 \\ p_1, p_2 \equiv -1 \pmod{q}}} \frac{1}{p_1 p_2} \left(1 - \frac{\log p_1 p_2}{\log 3x}\right)^{-1/2},$$

where the constraint  $q \leq \sqrt{x} + 1$  holds because  $q$  divides  $p_1 + 1 < \sqrt{x} + 1$ . It is easy to see that

$$\begin{aligned} \sum_{y^2 < q \leq \sqrt{x}+1} \sum_{\substack{p_1 p_2 \leq x^{2/3} \\ p_1 < p_2 \\ p_1, p_2 \equiv -1 \pmod{q}}} \frac{1}{p_1 p_2} \left(1 - \frac{\log p_1 p_2}{\log 3x}\right)^{-1/2} &\ll \sum_{y^2 < q \leq \sqrt{x}+1} \sum_{\substack{p_1, p_2 \leq x \\ p_1, p_2 \equiv -1 \pmod{q}}} \frac{1}{p_1 p_2} \\ &\ll y^2 \sum_{q > y^2} \frac{1}{\varphi(q)^2} \ll \frac{1}{\log y} \end{aligned}$$

and

$$\begin{aligned} \sum_{\log x < q \leq \sqrt{x}+1} \sum_{\substack{p_1 p_2 \leq x \\ p_1 < p_2 \\ p_1, p_2 \equiv -1 \pmod{q}}} \frac{1}{p_1 p_2} \left(1 - \frac{\log p_1 p_2}{\log 3x}\right)^{-1/2} &\ll \sum_{\log x < q \leq \sqrt{x}+1} \sum_{\substack{p_1, p_2 \leq x \\ p_1, p_2 \equiv -1 \pmod{q}}} \frac{(\log x)^{1/2}}{p_1 p_2} \\ &\leq (\log x)^{1/2} y^2 \sum_{q > \log x} \frac{1}{\varphi(q)^2} \\ &\ll \frac{y}{\sqrt{\log x}}. \end{aligned}$$

Hence, it remains to estimate the sum

$$\sum_{y^2 < q \leq \log x} \sum_{\substack{x^{2/3} < p_1 p_2 \leq x \\ p_1 < p_2 \\ p_1, p_2 \equiv -1 \pmod{q}}} \frac{1}{p_1 p_2} \left(1 - \frac{\log p_1 p_2}{\log 3x}\right)^{-1/2}.$$

But the argument used to estimate (40) shows that this sum is

$$\ll \sum_{y^2 < q \leq \log x} \frac{1}{\varphi(q)} \sum_{\substack{p \leq x \\ p \equiv -1 \pmod{q}}} \frac{1}{p} \ll y \sum_{q > y^2} \frac{1}{\varphi(q)^2} \ll \frac{1}{y \log y}.$$

Therefore, we have

$$S_\alpha(x)^{-1} \sum_{q \in I_4} \sum_{p_1 < p_2 \in \mathcal{Q}(q)} \sum_{\substack{f \leq x \\ p_1 p_2 | f}} \alpha(f) \ll \frac{1}{\log y},$$

from which we verify that all but  $o(S_\alpha(x))$  split-free  $f \leq x$  are divisible by at most one prime in  $\mathcal{Q}(q)$  for any  $q \in I_4$ .

Combining (21), (23), (37), (39) and (41) completes the proof of (18) and hence that of Proposition 2.6 for  $L(f)$ .

5. INTERLUDE: THE RADICAL OF  $\psi(f)/L(f)$ 

We devote this section to establishing the following result on the typical size of the radical of  $\psi(f)/L(f)$  with  $f$  split-free, which will be needed in the proof of Proposition 2.7.

**Proposition 5.1.** *For almost all split-free  $f$ ,*

$$\text{Rad} \frac{\psi(f)}{L(f)} = (\log f)^{\frac{1}{2} + O(1/\log_3 f)}.$$

Our proof of Proposition 5.1 adapts that of [21, Theorem 1] on the typical size of  $\omega(\varphi(n)/\lambda(n))$ . As in Section 4, the complication comes mainly from estimation of weighted sums. Our setup is similar to that in [21]. Let

$$W(f) := \log \text{Rad} \frac{\psi(f)}{L(f)} = \sum_{p \mid \frac{\psi(f)}{L(f)}} \log p.$$

Let  $y = \log_2 x$ , and define  $\mathcal{I} := (y/\log y, y \log y]$ , which is exactly same as the interval  $I_2$  introduced in Section 4, and

$$\mathcal{J}_f := \{p \in \mathcal{I} : \exists \text{ distinct primes } q_1, q_2 \mid f \text{ with } q_i \leq x^{1/y} \text{ and } q_i \equiv \chi(q_i) \pmod{p} \text{ for } i = 1, 2\}$$

for split-free  $f \in \mathbb{N}$ . Finally, we set

$$\widetilde{W}(f) := \sum_{p \in \mathcal{J}_f} \log p,$$

which we think of as an approximation to  $W(f)$ . It is not hard to see that Proposition 5.1 follows from the following estimates combined:

(I)  $W(f) - \widetilde{W}(f)$  on average:

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \left( W(f) - \widetilde{W}(f) \right) \ll \frac{y}{\log y}.$$

(II) The first moment of  $\widetilde{W}$ :

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \widetilde{W}(f) = \left( \frac{1}{2} + O\left( \frac{1}{\log y} \right) \right) y.$$

(III) The second moment of  $\widetilde{W}$ :

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \widetilde{W}(f)^2 = \left( \frac{1}{4} + O\left( \frac{1}{\log y} \right) \right) y^2.$$

We shall prove (I) and (II) but only sketch the proof of (III) while leaving the full details to the interested reader. Before embarking on the proof, we point out that the primes  $p$  included in the definition of  $W(f)$  satisfy either (i)  $p^2 \mid f$ , or (ii)  $f$  is divisible by two distinct primes  $q_1, q_2$  with  $q_i \equiv \chi(q_i) \pmod{p}$  for  $i = 1, 2$ . The primes in set  $\mathcal{J}_f$  hence belong to the second category.

5.1.  $W(f) - \widetilde{W}(f)$  **on average.** We start by proving (I). Write  $W(f) - \widetilde{W}(f) = T_0(f) + T_1(f)$ , where

$$T_0(f) = \sum_{\substack{p \mid \frac{\psi(f)}{L(f)} \\ p \leq y/\log y}} \log p,$$

$$T_1(f) = \sum_{\substack{p \mid \frac{\psi(f)}{L(f)}, p \notin \mathcal{J}_f \\ p > y/\log y}} \log p.$$

The Prime Number Theorem implies that  $T_0(f) < 2y/\log y$ , so that

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) T_0(f) < \frac{2y}{\log y}.$$

To estimate the mean value of  $T_1$ , we observe that the primes  $p$  included in definition of  $T_1(f)$  satisfy (i)  $p^2 \mid f$ , or (ii)  $p \in \mathcal{I}$  and  $q \mid f$  for some prime  $q \equiv \chi(q) \pmod{p}$  with  $q > x^{1/y}$ , or (iii)  $p > y \log y$  and there exist distinct primes  $q_1, q_2 \mid f$  with  $q_i \equiv \chi(q_i) \pmod{p}$  for  $i = 1, 2$ . The contribution from those primes  $p$  satisfying (i) is

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \sum_{\substack{p > y/\log y \\ p^2 \mid f}} \log p = S_\alpha(x)^{-1} \sum_{p > y/\log y} \alpha(p^2) \log p \sum_{f \leq x/p^2} \alpha(f) \ll \frac{\log y}{y},$$

by the same argument at the beginning of Section 4. Next, the contribution from those primes  $p$  satisfying (ii) is

$$\begin{aligned} S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \sum_{p \in \mathcal{I}} \log p \sum_{\substack{x^{1/y} < q \leq x \\ q \mid f \\ q \equiv \chi(q) \pmod{p}}} 1 &= S_\alpha(x)^{-1} \sum_{p \in \mathcal{I}} \log p \sum_{\substack{x^{1/y} < q \leq x \\ q \equiv \chi(q) \pmod{p}}} \sum_{\substack{f \leq x \\ q \mid f}} \alpha(f) \\ &\ll \sum_{p \in \mathcal{I}} \log p \sum_{\substack{x^{1/y} < q \leq x \\ q \equiv -1 \pmod{p}}} \frac{1}{q} \left( 1 - \frac{\log q}{\log 3x} \right)^{-1/2}. \end{aligned}$$

Since Brun–Titchmarsh and partial summation imply

$$\begin{aligned} \sum_{\substack{x^{1/y} < q \leq \sqrt{x} \\ q \equiv -1 \pmod{p}}} \frac{1}{q} \left( 1 - \frac{\log q}{\log 3x} \right)^{-1/2} &\ll \sum_{\substack{x^{1/y} < q \leq \sqrt{x} \\ q \equiv -1 \pmod{p}}} \frac{1}{q} \ll \frac{\log y}{\varphi(p)}, \\ \sum_{\substack{\sqrt{x} < q \leq x \\ q \equiv -1 \pmod{p}}} \frac{1}{q} \left( 1 - \frac{\log q}{\log 3x} \right)^{-1/2} &\ll \frac{1}{\varphi(p)}, \end{aligned}$$

we find that the contribution from those primes  $p$  satisfying (ii) is

$$\ll \log y \sum_{p \in \mathcal{I}} \frac{\log p}{\varphi(p)} \ll (\log y) \log_2 y.$$

Finally, the contribution from those primes  $p$  satisfying (iii) is

$$\begin{aligned} & S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \sum_{p > y \log y} \log p \sum_{\substack{q_1 q_2 \leq x \\ q_1 q_2 | f, q_1 \neq q_2 \\ \forall i, q_i \equiv \chi(q_i) \pmod{p}}} 1 \\ & \ll \sum_{p > y \log y} \log p \sum_{\substack{q_1 q_2 \leq x \\ q_1 < q_2 \\ q_1, q_2 \equiv -1 \pmod{p}}} \frac{1}{q_1 q_2} \left( 1 - \frac{\log q_1 q_2}{\log 3x} \right)^{-1/2}. \end{aligned}$$

