

MODULAR FORMS AND AN EXPLICIT CHEBOTAREV VARIANT OF THE BRUN–TITCHMARSH THEOREM

DANIEL HU, HARI R. IYER, AND ALEXANDER SHASHKOV

ABSTRACT. We prove an explicit Chebotarev variant of the Brun–Titchmarsh theorem. This leads to explicit versions of the best known unconditional upper bounds toward conjectures of Lang and Trotter for the coefficients of holomorphic cuspidal newforms. In particular, we prove that

$$\lim_{x \rightarrow \infty} \frac{\#\{1 \leq n \leq x \mid \tau(n) \neq 0\}}{x} > 1 - 1.15 \times 10^{-12},$$

where $\tau(n)$ is Ramanujan’s tau-function. This is the first known positive unconditional lower bound for the proportion of positive integers n such that $\tau(n) \neq 0$.

CONTENTS

1. Introduction	1
2. Preliminaries	7
3. Reduction to the abelian case	13
4. Sums over integral ideals	14
5. Implementing the Selberg sieve	20
6. Brun–Titchmarsh for abelian extensions	22
7. Upper bounds for the Lang–Trotter conjecture	23
8. Proof of Theorems 1.2 and 1.4	33
9. Proof of Theorems 1.3 and 1.5	36
References	38

1. INTRODUCTION

Let $\pi(x; q, a)$ be the number of primes $p \leq x$ such that $p \equiv a \pmod{q}$. The prime number theorem for primes in arithmetic progressions states that if $\gcd(a, q) = 1$, then for any $N > 0$, there exists an (ineffective) constant $C_N > 0$ such that if $q \leq (\log x)^N$, then

$$\left| \pi(x; q, a) - \frac{\text{Li}(x)}{\varphi(q)} \right| \ll_N x \exp(-C_N \sqrt{\log x}), \quad (1.1)$$

where $\text{Li}(x)$ is the logarithmic integral

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}.$$

Date: August 22, 2022.

2020 Mathematics Subject Classification. Primary: 11R44; Secondary: 11N36, 11F30.

Under the generalized Riemann hypothesis (GRH) for Dirichlet L -functions, we can extend the range to $q \leq x^{1/2}(\log x)^{-1}$, and reduce the error term to $O(x^{1/2} \log x)$. For many applications, providing a better range for x is of crucial importance, though this may require the tradeoff that we work with upper or lower bounds for $\pi(x; q, a)$ in lieu of an asymptotic. For instance, the Brun–Titchmarsh theorem in the form proved by Montgomery and Vaughan [MV73] states that if $q < x$, then

$$\pi(x; q, a) \leq \frac{2x}{\varphi(q) \log(x/q)}. \quad (1.2)$$

We consider analogous results over number fields. Let L/F be a Galois extension of number fields with Galois group G . For each prime ideal \mathfrak{p} of F which does not ramify in L , we use the Artin symbol $\left(\frac{L/F}{\mathfrak{p}}\right)$ to denote the conjugacy class in G of Frobenius elements of primes in L lying over \mathfrak{p} . Given a fixed conjugacy class C of G , define

$$\pi_C(x, L/F) := \#\left\{\mathfrak{p} \text{ unramified in } L, \left(\frac{L/F}{\mathfrak{p}}\right) = C, N_{F/\mathbb{Q}}\mathfrak{p} \leq x\right\}. \quad (1.3)$$

The Chebotarev density theorem states that

$$\lim_{x \rightarrow \infty} \frac{\pi_C(x, L/F)}{\text{Li}(x)} = \frac{|C|}{|G|}. \quad (1.4)$$

The first asymptotic version of this result with an effective error term was obtained by Lagarias and Odlyzko [LO77]. They showed that if $x \geq \exp(10[L : \mathbb{Q}](\log D_L)^2)$, then there exist absolute, effectively computable constants $c_0, c_1 > 0$ such that

$$\left|\pi_C(x, L/F) - \frac{|C|}{|G|} \text{Li}(x)\right| \leq \frac{|C|}{|G|} \text{Li}(x^{\beta_0}) + c_0 x \exp(-c_1 [L : \mathbb{Q}]^{-1/2} (\log x)^{1/2}), \quad (1.5)$$

where the β_0 term is only present when the Dedekind zeta function $\zeta_L(s)$ has a Siegel zero at β_0 . Lagarias, Montgomery, and Odlyzko [LMO79] improved the range at the cost of only proving an upper bound for $\pi_C(x, L/F)$. They showed that there exist absolute, effectively computable constants $c_2, c_3 > 0$ such that

$$\pi_C(x, L/F) \leq c_2 \frac{|C|}{|G|} \text{Li}(x), \quad \log x \geq c_3 (\log D_L)(\log \log D_L)(\log \log \log e^{20} D_L). \quad (1.6)$$

Refinements to the effective version of the Chebotarev density theorem were later made by Serre [Ser81] and V. K. Murty [Mur97].

In a series of papers [TZ17, TZ18, TZ19], Thorner and Zaman improved the previous results on the asymptotic form and upper and lower bounds for the Chebotarev density theorem. Here we focus on their analogue of the Brun–Titchmarsh theorem (1.2). Let $A \subseteq G$ be an abelian subgroup such that $C \cap A$ is nonempty, and let K be the fixed field of A . Set $n_K = [K : \mathbb{Q}]$. Let \hat{A} be the dual group, \mathfrak{f}_χ the conductor of $\chi \in \hat{A}$, and define

$$\mathcal{Q} = \mathcal{Q}(L/K) := \max_{\chi \in \hat{A}} N_{K/\mathbb{Q}} \mathfrak{f}_\chi. \quad (1.7)$$

Thorner and Zaman [TZ18, Theorem 1.1] proved that there exists an absolute, effectively computable constant $c_4 > 0$ such that if

$$x \geq c_4 \left(D_K^{164} \mathcal{Q}^{123} + D_K^{55} \mathcal{Q}^{87} n_K^{68n_K} + D_K^2 \mathcal{Q}^2 n_K^{14,000n_K} \right), \quad (1.8)$$

then the bound on $\pi_C(x, L/F)$ in (1.6) holds. We have that $D_K \mathcal{Q} \leq D_L$ by the conductor-discriminant formula, and by Minkowski's bound, there exists an absolute, effectively computable constant $c_5 > 0$ such that $n_K \leq c_5 \log D_K \leq c_5 \log D_L$. Thus, there exists an absolute, effectively computable constant $c_6 > 0$ such that (1.8) holds when $\log x \geq c_6 (\log D_L) (\log \log D_L)$, so (1.8) is a uniform improvement over the range in (1.6). There also exists an absolute, effectively computable constant $c_7 > 0$ such that for most number fields K , $n_K \leq c_7 (\log D_K) / \log \log D_K$. In this case, there exists an absolute, effectively computable constant $c_8 > 0$ such that (1.8) holds when $\log x \geq c_8 \log D_L$.

Our main result is a completely explicit Chebotarev variant of the Brun–Titchmarsh theorem with a range of x that improves upon (1.8).

Theorem 1.1. *Let L/F be a Galois extension of number fields with Galois group G , and let $C \subset G$ be a conjugacy class. Let A be an abelian subgroup of G such that $C \cap A$ is nonempty, and let K be the fixed field of A . If*

$$x \geq e^{92n_K+36} (D_K \mathcal{Q})^{8.4} n_K^{4.2n_K}, \quad (1.9)$$

then

$$\pi_C(x, L/F) \leq 11.3 \frac{|C|}{|G|} \frac{x}{\log x}. \quad (1.10)$$

Remark 1.1. Note that $\frac{x}{\log x} \leq \text{Li}(x)$ for all $x \geq 10$.

Remark 1.2. In the case where $F = K = \mathbb{Q}$ and $L = \mathbb{Q}(e^{2\pi i/q})$, we recover a weakened leading constant in the classical Brun–Titchmarsh theorem, valid in the range $x \geq e^{128} q^{8.4}$.

To prove Theorem 1.1, we use the Selberg sieve over number fields as in [Wei83]. In order to implement this strategy, we obtain estimates for the number of integral ideals in K with norm less than x satisfying certain congruence conditions. We prove these by bounding contour integrals of Hecke L -functions smoothed by a test function. This input may alternatively be treated by translation to a lattice point-counting argument, as in work of Debaene [Deb19], who obtained a similar result with better exponents of D_K and \mathcal{Q} but worse dependence on n_K . On the other hand, Debaene only works with the base field $F = \mathbb{Q}$, whereas the applications which motivate our work involve results over a general base field F . Moreover, the n_K -dependence is crucial for our applications.

We apply Theorem 1.1 to study values of the Fourier coefficients of modular forms. For $\text{Im}(z) > 0$, let

$$f(z) = \sum_{n=1}^{\infty} a_f(n) e^{2\pi i n z} \in \mathcal{S}_k^{\text{new}}(\Gamma_0(N))$$

be a normalized cusp form of even weight $k \geq 2$ which is a newform of level $N = N_f$ with trivial nebentypus and without complex multiplication. Fix $a \in \mathbb{Z}$, and define

$$\pi_f(x, a) := \#\{p \leq x, p \nmid N_f, a_f(p) = a\}. \quad (1.11)$$

One of the most celebrated such examples is the function

$$\Delta(z) = e^{2\pi iz} \prod_{n=1}^{\infty} (1 - e^{2\pi inz})^{24} = \sum_{n=1}^{\infty} \tau(n) e^{2\pi inz} \quad (1.12)$$

$$= e^{2\pi iz} - 24e^{4\pi iz} + 252e^{6\pi iz} - 1472e^{8\pi iz} + 4830e^{10\pi iz} - \dots, \quad (1.13)$$

where $\tau(n)$ is Ramanujan's tau-function. Lehmer [Leh47] pondered whether $\tau(n) \neq 0$ for all $n \geq 1$, and showed that proving $\tau(p) \neq 0$ for all primes p would imply this. The question remains open, with computations by Bosman [EC11] verifying that $\tau(n) \neq 0$ for $n \leq 2 \times 10^{19}$. Closely related to Lehmer's speculation is the following conjecture of Atkin and Serre [Ser76].

Conjecture (Atkin–Serre). *Let $f \in \mathcal{S}_k^{\text{new}}(\Gamma_0(N))$ be a non-CM newform with trivial nebentypus. For all $\epsilon > 0$, there exist constants $c_f(\epsilon), c'_f(\epsilon) > 0$ such that if $p \geq c_f(\epsilon)$, then $|a_f(p)| \geq c'_f(\epsilon)p^{(k-3)/2-\epsilon}$.*

In particular, the truth of this conjecture would imply for all $a \in \mathbb{Z}$ that $\tau(p) = a$ for only finitely many p . In light of this conjecture, it is natural to ask for bounds on the function $\pi_{\Delta}(x, a)$. Serre [Ser81] used refined versions of (1.5) and (1.6) to show that for all $\delta < 1/4$, there exists an effectively computable constant $c(\delta) > 0$ such that

$$\pi_{\Delta}(x, a) \leq c(\delta) \frac{x}{(\log x)^{1+\delta}}, \quad x \geq 3. \quad (1.14)$$

Following subsequent improvements by Wan [Wan90] and V. K. Murty [Mur97], Thorner and Zaman [TZ18] proved that there exists an absolute, effectively computable constant $c_9 > 0$ such that

$$\pi_{\Delta}(x, a) \leq c_9 \frac{x(\log \log x)^2}{(\log x)^2}, \quad x \geq 16. \quad (1.15)$$

Under GRH for symmetric power L -functions, Rouse and Thorner [RT17] proved a stronger bound using arguments based on the Sato–Tate conjecture. They proved, under GRH for symmetric power L -functions, that there exists an absolute, effectively computable constant $c_{10} > 0$ such that for all $a \in \mathbb{Z}$, there exists an effectively computable constant $c(a) > 0$ such that

$$\pi_{\Delta}(x, a) \leq c_{10} \frac{x^{3/4}}{\sqrt{\log x}}, \quad x \geq c(a). \quad (1.16)$$

In the case $a = 0$, Zywina [Zyw15] matched this bound under GRH for Hecke L -functions using arguments based on the Chebotarev density theorem.

We make the result (1.15) explicit by proving the following.

Theorem 1.2. *For all $a \in \mathbb{Z}$, we have that*

$$\pi_{\Delta}(x, a) \leq 4627 \frac{x(\log \log x)^2}{(\log x)^2}, \quad x \geq e^{e^{16}}.$$

When $a = 0$, this bound may be strengthened to

$$\pi_{\Delta}(x, 0) \leq (3.01 \times 10^{-10}) \frac{x(\log \log x)^2}{(\log x)^2}, \quad x \geq e^{\epsilon^{16}}.$$

For the weight 2 newform

$$f_E(z) = \sum_{n=1}^{\infty} a_E(n) e^{2\pi i n z} \in \mathcal{S}_2^{\text{new}}(\Gamma(N_E))$$

associated to a non-CM elliptic curve E/\mathbb{Q} of conductor N_E , Lang and Trotter [LT76] conjectured that there exists a constant $c_{E,a} \geq 0$ such that

$$\pi_E(x, a) := \pi_{f_E}(x, a) \sim c_{E,a} \frac{\sqrt{x}}{\log x}. \quad (1.17)$$

When $a = 0$, Elkies [Elk87, Elk91] and Fouvry and M. R. Murty [FM96] showed that for all $\epsilon > 0$, there exist positive constants $c(E, \epsilon)$, $c'(E, \epsilon)$, and $c(E)$ such that if $x \geq c(E, \epsilon)$, then

$$c'(E, \epsilon) \frac{\log \log \log x}{(\log \log \log x)^{1+\epsilon}} \leq \pi_E(x, a) \leq c(E) x^{3/4}. \quad (1.18)$$

In particular, $a_E(p) = 0$ infinitely often. In the general case where $a \in \mathbb{Z}$ is fixed, Serre [Ser81] proved that for all $\delta < 1/4$, there exists an effectively computable constant $c(N_E, \delta) > 0$ such that

$$\pi_E(x, a) \leq c(N_E, \delta) \frac{x}{(\log x)^{1+\delta}}, \quad x \geq 3. \quad (1.19)$$

After subsequent improvements by Wan [Wan90] and V. K. Murty [Mur97], Thorner and Zaman [TZ18] proved that there exists an effectively computable constant $c(N_E) > 0$ such that

$$\pi_E(x, a) \leq c(N_E) \frac{x(\log \log x)^2}{(\log x)^2}, \quad x \geq 3. \quad (1.20)$$

For an example, consider the elliptic curve

$$E : y^2 - y = x^3 - x^2. \quad (1.21)$$

This elliptic curve has conductor 11, the least conductor of any elliptic curve over \mathbb{Q} . Its associated modular form is given by

$$f_E(z) = \eta^2(z) \eta^2(11z), \quad \eta(z) := e^{\pi i z / 12} \prod_{n \geq 1} (1 - e^{2\pi i n z}). \quad (1.22)$$

We prove the following theorem.

Theorem 1.3. *Let E be the elliptic curve given by (1.21) and $a \in \mathbb{Z}$. Then,*

$$\pi_E(x, a) \leq 631 \frac{x(\log \log x)^2}{(\log x)^2}, \quad x \geq e^{e^{13}}. \quad (1.23)$$

Remark 1.3. Analogues of Theorems 1.2 and 1.3 can be obtained for a broad class of other newforms, see Remark 7.1.

Suitably strong bounds for the quantity $\pi_f(x, 0)$ as in (1.11) can be used to study the proportion of integers $n \geq 1$ such that $a_f(n) \neq 0$. Define

$$D_f := \lim_{x \rightarrow \infty} \frac{\#\{1 \leq n \leq x \mid a_f(n) \neq 0\}}{x}.$$

For $f = \Delta$, Serre [Ser81, p. 379] proved that

$$D_\Delta = \prod_{\tau(p)=0} \left(1 - \frac{1}{p+1}\right). \quad (1.24)$$

As a consequence of (1.14), this product converges absolutely. Rouse and Thorner [RT17] showed that $D_\Delta > 1 - 1.54 \times 10^{-13}$ under the generalized Riemann hypothesis for the symmetric power L -functions of Δ . Here, we prove the first unconditional positive lower bound for D_Δ .

Theorem 1.4. *We have*

$$D_\Delta > 1 - 1.15 \times 10^{-12}. \quad (1.25)$$

For the cusp form f_E associated to the elliptic curve given in (1.21), Serre [Ser81, p. 379] proved that

$$D_{f_E} = \frac{14}{15} \prod_{a_E(p)=0} \left(1 - \frac{1}{p+1}\right). \quad (1.26)$$

As a consequence of (1.19), the product converges absolutely. Serre showed that $D_{f_E} < 0.847$ and conjectured a lower bound of 0.845. Rouse and Thorner [RT17] proved that $D_{f_E} > 0.8306$ under the generalized Riemann hypothesis for the symmetric power L -functions associated to E . We prove the first unconditional positive lower bound for D_{f_E} .