If  $p > \log x$ , then we have

$$\sum_{\substack{q_1 q_2 \leq x \\ q_1 < q_2 \\ q_1, q_2 \equiv -1 \pmod{p}}} \frac{1}{q_1 q_2} \left( 1 - \frac{\log q_1 q_2}{\log 3x} \right)^{-1/2} \ll (\log x)^{1/2} \left( \sum_{\substack{q \leq x \\ q \equiv -1 \pmod{p}}} \frac{1}{q} \right)^2 \ll \frac{(\log x)^{1/2} y^2}{\varphi(p)^2};$$

if  $y \log y < p \leq \log x$ , then we have

$$\begin{aligned} & \sum_{\substack{q_1 q_2 \leq x^{2/3} \\ q_1 < q_2 \\ q_1, q_2 \equiv -1 \pmod{p}}} \frac{1}{q_1 q_2} \left( 1 - \frac{\log q_1 q_2}{\log 3x} \right)^{-1/2} \ll \left( \sum_{\substack{q \leq x \\ q \equiv -1 \pmod{p}}} \frac{1}{q} \right)^2 \ll \frac{y^2}{\varphi(p)^2}, \\ & \sum_{\substack{x^{2/3} < q_1 q_2 \leq x \\ q_1 < q_2 \\ q_1, q_2 \equiv -1 \pmod{p}}} \frac{1}{q_1 q_2} \left( 1 - \frac{\log q_1 q_2}{\log 3x} \right)^{-1/2} \leq \sum_{\substack{q_1 \leq \sqrt{x} \\ q_1 \equiv -1 \pmod{p}}} \frac{1}{q_1} \sum_{\substack{x^{2/3}/q_1 < q_2 \leq x/q_1 \\ q_2 \equiv -1 \pmod{p}}} \frac{1}{q_2} \left( 1 - \frac{\log q_1 q_2}{\log 3x} \right)^{-1/2} \\ & \ll \frac{1}{\varphi(p)} \sum_{\substack{q_1 \leq \sqrt{x} \\ q_1 \equiv -1 \pmod{p}}} \frac{1}{q_1} \ll \frac{y}{\varphi(p)^2}, \end{aligned}$$

where the estimate for the inner sum over  $x^{2/3}/q_1 < q_2 \leq x/q_1$  follows from the proof of (40) in Subsection 4.4. Hence, the contribution from those primes  $p$  satisfying (iii) is

$$\ll y^2 (\log x)^{1/2} \sum_{p > \log x} \frac{\log p}{\varphi(p)^2} + y^2 \sum_{p > y \log y} \frac{\log p}{\varphi(p)^2} \ll \frac{y}{\log y}.$$

Gathering all the contributions to the mean value of  $T_1$  above yields

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) T_1(f) \ll \frac{y}{\log y}.$$

Combining this with the mean value estimate for  $T_0$  proves (I).

**5.2. The first moment of  $\widetilde{W}(f)$ .** We now turn to the proof of (II). Following [21], let us write

$$\sum_{f \leq x} \alpha(f) \widetilde{W}(f) = \sum_{p \in \mathcal{I}} \log p \sum_{\substack{f \leq x \\ p \in \mathcal{J}_f}} \alpha(f) = \sum_{p \in \mathcal{I}} (S_\alpha(x) - N_0(p) - N_1(p)) \log p \quad (42)$$

where  $N_i(p)$  is defined to be

$$\#\{f \leq x \text{ split-free: } \exists \text{ exactly } i \text{ distinct primes } q \mid f \text{ with } q \leq x^{1/y} \text{ and } q \equiv \chi(q) \pmod{p}\}$$

for  $i = 0, 1$ . By the Prime Number Theorem, we have

$$S_\alpha(x)^{-1} \sum_{p \in \mathcal{I}} S_\alpha(x) \log p = \int_{\mathcal{I}} 1 dt + O\left(\frac{y}{(\log y)^A}\right) \quad (43)$$

for any fixed  $A > 0$ .

To estimate the mean value of  $N_0(p) \log p$ , we apply the fundamental lemma of sieve theory to the set of primes  $q \leq x^{1/y}$  with  $q \notin \mathcal{P}_1$  and  $q \equiv \chi(q) \pmod{p}$ , where  $D = x^{u/y}$  and  $u = \log y$ , in exactly the same way as in Subsection 4.3, to obtain

$$S_\alpha(x)^{-1} N_0(p) = (1 + O(u^{-u/2})) \prod_{\substack{q \leq x^{1/y} \\ q \in \mathcal{P}_{-1} \\ q \equiv -1 \pmod{p}}} \left(1 - \frac{1}{q}\right) + O\left(\frac{\log y}{y} e^{\frac{y}{2p}}\right).$$

Since

$$\sum_{\substack{q \leq x^{1/y} \\ q \in \mathcal{P}_{-1} \\ q \equiv -1 \pmod{p}}} \frac{1}{q} = \frac{\varphi(|\Delta|)}{2} \cdot \frac{\log \log x^{1/y} + O(\log p)}{\varphi(|\Delta|)\varphi(p)} = \frac{y}{2p} + O\left(\frac{(\log y)^2}{y}\right),$$

we have

$$\begin{aligned} S_\alpha(x)^{-1} N_0(p) &= (1 + O(u^{-u/2})) \exp\left(-\frac{y}{2p} + O\left(\sum_{q \equiv -1 \pmod{p}} \frac{1}{q^2} + \frac{(\log y)^2}{y}\right)\right) + O\left(\frac{\log y}{y} e^{\frac{y}{2p}}\right) \\ &= (1 + O(u^{-u/2})) \exp\left(-\frac{y}{2p} + O\left(\frac{1}{p \log p} + \frac{(\log y)^2}{y}\right)\right) + O\left(\frac{\log y}{y} e^{\frac{y}{2p}}\right) \\ &= \left(1 + O\left(\frac{(\log y)^2}{y}\right)\right) e^{-\frac{y}{2p}} + O\left(\frac{\log y}{y} e^{\frac{y}{2p}}\right). \end{aligned}$$

It follows from (32) that

$$S_\alpha(x)^{-1} \sum_{p \in \mathcal{I}} N_0(p) \log p = \left(1 + O\left(\frac{(\log y)^2}{y}\right)\right) \sum_{p \in \mathcal{I}} e^{-\frac{y}{2p}} \log p + O(\sqrt{y}).$$

By partial summation and the Prime Number Theorem, we have

$$\sum_{p \in \mathcal{I}} e^{-\frac{y}{2p}} \log p = \int_{\mathcal{I}} e^{-\frac{y}{2t}} dt + O\left(\frac{y}{(\log y)^A}\right)$$

for any fixed  $A > 0$ . Inserting this into the last equation above, we find that

$$S_\alpha(x)^{-1} \sum_{p \in \mathcal{I}} N_0(p) \log p = \int_{\mathcal{I}} e^{-\frac{y}{2t}} dt + O\left(\frac{y}{(\log y)^A}\right). \quad (44)$$

Finally, we estimate the mean value of  $N_1(p)$ . Note that  $N_1(p)$  can be approximated by

$$\sum_{\substack{q \leq x^{1/y} \\ q \notin \mathcal{P}_1 \\ q \equiv \chi(q) \pmod{p}}} \#\{m \leq x/q \text{ split-free: } m \text{ not divisible by any } q' \leq x^{1/y} \text{ with } q' \equiv \chi(q') \pmod{p}\},$$

with an error being

$$\ll \#\{f \leq x \text{ split-free: } f \text{ divisible by any } q^2 \text{ for some } q > y/\log y\}.$$

This error is evidently

$$\ll \sum_{q > y/\log y} \sum_{\substack{f \leq x \\ q^2 | f}} \alpha(f) \ll \frac{S_\alpha(x)}{y},$$

as we have seen at the beginning of Section 4. For each  $q$  included in the approximation of  $N_1(p)$  above, our application of the fundamental lemma of sieve theory in Subsection 4.3, again with  $D = x^{u/y}$  and  $u = \log y$ , implies that the corresponding term is

$$\begin{aligned} &= (1 + O(u^{-u/2})) \frac{S_\alpha(x)}{q} \prod_{\substack{q' \leq x^{1/y} \\ q' \in \mathcal{P}_{-1} \\ q' \equiv -1 \pmod{p}}} \left(1 - \frac{1}{q'}\right) + O\left(\frac{S_\alpha(x) \log y}{yq} e^{\frac{y}{2p}}\right) \\ &= \left(1 + O\left(\frac{(\log y)^2}{y}\right)\right) \frac{S_\alpha(x)}{q} e^{-\frac{y}{2p}} + O\left(\frac{S_\alpha(x) \log y}{yq} e^{\frac{y}{2p}}\right), \end{aligned}$$

as shown in the preceding subsection. Summing over  $q$ , we see that  $N_1(p)$  is

$$\begin{aligned} &= S_\alpha(x) \left(1 + O\left(\frac{(\log y)^2}{y}\right)\right) \left(\frac{y}{2p} + O\left(\frac{(\log y)^2}{y}\right)\right) e^{-\frac{y}{2p}} + O\left(S_\alpha(x) \frac{e^{\frac{y}{2p}}}{p} \log y\right), \\ &= S_\alpha(x) \left(1 + O\left(\frac{(\log y)^2}{y}\right)\right) \frac{y}{2p} e^{-\frac{y}{2p}} + O\left(S_\alpha(x) \frac{e^{\frac{y}{2p}}}{p} \log y\right). \end{aligned}$$

By the Prime Number Theorem and partial summation, we have

$$\begin{aligned} \sum_{p \in \mathcal{I}} e^{\frac{y}{2p}} \frac{\log p}{p} &= \int_{\mathcal{I}} e^{\frac{y}{2t}} d\left(\log t + O\left(\frac{1}{\log t}\right)\right) \\ &= \int_{\mathcal{I}} e^{\frac{y}{2t}} \frac{dt}{t} + O\left(\frac{\sqrt{y}}{\log y}\right) \\ &= \int_{\frac{1}{2 \log y}}^{\frac{\log y}{2}} \frac{e^v}{v} dv + O\left(\frac{\sqrt{y}}{\log y}\right) \\ &\ll x^{1/3} \int_{\frac{1}{2 \log y}}^{\frac{\log y}{3}} \frac{dv}{v} + \frac{1}{\log y} \int_{\frac{\log y}{3}}^{\frac{\log y}{2}} e^v dv + O\left(\frac{\sqrt{y}}{\log y}\right) \\ &\ll \frac{\sqrt{y}}{\log y}. \end{aligned}$$

Thus, it follows, upon summing over  $p \in \mathcal{I}$  and applying partial summation and the Prime Number Theorem, that

$$\begin{aligned} S_\alpha(x)^{-1} \sum_{p \in \mathcal{I}} N_1(p) \log p &= \left(1 + O\left(\frac{(\log y)^2}{y}\right)\right) \int_{\mathcal{I}} \frac{y}{2t} e^{-\frac{y}{2t}} dt + O\left(\frac{y}{(\log y)^A}\right) \\ &= \int_{\mathcal{I}} \frac{y}{2t} e^{-\frac{y}{2t}} dt + O\left(\frac{y}{(\log y)^A}\right) \end{aligned} \tag{45}$$

for any fixed  $A > 0$ , since the integral is  $\asymp y \log_2 y$ .

Inserting (43), (44) and (45) into (42) and observing that

$$\frac{d}{dt} \left( t - te^{-\frac{y}{2t}} \right) = 1 - e^{-\frac{y}{2t}} - \frac{y}{2t} e^{-\frac{y}{2t}},$$

we conclude, by taking  $A = 1$ , that

$$\begin{aligned} S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \widetilde{W}(f) &= \int_{\mathcal{I}} \left( 1 - e^{-\frac{y}{2t}} - \frac{y}{2t} e^{-\frac{y}{2t}} \right) dt + O \left( \frac{y}{\log y} \right) \\ &= y \log y \left( 1 - e^{-\frac{1}{2 \log y}} \right) - \frac{y}{\log y} \left( 1 - \frac{1}{\sqrt{y}} \right) + O \left( \frac{y}{\log y} \right) \\ &= \left( \frac{1}{2} + O \left( \frac{1}{\log y} \right) \right) y, \end{aligned}$$

which is (II). It may be worth noting that one can obtain an asymptotic expansion of any length for the first weighted moment of  $\widetilde{W}$  by taking  $A$  suitably large but fixed.

**5.3. The second moment of  $\widetilde{W}(f)$ : a sketch.** Finally, we outline the proof (III) and invite the reader to fill in the necessary details. We start by writing

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \widetilde{W}(f)^2 = S_\alpha(x)^{-1} \sum_{p_1, p_2 \in \mathcal{I}} \log p_1 \log p_2 \sum_{\substack{f \leq x \\ p_1, p_2 \in \mathcal{J}_f}} \alpha(f). \quad (46)$$

For each pair  $(i_1, i_2) \in \{0, 1\}^2$ , we denote by  $N_{i_1, i_2}(p_1, p_2)$  the number of split-free  $f \leq x$  such that for every  $k \in \{1, 2\}$ , there are exactly  $i_k$  distinct primes  $q_k \mid f$  with  $q_k \leq x^{1/y}$  and  $q_k \equiv \chi(q_k) \pmod{p_k}$ . Furthermore, let

$$M_{i_1, i_2} := \int_{\mathcal{I}} \left( \frac{y}{2t} \right)^{i_1} e^{-i_2 \frac{y}{2t}} dt.$$

By the inclusion-exclusion principle, we have

$$\sum_{\substack{f \leq x \\ p_1, p_2 \in \mathcal{J}_f}} \alpha(f) = S_\alpha(x) - \sum_{k \in \{1, 2\}} \sum_{i_k \in \{0, 1\}} N_{i_k}(p_k) + \sum_{(i_1, i_2) \in \{0, 1\}^2} N_{i_1, i_2}(p_1, p_2). \quad (47)$$

The contribution to (46) from the term  $S_\alpha(x)$  in (47) is obviously

$$\left( \sum_{p \in \mathcal{I}} \log p \right)^2 = M_{0,0}^2 + O \left( \frac{y^2}{(\log y)^A} \right)$$

for any fixed  $A > 0$ . In addition, the contribution to (46) from the double sum in (47) is

$$2 \left( \sum_{p \in \mathcal{I}} \log p \right) \left( S_\alpha(x)^{-1} \sum_{p \in \mathcal{I}} N_0(p) \log p + S_\alpha(x)^{-1} \sum_{p \in \mathcal{I}} N_1(p) \log p \right),$$

which, according to (44) and (45), is equal to

$$2M_{0,0} (M_{0,1} + M_{1,1}) + O \left( \frac{y^2}{(\log y)^A} \right)$$



for any fixed  $A > 0$ . Hence, it remains to estimate the contribution to (46) from the last sum in (47). Note first that the contribution to (46) from the diagonal terms with  $p_1 = p_2$  in the last sum in (47) is

$$S_\alpha(x)^{-1} \sum_{p \in \mathcal{I}} N_0(p)(\log p)^2 + S_\alpha(x)^{-1} \sum_{p \in \mathcal{I}} N_1(p)(\log p)^2 \ll \frac{y \log_2 y}{(\log y)^A}$$

for any fixed  $A > 0$ , which is negligible. Thus, it is sufficient to estimate the contribution to (46) from the off-diagonal terms with  $p_1 \neq p_2$ . We claim that

$$S_\alpha(x)^{-1} \sum_{p_1 \neq p_2 \in \mathcal{I}} N_{i_1, i_2}(p_1, p_2) \log p_1 \log p_2 = M_{i_1, 1} M_{i_2, 1} + O\left(\frac{y^2 \log_2 y}{(\log y)^2}\right) \quad (48)$$

for each pair  $(i_1, i_2) \in \{0, 1\}^2$ . Inserting all the estimates above into (46) yields

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \widetilde{W}(f)^2 = (M_{0,0} - M_{0,1} - M_{1,1})^2 + O\left(\frac{y^2 \log_2 y}{(\log y)^2}\right) = \left(\frac{1}{4} + O\left(\frac{1}{\log y}\right)\right) y^2,$$

which is (III). Again, it is possible to make  $O(y^2/\log y)$  explicit and have  $O(y^2 \log_2 y/(\log y)^2)$  as the error instead.

Taking the case  $(i_1, i_2) = (1, 1)$  for example, we now illustrate briefly how (48) can be derived by adapting the argument in [21]. For any  $p_1 \neq p_2 \in \mathcal{I}$ , the quantity  $S_\alpha(x)^{-1} N_{1,1}(p_1, p_2)$  includes particularly the contribution from those split-free  $f \leq x$  of the form  $f = q_1 q_2 m$ , where  $q_1, q_2 \leq x^{1/y}$  are distinct primes not in  $\mathcal{P}_1$ , satisfying  $q_k \equiv \chi(q_k) \pmod{p_k}$  for all  $k = 1, 2$  and  $q_k \not\equiv \chi(q_k) \pmod{p_l}$  for all  $(k, l) = (1, 2), (2, 1)$ , and where  $m \leq x/q_1 q_2$  is split-free and free of prime factors  $q \leq x^{1/y}$  with  $q \equiv \chi(q) \pmod{p_k}$  for all  $k = 1, 2$ . The rest of the split-free  $f \leq x$  that contribute to  $S_\alpha(x)^{-1} N_{1,1}(p_1, p_2)$  satisfy either  $q^2 \mid f$  for some prime  $q \geq y/\log y - 1 > y/2 \log y$  or  $q \mid f$  for some prime  $q$  with  $q \equiv \chi(q) \pmod{p_1 p_2}$ . Thus, the contribution to  $S_\alpha(x)^{-1} N_{1,1}(p_1, p_2)$  from these residual split-free  $f \leq x$  does not exceed

$$S_\alpha(x)^{-1} \sum_{y/2 \log y < q \leq \sqrt{x}} \sum_{\substack{f \leq x \\ q^2 \mid f}} \alpha(f) + S_\alpha(x)^{-1} \sum_{\substack{q \leq x \\ q \equiv \chi(q) \pmod{p_1 p_2}}} \sum_{\substack{f \leq x \\ q \mid f}} \alpha(f) \ll \frac{1}{y} + \frac{y}{p_1 p_2},$$

where the sums over  $q$  can be easily estimated by dividing the ranges of  $q$  as in Section 4. Summing on  $p_1, p_2 \in \mathcal{I}$ , we see that the contribution to the left-hand side of (48) from these residual split-free  $f \leq x$  is  $O(y(\log y)^2)$ , which is negligible compared to the error term in (48). Now we turn to those split-free  $f \leq x$  of the form  $f = q_1 q_2 m$  with the properties described above. Given  $p_1, p_2, q_1, q_2$ , the count of these  $f$ , when divided by  $S_\alpha(x)$ , is

$$(1 + O(u^{-u/2})) \frac{1}{q_1 q_2} \prod_{\substack{q \leq x^{1/y} \\ q \notin \mathcal{P}_1 \\ \exists k=1,2, q \equiv \chi(q) \pmod{p_k}}} \left(1 - \frac{1}{p}\right) + O\left(\frac{\log_2 y}{y q_1 q_2} e^{\frac{y}{2p_1} + \frac{y}{2p_2}}\right),$$

by the fundamental lemma of sieve theory with  $D = x^{u/y}$  and  $u = \log_2 y$ , as in Subsection 4.3. The contribution to the left-hand side of (48) from the second error term above is

$$\begin{aligned} &\ll \frac{\log_2 y}{y} \sum_{p_1, p_2 \in \mathcal{I}} e^{\frac{y}{2p_1} + \frac{y}{2p_2}} \log p_1 \log p_2 \sum_{\substack{q_1, q_2 \leq x^{1/y} \\ \forall k=1,2, q_k \equiv -1 \pmod{p_k}}} \frac{1}{q_1 q_2} \\ &\ll y \log_2 y \sum_{p_1, p_2 \in \mathcal{I}} e^{\frac{y}{2p_1} + \frac{y}{2p_2}} \frac{\log p_1 \log p_2}{p_1 p_2} \\ &\ll y \log_2 y \left( \frac{\sqrt{y}}{\log y} \right)^2 \ll \frac{y^2 \log_2 y}{(\log y)^2}, \end{aligned}$$

which matches the error in (48). The main contribution to the left-hand side of (48) from those split-free  $f \leq x$  of the form  $f = q_1 q_2 m$  with the properties described above is

$$(1 + O(u^{-u/2})) \sum_{p_1, p_2 \in \mathcal{I}} \log p_1 \log p_2 \sum_{\substack{q_1, q_2 \leq x^{1/y} \\ q_1, q_2 \notin \mathcal{P}_1 \\ \forall k \neq l \in \{1,2\}, q_k \equiv \chi(q_k) \pmod{p_k} \\ q_k \not\equiv \chi(q_k) \pmod{p_l}}} \frac{1}{q_1 q_2} \prod_{\substack{q \leq x^{1/y} \\ q \notin \mathcal{P}_1 \\ \exists k=1,2, q \equiv \chi(q) \pmod{p_k}}} \left(1 - \frac{1}{p}\right).$$