Theorem 1.5. *Let E be given by (1.21). We have that*

$$D_{f_E} > 0.004769.$$

The density D_Δ naturally arises in a central limit theorem for $\tau(n)$ proved by Luca, Radziwiłł, and Shparlinski [LRS19]. Denote by $d(n)$ the number of divisors of n , and recall, by Deligne's proof of the Weil conjectures, that for all $n \geq 1$, the function $\tau(n)$ satisfies the bound

$$|\tau(n)| \leq d(n)n^{11/2}. \quad (1.27)$$

Consequently, it is natural to consider the distribution of a “normalized” tau-function $\tau(n)/n^{11/2}$ at the integers $n \geq 1$. For instance, the Sato–Tate conjecture implies that $|\tau(p)/p^{11/2}|$ stays arbitrarily near the value 2 for a positive proportion of primes p . In fact, an application of Theorem 1 of [LRS19] demonstrates that for all $\epsilon > 0$, there exists a density one subset S_ϵ of the integers such that if $n \in S_\epsilon$, then

$$|\tau(n)|/n^{11/2} \leq (\log n)^{-\frac{1}{2}+\epsilon}.$$

This implies that for almost all $n \geq 1$, Deligne's bound (1.27) for $\tau(n)/n^{11/2}$ is not sharp.

Moreover, Corollary 5 of [LRS19] shows that the exponent $-\frac{1}{2}$ above is optimal, in the sense that for fixed $v \in \mathbb{R}$, the central limit theorem

$$\lim_{x \rightarrow \infty} \frac{\#\left\{1 \leq n \leq x \mid \frac{\log |\tau(n)/n^{11/2}| + (\log \log n)/2}{\sqrt{(\frac{1}{2} + \frac{\pi^2}{12}) \log \log n}} \geq v\right\}}{\#\{1 \leq n \leq x \mid \tau(n) \neq 0\}} = \frac{1}{\sqrt{2\pi}} \int_v^\infty e^{-u^2/2} du$$

holds.

This gives the distribution as a proportion of the integers in the support of $\tau(n)$, but by substituting the upper bound $D_\Delta \leq 1$ and our lower bound for D_Δ as in Theorem 1.4, we establish upper and lower limits for the distribution as a proportion of all integers in the style of the Erdős–Kac theorem.

Corollary 1.6. *For fixed $v \in \mathbb{R}$, we have*

$$\begin{aligned} \frac{1}{\sqrt{2\pi}} \int_v^\infty e^{-u^2/2} du &\geq \lim_{x \rightarrow \infty} \frac{1}{x} \cdot \#\left\{1 \leq n \leq x : \frac{\log |\tau(n)/n^{11/2}| + \frac{1}{2} \log \log n}{\sqrt{(\frac{1}{2} + \frac{\pi^2}{12}) \log \log n}} \geq v\right\} \\ &> (1 - 1.15 \times 10^{-12}) \frac{1}{\sqrt{2\pi}} \int_v^\infty e^{-u^2/2} du. \end{aligned}$$

Outline of the paper. In Section 2, we introduce notation and prove some preliminary technical lemmas, including estimates for a certain test function and bounds for Hecke L -functions in the critical strip. In Section 3, we show that Theorem 1.1 follows from only considering abelian extensions of number fields. In Section 4, we use smoothing arguments to compute estimates for certain sums over integral ideals. We apply these estimates in Section 5, where we use the Selberg sieve over number fields to develop an upper bound for $\pi_C(x, L/K)$ for abelian extensions. In Section 6 we bound error terms arising from the Selberg sieve by choosing x in a large enough range relative to parameters depending on L/K , thereby yielding our Brun–Titchmarsh theorem for abelian extensions.

In Section 7, we deduce an upper bound for $\pi_f(x, a)$ from upper bounds for $\pi_C(x, L/K)$ for suitably chosen extensions L/K arising from ℓ -adic Galois representations attached to f . In Section 8 we make the results in Section 7 explicit for $\tau(n)$, proving Theorem 1.2 and Theorem 1.4. Finally, in Section 9 we prove Theorems 1.3 and 1.5 for the elliptic curve (1.21).

Acknowledgments. The authors would like to thank Ken Ono for his valuable suggestions. They are grateful for the support of grants from the National Science Foundation (DMS-2002265, DMS-2055118, DMS-2147273), the National Security Agency (H98230-22-1-0020), and the Templeton World Charity Foundation. This research was conducted as part of the 2022 Research Experiences for Undergraduates at the University of Virginia.

2. PRELIMINARIES

Throughout this paper $s = \sigma + it$ is a complex variable.

2.1. Notation. In this section we establish the notation utilized in the proof of Theorem 1.1. Subsequently K will be a number field and L a finite extension of K . We use the following notation:

- \mathcal{O}_K is the ring of integers of K .
- $n_K = [K : \mathbb{Q}]$ is the degree of K/\mathbb{Q} .
- $D_K = |\text{disc}(K/\mathbb{Q})|$.
- $N_{K/\mathbb{Q}}$ is the absolute norm of K . We write $N = N_{K/\mathbb{Q}}$ when there is no ambiguity about the field.
- $\zeta_K(s)$ is the Dedekind zeta function of K .
- κ_K is the value of the residue of the pole of $\zeta_K(s)$ at $s = 1$.
- h_K is the class number of K .
- \mathfrak{p} denotes a prime ideal of K .
- \mathfrak{a} denotes an integral ideal of K .
- $\omega(\mathfrak{a})$ is the number of distinct prime ideals dividing \mathfrak{a} .
- $\varphi_K(\mathfrak{a}) = (N\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} (1 - N\mathfrak{p}^{-1})$ is the Euler phi-function associated to K .

Suppose that L/K is a Galois extension of number fields, and let G be its Galois group. Recall the *Artin symbol* $(\frac{L/K}{\mathfrak{p}})$, also denoted $\text{Frob}_{\mathfrak{p}}$, associated to a prime ideal \mathfrak{p} of K unramified in L ; it is the conjugacy class in G consisting of Frobenius automorphisms corresponding to the prime ideals \mathfrak{P} lying over \mathfrak{p} .

Let L/K be abelian. Then, each conjugacy class of G is a singleton. Thus, the Artin symbol maps unramified prime ideals of K to elements of G . For \mathfrak{m} an integral ideal of K , let $I(\mathfrak{m})$ denote the group of fractional ideals relatively prime to \mathfrak{m} , and let $P_{\mathfrak{m}}$ be the subgroup of principal ideals (α) with $\alpha \in K^\times$ totally positive and $\alpha \equiv 1 \pmod{\mathfrak{m}}$. Then the *ray class group* modulo \mathfrak{m} is defined to be the finite group $I(\mathfrak{m})/P_{\mathfrak{m}}$.

If \mathfrak{m} is divisible by all ramified primes in L/K , then the Artin symbol extends multiplicatively to a surjective group homomorphism called the *Artin map*

$$F_{L/K} : I(\mathfrak{m}) \rightarrow \text{Gal}(L/K).$$

By Artin reciprocity, there exists an integral ideal \mathfrak{m} such that

$$H = \ker(F_{L/K})$$

contains $P_{\mathfrak{m}}$. In this case, $F_{L/K}$ induces an isomorphism

$$I(\mathfrak{m})/H \cong \text{Gal}(L/K). \tag{2.1}$$

Moreover, there exists a unique integral ideal $\mathfrak{f}_{L/K}$, called the *Artin conductor* of L/K , dividing all \mathfrak{m} with this property. Thus $[I(\mathfrak{f}_{L/K}) : H] = [L : K]$.

Let C be one conjugacy class of G . While our goal is to bound the quantity $\pi_C(x, L/K)$, the above discussion implies that this problem is equivalent to the problem of counting prime ideals in a given coset of H in the ray class group modulo $\mathfrak{f}_{L/K}$. In particular, our conjugacy class $C \subset G$ is identified with a unique coset $aH \in I(\mathfrak{f}_{L/K})/H$, so the prime ideals \mathfrak{p} with $\text{Frob}_{\mathfrak{p}} = C$ are precisely the prime ideals $\mathfrak{p} \in aH$. In summary, we have that

$$\pi_C(x, L/K) = \pi_{aH}(x, L/K), \tag{2.2}$$

where $\pi_C(x, L/K)$ is given by (1.3) and

$$\pi_{aH}(x, L/K) := \#\left\{ \mathfrak{p} \text{ unramified in } L/K, \mathfrak{p} \in aH, N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x \right\}. \quad (2.3)$$

We recall the basic theory of ray class characters and their associated L -functions. Let \mathfrak{m} be an integral ideal. A *ray class character* χ modulo \mathfrak{m} is defined to be a character of the group $I(\mathfrak{m})/P_{\mathfrak{m}}$, with the convention that $\chi(\mathfrak{a}) = 0$ if \mathfrak{a} and \mathfrak{m} are not coprime. Note that we will often view χ as acting on an ideal \mathfrak{a} itself rather than its ideal class $\mathfrak{a}P_{\mathfrak{m}}$ in the ray class group. If \mathfrak{m} divides \mathfrak{n} then the inclusion induces a map $I(\mathfrak{n})/P_{\mathfrak{n}} \rightarrow I(\mathfrak{m})/P_{\mathfrak{m}}$; composing a character χ mod \mathfrak{m} with this map induces a character χ' mod \mathfrak{n} . A character is *primitive* if it cannot be induced, except by itself. Given some χ mod \mathfrak{m} , there is a unique primitive character $\tilde{\chi}$ mod \mathfrak{f}_{χ} which induces χ . The integral ideal \mathfrak{f}_{χ} is the *conductor* of χ .

If $\mathfrak{m} = \mathfrak{f}_{L/K}$ and $H = \ker(F_{L/K})$, then we define the following quantity associated to the extension L/K ,

$$\mathcal{Q} = \mathcal{Q}(L/K) := \max_{\chi(H)=1} N_{K/\mathbb{Q}}\mathfrak{f}_{\chi},$$

where the maximum is over characters χ such that $\chi(H) = 1$; by (2.1), these correspond precisely to the irreducible characters of G .

Given an integral ideal \mathfrak{m} and a ray class character χ modulo \mathfrak{m} , the *Hecke L -function* associated to χ is given by the following Dirichlet series and Euler product:

$$L(s, \chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s} = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^s} \right)^{-1}, \quad \sigma > 1,$$

with the sum over all integral ideals of K and the product over all prime ideals of K .

For the purpose of obtaining explicit numerical constants, careful bounds on Hecke L -functions along vertical lines near the critical strip will also be of importance. These are derived by application of the Phragmén–Lindelöf principle for complex analytic functions in Lemma 2.1, taking as input the functional equation for the the Hecke L -functions and asymptotics for related gamma factors. First we define the quantities

$$D_{\chi} = D_K N_{K/\mathbb{Q}}\mathfrak{f}_{\chi}.$$

$$\delta_{\chi_0}(\chi) = \begin{cases} 1 & \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases}$$

Let r_1 be the number of real places of K and $2r_2$ the number of complex places of K . If χ is primitive, then let $0 \leq \mu_{\chi} \leq r_1$ be the number of real places at which χ ramifies, and set

$$A_{\chi} = 2^{-r_2} \pi^{n_K/2} D_{\chi}^{1/2},$$

$$\Gamma_{\chi}(s) = \Gamma\left(\frac{s}{2}\right)^{r_1 - \mu_{\chi}} \Gamma\left(\frac{s+1}{2}\right)^{\mu_{\chi}} \Gamma(s)^{r_2}.$$

The completed Hecke L -function is given by

$$\Lambda(s, \chi) = A_{\chi}^s \Gamma_{\chi}(s) L(s, \chi).$$

For χ a primitive character, $\Lambda(s, \chi)$ satisfies the functional equation

$$\Lambda(1-s, \bar{\chi}) = W(\chi)\Lambda(s, \chi),$$

with the root number $W(\chi)$ a complex constant of modulus 1.

2.2. Preliminary estimates. We begin by establishing explicit bounds for the Hecke L -function of a ray class character in the critical strip.

Lemma 2.1. *Let \mathfrak{m} be an integral ideal of K , and let χ be a primitive ray class character modulo \mathfrak{m} . If $\delta > 0$ and $-\delta < \sigma < 1$, then*

$$|L(s, \chi)| \leq \left(\frac{\delta+1}{1-\sigma}\right)^{\delta_{x_0}(\chi)} (1+\delta^{-1})^{n_K} \left(\frac{D_\chi}{(2\pi)^{n_K}} |s+1|^{n_K}\right)^{(1+\delta-\sigma)/2}. \quad (2.4)$$

Proof. Expanding the functional equation into unsymmetric form and taking absolute values yields

$$|L(s, \chi)| = |L(1-s, \chi)| \left| \frac{\Gamma_\chi(1-s)}{\Gamma_\chi(s)} \right| A_\chi^{1-2s}.$$

Using [Rad60, Lemmas 1, 2, 3], we bound the gamma factors at $s = -\delta + it$ with $\delta \in (0, 1/2)$:

$$\begin{aligned} \frac{\Gamma_\chi(1-s)}{\Gamma_\chi(s)} &= \left(\frac{\Gamma(\frac{1-s}{2})}{\Gamma(\frac{s}{2})}\right)^{r_1-\mu_\chi} \left(\frac{\Gamma(\frac{1}{2}+\frac{1-s}{2})}{\Gamma(\frac{1}{2}+\frac{s}{2})}\right)^{\mu_\chi} \left(\frac{\Gamma(1-s)}{\Gamma(s)}\right)^{r_2} \\ &\leq \left(\frac{1}{2}|s+1|\right)^{(1/2+\delta)(r_1-\mu_\chi)} \left(\frac{1}{2}|s+1/2|\right)^{(1/2+\delta)\mu_\chi} (|s+1|)^{(1+2\delta)r_2} \\ &\leq 2^{-(1/2+\delta)r_1} |s+1|^{(1/2+\delta)n_K} \end{aligned}$$

where we use that $r_1 + 2r_2 = n_K$. Therefore, if $\delta \in (0, 1/2)$, then

$$|L(-\delta + it, \chi)| \leq |L(1 + \delta + it, \chi)| \left(\frac{D_\chi}{(2\pi)^{n_K}} |s+1|^{n_K}\right)^{(1/2+\delta)}.$$

By the estimate

$$|L(s, \chi)| \leq \zeta_K(\sigma) \leq \zeta(\sigma)^{n_K} \leq \left(1 + \frac{1}{\sigma-1}\right)^{n_K}, \quad \sigma > 1,$$

we also have the bound

$$|L(1 + \delta + it, \chi)| \leq (1 + \delta^{-1})^{n_K}.$$

Now, assume that χ is nontrivial, so $L(s, \chi)$ is holomorphic in the strip $-\delta \leq \sigma \leq 1 + \delta$. Then in the strip $-\delta \leq \sigma \leq 1 + \delta$, applying the Phragmén–Lindelöf principle gives

$$|L(s, \chi)| \leq (1 + \delta^{-1})^{n_K} \left(\frac{D_\chi}{(2\pi)^{n_K}} |s+1|^{n_K}\right)^{(1+\delta-\sigma)/2}.$$

When χ is trivial, we have that $L(s, \chi) = \zeta_K(s)$. Since $\zeta_K(s)$ has a pole at $s = 1$, we choose any $B \geq 1$ and we instead estimate $\frac{s+B}{s-1}\zeta_K(s)$. By a similar argument as above, in the strip $-\delta \leq \sigma \leq \delta + 1$ we have that

$$|\zeta_K(\sigma + it)| \leq \left| \frac{\delta+1}{\delta-B} \right| \left| \frac{s+B}{s-1} \right| (1 + \delta^{-1})^{n_K} \left(\frac{D_K}{(2\pi)^n} |s+1|^{n_K}\right)^{(1+\delta-\sigma)/2}. \quad (2.5)$$

Using the bound

$$\left| \frac{s+B}{s-1} \right| = \left| \frac{B+1}{s-1} + 1 \right| \leq \frac{B+1}{1-\sigma} + 1 = \frac{B+\sigma}{1-\sigma}, \quad (2.6)$$

we find that

$$|\zeta_K(\sigma + it)| \leq \left(\frac{\delta+1}{1-\sigma} \right) (1+\delta^{-1})^{n_K} \left(\frac{D_K}{(2\pi)^{n_K}} |s+1|^{n_K} \right)^{(1+\delta-\sigma)/2}, \quad (2.7)$$

since $|B+\sigma|/|\delta-B|$ can be made arbitrarily close to 1 as $B \rightarrow \infty$. \square

In order to obtain explicit estimates for $\pi_C(x, L/K)$, we utilize a test function which approximates the indicator function of the interval $[\frac{1}{2}, 1]$.