Now an argument analogous to the one displayed on [21, p. 214] shows that

$$\sum_{\substack{q_1, q_2 \leq x^{1/y} \\ q_1, q_2 \notin \mathcal{P}_1 \\ \forall k \neq l \in \{1,2\}, q_k \equiv \chi(q_k) \pmod{p_k} \\ q_k \not\equiv \chi(q_k) \pmod{p_l}}} \frac{1}{q_1 q_2} \prod_{\substack{q \leq x^{1/y} \\ q \notin \mathcal{P}_1 \\ \exists k=1,2, q \equiv \chi(q) \pmod{p_k}}} \left(1 - \frac{1}{p}\right) = \left(1 + O\left(\frac{(\log y)^2}{y}\right)\right) \frac{y^2}{4p_1 p_2} e^{-\frac{y}{2p_1} - \frac{y}{2p_2}}.$$

Summing over  $p_1 \neq p_2 \in \mathcal{I}$  with the weights  $\log p_1 \log p_2$  attached, we find that the main contribution to the left-hand side of (48) from those split-free  $f \leq x$  of the form  $f = q_1 q_2 m$  is

$$\begin{aligned} &= (1 + O(u^{-u/2})) \left( y \sum_{p \in \mathcal{I}} e^{-\frac{y}{2p}} \frac{\log p}{2p} \right)^2 + O\left( y^2 \sum_{p \in \mathcal{I}} \frac{(\log p)^2}{p^2} e^{-\frac{y}{p}} \right) \\ &= (1 + O(u^{-u/2})) \left( \int_{\mathcal{I}} \frac{y}{2t} e^{-\frac{y}{2t}} dt + O\left( \frac{y}{(\log y)^{A+1}} \right) \right)^2 + O(y(\log y)^2) \\ &= M_{1,1}^2 + O\left( \frac{y^2}{(\log y)^A} \right) \end{aligned}$$

for any fixed  $A > 0$ . Gathering the contributions above verifies (48) in the case  $(i_1, i_2) = (1, 1)$ .

## 6. APPLICATION OF THE ALGEBRO-ANALYTIC MACHINE: GRH AND THE UNIT INDEX CORRESPONDING TO AN INERT PRIME

For the rest of the paper, we assume that  $K = \mathbb{Q}(\sqrt{D})$ , where  $D > 1$  is squarefree. We write  $\varepsilon$  for the fundamental unit of  $\mathcal{O}_K$  and  $\sigma_0$  for the nontrivial element of  $\text{Gal}(K/\mathbb{Q})$ . All number fields appearing below are viewed as subfields of  $\mathbb{C}$ , and odd order roots of real numbers are understood as taking their real values.

Recall from §2 that  $\ell(f)$  denotes the order of (the image of)  $\varepsilon$  in the group  $\text{PreCl}(\mathcal{O}_f) = (\mathcal{O}_K/f\mathcal{O}_K)^\times / \langle \text{images of integers prime to } f \rangle$ . It will be important for the proof of Proposition 2.7 to understand the distribution of the numbers  $\ell(p)$ , as  $p$  varies over primes inert in  $K$ . Certainly

$\ell(p)$  divides  $\#\text{PreCl}(\mathcal{O}_p) = \psi(p) = p + 1$  for each such  $p$ . The main result of this section is a GRH-conditional estimate for how often  $\ell(p) \mid \frac{p+1}{q}$  for a given odd prime  $q$  (Proposition 6.5).

The method of proof is essentially that introduced by Hooley [13] to study Artin's primitive root conjecture under the assumption of GRH. Of course, our setting is a bit different than Hooley's, as the arithmetic is taking place over a real quadratic field instead of  $\mathbb{Q}$ . Happily, we can quickly deduce what we need from work of Chen [3]. (Closely related arguments can be found in papers of Roskam [26], Kataoka [14], and Pollack [23, §2].)

Let  $q$  be an odd prime. We will relate the condition that  $\ell(p) \mid \frac{p+1}{q}$  to the splitting behavior of  $p$  in the number field

$$E_q := \mathbb{Q}(\zeta_q, \sqrt[q]{\varepsilon}).$$

(As usual,  $\zeta_m := \exp(2\pi i/m)$ .) Note that  $E_q$  contains  $\mathbb{Q}(\varepsilon) = K$ , so that  $E_q = K(\zeta_q, \sqrt[q]{\varepsilon})$ .

To bring our setup into alignment with Chen's, we need to write  $E_q$  in a slightly different way. Let  $s = 1$  if  $\text{Nm}_{K/\mathbb{Q}}(\varepsilon) = 1$  and let  $s = 2$  if  $\text{Nm}_{K/\mathbb{Q}}(\varepsilon) = -1$ . Put  $\eta = \varepsilon^s$ . Then  $\text{Nm}_{K/\mathbb{Q}}(\eta) = 1$  (in fact,  $\eta$  generates the group of norm 1 units). Since  $q$  is an odd prime while  $s = 1$  or  $s = 2$ , we have that  $E_q = K(\zeta_q, \sqrt[q]{\varepsilon}) = K(\zeta_q, \sqrt[q]{\eta})$ .

The next three lemmas are special cases of Chen's results in [3]. After all three results have been stated, we say a few words about how they may be deduced from [3].

**Lemma 6.1.** *Let  $q$  be an odd prime. If  $q \nmid D$ , then  $[E_q : \mathbb{Q}] = 2q\varphi(q)$ ,*

Set  $\tilde{\eta} = \sigma_0(\eta)$ . Then  $\eta\tilde{\eta} = 1$  and  $E_q$  contains a  $q$ th root of  $\tilde{\eta}$ , namely  $1/\sqrt[q]{\eta}$ . It follows that

$$E_q = K(\zeta_q, \sqrt[q]{\eta}) = K(\zeta_q, \sqrt[q]{\eta}, \sqrt[q]{\tilde{\eta}}) = \mathbb{Q}(\zeta_q, \sqrt[q]{\eta}, \sqrt[q]{\tilde{\eta}}),$$

rendering apparent that  $E_q$  is the splitting field over  $\mathbb{Q}$  of

$$\begin{aligned} F_q(X) &:= (X^q - \eta)(X^q - \tilde{\eta}) \\ &= X^{2q} - \text{Tr}_{K/\mathbb{Q}}(\eta)X^q + 1 \in \mathbb{Z}[X]. \end{aligned} \tag{49}$$

Hence,  $E_q$  is a Galois extension of  $\mathbb{Q}$ .

Let  $\tau$  represent complex conjugation. Define  $\mathcal{C}_q^- \subseteq \text{Gal}(E_q/\mathbb{Q})$  by

$$\mathcal{C}_q^- = \{\sigma \in \text{Gal}(E_q/\mathbb{Q}) : \sigma|_K = \sigma_0, \sigma|_{\mathbb{Q}(\zeta_q)} = \tau|_{\mathbb{Q}(\zeta_q)}, \sigma^2 = \text{id}\}.$$

It is straightforward to check that  $\mathcal{C}_q^-$  is a conjugation-stable subset of  $\text{Gal}(E_q/\mathbb{Q})$ .

**Lemma 6.2.** *Let  $q$  be an odd prime not dividing  $D$ . Then  $\#\mathcal{C}_q^- = 1$ .*

Write  $\eta = \frac{1}{2}(u + v\sqrt{D})$  with integers  $u$  and  $v$ .

**Lemma 6.3.** *Suppose that  $p$  is an odd prime not dividing  $v$ . Let  $q$  be an odd prime. Then*

$$p \text{ is inert in } K, \ p \equiv -1 \pmod{q}, \ \text{and } \eta^{\frac{p+1}{q}} \equiv 1 \pmod{p\mathcal{O}_K} \iff \text{Frob}_{E_q/\mathbb{Q},p} \in \mathcal{C}_q^-.$$

*Deduction of Lemmas 6.1–6.3 from Chen's work.* Chen's setup in [3] is as follows:  $K_0$  is a quadratic field (not necessarily real) with nontrivial automorphism  $\sigma_0$ . The element  $\alpha \in K_0^\times$  has norm 1

but is not a root of unity. For each prime  $q$ , the field  $E_q$  is defined as  $K_0(\zeta_q, \sqrt[q]{\alpha})$ , and when  $n$  is squarefree,  $E_n$  is defined as the compositum of the  $E_q$  for primes  $q$  dividing  $n$ .

Under these assumptions, Chen determines the degrees of the extensions  $E_n/\mathbb{Q}$  in Lemma 1.6 of [3], while Lemma 1.7 of [3] describes the sizes of the sets

$$\mathcal{C}_n^- := \{\sigma \in \text{Gal}(E_n/\mathbb{Q}) : \sigma|_K = \sigma_0, \sigma|_{\mathbb{Q}(\zeta_n)} = \tau|_{\mathbb{Q}(\zeta_n)}, \sigma^2 = \text{id}, \text{ and } \sigma|_{K_0(\sqrt{\alpha+1}/\sqrt{\alpha})} = \text{id if } 2 \mid n\}.$$

For brevity, we quote only the relevant cases: Suppose  $n$  is odd and squarefree and that  $K_0$  is real. Let  $s_0$  be the largest positive integer for which  $\alpha \in (K_0^\times)^{s_0}$ , and let  $n_1 = n/\text{gcd}(n, s_0)$ . Then Chen's Lemma 1.6 asserts that

$$[E_n : \mathbb{Q}] = \frac{2n_1\varphi(n)}{[K_0 \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]},$$

while her Lemma 1.7 claims that  $\#\mathcal{C}_n^- = 1$  unless  $K \subseteq \mathbb{Q}(\zeta_n)$ .

Our Lemmas 6.1 and 6.2 follow from these two results (respectively) upon taking  $K_0 = K$ ,  $\alpha = \eta$ , and  $n = q$ . Here we note that Chen's  $s_0$  coincides with our integer  $s$ , and that

$$\mathbb{Q} \subseteq K \cap \mathbb{Q}(\zeta_q) \subseteq \mathbb{Q}(\zeta_{4|D|}) \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}(\zeta_{\text{gcd}(4|D|, q)}) = \mathbb{Q},$$

since we are assuming  $q$  is an odd prime not dividing  $D$ .

What about Lemma 6.3? Write  $K_0 = \mathbb{Q}(\sqrt{D_0})$  with  $D_0$  squarefree, and express  $\alpha$  as  $u_0 + v_0\sqrt{D_0}$  with  $u_0, v_0 \in \mathbb{Q}$ . In Lemma 1.4(a), Chen assumes that  $p$  is an odd prime inert in  $K$  for which  $v_p(v_0) = 0$ . She then shows that for each odd prime  $q$ ,

$$p \equiv -1 \pmod{q} \text{ and } \eta^{\frac{p+1}{q}} \equiv 1 \pmod{p\mathcal{O}_K} \iff \text{Frob}_{E_q/\mathbb{Q}, p} \in \mathcal{C}_q^-. \quad (50)$$

Specializing to  $K = K_0$  (so that  $D = D_0$ ) and  $\alpha = \eta$  (so that  $u_0 = \frac{1}{2}u, v_0 = \frac{1}{2}v$ ), the forward implication in (50) yields the forward implication of Lemma 6.3. One can also deduce the backward implication of Lemma 6.3 from the backward implication in (50); it suffices to observe that  $\text{Frob}_{E_q/\mathbb{Q}, p} \in \mathcal{C}_q^-$  implies that  $p$  is inert in  $K_0$ . Indeed, if  $\text{Frob}_{E_q/\mathbb{Q}, p} \in \mathcal{C}_q^-$ , then  $\text{Frob}_{K_0/\mathbb{Q}, p} = \text{Frob}_{E_q/\mathbb{Q}, p}|_{K_0} = \sigma_0$ .  $\square$

The following conditional version of the Chebotarev density theorem has been extracted from Serre's paper [27] (take  $K = \mathbb{Q}$  in Serre's eq. (20<sub>R</sub>)).

**GRH-dependent Chebotarev density theorem.** *Let  $L/\mathbb{Q}$  be a Galois extension, and let  $\mathcal{C}$  be a subset of  $\text{Gal}(L/\mathbb{Q})$  stable under conjugation. For all  $y \geq 2$ ,*

$$\#\{\text{primes } p \leq y : \text{Frob}_{L/\mathbb{Q}, p} \subseteq \mathcal{C}\} = \frac{|\mathcal{C}|}{[L : \mathbb{Q}]} \text{Li}(y) + O\left((\#\mathcal{C})y^{1/2} \log\left([L : \mathbb{Q}]y \prod_{\ell \mid \Delta_L} \ell\right)\right).$$

*Here the implied constant is absolute.*

**Lemma 6.4** (assuming GRH). *Let  $q$  be an odd prime not dividing  $D$ . For every real number  $y \geq 2$ , the number of primes  $p \leq y$  inert in  $K$  for which  $p \equiv -1 \pmod{q}$  and  $\eta^{(p+1)/q} \equiv 1 \pmod{p\mathcal{O}_K}$  is*

$$\frac{\text{Li}(y)}{2q\varphi(q)} + O(y^{1/2} \log(qy)).$$

*Here and below, implied constants may depend on  $K$ .*

*Proof.* By adjusting the  $O$ -constant, we may ignore any set of primes  $p$  of cardinality  $O_K(1)$ . Bearing in mind the results of Lemmas 6.2 and 6.3, Lemma 6.4 follows from the GRH-dependent Chebotarev density theorem upon taking  $L = E_q$  and  $\mathcal{C} = \mathcal{C}_q^-$ , once we show that the error term of the theorem is subsumed by our  $O$ -expression.

To that end, we argue that a rational prime  $p$  is unramified in  $E_q$  whenever  $p \nmid 2qDv_0$ . Observe that  $p$  is unramified in  $E_q$  as long as  $F_q(X)$ , as defined in (49), has no multiple roots mod  $p$ . We test this condition by checking for common roots of  $F_q$  and  $F'_q$ . If  $p \nmid 2q$ , then each root  $\rho \in \overline{\mathbb{F}}_p$  of  $F'_q(X)$  has  $2\rho^q = \text{Tr}_{K/\mathbb{Q}}(\eta)$ . But then

$$\begin{aligned} 4F_q(\rho) &= 4\rho^{2q} - 4\text{Tr}_{K/\mathbb{Q}}(\eta)\rho^q + 4 \\ &= 4\text{Nm}_{K/\mathbb{Q}}(\eta) - \text{Tr}_{K/\mathbb{Q}}(\eta)^2 \\ &= -Dv^2, \end{aligned}$$

which is nonvanishing mod  $p$  under our assumption that  $p \nmid 2qDv$ .

The primes that ramify in  $E_q$  are precisely those dividing  $\Delta_{E_q}$ . Hence,

$$\prod_{\ell|\Delta_{E_q}} \ell \leq 2qDv, \quad \text{and} \quad [E_q : \mathbb{Q}]y \prod_{\ell|\Delta_{E_q}} \ell \leq 4q^3Dvy,$$

using Lemma 6.1 for the last inequality. Therefore,

$$\log([E_q : \mathbb{Q}]y \prod_{\ell|\Delta_{E_q}} \ell) \ll \log(qy),$$

and  $(\#\mathcal{C})y^{1/2} \log([E_q : \mathbb{Q}]y \prod_{\ell|\Delta_{E_q}} \ell) \ll y^{1/2} \log(qy)$ .  $\square$

We now come to the main result of this section.

**Proposition 6.5** (assuming GRH). *Let  $q$  be an odd prime, and let  $y \geq 2$ . The number of primes  $p \leq y$  for which  $p$  is inert in  $K$ ,  $p \equiv -1 \pmod{q}$ , and  $\ell(p) \mid \frac{p+1}{q}$  is*

$$\ll \frac{\text{Li}(y)}{q^2} + y^{1/2} \log(qy).$$

*Proof.* For the finitely many odd primes  $q$  dividing  $D$ , the result is trivial if we choose a sufficiently large implied constant (depending on  $K$ ). So we may suppose that  $q \nmid D$ .

We now argue that if  $p$  is inert in  $K$  and  $p \equiv -1 \pmod{q}$ , then

$$\ell(p) \mid \frac{p+1}{q} \iff \eta^{\frac{p+1}{q}} \equiv 1 \pmod{p\mathcal{O}_K}.$$

Once this is proved, Proposition 6.5 follows from Lemma 6.4.

If  $\eta^{(p+1)/q} \equiv 1 \pmod{p\mathcal{O}_K}$ , then  $\varepsilon^{(p+1)/q} \equiv \pm 1 \pmod{p\mathcal{O}_K}$ . Thus,  $\varepsilon^{(p+1)/q} \in \mathcal{O}_p$ , and  $\ell(p) \mid \frac{p+1}{q}$ . Conversely, if  $\ell(p) \mid \frac{p+1}{q}$ , then  $\varepsilon^{(p+1)/q} \equiv h \pmod{p\mathcal{O}_K}$  for some rational integer  $h$  coprime to  $p$ . As  $p$  is inert in  $K$ , the  $p$ th power map modulo  $p\mathcal{O}_K$  is induced by  $\sigma_0$ , and

$$(\eta^{(p+1)/q})^q \equiv \eta \cdot \eta^p \equiv \text{Nm}_{K/\mathbb{Q}}(\eta) \equiv 1 \pmod{p\mathcal{O}_K}.$$

Hence, if  $s$  denotes the order of  $\eta^{(p+1)/q}$  in  $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ , then  $s \mid q$ . On the other hand,  $s$  coincides with the order of  $h$  in  $(\mathbb{Z}/p\mathbb{Z})^\times$ , and so  $s \mid p-1$ . Using that  $q \mid p+1$ , we conclude that  $s$  divides

$$\gcd(q, p-1) = \gcd(q, (p+1)-2) = \gcd(q, -2) = 1.$$

Thus,  $s = 1$  and  $\eta^{(p+1)/q} \equiv 1 \pmod{p\mathcal{O}_K}$ . □

We conclude this section with a bound on the number of small values of  $\ell(p)$ .

**Lemma 6.6.** *For each  $y \geq 1$ , the number of inert primes  $p$  for which  $\ell(p) \leq y$  is  $O(y^2)$ .*

As a consequence of Lemma 6.6, the number of inert primes  $p \leq t$  with  $\ell(p) \leq 2p^{1/2}/\log p$  is  $O(t/(\log t)^2)$ , for all  $t \geq 2$ . This will be needed in the arguments of Section 7.

*Proof.* Let  $p$  be a prime inert in  $K$ , and let  $s$  be the order of  $\varepsilon^{\ell(p)}$  in  $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ . Since  $\varepsilon^{\ell(p)}$  is congruent to a rational integer unit mod  $p$ , we have that  $s \mid p-1$ . Noting that  $\varepsilon^{p+1} \equiv \varepsilon \cdot \varepsilon^p \equiv \text{Nm}_{K/\mathbb{Q}}(\varepsilon) \equiv \pm 1 \pmod{p\mathcal{O}_K}$ , we also have that  $s \mid 2(p+1)$ . Thus,  $s \mid \gcd(p-1, 2(p+1)) \mid 4$ , and  $\varepsilon^{4\ell(p)} = 1$  in  $\mathcal{O}_K/p\mathcal{O}_K$ .