Lemma 2.2 (Thorner–Zaman [TZ18, Lemma 2.2]). *For any $x \geq 3$, $\epsilon \in (0, \frac{1}{2})$, and positive integer $\ell \geq 1$, set*

$$A = \frac{\epsilon}{2\ell \log x}.$$

There exists a real-variable function $\phi(t) = \phi(t; x, \ell, \epsilon)$ such that:

- (a) $0 \leq \phi(t) \leq 1$ for all $t \in \mathbb{R}$, and $\phi(t) \equiv 1$ for $\frac{1}{2} \leq t \leq 1$.
- (b) *The support of ϕ is contained in the interval $[\frac{1}{2} - \frac{\epsilon}{\log x}, 1 + \frac{\epsilon}{\log x}]$.*
- (c) *Its Laplace transform $F(z) = \int_{\mathbb{R}} \phi(t) e^{-zt} dt$ is entire and is given by*

$$F(z) = e^{-(1+2\ell A)z} \cdot \left(\frac{1 - e^{(\frac{1}{2}+2\ell A)z}}{-z} \right) \left(\frac{1 - e^{2Az}}{-2Az} \right)^\ell. \quad (2.8)$$

- (d) *Let $s = \sigma + it \in \mathbb{C}$, $\sigma > 0$ and let α be any real number satisfying $0 \leq \alpha \leq \ell$. Then*

$$|F(-s \log x)| \leq \frac{e^{\sigma\epsilon} x^\sigma}{|s| \log x} \cdot (1 + x^{-\sigma/2}) \cdot \left(\frac{2\ell}{\epsilon|s|} \right)^\alpha. \quad (2.9)$$

- (e) *We have*

$$F(0) = \frac{1}{2} + \frac{\epsilon}{\log x} \quad \text{and} \quad F(-\log x) \leq e^\epsilon \frac{x}{\log x}. \quad (2.10)$$

- (f) *If $s = \sigma + it \in \mathbb{C}$ and $\sigma \leq 0$, then*

$$|F(-s \log x)| \leq \frac{2x^{\sigma/2}}{|s| \log x} \cdot \left(\frac{\ell(1 + e^{-\epsilon\sigma})}{\epsilon|s|} \right)^\ell. \quad (2.11)$$

- (g) *If $s = \sigma + it$ with $\sigma < 0$ and $|s| < \frac{2\ell}{\epsilon}$, we have that*

$$|F(-s \log x)| \leq \frac{2x^{\sigma/2}}{|s| \log x} \cdot \left(\frac{2}{2 - |s\epsilon/\ell|} \right)^\ell. \quad (2.12)$$

Proof. Parts (a)–(e) are proven in Lemma 2.2 of [TZ18]. Part (f) follows from (2.8). Part (g) follows from (2.8) and the following identity, which is valid for any complex $|z| < 2$:

$$\left| \frac{1 - e^z}{-z} \right| \leq \frac{2}{2 - |z|}. \quad (2.13)$$

Thorner and Zaman [TZ18] additionally assumed that $\epsilon \in (0, \frac{1}{4})$ in order to obtain bounds for $F(-s \log x)$ on the line $\sigma = -1/2$. We have no need for such estimates, so we can relax this to $\epsilon \in (0, \frac{1}{2})$. \square

2.3. Auxiliary results. Assume throughout that L/K is an abelian extension of number fields. The following lemmas will also be useful.

Lemma 2.3. *For all $0 < \gamma \leq 1$, we have*

$$\sum_{N(\mathfrak{a}) \leq x} 1 \leq (1 + \gamma^{-1})^{n_K} x^{1+\gamma}. \quad (2.14)$$

Proof. See [Wei83, Lemma 1.12(a)]. \square

Lemma 2.4. *Let $a, b > 0$. If $x \geq (ab)^{a(\sqrt{2/\log(ab)+1})}$, then*

$$\frac{x^{1/a}}{\log x} \geq b. \quad (2.15)$$

Proof. By properties of the Lambert W -function [CGH⁺96], we have that (2.15) holds when

$$\log x \geq -aW_{-1}\left(\frac{-1}{ab}\right)$$

where $W_{-1}(z)$ is the negative branch of the Lambert W -function. By Theorem 1 of [Cha13], we have that

$$-aW_{-1}\left(\frac{-1}{ab}\right) \leq a\left(\sqrt{2\log(ab)} + \log(ab)\right) \leq a(\sqrt{2/\log(ab)} + 1)\log(ab),$$

and the lemma follows by taking exponents. \square

Next, we bound $[L : K]$ in terms of n_K , D_K and \mathcal{Q} alone.

Lemma 2.5. *For all $0 < \epsilon \leq 1$,*

$$[L : K] \leq 2^{n_K} (1 + \epsilon^{-1})(n_K e)^{1+\epsilon} \left(\frac{4}{e^{2\pi}}\right)^{n_K(1+\epsilon)/2} D_K^{(1+\epsilon)/2} \mathcal{Q}.$$

At $\epsilon = 1$, for instance, this yields

$$[L : K] \leq (14.779)(0.7169)^{n_K} D_K \mathcal{Q}.$$

Proof. By [Wei83, Lemma 1.16], for H the congruence subgroup attached to the Artin conductor $\mathfrak{f}_{L/K}$, we have $[L : K] = [I(\mathfrak{f}_{L/K}) : H] \leq 2^{n_K} h_K \mathcal{Q}$. By Minkowski's bound and [Wei83, Lemma 1.12],

$$h_K \leq \sum_{N(\mathfrak{a}) \leq x_0} 1 \leq (1 + \epsilon^{-1})^{n_K} x_0^{1+\epsilon}$$

for $x_0 = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{n/2} D_K^{1/2} \leq \left(\frac{n}{e^{n-1}}\right) \left(\frac{4}{\pi}\right)^{n/2} D_K^{1/2}$. Then, an explicit bound is

$$h_K \leq (1 + \epsilon^{-1})(n_K e)^{1+\epsilon} \left(\frac{4}{e^{2\pi}}\right)^{n_K(1+\epsilon)/2} D_K^{(1+\epsilon)/2}.$$

Note that for $n_K \geq 1$ we have $n_K \leq e^{n_K-1}$. At $\epsilon = 1$, note that $n^2 \leq (3^{2/3})^n$ for all $n \in \mathbb{Z}_{\geq 1}$. \square

Next, we set $\mathfrak{m} = \mathfrak{f}_{L/K}$ and state the following bound for the quantity $\omega(\mathfrak{m})$.

Lemma 2.6. *Let $\mathfrak{m} = \mathfrak{f}_{L/K}$. For every $b > 0$ we have that*

$$\omega(\mathfrak{m}) < 2e^{1+2/b}n_K + b \log D_K \mathcal{Q}. \quad (2.16)$$

Proof. See [Wei83, Lemma 1.13(b)]. \square

Next, we introduce and bound the following product factor to appear in our treatment of non-primitive Hecke L -functions.

Lemma 2.7. *Let $M, b, \sigma, x > 0$. Define*

$$Z_{\mathfrak{m}}(\sigma) := \prod_{\mathfrak{p}|\mathfrak{m}} (1 + N\mathfrak{p}^{-\sigma}). \quad (2.17)$$

Let $\pi(x) := \#\{p \leq x, p \text{ prime}\}$. We have that

$$\begin{aligned} \log Z_{\mathfrak{m}}(\sigma) &\leq n_K \left[\log(1 + M^{-\sigma})(2e^{1+2/b} - \pi(M-1)) + \sum_{p < M} \log(1 + p^{-\sigma}) \right] \\ &\quad + b \log(1 + M^{-\sigma}) \log(D_K \mathcal{Q}). \end{aligned} \quad (2.18)$$

Proof. Given a rational prime p , there are at most n_K prime ideals in K with norm p . Thus, the product over all the factors in $Z_{\mathfrak{m}}(\sigma)$ with norm at most M is bounded by

$$\prod_{p < M} (1 + p^{-\sigma})^{n_K}. \quad (2.19)$$

There are at most $\omega(\mathfrak{m}) - n_K \pi(M-1)$ prime ideals \mathfrak{p} dividing \mathfrak{m} such that $N(\mathfrak{p}) \geq M$. In the product for $Z_{\mathfrak{m}}(\sigma)$, the factor corresponding to these primes can be bounded above by $(1 + M^{-\sigma})$, so that the product over all the factors in $Z_{\mathfrak{m}}(\sigma)$ with norm at least M is bounded by

$$(1 + M^{-\sigma})^{\omega(\mathfrak{m}) - n_K \pi(M-1)}. \quad (2.20)$$

Multiplying equations (2.19) and (2.20), taking logarithms, and applying Lemma 2.6 completes the proof. \square

Note that we could trivially bound $Z_{\mathfrak{m}}(\sigma)$ by $2^{\omega(\mathfrak{m})}$, but using Lemma 2.7 allows us to separately bound the contribution from small divisors of \mathfrak{m} by choosing M optimally, which provides sharper bounds later on.

3. REDUCTION TO THE ABELIAN CASE

In this section, we show that Theorem 1.1 follows from the following version of the Brun–Titchmarsh theorem for abelian extensions, which we prove in Section 6. This allows us to specialize to abelian extensions in Sections 4 and 5, wherein we develop auxiliary technical results.

Lemma 3.1. *Let L/K be an abelian extension of number fields, let C be a conjugacy class (which will necessarily be a singleton) of $\text{Gal}(L/K)$, and let $\pi_C(x, L/K)$ be the prime-counting function given in (1.3). If*

$$x \geq e^{36} e^{92n} (D_K \mathcal{Q})^{8.4} n^{4.2n}, \quad (3.1)$$

then

$$\pi_C(x, L/K) \leq 11.29 \frac{x}{[L : K] \log x}. \quad (3.2)$$

We show that Theorem 1.1 follows from this theorem for a general (nonabelian) Galois extension of number fields L/F . To do this, we change the base field from F to an intermediate field K such that L/K is abelian, so that we can apply Lemma 3.1.

The key tool is the following result from [MMS88, Proof of Proposition 3.9].

Lemma 3.2 (Murty–Murty–Saradha [MMS88]). *Let L/F be a Galois extension of number fields with Galois group G , and let $C \subset G$ be a conjugacy class. Let A be an abelian subgroup of G such that $C \cap A$ is nonempty, and let K be the fixed field of A . Let $g \in C \cap A$, and let $C_A = C_A(g)$ denote the conjugacy class of A which contains g . If $x \geq 2$, then*

$$\left| \pi_C(x, L/F) - \frac{|C|}{|G|} \frac{|A|}{|C_A|} \pi_{C_A}(x, L/K) \right| \leq \frac{|C|}{|G|} \left(n_L x^{1/2} + \frac{2}{\log 2} \log D_L \right).$$

Proof of Theorem 1.1. Let L/F be a Galois extension of number fields and let C be a conjugacy class of the Galois group $G = \text{Gal}(L/F)$. Let A be an abelian subgroup of G such that $C \cap A$ is nonempty, and let K be the fixed field of A . We apply Lemma 3.1 to the abelian extension L/K . If (3.1) holds, then

$$n_L x^{1/2} = n_K [L : K] x^{1/2} \leq \frac{x}{200 \log x}. \quad (3.3)$$

By the conductor discriminant formula we have that $D_L \leq D_K \mathcal{Q}^{[L:K]}$. Thus if (3.1) holds, then

$$\frac{2}{\log 2} \log D_L \leq \frac{2}{\log 2} (\log D_K + [L : K] \log \mathcal{Q}) \leq \frac{x}{200 \log x}. \quad (3.4)$$

Thus by Lemmas 3.1 and 3.2 we have that if (3.1) holds, then

$$\pi_C(x, L/F) \leq 11.3 \frac{|C|}{|G|} \frac{x}{\log x} \quad (3.5)$$

completing the proof of Theorem 1.1. \square

To prove Lemma 3.1, we utilize a version of the Selberg sieve developed by Weiss [Wei83]. First, we need explicit bounds on certain sums over ideals, which we develop in Section 4. We use these bounds in Section 5, where we implement the Selberg sieve.

4. SUMS OVER INTEGRAL IDEALS

Let aH be a coset of $I(\mathfrak{m})/H$ and \mathfrak{n} an integral ideal coprime to $\mathfrak{f}_{L/K}$. Define

$$A(x; a, \mathfrak{n}) := \sum_{\substack{\mathfrak{a} \in aH \\ \mathfrak{n} | \mathfrak{a}}} \phi \left(\frac{\log N(\mathfrak{a})}{\log x} \right), \quad (4.1)$$

where ϕ is the test function described in Lemma 2.2. We obtain estimates for $A(x; a, \mathfrak{n})$ in Section 4.1.

The second quantity we consider is

$$V(z) := \sum_{\mathbf{N}(\mathbf{a}) \leq z} \frac{1}{\mathbf{N}(\mathbf{a})}. \quad (4.2)$$

We establish lower bounds for $V(z)$ in Section 4.2.

4.1. Bounding $A(x; a, \mathbf{n})$. We begin by computing a smoothed character sum over integral ideals.

Lemma 4.1. *Let $x \geq 3$ and $\epsilon, \delta \in (0, 1/2)$. Let χ be a ray class character of K modulo \mathbf{m} , and let \mathbf{n} be an integral ideal coprime to \mathbf{m} . Let $Z_{\mathbf{m}}(\delta)$ be defined as in (2.17). If*

$$E(x) := Z_{\mathbf{m}}(\delta) \frac{8}{3\pi} \frac{1+\delta}{\delta(1-\delta)} (1+\delta^{-1})^{n_K} e^{\delta\epsilon} \left(\frac{D_K \mathcal{Q}}{(2\pi)^{n_K}} \right)^{1/2} 2^{n_K/2} \left[\frac{2}{\epsilon} (1+\epsilon) \right]^{n_K/2+1} n_K^{n_K/2} x^\delta, \quad (4.3)$$

then

$$\left| \sum_{\substack{\mathbf{a} \\ \mathbf{n}|\mathbf{a}}} \chi(\mathbf{a}) \phi\left(\frac{\log \mathbf{N}\mathbf{a}}{\log x}\right) - \delta_{\chi_0}(\chi) \chi(\mathbf{n}) \frac{\varphi_K(\mathbf{m}) \kappa_K}{\mathbf{N}\mathbf{m} \mathbf{N}\mathbf{n}} \cdot \log x \cdot F(-\log x) \right| \leq E(x),$$

Proof. By Laplace inversion, for $\delta > 0$ we have

$$\sum_{\substack{\mathbf{a} \\ \mathbf{n}|\mathbf{a}}} \chi(\mathbf{a}) \phi\left(\frac{\log \mathbf{N}\mathbf{a}}{\log x}\right) = \chi(\mathbf{n}) \frac{\log x}{2\pi i} \int_{1+\delta-i\infty}^{1+\delta+i\infty} \frac{L(s, \chi)}{(\mathbf{N}\mathbf{n})^s} F(-s \log x) ds.$$

We shift the line of integration from $\operatorname{Re}(s) = 1+\delta$ to $\operatorname{Re}(s) = \delta$, justifying the vanishing of the horizontal integrals by rapid decay of the function $F(-s \log x)$ as $|t| \rightarrow \infty$. In doing so, we pick up a residue at $s = 1$, so the above is equal to

$$\delta_{\chi_0}(\chi) \chi(\mathbf{n}) \frac{\varphi_K(\mathbf{m}) \kappa_K}{\mathbf{N}\mathbf{m} \mathbf{N}\mathbf{n}} \log x \cdot F(-\log x) + \chi(\mathbf{n}) \frac{\log x}{2\pi i} \int_{\delta-i\infty}^{\delta+i\infty} \frac{L(s, \chi)}{(\mathbf{N}\mathbf{n})^s} F(-s \log x) ds.$$

To estimate the integral, we first express $L(s, \chi)$ in terms of an L -function of a primitive character. If $\tilde{\chi}$ is the primitive character which induces χ , we have that

$$L(s, \chi) = L(s, \tilde{\chi}) \prod_{\mathfrak{p}|\mathbf{m}} (1 - \tilde{\chi}(\mathfrak{p}) \mathbf{N}\mathfrak{p}^{-s}). \quad (4.4)$$

We can bound the product over primes in (4.4) by $Z_{\mathbf{m}}(\sigma)$, defined in (2.17). Thus we have

$$\left| \chi(\mathbf{n}) \frac{\log x}{2\pi i} \int_{\delta-i\infty}^{\delta+i\infty} \frac{L(s, \chi)}{(\mathbf{N}\mathbf{n})^s} F(-s \log x) ds \right| \leq \frac{\log x}{2\pi} Z_{\mathbf{m}}(\delta) \int_{\delta-i\infty}^{\delta+i\infty} |L(s, \tilde{\chi})| |F(-s \log x)| ds. \quad (4.5)$$

We split the remaining integral into two pieces, the first with $|t| \leq M$ and the second with $|t| > M$, for some constant $M > 0$ which will be specified later. We bound the

contribution from $L(s, \chi)$ with Lemma 2.1 and the contribution from $F(-s \log x)$ with Lemma 2.2(d). Using these bounds and (4.5) gives

$$\begin{aligned} & \left| \chi(\mathbf{n}) \frac{\log x}{2\pi i} \int_{\delta-i\infty}^{\delta+i\infty} L(s, \chi) F(-s \log x) ds \right| \\ & \leq Z_{\mathfrak{m}}(\delta) \frac{1}{\pi} \left(\frac{D_{\chi}}{(2\pi)^{n_K}} \right)^{1/2} \left(\frac{1+\delta}{1-\delta} \right) (1+\delta^{-1})^{n_K} e^{\delta\epsilon} x^{\delta} (1+x^{-\delta/2}) \\ & \times \left[\int_0^M \frac{|\delta+1+it|^{n_K/2}}{|\delta+it|} dt + \left(\frac{2\ell}{\epsilon} \right)^{n_K/2+1} \int_M^{\infty} \frac{|\delta+1+it|^{n_K/2}}{|\delta+it|^{n_K/2+2}} dt \right]. \end{aligned}$$

We bound the first integral by

$$\begin{aligned} \int_0^M \frac{|\delta+1+it|^{n_K/2}}{|\delta+it|} dt & \leq \frac{1}{\delta} \int_0^M (\delta+1+t)^{n_K/2} dt \\ & \leq \frac{1}{\delta(n_K/2+1)} (\delta+1+M)^{n_K/2+1}. \end{aligned}$$

We set $\ell = \lceil n_K/2 + 1 \rceil$ and substitute $u = 1 + t^{-1}$ to bound the second integral by

$$\begin{aligned} \int_M^{\infty} \frac{|\delta+1+it|^{n_K/2}}{|\delta+it|^{\alpha+1}} dt & \leq \int_M^{\infty} \left| 1 + \frac{1}{\delta+it} \right|^{n_K/2} |\delta+it|^{-2} dt \\ & \leq \int_M^{\infty} \left(1 + \frac{1}{t} \right)^{n_K/2} t^{-2} dt \\ & \leq \int_1^{1+M^{-1}} u^{n_K/2} du \\ & \leq \frac{1}{n_K/2+1} \left[(1+M^{-1})^{n_K/2+1} - 1 \right]. \end{aligned} \tag{4.6}$$

Our bound on the sum of the two integrals is then

$$\frac{1}{n_K/2+1} \left[\frac{1}{\delta} (\delta+1+M)^{n_K/2+1} + \left(\frac{2\ell}{\epsilon} \right)^{n_K/2+1} \left((1+M^{-1})^{n_K/2+1} - 1 \right) \right].$$

If we choose M so that

$$\delta+1+M < \frac{2\ell}{\epsilon}, \tag{4.7}$$

we can bound the sum of the two integrals (using $\delta < 1$) by

$$\frac{1}{(n_K/2+1)\delta} \left[\frac{2\ell}{\epsilon} (1+M^{-1}) \right]^{n_K/2+1}. \tag{4.8}$$

Choosing $M = \frac{1}{\epsilon}$ satisfies (4.7). Then, using $n_K \geq 1$ and recalling that $\ell = \lceil n_K/2 \rceil + 1 \leq (n_K + 3)/2 \leq 2n_K$, we can bound (4.8) by

$$\frac{1}{\delta} \cdot \frac{4}{3} (2n_K)^{n_K/2} \left[\frac{2}{\epsilon} (1+\epsilon) \right]^{n_K/2+1}.$$

The error term is then bounded by

$$Z_{\mathfrak{m}}(\delta) \frac{1}{\pi} \left(\frac{d_{\chi}}{(2\pi)^{n_K}} \right)^{1/2} \frac{1+\delta}{1-\delta} (1+\delta^{-1})^{n_K} e^{\delta\epsilon} x^{\delta} (1+x^{-\delta/2}) \frac{1}{\delta} \cdot \frac{4}{3} (2n_K)^{n_K/2} \left[\frac{2}{\epsilon} (1+\epsilon) \right]^{n_K/2+1}$$

as desired. \square

We now sum over integral ideals in a given coset of the ray class group via Lemma 4.1.

Lemma 4.2. *Let $\mathfrak{m} = \mathfrak{f}_{L/K}$, let $H = \ker(F_{L/K})$, and let aH be a coset in $I(\mathfrak{m})/H$. Let \mathfrak{n} be an integral ideal coprime to \mathfrak{m} . Then*

$$\left| \sum_{\substack{\mathfrak{a} \in aH \\ \mathfrak{n} | \mathfrak{a}}} \phi \left(\frac{\log N(\mathfrak{a})}{\log x} \right) - \frac{1}{[L:K]} \frac{\varphi_K(\mathfrak{m})}{N(\mathfrak{m})} \frac{\kappa_K}{N(\mathfrak{n})} \cdot \log x \cdot F(-\log x) \right| \leq E(x),$$

where $E(x)$ is as in (4.3).

Proof. By character orthogonality applied to the group $I(\mathfrak{m})/H$, we have that

$$\sum_{\substack{\mathfrak{a} \in aH \\ \mathfrak{n} | \mathfrak{a}}} \phi \left(\frac{\log N(\mathfrak{a})}{\log x} \right) = \frac{1}{[L:K]} \sum_{\chi(H)=1} \bar{\chi}(aH) \sum_{\substack{\mathfrak{a} \\ \mathfrak{n} | \mathfrak{a}}} \chi(\mathfrak{a}) \phi \left(\frac{\log N(\mathfrak{a})}{\log x} \right).$$

Note that $\chi(\mathfrak{a}) = 0$ is defined if \mathfrak{a} and \mathfrak{m} are not coprime. Summing over each character using the previous lemma gives the desired result. \square

4.2. Bounding $V(z)$. We proceed similarly to the proof of Lemma 4.1. In particular, we bound $V(z)$ by a sum of test functions, and apply an inverse Laplace transform. Our main result is the following.

Lemma 4.3. *Let $0 < \omega < 1/2$ and let $\eta, \epsilon \in (0, 1/2)$. Set $z = x^{\omega}$. Set*

$$\begin{aligned} e^{c_{11}} &= \frac{2^{1/2}}{e^{1/2}\pi} \left(\frac{\eta+1}{\eta(1-\eta)} \right) e^{\epsilon\omega/2} \left[\frac{1}{\epsilon\omega} (1+\epsilon\omega)(1+e^{\epsilon}) \right]^{3/2} \\ e^{c_{12}} &= \frac{e^{1/2}}{\pi^{1/2}} \left(\frac{\eta+1}{\eta} \right) \left[\frac{1}{\epsilon\omega} (1+\epsilon\omega)(1+e^{\epsilon}) \right]^{1/2}. \end{aligned} \quad (4.9)$$

Denote by κ_K the residue of $\zeta_K(s)$ at $s = 1$. If

$$x \geq e^{\epsilon} \left(e^{c_{11}} e^{c_{12}n_K} n_K^{n_K/2} D_K^{1/2} \right)^{\frac{2}{(1-\eta)\omega}}, \quad (4.10)$$

then

$$V(z) \geq \frac{\kappa_K \omega}{2} \log x. \quad (4.11)$$

Proof. Choose z' such that

$$\frac{\log z}{\log z'} \geq 1 + \frac{\epsilon}{\log x}$$

This arises from the support condition $\text{supp } \phi \subset [\frac{1}{2} - \frac{\epsilon}{\log x}, 1 + \frac{\epsilon}{\log x}]$. Rearranging gives

$$\log z' \leq \frac{\log z}{1 + \frac{\epsilon}{\log x}}.$$

Since $(1 + \epsilon/\log x)^{-1} > 1 - \epsilon/\log x$, we can set

$$z' = z^{1-\epsilon/\log x} = ze^{-\epsilon\omega} = (xe^{-\epsilon})^\omega. \quad (4.12)$$

We have the inequality

$$V(z) := \sum_{\mathbf{N}(\mathbf{a}) \leq z} \frac{1}{\mathbf{N}(\mathbf{a})} \geq 1 + \sum_{\mathbf{a}} \frac{1}{\mathbf{N}(\mathbf{a})} \phi\left(\frac{\log \mathbf{N}(\mathbf{a})}{\log z'}\right).$$

By Laplace inversion, since $0 < \eta \leq 1/2$, we have that

$$\begin{aligned} \sum_{\mathbf{a}} \frac{1}{\mathbf{N}(\mathbf{a})} \phi\left(\frac{\log \mathbf{N}(\mathbf{a})}{\log z'}\right) &= \frac{\log z'}{2\pi i} \int_{\eta-i\infty}^{\eta+i\infty} \zeta_K(s+1) F(-s \log z') ds \\ &= \kappa_K F(0) \cdot \log z' + \frac{\log z'}{2\pi i} \int_{-1+\eta-i\infty}^{-1+\eta+i\infty} \zeta_K(s+1) F(-s \log z') ds. \end{aligned}$$

Using the definition of z' and Lemma 2.2(e), we can bound the contribution of the residue from below as

$$\begin{aligned} \kappa_K F(0) \cdot \log z' &= \kappa_K \omega (\log x - \epsilon) \left(\frac{1}{2} + \frac{\epsilon}{\log x} \right) \\ &\geq \frac{\kappa_K \omega}{2} \log x. \end{aligned}$$

As before, we break up the integral into two parts, the first with $|t| \leq M$ and the second with $|t| > M$. In both regions we use Lemma 2.1 to bound $\zeta_K(s+1)$. We use Lemma 2.2(g) to bound the integrand with $|t| \leq M$, and Lemma 2.2(f) for $|t| > M$. Applying these bounds gives

$$\begin{aligned} &\left| \int_{-1+\eta-i\infty}^{-1+\eta+i\infty} \zeta_K(s+1) F(-s \log z') ds \right| \quad (4.13) \\ &\leq \left(\frac{1+\eta}{1-\eta} \right) (1+\eta^{-1})^{n_K} \left(\frac{D_K}{(2\pi)^{n_K}} \right)^{1/2} \frac{2e^{\epsilon\omega/2} (z')^{(-1+\eta)/2}}{\log z'} \\ &\quad \times \left[\int_0^M \frac{|\eta+1+it|^{n_K/2}}{|\eta+it|} \left(\frac{2}{2-|\eta+it|\epsilon\omega/\ell} \right)^\ell dt + \left(\frac{\ell(1+e^\epsilon)}{\epsilon} \right)^\ell \int_M^\infty \frac{|\eta+1+it|^{n_K/2}}{|\eta+it|^{\ell+1}} dt \right]. \quad (4.14) \end{aligned}$$

To bound these integrals, we set $\ell = \lceil n_K/2 \rceil + 1$, so that $n_K/2 \leq \ell - 1$. We bound the first integral by

$$\begin{aligned} \int_0^M \frac{|\eta+1+it|^{n_K/2}}{|\eta+it|} \left(\frac{2}{2-|\eta+it|\epsilon\omega/\ell} \right)^\ell dt &\leq \frac{1}{\eta} \left(\frac{2}{2-(\eta+M)\epsilon\omega/\ell} \right)^\ell \int_0^M (\eta+1+t)^{\ell-1} dt \\ &\leq \frac{1}{\eta} \left(\frac{2}{2-(\eta+M)\epsilon\omega/\ell} \right)^\ell \frac{1}{\ell} (\eta+1+M)^\ell. \end{aligned}$$

We bound the second integral using the fact that $|\eta + 1 + it|^{n_K/2} \leq |\eta + 1 + it|^{\ell-1}$ and then integrating as in (4.6)

$$\begin{aligned} \int_M^\infty \frac{|\eta + 1 + it|^{n_K/2}}{|\eta + it|^{\ell+1}} dt &\leq \int_M^\infty \frac{|\eta + 1 + it|^{\ell-1}}{|\eta + it|^{\ell+1}} dt \\ &\leq \int_M^\infty \left| 1 + \frac{1}{\eta + it} \right|^{\ell-1} |\eta + it|^{-2} dt \\ &\leq \frac{1}{\ell} \left[(1 + M^{-1})^\ell - 1 \right]. \end{aligned}$$

So overall, our bound on the sum of the two integrals in (4.14) is

$$\frac{1}{\ell} \left[\frac{1}{\eta} \left(\frac{2(\eta + 1 + M)}{2 - (\eta + M)\epsilon\omega/\ell} \right)^\ell + \left(\frac{\ell(1 + e^\epsilon)}{\epsilon\omega} \right)^\ell \left((1 + M^{-1})^\ell - 1 \right) \right]$$

We want to choose M small enough so that

$$\frac{2(\eta + 1 + M)}{2 - (\eta + M)\epsilon\omega/\ell} < \frac{\ell(1 + e^\epsilon)}{\epsilon\omega} \quad (4.15)$$

and we can then bound the entire quantity (using $\eta < 1$) by

$$\frac{1}{\ell\eta} \left[\frac{\ell}{\epsilon\omega} (1 + M^{-1})(1 + e^\epsilon) \right]^\ell. \quad (4.16)$$

Setting $M = \frac{1}{\epsilon\omega}$ satisfies (4.15). Then, by recalling that $\ell = \lceil n_K/2 \rceil + 1 \leq 2n_K$ and using that $n_K \leq e^{n_K-1}$, we can bound (4.16) by

$$\frac{1}{\eta} n_K^{n_K/2} 2^{n_K/2} 2^{1/2} e^{n_K/2} e^{-1/2} \left[\frac{1}{\epsilon\omega} (1 + \epsilon\omega)(1 + e^\epsilon) \right]^\ell$$

So in all, our bound for the integral in (4.13) is

$$(z')^{(-1+\eta)/2} e^{c_{11}} e^{c_{12}n_K} n_K^{n_K/2} D_K^{1/2}$$

where

$$\begin{aligned} e^{c_{11}} &= \frac{2^{1/2}}{e^{1/2}\pi} \frac{\eta + 1}{\eta(1 - \eta)} e^{\epsilon\omega/2} \left[\frac{1}{\epsilon\omega} (1 + \epsilon\omega)(1 + e^\epsilon) \right]^{3/2} \\ e^{c_{12}} &= (1 + \eta^{-1})(2\pi)^{-1/2} 2^{1/2} e^{1/2} \left[\frac{1}{\epsilon\omega} (1 + \epsilon\omega)(1 + e^\epsilon) \right]^{1/2}. \end{aligned}$$

We need the error term to be less than 1, which is satisfied when

$$z' \geq \left(e^{c_{11}} e^{c_{12}n_K} n_K^{n_K/2} D_K^{1/2} \right)^{2/(1-\eta)}.$$

Recalling that $z' = (xe^{-\epsilon})^\omega$ completes the proof. \square

5. IMPLEMENTING THE SELBERG SIEVE

Let L/K be an abelian extension of number fields. In this section we prove an upper bound for $\pi_C(x, L/K)$ via the Selberg sieve. Our implementation closely follows the classical method of proof of the Brun–Titchmarsh theorem via the Selberg sieve (see [CM⁺06] for one such proof). We apply the analogue for number fields outlined in [Wei83]. Our main result is the following.

Lemma 5.1. *Let L/K be an abelian extension of number fields and C a conjugacy class (which will necessarily be a single element) of $\text{Gal}(L/K)$. Let $\pi_C(x, L/K)$ be as in (1.3), $E(x)$ be as in (4.3), and $0 < \omega, \eta, \epsilon, \gamma < 1/2$. If x satisfies the range condition (4.10), then*

$$\pi_C(x, L/K) \leq 2.52 \frac{n_K \sqrt{x}}{\log x} + \frac{2e^\epsilon x}{\omega[L:K] \log x} + E(x) \left((1 + \gamma^{-1})^{n_K} x^{\omega(1+\gamma)} \right)^2, \quad (5.1)$$

Proof. Let $aH := F_{L/K}^{-1}(C)$ and recall (2.2). We would then like to bound

$$\pi_C(x, L/K) = \pi_{aH}(x, L/K) = \sum_{\substack{\mathfrak{p} \text{ unramified} \\ \mathfrak{p} \in aH \\ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x}} 1.$$

To begin, we split the sum into two pieces as follows.

$$\pi_{aH}(x, L/K) \leq \sum_{\substack{\mathfrak{p} \in aH \\ N(\mathfrak{p}) \leq x}} 1 = \sum_{\substack{\mathfrak{p} \in aH \\ N(\mathfrak{p}) \leq \sqrt{x}}} 1 + \sum_{\substack{\mathfrak{p} \in aH \\ \sqrt{x} < N(\mathfrak{p}) \leq x}} 1. \quad (5.2)$$

Since at most n_K prime ideals \mathfrak{p} of K lie over a given rational prime p , we can use the universal bound $\sum_{p \leq x} 1 \leq 1.26 \frac{x}{\log x}$ from Corollary 1 of [RS62] to bound the first sum in (5.2) by

$$\sum_{\substack{\mathfrak{p} \in aH \\ N(\mathfrak{p}) \leq \sqrt{x}}} 1 \leq \sum_{p \leq \sqrt{x}} \sum_{\mathfrak{p} | (p)} 1 \leq n_K \sum_{p \leq \sqrt{x}} 1 \leq 2.52 \frac{n_K \sqrt{x}}{\log x}. \quad (5.3)$$

We bound the second term via the Selberg sieve. For an integral ideal \mathfrak{a} , we define the quantity $\mathcal{P}^-(\mathfrak{a})$ to be the least norm of a prime ideal factor of \mathfrak{a} . Let $0 < z < \sqrt{x}$. Let S_z be the set of those integral ideals satisfying $\mathcal{P}^-(\mathfrak{a}) > z$; that is, integral ideals with no prime ideal factor having norm $\leq z$. It follows that

$$\sum_{\substack{\mathfrak{p} \in aH \\ \sqrt{x} < N(\mathfrak{p}) \leq x}} 1 \leq \sum_{\substack{\mathfrak{a} \in aH \cap S_z \\ \sqrt{x} < N(\mathfrak{a}) \leq x}} 1.$$

For the test function ϕ defined in Lemma 2.2, we have that $\phi(t) = 1$ for $t \in [\frac{1}{2}, 1]$ and ϕ is nonnegative, so

$$\sum_{\substack{\mathfrak{a} \in aH \cap S_z \\ \sqrt{x} < N(\mathfrak{p}) \leq x}} 1 \leq \sum_{\mathfrak{a} \in aH \cap S_z} \phi\left(\frac{\log N(\mathfrak{a})}{\log x}\right).$$

Now, consider any real-valued function λ on integral ideals of \mathcal{O}_K satisfying

$$(a) \quad \lambda(\mathcal{O}_K) = 1;$$

- (b) $\lambda(\mathfrak{b}) = 0$ unless \mathfrak{b} is squarefree, coprime to \mathfrak{m} and $N(\mathfrak{b}) \leq z$;
- (c) $|\lambda(\mathfrak{b})| \leq 1$ for all \mathfrak{b} .