Now assume that  $\ell(p) \leq y$ . Then  $\varepsilon^j \equiv 1 \pmod{p\mathcal{O}_K}$  for some positive integer  $j \leq 4y$ , and

$$p \text{ divides } \prod_{1 \leq j \leq 4y} \text{Nm}(\varepsilon^j - 1).$$

As  $\text{Nm}(\varepsilon^j - 1) = \exp(O(j))$ , the product on  $j$  has size  $\exp(O(y^2))$  and so is divisible by  $O(y^2)$  distinct primes. □

## 7. PROOF OF PROPOSITION 2.7

We now turn to the proof of Proposition 2.7. Our arguments borrow heavily from those of Erdős–Pomerance–Schmutz and Li–Pomerance [16]. Let

$$z_f := \frac{\log_2 f}{\log_4 f}.$$

The next lemma is proved by an averaging argument analogous to one appearing on p. 368 of [5].

**Lemma 7.1.** *For almost all split-free  $f$ , the  $z_f$ -smooth part of  $L(f)$  is of size  $(\log f)^{O(1/\log_4 f)}$ .*

*Proof.* The proof bears a great resemblance to that of (24) in Subsection 4.2. For any  $n \in \mathbb{N}$  and  $y, w \geq 1$ , denote by  $S(n, y)$  the  $y$ -smooth part of  $n$  and put

$$S(n, y, w) := \prod_{\substack{p^k \parallel n \\ p \leq y \\ p^k > w}} p^k.$$

With  $z = \log_2 x / \log_4 x$  and  $w = (\log_2 x) \log_4 x$ , we have

$$\begin{aligned} S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \log S(L(f), z_f, w) &= S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \sum_{\substack{p^k \parallel L(f) \\ p \leq z_f, p^k > w}} \log p^k \\ &\leq S_\alpha(x)^{-1} \sum_{\substack{p \leq z \\ p^k > w}} \log p^k \sum_{\substack{f \leq x \\ p^k \mid L(f)}} \alpha(f). \end{aligned}$$

Observe that if  $p^k \mid L(f)$ , then  $p^k \mid f$  with  $p$  ramified, or  $p^{k+1} \mid f$  with  $p$  unramified, or  $f$  has a prime factor  $q$  with  $q \equiv \chi(q) \pmod{p^k}$ . The contribution from the first case is

$$\begin{aligned} &\leq S_\alpha(x)^{-1} \sum_{\substack{p \mid \Delta \\ w < p^k \leq x}} \log p^k \sum_{f \leq x/p^k} \alpha(f) \\ &\ll \sum_{\substack{p \mid \Delta \\ w < p^k \leq x}} \frac{\log p^k}{p^k} \left(1 - \frac{\log p^k}{\log 3x}\right)^{-1/2} \\ &\ll \sum_{\substack{p \mid \Delta \\ w < p^k \leq \sqrt{x}}} \frac{\log p^k}{p^k} + (\log x)^{1/2} \sum_{\substack{p \mid \Delta \\ p^k > \sqrt{x}}} \frac{\log p^k}{p^k} \\ &\ll \frac{\log w}{w} + \frac{(\log x)^{3/2}}{\sqrt{x}} \ll \frac{\log w}{w}, \end{aligned}$$

Analogously, the second case contributes an amount

$$\begin{aligned} &\leq S_\alpha(x)^{-1} \sum_{\substack{p \leq z \\ w < p^k \leq x/p}} \log p^k \sum_{f \leq x/p^{k+1}} \alpha(f) \\ &\ll \sum_{\substack{p \leq z \\ w < p^k \leq x/p}} \frac{\log p^k}{p^{k+1}} \left(1 - \frac{\log p^{k+1}}{\log 3x}\right)^{-1/2} \\ &\ll \sum_{\substack{p \leq z \\ w < p^k \leq \sqrt{x}/p}} \frac{\log p^k}{p^{k+1}} + (\log x)^{1/2} \sum_{\substack{p \leq z \\ p^{k+1} > \sqrt{x}}} \frac{\log p^k}{p^{k+1}} \\ &\ll \frac{\log w}{w} \sum_{p \leq z} \frac{1}{p} + \frac{(\log x)^{3/2}}{\sqrt{x}} \sum_{p \leq z} 1 \ll \frac{(\log w) \log_2 z}{w}. \end{aligned}$$

Finally, the last case contributes an amount

$$\begin{aligned}
&\leq S_\alpha(x)^{-1} \sum_{\substack{p \leq z \\ p^k > w}} \log p^k \sum_{\substack{q \leq x \\ q \equiv \chi(q) \pmod{p^k}}} \alpha(q) \sum_{f \leq x/q} \alpha(f) \\
&\ll \sum_{\substack{p \leq z \\ p^k > w}} \log p^k \sum_{\substack{q \leq x \\ q \equiv \chi(q) \pmod{p^k}}} \frac{\alpha(q)}{q} \left(1 - \frac{\log q}{\log 3x}\right)^{-1/2} \\
&\leq \sum_{\substack{p \leq z \\ p^k > w}} \log p^k \sum_{\substack{q \leq x \\ q \equiv -1 \pmod{p^k}}} \frac{1}{q} \left(1 - \frac{\log q}{\log 3x}\right)^{-1/2} \\
&\ll \sum_{\substack{p \leq z \\ p^k > w}} \log p^k \sum_{\substack{q \leq \sqrt{x} \\ q \equiv -1 \pmod{p^k}}} \frac{1}{q} + \sum_{\substack{p \leq z \\ p^k > w}} \log p^k \sum_{\substack{\sqrt{x} < q \leq x \\ q \equiv -1 \pmod{p^k}}} \frac{1}{q} \left(1 - \frac{\log q}{\log 3x}\right)^{-1/2}.
\end{aligned}$$

The first double sum on the last line is clearly

$$\ll \sum_{\substack{p \leq z \\ p^k > w}} \frac{\log p^k}{\varphi(p^k)} \log_2 x \ll \frac{(\log w) \log_2 x}{w} \sum_{p \leq z} 1 \ll \frac{z(\log w) \log_2 x}{w \log z}$$

by Brun–Titchmarsh and partial summation. To estimate the second double sum, we split it into the two following subsums

$$\begin{aligned}
&\sum_{\substack{p \leq z \\ w < p^k \leq x^{1/3}}} \log p^k \sum_{\substack{\sqrt{x} < q \leq x \\ q \equiv -1 \pmod{p^k}}} \frac{1}{q} \left(1 - \frac{\log q}{\log 3x}\right)^{-1/2}, \\
&\sum_{\substack{p \leq z \\ p^k > x^{1/3}}} \log p^k \sum_{\substack{\sqrt{x} < q \leq x \\ q \equiv -1 \pmod{p^k}}} \frac{1}{q} \left(1 - \frac{\log q}{\log 3x}\right)^{-1/2}.
\end{aligned}$$

Since Brun–Titchmarsh and partial summation imply that

$$\sum_{\substack{\sqrt{x} < q \leq x \\ q \equiv -1 \pmod{p^k}}} \frac{1}{q} \left(1 - \frac{\log q}{\log 3x}\right)^{-1/2} \ll \frac{1}{\varphi(p^k)}$$

whenever  $p^k \leq x^{1/3}$ , the first subsum above is

$$\ll \sum_{\substack{p \leq z \\ p^k > w}} \frac{\log p^k}{\varphi(p^k)} \ll \frac{z(\log w)}{w \log z}.$$



On the other hand, the second subsum is

$$\begin{aligned}
 &\ll (\log x)^{1/2} \sum_{\substack{p \leq z \\ p^k > x^{1/3}}} \log p^k \sum_{\substack{q \leq x \\ q \equiv -1 \pmod{p^k}}} \frac{1}{q} \\
 &\ll (\log x)^{1/2} \log_2 x \sum_{\substack{p \leq z \\ p^k > x^{1/3}}} \frac{\log p^k}{\varphi(p^k)} \\
 &\ll \frac{z(\log x)^{3/2} \log_2 x}{x^{1/3} \log z}.
 \end{aligned}$$

Collecting the estimates above, we find

$$S_\alpha(x)^{-1} \sum_{f \leq x} \alpha(f) \log S(L(f), z_f, w) \ll \frac{z(\log w) \log_2 x}{w \log z} \ll \frac{z}{\log_4 x},$$

from which it follows that for all but  $o(S_\alpha(x))$  split-free  $f \in \mathbb{N} \cap [1, x]$ , we have  $\log S(L(f), z_f, w) \leq z$ . Since

$$\sum_{\substack{p \leq z \\ p^k \leq w}} \log p^k \ll z \left( \frac{\log w}{\log z} \right)^2 \ll z,$$

we have

$$\log S(L(f), z_f) \leq \sum_{\substack{p \leq z \\ p^k \leq w}} \log p^k + \log S(L(f), z_f, w) \ll z$$

for all but  $o(S_\alpha(x))$  split-free  $f \in \mathbb{N} \cap [1, x]$ . If we restrict to  $f \in (\sqrt{x}, x]$ , then  $z$  and  $z_f$  are of the same order of magnitude, and the final “ $\ll z$ ” can be replaced with “ $\ll z_f$ .” This completes the proof of Lemma 7.1.  $\square$

A similar argument shows that  $L(f)$  is rarely divisible by the square of a prime exceeding  $z_f$ .