We will eventually specify the choice of such a function.

Denote by $[\mathfrak{b}_1, \mathfrak{b}_2]$ and $(\mathfrak{b}_1, \mathfrak{b}_2)$ the least common multiple and greatest common divisor of two integral ideals $\mathfrak{b}_1, \mathfrak{b}_2$. Also denote by μ_K the Möbius function on integral ideals associated to the number field K , which is defined for an integral ideal \mathfrak{a} of \mathcal{O}_K as

$$\mu_K(\mathfrak{a}) := \begin{cases} (-1)^{\omega(\mathfrak{a})} & \mathfrak{a} \text{ is squarefree,} \\ 0 & \mathfrak{a} \text{ is not squarefree.} \end{cases}$$

Note that if $\mathfrak{a} \in S_z$, then $\mathfrak{b} \mid \mathfrak{a}$ implies $\mathfrak{b} = \mathcal{O}_K$ or $N(\mathfrak{b}) > z$, which by conditions (a) and (b) implies that $\mathfrak{b} = \mathcal{O}_K$ or $\lambda(\mathfrak{b}) = 0$. Hence, we have

$$\begin{aligned} \sum_{\mathfrak{a} \in aH \cap S_z} \phi\left(\frac{\log N(\mathfrak{a})}{\log x}\right) &\leq \sum_{\mathfrak{a} \in aH} \phi\left(\frac{\log N(\mathfrak{a})}{\log x}\right) \left(\sum_{\mathfrak{b} \mid \mathfrak{a}} \lambda(\mathfrak{b})\right)^2 \\ &= \sum_{\mathfrak{b}_1, \mathfrak{b}_2} \lambda(\mathfrak{b}_1)\lambda(\mathfrak{b}_2) \sum_{\substack{\mathfrak{a} \in aH \\ [\mathfrak{b}_1, \mathfrak{b}_2] \mid \mathfrak{a}}} \phi\left(\frac{\log N(\mathfrak{a})}{\log x}\right). \end{aligned} \quad (5.4)$$

Now by Lemma 4.2, we have for $\mathfrak{n}, \mathfrak{m}$ coprime that

$$\sum_{\substack{\mathfrak{a} \in aH \\ \mathfrak{n} \mid \mathfrak{a}}} \phi\left(\frac{\log N(\mathfrak{a})}{\log x}\right) \leq \frac{1}{[L : K]} \frac{\varphi_K(\mathfrak{m})}{N(\mathfrak{m})} \frac{\kappa_K}{N(\mathfrak{n})} (\log x) \cdot F(-\log x) + |E(x)|,$$

If $[\mathfrak{b}_1, \mathfrak{b}_2]$ is not coprime to \mathfrak{m} , then $\lambda(\mathfrak{b}_1)\lambda(\mathfrak{b}_2) = 0$ by condition (b), so (5.4) is bounded by

$$\sum_{\mathfrak{b}_1, \mathfrak{b}_2} \lambda(\mathfrak{b}_1)\lambda(\mathfrak{b}_2) \left(\frac{1}{[L : K]} \frac{\varphi_K(\mathfrak{m})}{N(\mathfrak{m})} \frac{\kappa_K}{N([\mathfrak{b}_1, \mathfrak{b}_2])} (\log x) \cdot F(-\log x) + |E(x)| \right).$$

Since $\mathfrak{b}_1\mathfrak{b}_2 = (\mathfrak{b}_1, \mathfrak{b}_2)[\mathfrak{b}_1, \mathfrak{b}_2]$, we can rewrite this as

$$\sum_{\mathfrak{b}_1, \mathfrak{b}_2} \lambda(\mathfrak{b}_1)\lambda(\mathfrak{b}_2) \left(\frac{1}{[L : K]} \frac{\varphi_K(\mathfrak{m})}{N(\mathfrak{m})} \frac{\kappa_K N((\mathfrak{b}_1, \mathfrak{b}_2))}{N(\mathfrak{b}_1)N(\mathfrak{b}_2)} (\log x) \cdot F(-\log x) + E(x) \right).$$

Applying the identity $N(\mathfrak{a}) = \sum_{\mathfrak{b} \mid \mathfrak{a}} \varphi_K(\mathfrak{b})$ and $|\lambda(\mathfrak{b})| \leq 1$ yields

$$\begin{aligned} &\frac{\kappa_K (\log x) F(-\log x)}{[L : K]} \frac{\varphi_K(\mathfrak{m})}{N(\mathfrak{m})} \sum_{\mathfrak{b}_1, \mathfrak{b}_2} \frac{\lambda(\mathfrak{b}_1)\lambda(\mathfrak{b}_2)}{N(\mathfrak{b}_1)N(\mathfrak{b}_2)} \sum_{\mathfrak{a} \mid \mathfrak{b}_1, \mathfrak{a} \mid \mathfrak{b}_2} \varphi_K(\mathfrak{a}) + \sum_{\mathfrak{b}_1, \mathfrak{b}_2} \left| \lambda(\mathfrak{b}_1)\lambda(\mathfrak{b}_2) \right| |E(x)| \\ &\leq \frac{\kappa_K (\log x) F(-\log x)}{[L : K]} \frac{\varphi_K(\mathfrak{m})}{N(\mathfrak{m})} \sum_{\mathfrak{a}} \varphi_K(\mathfrak{a}) \left(\sum_{\mathfrak{a} \mid \mathfrak{b}} \frac{\lambda(\mathfrak{b})}{N(\mathfrak{b})} \right)^2 + E(x) \left(\sum_{\substack{\mathfrak{b} \\ N(\mathfrak{b}) \leq z}} 1 \right)^2. \end{aligned} \quad (5.5)$$

By considering the Möbius inversion pair

$$\xi(\mathfrak{a}) = \sum_{\mathfrak{b} \mid \mathfrak{a}} \frac{\lambda(\mathfrak{b})}{N(\mathfrak{b})}, \quad \frac{\lambda(\mathfrak{a})}{N(\mathfrak{a})} = \sum_{\mathfrak{b}} \mu_K(\mathfrak{b}) \xi(\mathfrak{a}\mathfrak{b}),$$

we seek to choose λ (equivalently, to choose ξ) such that the quadratic form $\sum_{\mathbf{a}} \varphi_K(\mathbf{a}) \xi(\mathbf{a})^2$ is minimized. Using the same choice as in [Wei83, p. 73] and recalling the definition of $V(z)$ in (4.2) yields the following bound from [Wei83, Lemma 3.6, eq. (iv)], which states that

$$\frac{\varphi_K(\mathbf{m})}{N(\mathbf{m})} \sum_{\mathbf{a}} \varphi_K(\mathbf{a}) \left(\sum_{\mathbf{a}|\mathbf{b}} \frac{\lambda(\mathbf{b})}{N(\mathbf{b})} \right)^2 \leq \frac{1}{V(z)}.$$

Substituting this into equation (5.5) yields the bound

$$\frac{\kappa_K(\log x) F(-\log x)}{[L : K] V(z)} + E(x) \left(\sum_{N(\mathbf{b}) \leq z} 1 \right)^2.$$

By Lemma 2.2(e) the above is bounded by

$$\frac{\kappa_K e^\epsilon x}{[L : K] V(z)} + E(x) \left(\sum_{N(\mathbf{b}) \leq z} 1 \right)^2.$$

Now, by the lower bound for $V(z)$ from Lemma 4.3 (in the appropriate range for x specified in that lemma, with $z = x^\omega$), the above is bounded by

$$\frac{2e^\epsilon x}{\omega [L : K] \log x} + E(x) \left(\sum_{N(\mathbf{b}) \leq z} 1 \right)^2.$$

Applying Lemma 2.3 and substituting $z = x^\omega$ yields a bound (for $0 < \gamma \leq 1$) of

$$\sum_{\substack{\mathbf{p} \in aH \\ \sqrt{x} < N(\mathbf{p}) \leq x}} 1 \leq \frac{2e^\epsilon x}{\omega [L : K] \log x} + E(x) \left((1 + \gamma^{-1})^{n_K} x^{\omega(1+\gamma)} \right)^2. \quad (5.6)$$

Combining (5.3) and (5.6) into (5.2) gives the desired result. \square

6. BRUN–TITCHMARSH FOR ABELIAN EXTENSIONS

In this section we prove Lemma 3.1. We begin by bounding the error terms in Lemma 5.1. We bound the first term in (5.1) as

$$2.52 \frac{n_K \sqrt{x}}{\log x} \leq \frac{x}{100 [L : K] \log x} \quad (6.1)$$

in the range

$$x \geq (252 n_K [L : K])^2. \quad (6.2)$$

Next we consider the last term in (5.1). Let $E(x)$ be as in (4.3). Then we define

$$C(\delta, \epsilon, \gamma) = E(x) (1 + \gamma^{-1})^{2n_K} [L : K] x^{-\delta}, \quad (6.3)$$

which does not depend on x . We want to choose x large enough so that

$$E(x) (1 + \gamma^{-1})^{2n_K} x^{2\omega(1+\gamma)} \leq \frac{x}{[L : K] \log x},$$

which is equivalent to

$$\frac{x^{1-\delta-2\omega(1+\gamma)}}{\log x} \geq C(\delta, \epsilon, \gamma). \quad (6.4)$$

By Lemma 2.4, we find that if

$$x \geq \left(\frac{C(\delta, \epsilon, \gamma)}{1 - \delta - 2\omega(1 + \gamma)} \right)^\nu, \quad (6.5)$$

where

$$\nu = \frac{1}{1 - \delta - 2\omega(1 + \gamma)} \left(1 + \left(\frac{2}{\log(C(\delta, \epsilon, \gamma)/(1 - \delta - 2\omega(1 + \gamma)))} \right)^{1/2} \right), \quad (6.6)$$

then (6.4) is satisfied. Combining the bounds in this section with Lemma 4.3 yields our first version of the Brun-Titchmarsh theorem for abelian extensions.

Lemma 6.1. *Let L/K be an abelian extension of number fields, let C be a conjugacy class (which will necessarily be a single element) of $\text{Gal}(L/K)$, and let $\pi_C(L/K)$ be the prime-counting function given in (1.3). Let $0 < \epsilon, \delta, \gamma, \eta, \omega < 1/2$ be such that $1 - \delta - 2\omega(1 + \gamma) > 0$, and let c_{11}, c_{12} be as in (4.9), $C(\delta, \epsilon, \gamma)$ be as in (6.3), and ν be as in (6.6). If*

$$x \geq \max \left(e^\epsilon \left(e^{c_{11}} e^{c_{12} n_K} n_K^{n_K/2} D_K^{1/2} \right)^{\frac{2}{(1-\eta)\omega}}, (252 n_K [L : K])^2, \left(\frac{C(\delta, \epsilon, \gamma)}{1 - \delta - 2\omega(1 + \gamma)} \right)^\nu \right) \quad (6.7)$$

then

$$\pi_C(x, L/K) \leq \left(1.01 + \frac{2e^\epsilon}{\omega} \right) \frac{x}{[L : K] \log x}. \quad (6.8)$$

We state the above version of the Brun-Titchmarsh theorem as it allows us flexibility in choosing parameters when the field extension L/K is known, as in Section 7. For L/K a general abelian extension of number fields, we derive an explicit form of Lemma 6.1 by fixing parameters. Note that different choices of parameters may improve the dependence of the range on certain field constants (such as n_K, D_K, \mathcal{Q}) at the expense of others.

Proof of Lemma 3.1. Let $\delta = 1/10$, $\eta = 1/21$, $\epsilon = \omega = 1/4$, and $\gamma = 1/5$. We wish to obtain a range for x in terms of n_K, D_K , and \mathcal{Q} via Lemma 6.1. To do so, we use Lemma 2.5 with the parameter $\epsilon = 1$ to bound $[L : K]$ and Lemma 2.7 with the parameters $M = 400$ and $b = (2 \log(1 + M^{-\delta}))^{-1}$ to bound $Z_m(\delta)$. Doing so gives

$$C(\delta, \epsilon, \gamma) \leq e^{7.36} e^{22.85n} (D_K \mathcal{Q})^2 n^{n/2}. \quad (6.9)$$

Applying these bounds to (6.6) gives $\nu \leq 4.189$. Now, combining the bounds given in Lemma 6.1 and substituting our parameters gives the desired result. \square

7. UPPER BOUNDS FOR THE LANG-TROTTER CONJECTURE

In this section we apply our Brun-Titchmarsh results to study coefficients of modular forms. Let $f(z) \in \mathcal{S}_{k_f}^{\text{new}}(\Gamma_0(N_f))$ be a non-CM cusp form of even weight $k_f \geq 2$, level N_f , trivial nebentypus, and integral coefficients $a_f(n)$ which is an eigenform for all Hecke operators and Atkin-Lehner operators. Let

$$\pi_f(x, a) := \#\{p \leq x \text{ prime, } p \nmid N_f, \text{ and } a_f(p) = a\}.$$

We use a sieving procedure to bound $\pi_f(x, a)$ by a sum of auxiliary prime-counting functions $\pi_f(x, a, \ell)$ (for a suitably chosen collection of primes ℓ) which count coefficients $a_f(p)$ congruent to $a \pmod{\ell}$, with some additional conditions. The projection onto \mathbb{F}_ℓ of the ℓ -adic Galois representation $\rho_{f, \ell}$ attached to f allows us to express these conditions as a condition on the image of Frob_p under the residual representation. This allows the count of rational primes p with given $a_f(p)$ to be compared with the count of prime ideals with prescribed Frobenius class in a certain abelian extension of number fields. This extension is a subextension of the fixed field of $\ker \rho_{f, \ell}$ in $\overline{\mathbb{Q}}$, through which $\rho_{f, \ell}$ factors. This enables us to compute an explicit upper bound for $\pi_f(x, a)$ using Lemma 6.1.

7.1. Sieving $\pi_f(x, a)$ by primes. For a prime number p , define

$$\omega_p = (a_f(p)^2 - 4p^{k_f-1})^{1/2}. \quad (7.1)$$

We know from Deligne's proof of the Weil conjectures that $|a_f(p)| \leq 2p^{(k_f-1)/2}$ for all p , so $\mathbb{Q}(\omega_p)$ is an imaginary quadratic extension of \mathbb{Q} . For an odd prime ℓ , set

$$\pi_f(x, a; \ell) = \#\left\{p \leq x \text{ prime, } p \nmid N_f, a_f(p) \equiv a \pmod{\ell}, \left(\frac{a^2 - 4p^{k_f-1}}{\ell}\right) = +1\right\}.$$

Here, $\left(\frac{\cdot}{\ell}\right)$ is the Legendre symbol; in other words the latter condition says ℓ splits in $\mathbb{Q}(\omega_p)$. Our sieve result is the following lemma adapted from [Wan90, Lemma 4.1].

Lemma 7.1. *Let $x, t > 0$ be integers, and let $\ell_1 < \ell_2 < \dots < \ell_t$ be t odd primes, each less than x . Assume furthermore that $\gcd(\ell_j - 1, k_f - 1) = 1$ for all $j = 1, \dots, t$. Then*

$$\pi_f(x, a) \leq \sum_{j=1}^t \pi_f(x, a; \ell_j) + \sqrt{2} \cdot \frac{x}{2^{t/2}} + \sqrt{2} \cdot 2^{t/2} \ell_t^t + 2^t + \frac{70}{2^t}. \quad (7.2)$$

Proof. Let $\ell_1 < \ell_2 < \dots < \ell_t$ be as above, and let $M_t(x)$ be the number of primes $p \leq x$ such that $\left(\frac{a^2 - 4p^{k_f-1}}{\ell_j}\right) \neq +1$ for all $j = 1, \dots, t$, that is, the number of primes $p \leq x$ that are not counted in any of the $\pi_f(x, a; \ell_j)$. Then

$$\pi_f(x, a) \leq \sum_{j=1}^t \pi_f(x, a, \ell_j) + M_t(x). \quad (7.3)$$

To estimate $M_t(x)$, we introduce a weight function $w_t(p)$ on the set of primes. Given a prime p , suppose that $\left(\frac{a^2 - 4p^{k_f-1}}{\ell}\right) = +1, 0, -1$ for, respectively, $t_1(p), t_2(p), t_3(p)$ of the primes ℓ_j . So $t_1 + t_2 + t_3 = t$. Define

$$w_t(p) = \frac{1}{2^t} \prod_{j=1}^t \left(1 - \left(\frac{a^2 - 4p^{k_f-1}}{\ell_j}\right)\right) = \begin{cases} 0 & \text{if } t_1(p) \neq 0, \\ 2^{-t_2(p)} & \text{if } t_1(p) = 0, \end{cases}$$

and let

$$W_t(x) = \sum_{p \leq x} w_t(p).$$

Then

$$\begin{aligned} W_t(x) &\leq \frac{1}{2^t} \sum_{n \leq x} \prod_{j=1}^t \left(1 - \left(\frac{a^2 - 4n^{k_f-1}}{\ell_j} \right) \right) \\ &= \sum_{n \leq x} \left(\frac{1}{2} \right)^t + \max_{\substack{d \geq 2 \\ d|L_t}} \left| \sum_{n \leq x} \left(\frac{a^2 - 4n^{k_f-1}}{d} \right) \right|, \end{aligned}$$

where $L_j = \ell_1 \cdots \ell_j$ for $j = 1, \dots, t$, so $L_t \leq \ell_t^t$. The last sum is a character sum mod d since we assume that $\gcd(\ell_j - 1, k_f - 1) = 1$ for all j . We trivially bound this character sum above by $d \leq L_t$. Thus,

$$W_t(x) \leq \frac{x}{2^t} + \ell_t^t.$$

Let $M'_t(x)$ be the number of primes $p \leq x$ such that $t_2(p) \geq t/2$ (that is, $\left(\frac{a^2 - 4p^{k_f-1}}{\ell_j} \right) = 0$). So

$$M_t(x) - M'_t(x) \leq 2^{\lceil t/2 \rceil} W_t(x) \leq \sqrt{2} \cdot 2^{t/2} W_t(x).$$

Arguing via the Chinese remainder theorem, appealing again to our assumption that $\gcd(\ell_i - 1, k_f - 1) = 1$, we have that

$$M'_t(x) \leq \binom{t}{\lceil t/2 \rceil} \left(\frac{x}{\ell_1 \cdots \ell_{\lceil t/2 \rceil}} + 1 \right) \leq 2^t \frac{x}{\ell_1 \cdots \ell_{\lceil t/2 \rceil}} + 2^t.$$

Therefore

$$M_t(x) \leq \sqrt{2} \cdot \frac{x}{2^{t/2}} + \sqrt{2} \cdot 2^{t/2} \ell_t^t + 2^t \frac{x}{L_{\lceil t/2 \rceil}} + 2^t. \quad (7.4)$$

Since $\ell_j \geq 2^4$ except possibly for the first 5 odd primes, we have that

$$L_{\lceil t/2 \rceil} \geq \frac{3 \cdot 5 \cdot 7 \cdot 11 \cdot 13}{16^5} \cdot \prod_{i=1}^{\lceil t/2 \rceil} 16 \geq 70^{-1} \cdot 4^t,$$

and inserting (7.4) into (7.3) gives the lemma. \square

For our application, we state the following special case of Lemma 7.1.

Corollary 7.2. *Let $r, x > 1$, let $t = \lceil (2r/\log 2) \log \log x \rceil$, and let $\ell_1 < \ell_2 < \cdots < \ell_t$ be t odd primes, each less than $\exp(\frac{\log x}{2t})$. Assume furthermore that $\gcd(\ell_j - 1, k_f - 1) = 1$ for all $j = 1, \dots, t$. Then*

$$\begin{aligned} \pi_f(x, a) &\leq \left(\frac{2r}{\log 2} \log \log x + 1 \right) \max_{1 \leq t \leq j} \pi_f(x, a; \ell_j) \\ &\quad + \frac{x\sqrt{2}}{(\log x)^r} + \frac{2x^{1/2}}{(\log x)^r} + 2(\log x)^{2r} + 35. \end{aligned} \quad (7.5)$$

Proof. Observe that we have

$$\frac{2r}{\log 2} \log \log x \leq t < \frac{2r}{\log 2} \log \log x + 1$$

with this choice of t , and use this to bound all terms in (7.2) from above. \square

7.2. Reduction to a Chebotarev problem. Let ℓ be any odd prime, and let \mathbb{F}_ℓ be the field of ℓ elements. For any prime p , let Frob_p be the Frobenius automorphism of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at p . By a theorem of Deligne, one associates to each newform $f \in \mathcal{S}_{k_f}^{\text{new}}(\Gamma_0(N_f))$ an ℓ -adic representation, and, by projection onto \mathbb{F}_ℓ , a representation

$$\rho_{f,\ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_\ell),$$

which is unramified outside $N_f\ell$, and such that for all primes $p \nmid N_f\ell$, we have that $\text{tr}(\rho_{f,\ell}(\text{Frob}_p)) \equiv a_f(p) \pmod{\ell}$ and $\det(\rho_{f,\ell}(\text{Frob}_p)) \equiv 4p^{k_f-1} \pmod{\ell}$.

Let $L = L_\ell$ be the subfield of $\overline{\mathbb{Q}}$ fixed by $\ker \rho_{f,\ell}$. It is known that there exists ℓ_0 depending on f such that, if $\ell > \ell_0$, then L/\mathbb{Q} is a Galois extension, unramified outside of $N_f\ell$, whose Galois group is $G = \{g \in \text{GL}_2(\mathbb{F}_\ell) \mid \det(g) \in (\mathbb{F}_\ell^\times)^{k_f-1}\}$. Hence, if $\gcd(\ell-1, k_f-1) = 1$, then $G = \text{GL}_2(\mathbb{F}_\ell)$; that is, the representation $\rho_{f,\ell}$ is surjective.

From now on we let $\ell > \ell_0$ be a prime number with $\gcd(\ell-1, k_f-1) = 1$, and let

$$C = \{A \in G \mid \text{tr}(A) \equiv a \pmod{\ell} \text{ and } \text{tr}(A)^2 - 4\det(A) \in \mathbb{F}_\ell \text{ is a nonzero square}\}.$$

The latter condition is equivalent to saying that the matrix A has distinct eigenvalues in \mathbb{F}_ℓ . The set C is stable under conjugation in G , and can be expressed as

$$C = \bigcup_{\gamma \in \Gamma} C_G(\gamma)$$

where

$$\Gamma = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in G \mid \alpha \neq \beta, \alpha + \beta \equiv a \pmod{\ell} \right\},$$

and $C_G(\gamma)$ denotes the conjugacy class in G that contains γ . Let B denote the Borel subgroup of upper triangular matrices in G , and let L^B be the subfield of L fixed by B . Let H be the subgroup of B consisting of matrices whose eigenvalues are both equal, and let L^H be the subfield of L fixed by H . Let U be the subgroup of unipotent elements in B , and let L^U be the subfield of L fixed by U . We have

$$\{1\} \subset U \subset H \subset B \subset G = \text{GL}_2(\mathbb{F}_\ell).$$

Note that U and H are normal subgroups of B and that B/U , B/H are abelian. We have the tower of field extensions

$$\mathbb{Q} \subset L^B \subset L^H \subset L^U \subset L,$$

with L^U/L^B and L^H/L^B both abelian extensions. Finally, let C' be the image of $C \cap B$ in B/U and let C'' be the image of $C \cap B$ in B/H .

Before stating the reduction to counting prime ideals in conjugacy classes of Galois groups, we collect some basic facts about the cardinality of these groups and conjugacy classes.

Proposition 7.3. *We have $|C'| \leq \ell$,*

$$\frac{|C'|}{|B/U|} \leq \frac{1}{\ell-1} \quad \text{and} \quad \frac{|C''|}{|B/H|} = \frac{1}{\ell-1},$$

and $[L^B : \mathbb{Q}] = \ell + 1$, $[L^H : L^B] = \ell - 1$, and $[L^U : L^H] = \ell$.

Proof. By [Zyw15, Proof of Lemma 4.4], we have $|G| = (\ell - 1)^2(\ell + 1)\ell$, $|B| = (\ell - 1)^2\ell$, $|H| = (\ell - 1)\ell$, $|U| = \ell - 1$, $|C'| \leq \ell$, and $|C''| = 1$. \square

We now compare $\pi_f(x, a; \ell)$ to a prime-counting function of the form $\pi_C(x, L/K)$. Namely, for all $a \in \mathbb{Z}$, we will bound $\pi_f(x, a; \ell)$ in terms of $\pi_{C'}(x, L^U/L^B)$. However, when $a \equiv 0 \pmod{\ell}$, the conjugacy class C consists of matrices of zero trace over \mathbb{F}_ℓ , which allows us to work with the subextension L^H/L^B and its corresponding conjugacy class C'' . In view of this we state two versions of the reduction step, one applicable to all $a \in \mathbb{Z}$ and another specialized to the case $a \equiv 0 \pmod{\ell}$.

For a given modular form, we may also know additional congruence relations which its Fourier coefficients must satisfy. For instance, say we know that if $a_f(p) = a$, then p lies in some fixed set S of residue classes modulo $q \geq 1$. This condition imposes further conditions on the Artin symbol; via our reduction, it translates to counting primes in a compositum with a q -cyclotomic extension (that is, $L^U(\zeta_q)/L^B$ or $L^H(\zeta_q)/L^B$).

For L/K a Galois extension of number fields with Galois group G , and $C \subseteq G$ a conjugacy class, we set

$$\tilde{\pi}_C(x, L/K) := \sum_{\substack{m \geq 1 \\ \mathbb{N}_{K/\mathbb{Q}}(\mathfrak{p})^m \leq x \\ \text{Frob}_{\mathfrak{p}}^m = C}} \frac{1}{m},$$

a modified version of $\pi_C(x, L/K)$. Then it is clear that $\pi_C(x, L/K) \leq \tilde{\pi}_C(x, L/K)$. See [Zyw15, Section 2.3] for elegant functorial properties enjoyed by the function $\tilde{\pi}_C$.

Lemma 7.4. *Let f and ℓ be as above, let $\mathbb{Q} \subset L^B \subset L^H \subset L^U \subset L$ be constructed as above, and let a be an integer. Let $q \geq 1$ be an integer with $\gcd(q, N_f \ell) = 1$, let $S \subseteq (\mathbb{Z}/q\mathbb{Z})^\times$ be a set of residue classes modulo q , and suppose we have the following: for a prime number p , if $a_f(p) = a$, then $p \in S$.*

(a) *We have*

$$\pi_f(x, a; \ell) \leq \tilde{\pi}_{C' \times S}(x, L^U(\zeta_q)/L^B) + 1. \quad (7.6)$$

(b) *If $a \equiv 0 \pmod{\ell}$, we have*

$$\pi_f(x, 0; \ell) \leq \tilde{\pi}_{C'' \times S}(x, L^H(\zeta_q)/L^B) + 1. \quad (7.7)$$

Note that if $q = 1$, then $\pi_f(x, a; \ell) \leq \tilde{\pi}_{C'}(x, L^U/L^B)$ and $\pi_f(x, 0; \ell) \leq \tilde{\pi}_{C''}(x, L^H/L^B)$.

Proof. From the condition $\gcd(q, N_f \ell) = 1$, the fields L and $\mathbb{Q}(\zeta_q)$ are linearly disjoint, so $\text{Gal}(L(\zeta_q)/\mathbb{Q}) = \text{Gal}(L/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) = G \times (\mathbb{Z}/q\mathbb{Z})^\times$. We claim that

$$\pi_f(x, a; \ell) \leq \pi_{C \times S}(x, L(\zeta_q)/\mathbb{Q}) + 1.$$

Indeed, let $p \leq x$ be a prime such that $p \nmid N_f \ell$, $a_f(p) = a$ and $a^2 - 4p^{k_f-1}$ is a square in \mathbb{F}_ℓ^\times . The representation $\rho_{f,\ell}$ is unramified at p and we have $\text{tr}(\rho_{f,\ell}(\text{Frob}_p)) \equiv a_f(p) = a \pmod{\ell}$ and $\det(\rho_{f,\ell}(\text{Frob}_p)) \equiv p^{k_f-1} \pmod{\ell}$. Thus $\text{tr}(\rho_{f,\ell}(\text{Frob}_p))^2 - 4\det(\rho_{f,\ell}(\text{Frob}_p)) \in \mathbb{F}_\ell$ is a square. We have thus shown that $\rho_{f,\ell}(\text{Frob}_p) \subseteq C$. By hypothesis, we also know that if $a_f(p) = a$, then $p \in S \pmod{q}$. Adding an extra 1 to account for the excluded prime $p = \ell$, this implies that

$$\begin{aligned} \pi_f(x, a; \ell) &\leq \pi_{C \times S}(x, L(\zeta_q)/\mathbb{Q}) + 1 \\ &\leq \tilde{\pi}_{C \times S}(x, L(\zeta_q)/\mathbb{Q}) + 1. \end{aligned}$$

By [Zyw15, Lemma 2.6(i)], and since L^B is the fixed field in $L(\zeta_q)$ of the subgroup $B \times (\mathbb{Z}/q\mathbb{Z})^\times$, we have that

$$\pi_f(x, a; \ell) \leq \tilde{\pi}_{(C \cap B) \times S}(x, L(\zeta_q)/L^B) + 1.$$

By [Zyw15, Lemma 2.6(ii)], and since $U \times \{1\}$ is a normal subgroup of $B \times (\mathbb{Z}/q\mathbb{Z})^\times$ with $(U \times \{1\}) \cdot ((C \cap B) \times (\mathbb{Z}/q\mathbb{Z})^\times) \subseteq ((C \cap B) \times (\mathbb{Z}/q\mathbb{Z})^\times)$, we also have that

$$\pi_f(x, a; \ell) \leq \tilde{\pi}_{C' \times S}(x, L^U(\zeta_q)/L^B) + 1,$$

which is part (a). If $a \equiv 0 \pmod{\ell}$, then C consists of trace zero matrices, and so we repeat the last line with the subgroup $H \times \{1\}$ in the place of the subgroup $U \times \{1\}$. \square

Now, for a Galois extension of number fields L/K , let $\mathcal{P}(L/K)$ denote the set of rational primes p that are divisible by some prime ideal \mathfrak{p} of K that ramifies in L . Define

$$M(L/K) := 2[L : K]D_K^{1/[K:\mathbb{Q}]} \cdot \prod_{p \in \mathcal{P}(L/K)} p. \quad (7.8)$$

The next lemma transitions from the modified $\tilde{\pi}_C$ to π_C , with explicit remainder term.

Lemma 7.5. *Let L/K be a normal extension of number fields with Galois group G and let $C \subseteq G$ be a union of conjugacy classes. If $x \geq 4$, then*

$$\tilde{\pi}_C(x, L/K) \leq \pi_C(x, L/K) + 3.15546n_K \frac{x^{1/2}}{\log x} + n_K \log M(L/K).$$

Proof. The lemma follows from inspection of the proof of [Zyw15, Lemma 2.7], using the identity $\sum_{m=2}^{\infty} m^{-2} = \frac{1}{6}\pi^2 - 1$ and the universal bound $\pi(x) < 1.25506 \frac{x}{\log x}$. \square

7.3. Bounding $M(L/K)$. The combination of Corollary 7.2, Lemma 7.4, and Lemma 7.5 allows us to express $\pi_f(x, a)$ in terms of $\pi_{C' \times S}(x, L^U(\zeta_q)/L^B)$ or $\pi_{C' \times S}(x, L^H(\zeta_q)/L^B)$ if $a = 0$. Before proceeding, we want to establish bounds for the size of the field constants $M(L^U(\zeta_q)/L^B)$ and $M(L^H(\zeta_q)/L^B)$ in terms of the quantities q , N_f , and ℓ . First we need the following result due to [Ser81].

Lemma 7.6. *We have*

$$D_{L^B}^{1/[L^B:\mathbb{Q}]} \leq \text{rad}(N_f)\ell \cdot (\ell + 1)^{\omega(N_f)+1}. \quad (7.9)$$

Proof. An application of Proposition 6 of [Ser81] gives

$$\log D_{L^B} \leq \ell \sum_{p \in \mathcal{P}(L^B/\mathbb{Q})} \log p + |\mathcal{P}(L^B/\mathbb{Q})|(\ell + 1) \log(\ell + 1). \quad (7.10)$$

Since $p \in \mathcal{P}(L^B/\mathbb{Q})$ implies $p \mid N_f\ell$, we may bound the above sum by $\log(\text{rad}(N_f)\ell)$. Similarly, we may bound $|\mathcal{P}(L^B/\mathbb{Q})|$ by $\omega(N_f) + 1$, proving the lemma. \square

We use this result to prove the next lemma.

Lemma 7.7. *Suppose that $\ell > \ell_0$ with $\gcd(\ell - 1, k_f - 1) = 1$, and $\mathbb{Q} \subset L^B \subset L^H \subset L^U \subset L$ are constructed as above, and $q \geq 1$ is an integer with $\gcd(q, N_f\ell) = 1$. Let*

$\omega(n)$ denote the number of distinct prime factors dividing a positive integer n , and let $\text{rad}(n)$ denote their product, with $\text{rad}(1) = 1$. We have that

$$M(L^U(\zeta_q)/L^B) \leq 2(\ell + 1)^{\omega(N_f)+4} \text{rad}(N_f)^2 \varphi(q) \text{rad}(q) \quad (7.11)$$

and

$$M(L^H(\zeta_q)/L^B) \leq 2(\ell + 1)^{\omega(N_f)+3} \text{rad}(N_f)^2 \varphi(q) \text{rad}(q). \quad (7.12)$$

Proof. Using the previous lemma with $[L^U(\zeta_q) : L^B] = \varphi(q)(\ell - 1)\ell$ gives

$$\begin{aligned} M(L^U(\zeta_q)/L^B) &= 2[L^U(\zeta_q) : L^B] D_{L^B}^{1/[L^B:\mathbb{Q}]} \cdot \prod_{p \in \mathcal{P}(L^U(\zeta_q)/L^B)} p \\ &\leq 2\varphi(q)(\ell - 1)\ell \cdot \text{rad}(N_f)\ell \cdot (\ell + 1)^{\omega(N_f)+1} \prod_{p \in \mathcal{P}(L^U(\zeta_q)/L^B)} p. \end{aligned}$$

Since $p \in \mathcal{P}(L^U(\zeta_q)/L^B)$ implies $p \mid qN_f\ell$, where q , ℓ and N_f are assumed pairwise coprime, we may bound the product by $\text{rad}(qN_f)\ell$.