**Lemma 7.2.** *For almost all split-free  $f$ , there is no prime  $p > z_f$  for which  $p^2 \mid L(f)$ .*

*Proof.* Observe that

$$\begin{aligned}
 S_\alpha(x)^{-1} \sum_{\substack{f \leq x \\ p^2 \mid L(f) \text{ for some } p > z_f}} \alpha(f) &\leq S_\alpha(x)^{-1} \sum_{p > z/2} \sum_{\substack{\sqrt{x} < f \leq x \\ p^2 \mid L(f)}} \alpha(f) + O(x^{-1/2}) \\
 &\leq S_\alpha(x)^{-1} \sum_{p > z/2} \sum_{\substack{f \leq x \\ p^2 \mid L(f)}} \alpha(f) + O(x^{-1/2}),
 \end{aligned}$$

where  $z = \log_2 x / \log_4 x$ . The double sum on the last line is bounded above by

$$S_\alpha(x)^{-1} \sum_{p > z/2} \sum_{\substack{f \leq x \\ p^3 \mid f}} \alpha(f) + S_\alpha(x)^{-1} \sum_{p > z/2} \sum_{\substack{q \leq x \\ q \equiv \chi(q) \pmod{p^2}}} \sum_{\substack{f \leq x \\ q \mid f}} \alpha(f).$$

Note that

$$\begin{aligned}
S_\alpha(x)^{-1} \sum_{p > z/2} \sum_{\substack{f \leq x \\ p^3 | f}} \alpha(f) &\ll \sum_{z/2 < p \leq x^{1/3}} \frac{1}{p^3} \left(1 - \frac{\log p^3}{\log 3x}\right)^{-1/2} \\
&\ll \sum_{z/2 < p \leq x^{1/4}} \frac{1}{p^3} + (\log x)^{1/2} \sum_{x^{1/4} < p \leq x^{1/3}} \frac{1}{p^3} \\
&\ll \frac{1}{z^2 \log z}
\end{aligned}$$

and that

$$\begin{aligned}
S_\alpha(x)^{-1} \sum_{p > z/2} \sum_{\substack{q \leq x \\ q \equiv \chi(q) \pmod{p^2}}} \sum_{\substack{f \leq x \\ q | f}} \alpha(f) \\
&\ll \sum_{z/2 < p \leq \sqrt{x}} \sum_{\substack{q \leq x \\ q \equiv \chi(q) \pmod{p^2}}} \frac{\alpha(q)}{q} \left(1 - \frac{\log q}{\log 3x}\right)^{-1/2} \\
&\leq \sum_{z/2 < p \leq \sqrt{x}} \sum_{\substack{q \leq x \\ q \equiv -1 \pmod{p^2}}} \frac{1}{q} \left(1 - \frac{\log q}{\log 3x}\right)^{-1/2} \\
&\ll \sum_{z/2 < p \leq \sqrt{x}} \sum_{\substack{q \leq \sqrt{x} \\ q \equiv -1 \pmod{p^2}}} \frac{1}{q} + \sum_{z/2 < p \leq \sqrt{x}} \sum_{\substack{\sqrt{x} < q \leq x \\ q \equiv -1 \pmod{p^2}}} \frac{1}{q} \left(1 - \frac{\log q}{\log 3x}\right)^{-1/2} \\
&\ll \sum_{z/2 < p \leq \sqrt{x}} \frac{\log_2 x}{\varphi(p^2)} + \sum_{z/2 < p \leq x^{1/6}} \frac{1}{\varphi(p^2)} + (\log x)^{1/2} \sum_{x^{1/6} < p \leq \sqrt{x}} \frac{\log_2 x}{\varphi(p^2)} \\
&\ll \frac{\log_2 x}{z \log z}.
\end{aligned}$$

So

$$S_\alpha(x)^{-1} \sum_{\substack{f \leq x \\ p^2 | L(f) \text{ for some } p > z_f}} \alpha(f) \ll \frac{\log_2 x}{z \log z} \ll \frac{\log_4 x}{\log_3 x}. \quad \square$$

The following lemma is a variant of [16, Proposition 1].

**Lemma 7.3** (under GRH). *For almost all split-free  $f$ , the ratio  $\frac{L(f)}{\ell(f)}$  is  $z_f$ -smooth.*

*Proof.* Put

$$z := \frac{1 \log_2 x}{2 \log_4 x}.$$

Since  $z < z_f$  whenever  $\sqrt{x} < f \leq x$ , it is enough to show all but  $o(S_\alpha(x))$  split-free  $f \leq x$  have  $L(f)/\ell(f)$  being  $z$ -smooth.

We first show that the number of split-free  $f \in \mathbb{N} \cap [1, x]$  divisible by an inert prime  $p > z - 1$  with  $\ell(p) < 2p^{1/2}/\log p$  is  $o(S_\alpha(x))$ . It is clear that the count is at most

$$\sum_{\substack{p \in (z-1, x] \cap \mathcal{P}_{-1} \\ \ell(p) < 2p^{1/2}/\log p}} \sum_{\substack{f \leq x \\ p|f}} \alpha(f) \ll S_\alpha(x) \sum_{\substack{p \in (z-1, x] \cap \mathcal{P}_{-1} \\ \ell(p) < 2p^{1/2}/\log p}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2}.$$

By Lemma 6.6, the number of inert primes  $p \leq t$  with  $\ell(p) < 2p^{1/2}/\log p$  is  $O(t/\log^2 t)$ , for all  $t \geq 2$ . By partial summation, we obtain

$$\sum_{\substack{p \in [2, t] \cap \mathcal{P}_{-1} \\ \ell(p) < 2p^{1/2}/\log p}} \frac{1}{p} = c + O\left(\frac{1}{\log t}\right),$$

where  $c \geq 0$  is constant. From this it follows by partial summation again that

$$\sum_{\substack{p \in (\sqrt{x}, x] \cap \mathcal{P}_{-1} \\ \ell(p) < 2p^{1/2}/\log p}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \ll \frac{1}{\sqrt{\log x}}.$$

Thus, the number of split-free  $f \in \mathbb{N} \cap [1, x]$  divisible by an inert prime  $p > z - 1$  with  $\ell(p) < 2p^{1/2}/\log p$  is

$$\ll S_\alpha(x) \sum_{\substack{p \in (z-1, \sqrt{x}] \cap \mathcal{P}_{-1} \\ \ell(p) < 2p^{1/2}/\log p}} \frac{1}{p} + S_\alpha(x) \sum_{\substack{p \in (\sqrt{x}, x] \cap \mathcal{P}_{-1} \\ \ell(p) < 2p^{1/2}/\log p}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \ll \frac{S_\alpha(x)}{\log z}.$$

Next, we claim that for each odd prime  $q$ , the number of split-free  $f \in \mathbb{N} \cap [1, x]$  divisible by a prime  $p \equiv -1 \pmod{q}$  with  $q^2/(4\log^2 q) < p \leq q^2 \log^4 q$  is  $O(S_\alpha(x) \log_2 q / \sqrt{\log q})$ . Evidently, the count is bounded above by

$$\sum_{\substack{q^2/(4\log^2 q) < p \leq \min(q^2 \log^4 q, x) \\ p \equiv -1 \pmod{q}}} \sum_{\substack{f \leq x \\ p|f}} \alpha(f) \ll S_\alpha(x) \sum_{\substack{q^2/(4\log^2 q) < p \leq \min(q^2 \log^4 q, x) \\ p \equiv -1 \pmod{q}}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2}.$$

By Brun–Titchmarsh and partial summation, we find that if  $q \leq x^{1/3}$ , then the count is

$$\ll S_\alpha(x) \sum_{\substack{q^2/(4\log^2 q) < p \leq q^2 \log^4 q \\ p \equiv -1 \pmod{q}}} \frac{1}{p} \ll \frac{S_\alpha(x) \log_2 q}{q \log q},$$

if  $q > x^{1/3}$ , then the count is

$$\ll S_\alpha(x) (\log x)^{1/2} \sum_{\substack{q^2/(4\log^2 q) < p \leq q^2 \log^4 q \\ p \equiv -1 \pmod{q}}} \frac{1}{p} \ll \frac{S_\alpha(x) \log_2 q}{q \sqrt{\log q}}.$$

This proves our claim.

Moving on, we assert that for each odd prime  $q$ , the number of split-free  $f \in \mathbb{N} \cap [1, x]$  divisible by an inert prime  $p \equiv -1 \pmod{q}$  with  $p > q^2 \log^4 q$  and  $q \mid \frac{p+1}{\ell(p)}$  is

$$\ll S_\alpha(x) \left( \frac{1}{q \sqrt{\log q}} + \frac{\log_2 x}{q^2} \right).$$

The count here is at most

$$\sum_{\substack{q^2 \log^4 q < p \leq x \\ p \in A_q}} \sum_{\substack{f \leq x \\ p|f}} \alpha(f) \ll S_\alpha(x) \sum_{\substack{q^2 \log^4 q < p \leq x \\ p \in A_q}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2}.$$

where  $A_q$  denotes the set of inert primes  $p \equiv -1 \pmod{q}$  with  $q \mid \frac{p+1}{\ell(p)}$ . By Proposition 6.5,

$$\#(A_q \cap [2, y]) \ll \frac{\text{Li}(y)}{q^2} + y^{1/2} \log(qy)$$

for any  $y \geq 2$ . In particular, we have  $\#(A_q \cap [2, y]) \ll \sqrt{y} \log q$  for  $y \in [2, q^4 \log^4 q]$  and  $\#(A_q \cap [2, y]) \ll y/(q^2 \log y)$  for  $q^4 \log^4 q < y \leq x$ . Thus, if  $q \leq x^{1/8}$ , then the count is

$$\ll S_\alpha(x) \left( \sum_{\substack{q^2 \log^4 q < p \leq q^4 \log^4 q \\ p \in A_q}} \frac{1}{p} + \sum_{\substack{q^4 \log^4 q < p \leq x^{2/3} \\ p \in A_q}} \frac{1}{p} + \sum_{\substack{x^{2/3} < p \leq x \\ p \in A_q}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} \right).$$

Since partial summation yields

$$\begin{aligned} \sum_{\substack{q^2 \log^4 q < p \leq q^4 \log^4 q \\ p \in A_q}} \frac{1}{p} &\ll \frac{1}{q \log q}, \\ \sum_{\substack{q^4 \log^4 q < p \leq x^{2/3} \\ p \in A_q}} \frac{1}{p} &\ll \frac{\log_2 x}{q^2}, \\ \sum_{\substack{x^{2/3} < p \leq x \\ p \in A_q}} \frac{1}{p} \left(1 - \frac{\log p}{\log 3x}\right)^{-1/2} &\ll \frac{1}{q^2}, \end{aligned}$$

it follows that the count is

$$\ll S_\alpha(x) \left( \frac{1}{q \log q} + \frac{\log_2 x}{q^2} \right).$$

If  $q > x^{1/8}$ , the count is

$$\begin{aligned} &\ll S_\alpha(x) (\log x)^{1/2} \left( \sum_{\substack{q^2 \log^4 q < p \leq q^4 \log^4 q \\ p \in A_q}} \frac{1}{p} + \sum_{\substack{q^4 \log^4 q < p \leq x \\ p \in A_q}} \frac{1}{p} \right) \\ &\ll S_\alpha(x) (\log q)^{1/2} \left( \frac{1}{q \log q} + \frac{1}{q^2} \right) \\ &\ll \frac{S_\alpha(x)}{q \sqrt{\log q}}. \end{aligned}$$

This confirms our assertion.