The proof for $M(L^H(\zeta_q)/L^B)$ is practically identical; the only change is due to the fact that $[L^H(\zeta_q) : L^B] = \varphi(q)(\ell - 1)$. \square

Observe that the bound (7.12) that we achieve for $M(L^H(\zeta_q)/L^B)$ appears with one less power of $\ell + 1$ than (7.11). Because of this, working with $\pi_{C''}(x, L^H(\zeta_q)/L^B)$ will be advantageous when possible.

Finally, if L/K is an abelian extension, we can relate $M(L/K)$ to the quantity $D_K \mathcal{Q}(L/K)$.

Lemma 7.8. *Let L/K be an abelian extension of number fields. Then*

$$D_K \mathcal{Q}(L/K) \leq \left(\frac{M(L/K)}{2} \right)^{2[K:\mathbb{Q}]}.$$

Proof. By [MMS88, Proposition 2.5], we have

$$\mathcal{Q}(L/K) \leq \left([L : K] \prod_{p \in \mathcal{P}(L/K)} p \right)^{2[K:\mathbb{Q}]}.$$

We multiply both sides by D_K^2 and use the definition (7.8) of $M(L/K)$. \square

7.4. Lang–Trotter type bounds. Let $f(z)$ be a non-CM cusp form of even weight $k_f \geq 2$, level N_f , and trivial nebentypus with integer coefficients $a_f(n)$ which is an eigenform for all Hecke operators and Atkin–Lehner operators. Suppose furthermore that for some integer $q \geq 1$, $\gcd(q, \ell) = 1$ and subset $S \subseteq (\mathbb{Z}/q\mathbb{Z})^\times$, it is known that if $a_f(p) = a$, then $p \in S \pmod{q}$. Finally, suppose that the Galois representation $\rho_{f,\ell}$ is surjective for all primes $\ell > \ell_0$ with $\gcd(\ell - 1, k_f - 1) = 1$. For such ℓ , constructing $L^B \subset L^H \subset L^U$ as before, we have the bounds for $M(L^U(\zeta_q)/L^B)$ and $M(L^H(\zeta_q)/L^B)$ provided in Lemma 7.7.

In this subsection, we are interested in estimating the prime counting function $\pi_f(x, a)$. Of particular interest is $\pi_f(x, 0)$, as this quantity is related to the non-vanishing of the Fourier coefficients $a_f(n)$ of f (see Proposition 8.4 below). First, using Lemma 6.1, we develop an estimate for $\pi_{C'' \times S}(x, L^H(\zeta_q)/L^B)$ and $\pi_{C' \times S}(x, L^U(\zeta_q)/L^B)$ in terms of only ℓ and q .

Lemma 7.9. *Let $\ell > \max\{\ell_0, 5\}$ be a prime with $\gcd(\ell - 1, k_f - 1) = 1$ and q a positive integer such that $\gcd(q, \ell) = 1$. Let*

$$\begin{aligned} c_{13} &= \max(62 + 4.2 \log \text{rad}(N_f), 4.2(2.9 + \log \varphi(q))), \\ c_{14} &= \max(42, 4.2(5.8 + \log \varphi(q) + \log \text{rad}(q) + \log 2(1 + \omega(q) + \omega(N_f))))), \\ c_{15} &= 4.2(\omega(N_f) + 3.5). \end{aligned}$$

If

$$x \geq e^{c_{13}} e^{c_{14}(\ell+1)} (\ell+1)^{c_{15}(\ell+1)}, \quad (7.13)$$

then

$$\pi_{C'' \times S}(x, L^H(\zeta_q)/L^B) \leq 11.29 \frac{|S|x}{\varphi(q)(\ell-1) \log x}. \quad (7.14)$$

Proof. We wish to express all the quantities present in Lemma 6.1 in terms of ℓ and q . For the extension $L^H(\zeta_q)/L^B$, we have that

$$\begin{aligned} n_{L^B} &= \ell + 1, \\ [L^H(\zeta_q) : L^B] &= \varphi(q)(\ell - 1) \leq \varphi(q)e^{\ell+1-3}. \end{aligned}$$

By Lemmas 7.8 and 7.7, we have that

$$D_{L^B} \mathcal{Q}(L^H(\zeta_q)/L^B) \leq (\ell + 1)^{2(\omega(N_f)+3)(\ell+1)} (\varphi(q) \text{rad}(q))^{2(\ell+1)}. \quad (7.15)$$

By Lemma 7.6, we also have

$$D_{L^B} \leq (\text{rad}(N_f)(\ell + 1))^{\ell+1} (\ell + 1)^{(\omega(N_f)+1)(\ell+1)}. \quad (7.16)$$

Lastly, to bound $Z_{\mathfrak{m}}(\delta)$, note that the Artin conductor for $L^H(\zeta_q)/L^B$ is divisible only by primes in L^B which ramify in $L^H(\zeta_q)$. By considering ramification of rational primes in L and $\mathbb{Q}(\zeta_q)$ separately, $\mathcal{P}(L^H(\zeta_q)/L^B)$ is a subset of the primes in L^B which lie over primes in $\mathcal{P}(L(\zeta_q)/\mathbb{Q})$, i.e. primes in L^B which divide $qN_f\ell$. So, we obtain the bound

$$\omega(\mathfrak{m}) \leq \omega(qN_f\ell)[L^B : \mathbb{Q}] = (1 + \omega(q) + \omega(N_f))(\ell + 1),$$

which gives

$$Z_{\mathfrak{m}}(\delta) \leq 2^{\omega(\mathfrak{m})} \leq 2^{(1+\omega(q)+\omega(N_f))(\ell+1)}. \quad (7.17)$$

Now, applying these bounds to Lemma 6.1 with the parameters $\delta = 1/10$, $\eta = 1/21$, $\epsilon = \omega = 1/4$, and $\gamma = 1/5$ gives

$$\begin{aligned} e^\epsilon \left(e^{c_{11}} e^{c_{12}n_{L^B}} n_{L^B}^{n_{L^B}/2} D_{L^B}^{1/2} \right)^{\frac{2}{(1-\eta)\omega}} &\leq e^{62} e^{42(\ell+1)} \text{rad}(N_f)^{4.2} (\ell + 1)^{4.2(\ell+1)(\omega(N_f)+3)} \\ (252n_{L^B} [L^H(\zeta_q) : L^B])^2 &\leq e^{12} e^{4(\ell+1)} \varphi(q)^2 \\ \left(\frac{C(\delta, \epsilon, \gamma)}{1 - \delta - 2\omega(1 + \gamma)} \right)^\nu &\leq \\ \left(e^{2.9} \varphi(q) (\varphi(q) \text{rad}(q))^{\ell+1} e^{5.8(\ell+1)} 2^{(1+\omega(q)+\omega(N_f))(\ell+1)} (\ell + 1)^{(\omega(N_f)+3.5)(\ell+1)} \right)^{4.2}. \end{aligned}$$

Taking the maximum of these three expressions gives the desired result. \square

A similar result holds for $\pi_{C' \times S}(x, L^U(\zeta_q)/L^B)$.

Lemma 7.10. *Let $\ell > \max\{\ell_0, 5\}$ be a prime with $\gcd(\ell - 1, k_f - 1) = 1$ and q a positive integer such that $\gcd(q, \ell) = 1$. Let*

$$\begin{aligned} c_{16} &= \max(62 + 4.2 \log \text{rad}(N_f), 4.2(0.9 + \log \varphi(q))), \\ c_{17} &= \max(42, 4.2(6.8 + \log \varphi(q) + \log \text{rad}(q) + \log 2(1 + \omega(q) + \omega(N_f))))), \\ c_{18} &= 4.2(\omega(N_f) + 4.5). \end{aligned}$$

If

$$x \geq e^{c_{16}} e^{c_{17}(\ell+1)} (\ell + 1)^{c_{18}(\ell+1)}, \quad (7.18)$$

then

$$\pi_{C' \times S}(x, L^U(\zeta_q)/L^B) \leq 11.29 \frac{|S|x}{\varphi(q)(\ell - 1) \log x}. \quad (7.19)$$

Proof. The proof is the same as that of Lemma 7.9, but we instead use the bound

$$D_{L^B} \mathcal{Q}(L^U(\zeta_q)/L^B) \leq (\ell + 1)^{2(\omega(N_f)+3)(\ell+1)} (\varphi(q) \text{rad}(q))^{2(\ell+1)} \quad (7.20)$$

from Lemmas 7.8 and 7.7 and

$$[L^U(\zeta_q) : L^B] = \varphi(q) \ell (\ell - 1) \leq \varphi(q) e^{2(\ell+1)-5}. \quad (7.21)$$

□

Note that if the range conditions (7.13) or (7.18) hold with $\ell \geq 5$, we have that $x \geq e^{272}$, regardless of N_f and q . Therefore, this will be established as an assumption throughout.

To conclude, we derive a general-purpose bound for $\pi_f(x, 0)$ and $\pi_f(x, a)$ for a newform f with the aforementioned specifications. We can do so using Lemmas 7.9 or 7.10 combined with Corollary 7.2, Lemma 7.4, and Lemma 7.5.

Theorem 7.11. *Let $a \in \mathbb{Z}$, $A > 272$ and $1 < m < 10$ be constants. Suppose $x \geq e^A$ and $\ell = \ell_1$ is a prime number, and set*

$$t = \left\lceil \frac{2r}{(\log 2)} \log \log x \right\rceil. \quad (7.22)$$

Suppose that the following also hold:

- (A) $\ell > \max\{\ell_0, 5\}$ and $\gcd(\ell - 1, k_f - 1) = 1$ and $\gcd(\ell, q) = 1$,
- (B) $x \geq e^{c_{16}} e^{c_{17}(\ell+1)} (\ell + 1)^{c_{18}(\ell+1)}$, where c_{16}, c_{17}, c_{18} are as in (7.18). If $a = 0$, we may instead take $x \geq e^{c_{13}} e^{c_{14}(\ell+1)} (\ell + 1)^{c_{15}(\ell+1)}$, where c_{13}, c_{14}, c_{15} are as in (7.13).
- (C) $\ell < \frac{1}{2} \exp(\frac{\log x}{2t})$,
- (D) There exist t primes $\ell = \ell_1 < \ell_2 < \dots < \ell_t$ in the interval $[\ell, 2\ell]$ such that $\gcd(\ell_j - 1, k_f - 1) = 1$ and $\gcd(\ell_j, q) = 1$.

We have that

$$\pi_f(x, a) \leq 34.7r \frac{|S|}{\varphi(q)(\ell - 1)} \frac{x \log \log x}{\log x} + 1.42 \frac{x}{(\log x)^r}. \quad (7.23)$$

Proof. We apply Lemma 7.4(a) along with Lemma 7.5. Using $[L^B : \mathbb{Q}] = \ell + 1$ and (7.11) to bound for $M(L^U(\zeta_q)/L^B)$ gives

$$\begin{aligned} \pi_f(x, a; \ell) &\leq \pi_{C' \times S}(x, L^U(\zeta_q)/L^B) + 3.15546\ell(\ell + 1) \frac{x^{1/2}}{\log x} \\ &\quad + (\omega(N_f) + 4)(\ell + 1) \log(\ell + 1) + (\ell + 1) \log(2 \operatorname{rad}(N_f)^2 \varphi(q) \operatorname{rad}(q)) + 1. \end{aligned} \quad (7.24)$$

If $a = 0$, we instead use Lemma 7.4(b), and (7.12) to bound $M(L^H(\zeta_q)/L^B)$. We obtain a similar bound for $\pi_f(x, 0; \ell)$, this time with a main term of $\pi_{C'' \times S}(x, L^H(\zeta_q)/L^B)$. Under the range condition (B), the sum of the error terms above will be less than $0.01 \frac{x}{\varphi(q)(\ell_1 - 1) \log x}$. Thus we have that

$$\pi_f(x, a; \ell) \leq \pi_{C' \times S}(x, L^U(\zeta_q)/L^B) + 0.01 \frac{x}{\varphi(q)(\ell_1 - 1) \log x}. \quad (7.25)$$

The analogous equation holds when $a = 0$. Since x and ℓ_1 satisfy the preconditions of Lemma 7.10, we have

$$\pi_{C'' \times S}(x, L^H(\zeta_q)/L^B) \leq \frac{11.29|S|x}{\varphi(q)(\ell_1 - 1) \log x}. \quad (7.26)$$

If $a = 0$, we instead use Lemma 7.9. (7.25) and (7.26) then give

$$\pi_f(x, a; \ell) \leq \frac{11.3|S|x}{\varphi(q)(\ell_1 - 1) \log x} \quad (7.27)$$

for all primes ℓ satisfying conditions (A) and (B) of the theorem statement.

Let $\ell_1 < \ell_2 < \dots < \ell_t$ be the t primes determined in condition (D) of the theorem statement. Due to (C) and (D), the preconditions of Corollary 7.2 hold so we have

$$\begin{aligned} \pi_f(x, a) &\leq \left(\frac{2r}{\log 2} \log \log x + 1 \right) \left(\max_{1 \leq j \leq t} \pi_f(x, a; \ell_j) \right) \\ &\quad + \frac{x\sqrt{2}}{(\log x)^r} + \frac{2x^{1/2}}{(\log x)^r} + 2(\log x)^{2r} + 35. \end{aligned} \quad (7.28)$$

Therefore, using that $x \geq e^{272}$ from (7.13), we can combine error terms to obtain that

$$\pi_f(x, a) \leq \left(\frac{2r}{\log 2} + \frac{1}{\log 272} \right) \log \log x \left(\max_{1 \leq j \leq t} \pi_f(x, a; \ell_j) \right) + 1.42 \frac{x}{(\log x)^r}. \quad (7.29)$$

Finally, we combine (7.29) with the estimates for $\pi_f(x, 0; \ell_j)$ provided in (7.27), and in order to take the maximum we note that the right-hand side of (7.27) is maximized over the ℓ_j 's when $j = 1$. \square

In the next sections, we make Theorem 7.11 explicit in two different cases, proving Theorems 1.2 and 1.3.

Remark 7.1. Theorem 7.11 can be made explicit for other non-CM cusp forms f if the surjectivity of the ℓ -adic representation $\rho_{f, \ell}$ is known beyond some threshold $\ell > \ell_0$. Explicit values of ℓ_0 are only known for certain forms, such as the newforms of level 1 and weights $k \in \{12, 16, 18, 20, 22, 26\}$.

We also require bounds for the number of primes in the interval $[\ell, 2\ell]$ such that $\gcd(\ell - 1, k_f - 1) = 1$; we supply such bounds for $k_f = 12$ in Lemma 8.3.

8. PROOF OF THEOREMS 1.2 AND 1.4

We first specialize to the delta function $f(z) = \Delta(z)$ defined in (1.12). Recall that Δ is a cuspidal newform of weight $k_\Delta = 12$ and level $N_\Delta = 1$ with its n -th Fourier coefficient equal to Ramanujan's tau-function $\tau(n)$. By work of Swinnerton-Dyer [SD73, Theorem 4, Corollary (i)], if $\ell > 691$ is prime, then the associated residual representation $\rho_{\Delta, \ell}$ is surjective. Since N_Δ has no prime factors, we have that $\omega(N_\Delta) = 0$ and $\text{rad}(N_\Delta) = 1$. Moreover, Serre [Ser73] proved that if $\tau(p) = 0$, then p lies in one of $|S| = 33$ congruence classes modulo

$$\begin{aligned} q &:= 3488033912832000 \\ &= 2^{14} \times 3^7 \times 5^3 \times 7^2 \times 23 \times 691. \end{aligned}$$

We apply this data to the statement of Theorem 7.11. First, we require bounds for functions which count rational primes.

8.1. Auxiliary results on bounds for prime-counting functions. We first state a version of the classical Brun–Titchmarsh theorem due to Montgomery–Vaughan [MV73]:

Theorem 8.1. *Let x and y be positive real numbers, and let d and q be relatively prime positive integers. If $\pi(x; q, d) = \#\{p \leq x \mid p \equiv d \pmod{q}\}$, then*

$$\pi(x + y; q, d) - \pi(x; q, d) < \frac{2y}{\varphi(q) \log(y/q)}.$$

We also need an estimate for the number of primes between y and $2y$ from [RS62].

Lemma 8.2 (Rossen–Schoenfeld [RS62, Corollary 3]). *For all $y \geq 20.5$, we have*

$$\pi(2y) - \pi(y) > 0.6 \frac{y}{\log y} \tag{8.1}$$

Combining these results gives the following lemma, which we use to verify conditions (C) and (D) of Theorem 7.11.