We can now complete the proof of Lemma 7.3. Suppose  $q_f := P^+(L(f)/\ell(f)) > z$ . Since  $x$  can be assumed large,  $q_f$  is unramified in  $K$ . As

$$L(f) = \text{lcm}\{\psi(p^k) : p^k \parallel f\} \quad \text{while} \quad \ell(f) = \text{lcm}\{\ell(p^k) : p^k \parallel f\},$$

there is a prime power  $p^k \parallel f$  which

$$v_{q_f}(\psi(p^k)) > v_{q_f}(\ell(p^k)).$$

Then either  $p = q_f$  and  $k \geq 2$ , implying  $q_f^2 \mid f$ , or  $p \in A_{q_f}$ . The number of split-free  $f \in \mathbb{N} \cap [1, x]$  with  $q^2 \mid f$  for some prime  $q > z$  does not exceed

$$\begin{aligned} \sum_{q>z} \sum_{\substack{f \leq x \\ q^2 \mid f}} \alpha(f) &\ll S_\alpha(x) \sum_{z < q \leq \sqrt{x}} \frac{1}{q^2} \left(1 - \frac{\log q^2}{\log 3x}\right)^{-1/2} \\ &\ll S_\alpha(x) \sum_{z < q \leq x^{1/3}} \frac{1}{q^2} + S_\alpha(x) (\log x)^{1/2} \sum_{x^{1/3} < q \leq \sqrt{x}} \frac{1}{q^2} \\ &\ll \frac{S_\alpha(x)}{z \log z}, \end{aligned}$$

which is negligible. It remains to estimate the number of split-free  $f \in \mathbb{N} \cap [1, x]$  divisible by some prime  $p \in A_{q_f}$ , where  $q_f > z$ . The assumption  $p \in A_{q_f}$  implies trivially that  $p \geq q_f - 1 > z - 1$ . We have handled the case when  $\ell(p) < 2p^{1/2}/\log p$ , so we may assume  $\ell(p) \geq 2p^{1/2} \log p$ . Since  $\ell(p) \leq (p+1)/q_f < 2p/q_f$ , we have  $p > q_f^2/(4 \log^2 q_f)$ . But the number of split-free  $f \in \mathbb{N} \cap [1, x]$  divisible by a prime  $p \in A_q$  with  $p > q^2/(4 \log^2 q)$  for some prime  $q > z$  is

$$\ll S_\alpha(x) \sum_{q>z} \left( \frac{\log_2 q}{q \sqrt{\log q}} + \frac{\log_2 x}{q^2} \right) \ll S_\alpha(x) \left( \frac{\log_2 z}{\sqrt{\log z}} + \frac{\log_2 x}{z \log z} \right) \ll S_\alpha(x) \frac{\log_4 x}{\sqrt{\log_3 x}},$$

which is acceptable. This completes the proof of Lemma 7.3.  $\square$

With Lemmas 7.1, 7.2, and 7.3 in hand, we can make short work of Proposition 2.7. Since

$$\#\text{PrinCl}(\mathcal{O}_f) = \frac{\psi(f)}{\ell(f)} = \frac{\psi(f)}{L(f)} \frac{L(f)}{\ell(f)},$$

we have both

$$\text{RadExp PrinCl}(\mathcal{O}_f) \geq \text{Rad} \frac{\psi(f)}{L(f)},$$

and

$$\text{RadExp PrinCl}(\mathcal{O}_f) \leq \left( \text{Rad} \frac{\psi(f)}{L(f)} \right) \left( \text{Rad} \frac{L(f)}{\ell(f)} \right).$$

By Lemma 7.3,

$$\text{Rad} \frac{L(f)}{\ell(f)} \leq \prod_{p \leq z_f} p \leq (\log f)^{O(1/\log_4 f)}$$

for almost all split-free  $f$ . Proposition 2.7(a) follows by combining the last three displays and inserting the estimate of Proposition 5.1 for  $\text{Rad} \frac{\psi(f)}{L(f)}$ .

Turning to (b), let  $R = \frac{\text{Exp PrinCl}(\mathcal{O}_f)}{\text{RadExp PrinCl}(\mathcal{O}_f)}$ . Then  $\text{Rad}(R) \mid \text{RadExp PrinCl}(\mathcal{O}_f)$ , and

$$R \cdot \text{Rad}(R) \mid \text{Exp PrinCl}(\mathcal{O}_f) \mid \text{Exp PreCl}(\mathcal{O}_f) \mid L(f).$$

Hence,  $R$  is a divisor of  $L(f)$  and  $R$  is supported on primes  $p$  for which  $p^2 \mid L(f)$ . By Lemmas 7.1 and 7.2,  $R \leq (\log f)^{O(1/\log_4 f)}$  for almost all split-free  $f$ .

Finally, Proposition 2.7(c) is immediate from Lemmas 7.1 and 7.3.

## REFERENCES

1. W. R. Alford, A. Granville, and Pomerance C., *There are infinitely many carmichael numbers*, Ann. of Math. (2) **139** (1994), 703–722.
2. L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. **11** (1960), 391–392.
3. Y.-M. J. Chen, *On primitive roots of one-dimensional tori*, J. Number Theory **93** (2002), 23–33.
4. J. Coykendall, *Half-factorial domains in quadratic fields*, J. Algebra **235** (2001), 417–430.
5. P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael’s lambda function*, Acta Arith. **58** (1991), 363–385.
6. K. (S.) Fan, *Weighted Erdős–Kac theorems via computing moments*, Acta Arith., to appear. arXiv:2306.11289.
7. ———, *Rough numbers and variations on the Erdős–Kac theorem*, Dartmouth College Ph.D Dissertations. **156** (2023).
8. A. Geroldinger and F. Halter-Koch, *Non-unique factorizations*, Pure and Applied Mathematics (Boca Raton), vol. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006.
9. R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, Cambridge, 1988.
10. F. Halter-Koch, *Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörpern*, J. Number Theory **4** (1972), 70–77.
11. ———, *Factorization of algebraic integers*, Grazer Math. Berichte **191** (1983).
12. ———, *Elasticity of factorizations in atomic monoids and integral domains*, J. Théor. Nombres Bordeaux **7** (1995), 367–385.
13. C. Hooley, *On Artin’s conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.
14. N. Kataoka, *The distribution of prime ideals in a real quadratic field with units having a given index in the residue class field*, J. Number Theory **101** (2003), 349–375.
15. D. Koukoulopoulos, *The distribution of prime numbers*, Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2019.
16. S. Li and C. Pomerance, *On generalizing Artin’s conjecture on primitive roots to composite moduli*, J. Reine Angew. Math. **556** (2003), 205–224.
17. Florian Luca and Carl Pomerance, *Irreducible radical extensions and Euler-function chains*, Combinatorial number theory, de Gruyter, Berlin, 2007, pp. 351–361.
18. P. Moree and J. Cazarán, *On a claim of Ramanujan in his first letter to Hardy*, Exposition. Math. **17** (1999), no. 4, 289–311.
19. W. Narkiewicz, *A note on elasticity of factorizations*, J. Number Theory **51** (1995), 46–47.
20. K. Norton, *On the number of restricted prime factors of an integer. I*, Illinois J. Math. **20** (1976), 681–705.
21. P. Pollack, *The number of non-cyclic Sylow subgroups of the multiplicative group modulo  $n$* , Canad. Math. Bull. **64** (2021), 204–215.
22. ———, *Half-factorial real quadratic orders*, Arch. Math. (Basel) **122** (2024), 491–500.
23. ———, *Maximally elastic quadratic fields*, J. Number Theory **267** (2025), 80–100.
24. C. Pomerance, *On the distribution of amicable numbers*, J. Reine Angew. Math. **293(294)** (1977), 217–222.
25. P. Ribenboim, *Classical theory of algebraic numbers*, Universitext, Springer-Verlag, New York, 2001.
26. H. Roskam, *A quadratic analogue of Artin’s conjecture on primitive roots*, J. Number Theory **81** (2000), 93–109, erratum in **85** (2000), 108.
27. J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401.
28. J.-L. Steffan, *Longueurs des décompositions en produits d’éléments irréductibles dans un anneau de Dedekind*, J. Algebra **102** (1986), 229–236.
29. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, 3rd ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015.
30. R. J. Valenza, *Elasticity of factorization in number fields*, J. Number Theory **36** (1990), 212–218.
31. P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite Abelian groups*, Math. Centrum Amsterdam Afd. Zuivere Wisk. (1967), 27 pp.
32. H. Weber, *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Math. Ann. **20** (1882), 301–329.
33. A. Zaks, *Half factorial domains*, Bull. Amer. Math. Soc. **82** (1976), 721–723, corrigendum in **82** (1976), 965.
34. ———, *Half-factorial-domains*, Israel J. Math. **37** (1980), 281–302.

MAX-PLANCK-INSTITUT FÜR MATHEMATIK, 53111 BONN, GERMANY

*Email address:* `steve.fan@mpim-bonn.mpg.de`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA 30602

*Email address:* `pollack@uga.edu`