Lemma 8.3. *Let $y \geq 2000$. Then*

$$\#\{p \in (y, 2y] \mid p \not\equiv 1 \pmod{11}\} > 0.3 \frac{y}{\log y}. \tag{8.2}$$

Proof. The count on the left-hand side of (8.2) is equal to

$$\pi(2y) - \pi(y) - (\pi(2y; 11, 1) - \pi(y; 11, 1)).$$

By Theorem 8.1 and the assumption that $y \geq 2000$, we bound $\pi(2y; 11, 1) - \pi(y; 11, 1)$ by

$$\pi(2y; 11, 1) - \pi(y; 11, 1) \leq 0.2 \frac{y}{\log y - \log 11} \leq 0.3 \frac{y}{\log y}. \tag{8.3}$$

Combining this estimate with Lemma 8.2 gives

$$\pi(2y) - \pi(y) - (\pi(2y; 11, 1) - \pi(y; 11, 1)) > (0.6 - 0.3) \frac{y}{\log y} = 0.3 \frac{y}{\log y} \tag{8.4}$$

as desired. \square

8.2. Proof of Theorem 1.2. We apply Theorem 7.11, choosing ℓ_1 and m so that the conditions of the theorem hold. For general $a \in \mathbb{Z}$, we take $q = 1$ and recall that $N_f = 1$ so that the range condition (B) becomes

$$x \geq e^{42} e^{62(\ell+1)} (\ell+1)^{18.9(\ell+1)}. \quad (8.5)$$

If $a = 0$, we instead use $q = 3488033912832000$ and the alternate range in condition (B), so we have

$$x \geq e^{156} e^{252(\ell+1)} (\ell+1)^{14.7(\ell+1)}. \quad (8.6)$$

Letting $\theta > 0$ be some fixed parameter to be specified shortly, we will choose the prime ℓ_1 to be near (but smaller than) the function

$$\ell(x) := \frac{\theta \log x}{\log \log x}. \quad (8.7)$$

We take $\theta = 0.06$ for general $a \in \mathbb{Z}$, and $\theta = 0.04$ when $a = 0$. When $x \geq e^{e^{16}}$, we can verify that (8.5) holds with $\ell = \ell(x)$ and $\theta = 0.06$ and that (8.5) holds with $\theta = 0.04$. We can also verify that condition (C) holds.

More precisely, we set ℓ_1 to be the largest prime number less than $\ell(x)$ which is not congruent to 1 modulo 11. By Lemma 8.3, we can take $\ell_1 > 0.5\ell(x)$. Now, setting $r = 4$, we use Lemma 8.3 to verify that condition (C) holds when $x \geq e^{e^{16}}$. Now, using $\theta = 0.06$, $r = 4$, and $q = 1$ gives

$$\pi_\Delta(x, a) \leq 4626.7 \frac{x(\log \log x)^2}{(\log x)^2} + 1.42 \frac{x}{(\log x)^4}. \quad (8.8)$$

Using $\theta = 0.04$, $r = 4$, and $q = 3488033912832000$ likewise gives

$$\pi_\Delta(x, 0) \leq 3.007 \cdot 10^{-10} \frac{x(\log \log x)^2}{(\log x)^2} + 1.42 \frac{x}{(\log x)^4}. \quad (8.9)$$

If $x \geq e^{e^{16}}$, then

$$1.42 \frac{x}{(\log x)^4} \leq 10^{-16} \frac{x(\log \log x)^2}{(\log x)^2}. \quad (8.10)$$

Absorbing the error term into the main term yields the desired result. \square

Next, we use Theorem 1.2 to prove Theorem 1.4.

8.3. Proof of Theorem 1.4. We compute a lower bound for

$$D_\Delta = \lim_{x \rightarrow \infty} \frac{\#\{1 \leq n \leq x \mid \tau(n) \neq 0\}}{x},$$

using our result for $\pi_\Delta(x, 0)$. These two quantities are related by the following result.

Proposition 8.4. *For all $X_0 \geq 2$, we have that*

$$D_\Delta = \prod_{\tau(p)=0} \left(1 - \frac{1}{p+1}\right) \quad (8.11)$$

$$> \exp\left(-\int_{X_0}^{\infty} \frac{\pi_\Delta(x, 0)}{x(x+1)} dx\right) \cdot \prod_{\substack{p \leq X_0 \\ \tau(p)=0}} \left(1 - \frac{1}{p+1}\right). \quad (8.12)$$

Proof. The first line follows from [Ser81, Equation 202]. The second line follows from a partial summation argument applied to the logarithm of the product in (8.11), and the identity for the truncated integral

$$\exp\left(-\int_2^{X_0} \frac{\pi_{\Delta}(x, 0)}{x(x+1)} dx\right) = \left(1 + \frac{1}{X_0}\right)^m \prod_{j=1}^m \left(1 - \frac{1}{p_j+1}\right)$$

where p_1, \dots, p_j are the primes less than X_0 with $\tau(p) = 0$. \square

Proof of Theorem 1.4. We use Proposition 8.4 with the cutoff $X_0 = 10^{23}$. By computer search, Rouse and Thorner [RT17] showed that all but 1810 prime numbers p less than 10^{23} satisfy $\tau(p) \neq 0$, using Swinnerton-Dyer's congruences for $\tau(n)$ and Galois representations at $\ell = 11, 13, 17, 19$, which are necessary conditions for $\tau(p) = 0$ [SD73]. They compute

$$\prod_{\substack{\tau(p)=0 \\ p \leq 10^{23}}} \left(1 - \frac{1}{p+1}\right) > 0.99999999999999999980399. \tag{8.13}$$

From the fact that if $\tau(p) = 0$, then p lies in one of 33 possible residue classes modulo q , Theorem 8.1 allows us to bound

$$\pi_{\Delta}(x, 0) \leq 1810 + \frac{2(x - 10^{23} + 2q)}{\varphi(q) \log((x - 10^{23} + 2q)/q)} \times 33, \quad x > 10^{23}. \tag{8.14}$$

To bound the contribution in this range, we use the following lemma.

Lemma 8.5. *If $X_0 > 2q > 0$, then*

$$\int_{X_0}^{X_1} \frac{x - X_0 + 2q}{x(x+1) \log((x - X_0 + 2q)/q)} dx < \int_2^{X_1/q} \frac{x}{(x + X_0/q - 2)^2 \log x} dx.$$

Proof. We use that $X_0 - 2q > 0$, $x(x+1) > x^2$ when $x > 0$, and set $u = x - X_0 + 2q$ to find that

$$\int_{X_0}^{X_1} \frac{x - X_0 + 2q}{x(x+1) \log((x - X_0 + 2q)/q)} dx < \int_{2q}^{X_1} \frac{u}{(u + X_0 - 2q)^2 \log(u/q)} du.$$

Now, setting $t = u/q$ and simplifying completes the proof. \square

We want to bound the integral in (8.12) between $X_0 = 10^{23}$ and $X_1 = e^{e^{16}}$. (8.14) and Lemma 8.5 allow us to numerically integrate to find that

$$\begin{aligned} \int_{X_0}^{X_1} \frac{\pi_{\Delta}(x, 0)}{x(x+1)} dx &< \int_{X_0}^{X_1} \frac{1810}{x(x+1)} dx + \frac{66}{\varphi(q)} \int_2^{X_1/q} \frac{x}{(x + X_0/q - 2)^2 \log x} dx \\ &\leq 1.1358 \times 10^{-12}. \end{aligned}$$

In the range $x > X_1$, we upper bound $\pi_\Delta(x, 0)$ using Theorem 1.2, which gives

$$\begin{aligned} \int_{X_1}^{\infty} \frac{\pi_\Delta(x, 0)}{x(x+1)} dx &\leq (3.01 \cdot 10^{-10}) \int_{X_1}^{\infty} \frac{(\log \log x)^2}{x(\log x)^2} dx \\ &= (3.01 \cdot 10^{-10}) \cdot \frac{(\log \log X_1)^2 + 2 \log \log X_1 + 2}{\log X_1} \\ &< 9.824 \cdot 10^{-15}. \end{aligned}$$

Thus we have that

$$\begin{aligned} \exp\left(-\int_{X_0}^{\infty} \frac{\pi_\Delta(x, 0)}{x(x+1)} dx\right) &> \exp(-1.1358 \times 10^{-12} - 9.824 \cdot 10^{-15}) \\ &> 0.999999999998854. \end{aligned} \tag{8.15}$$

Combining the estimates (8.13) and (8.15) via Proposition 8.4 yields

$$\begin{aligned} D_\Delta &> 0.999999999999999980399 \cdot 0.999999999998854 \\ &> 0.99999999999885 \\ &= 1 - 1.15 \cdot 10^{-12}, \end{aligned}$$

as desired. \square

9. PROOF OF THEOREMS 1.3 AND 1.5

Let E be the elliptic curve defined by (1.21). We apply our method from Section 8 to the modular form $f_E(z)$ associated to E , as defined in (1.22), in order to bound $\pi_E(x, a)$ and D_{f_E} . We first note the following congruence relation.

Lemma 9.1. *If $p \neq 11$, then $a_E(p) \equiv p + 1 \pmod{5}$.*

Proof. The elliptic curve E satisfies $E[5] \cong \mathbb{Z}/5\mathbb{Z}$ [LT76, p. 55]. If $p \neq 11$, then E has good reduction at p , so the reduction mod p map $E[5] \rightarrow E(\mathbb{F}_p)$ is injective [Sil09, Proposition VII.3.1]. Then, $\#E(\mathbb{F}_p) \equiv 0 \pmod{5}$, and by the modularity theorem $a_E(p) = p + 1 - \#E(\mathbb{F}_p)$, so we have that $p + 1 - a_E(p) \equiv 0 \pmod{5}$. \square

This allows us to set $q = 5$ below. Note that if $a \equiv 1 \pmod{5}$ and $a_E(p) = a$, then $p = 5$ or 11 . If $a \neq 1$ and $a \equiv 1 \pmod{5}$, then $\pi_E(x, a) = 0$ since $a_E(5) = a_E(11) = 1$. For other values of a , we use Theorem 1.3.

Proof of Theorem 1.3. We use Theorem 7.11 as in the proof of Theorem 1.2 in Section 8.2. Substituting $q = 5$ and $N_f = 11$ into (B) yields the range condition

$$x \geq e^{72} e^{46(\ell+1)} (\ell+1)^{18.9(\ell+1)}. \tag{9.1}$$

We repeat the arguments of Section 8.2, verifying that the conditions of Theorem 7.11 hold with $\theta = 0.055$, $r = 2$ and $x \geq e^{e^{13}}$. This implies that

$$\pi_E(x, a) \leq 630.91 \cdot \frac{x(\log \log x)^2}{(\log x)^2} + 1.42 \cdot \frac{x}{(\log x)^2}. \tag{9.2}$$

If $x \geq e^{e^{13}}$, then

$$1.42 \frac{x}{(\log x)^2} \leq 0.01 \cdot \frac{x(\log \log x)^2}{(\log x)^2}. \quad (9.3)$$

Substituting (9.2) into (9.3) completes the proof. \square

We now prove Theorem 1.5.

Proof of Theorem 1.5. We argue as in the proof of Theorem 1.4 in Section 8.3. By a similar argument as in the proof of Proposition 8.4 (applying [Ser81, Equation 201] instead of [Ser81, Equation 202]), we first note that

$$\begin{aligned} D_{f_E} &= \frac{14}{15} \prod_{a_E(p)=0} \left(1 - \frac{1}{p+1}\right) \\ &> \frac{14}{15} \exp\left(-\int_{X_0}^{\infty} \frac{\pi_E(x, 0)}{x(x+1)} dx\right) \cdot \prod_{\substack{p \leq X_0 \\ a_E(p)=0}} \left(1 - \frac{1}{p+1}\right). \end{aligned} \quad (9.4)$$

We use the cutoff $X_0 = 10^{11}$. By computer search, Rouse and Thorner [RT17] find that there are precisely 17857 primes $p \leq 10^{11}$ such that $a_E(p) = 0$, and they compute that

$$\frac{14}{15} \prod_{\substack{p \leq 10^{11} \\ a_E(p)=0}} \left(1 - \frac{1}{p+1}\right) = 0.8465247961\dots \quad (9.5)$$

If $x > 10^{11}$, then Lemma 9.1 and Theorem 8.1 imply that

$$\pi_E(x, 0) \leq 17857 + \frac{2(x - 10^{11} + 10)}{4 \log((x - 10^{11} + 10)/5)}. \quad (9.6)$$

We want to bound the integral in (9.4) between $X_0 = 10^{11}$ and $X_1 = e^{e^{13}}$. Applying (9.6), Lemma 8.5 and integrating numerically gives the bound

$$\int_{X_0}^{X_1} \frac{17857 + \frac{2(x-10^{11}+10)}{4 \log((x-10^{11}+10)/5)}}{x(x+1)} dx < 4.898.$$

When $x > X_1$, we upper bound $\pi_E(x, 0)$ using Theorem 1.3, which yields

$$\int_{X_1}^{\infty} \frac{\pi_E(x, 0)}{x^2 + x} dx \leq 631 \int_{X_1}^{\infty} \frac{(\log \log x)^2}{x(\log x)^2} dx < 0.281.$$

We then have that

$$\exp\left(-\int_{10^{11}}^{\infty} \frac{\pi_E(x, 0)}{x(x+1)} dx\right) > \exp(-4.898 - 0.281) > 0.00563364. \quad (9.7)$$

Combining (9.5) and (9.7) via (9.4) completes the proof. \square

REFERENCES

- [CGH⁺96] R. M Corless, G. H Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth. On the Lambert W -function. *Advances in Computational mathematics*, 5(1):329–359, 1996.
- [Cha13] I. Chatzigeorgiou. Bounds on the Lambert function and their application to the outage analysis of user cooperation. *IEEE Communications Letters*, 17(8):1505–1508, 2013.
- [CM⁺06] A. C. Cojocaru, M. R. Murty, et al. *An introduction to sieve methods and their applications*, volume 66. Cambridge University Press, 2006.
- [Cox13] D. A. Cox. *Primes of the form $x^2 + ny^2$* . Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.
- [CT17] L. Clozel and J. A. Thorne. Level-raising and symmetric power functoriality, III. *Duke Math. J.*, 166(2):325–402, 2017.
- [Deb19] K. Debaene. Explicit counting of ideals and a Brun-Titchmarsh inequality for the Chebotarev density theorem. *Int. J. Number Theory*, 15(5):883–905, 2019.
- [EC11] B. Edixhoven and J.-M. Couveignes, editors. *Computational aspects of modular forms and Galois representations*, volume 176 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2011. How one can compute in polynomial time the value of Ramanujan’s tau at a prime.
- [Elk87] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over \mathbf{Q} . *Invent. Math.*, 89(3):561–567, 1987.
- [Elk91] N. D. Elkies. Distribution of supersingular primes. Number 198-200, pages 127–132 (1992). 1991. Journées Arithmétiques, 1989 (Luminy, 1989).
- [FM96] E. Fouvry and M. R. Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.
- [GJ78] S. Gelbart and H. Jacquet. A relation between automorphic representations of $GL(2)$ and $GL(3)$. *Ann. Sci. École Norm. Sup. (4)*, 11(4):471–542, 1978.
- [Kim03] H. H. Kim. Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2 . *J. Amer. Math. Soc.*, 16(1):139–183, 2003. With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak.
- [KS02] H. H. Kim and F. Shahidi. Functorial products for $GL_2 \times GL_3$ and the symmetric cube for GL_2 . *Ann. of Math. (2)*, 155(3):837–893, 2002. With an appendix by Colin J. Bushnell and Guy Henniart.
- [Leh47] D. H. Lehmer. The vanishing of Ramanujan’s function $\tau(n)$. *Duke Math. J.*, 14:429–433, 1947.
- [LMO79] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3):271–296, 1979.
- [LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L -functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464, 1977.
- [LRS19] F. Luca, M. Radziwiłł, and I. E. Shparlinski. On the typical size and cancellations among the coefficients of some modular forms. *Math. Proc. Cambridge Philos. Soc.*, 166(1):173–189, 2019.
- [LT76] S. Lang and H. Trotter. *Frobenius distributions in GL_2 -extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2 -extensions of the rational numbers.
- [May13] J. Maynard. On the Brun-Titchmarsh theorem. *Acta Arith.*, 157(3):249–296, 2013.
- [MMS88] M. R. Murty, V. K. Murty, and N. Saradha. Modular forms and the Chebotarev density theorem. *Amer. J. Math.*, 110(2):253–281, 1988.
- [Mur97] V. K. Murty. Modular forms and the Chebotarev density theorem. II. In *Analytic number theory (Kyoto, 1996)*, volume 247 of *London Math. Soc. Lecture Note Ser.*, pages 287–308. Cambridge Univ. Press, Cambridge, 1997.

- [MV73] H. L. Montgomery and R. C. Vaughan. The large sieve. *Mathematika*, 20:119–134, 1973.
- [NT21a] J. Newton and J. A. Thorne. Symmetric power functoriality for holomorphic modular forms. *Publ. Math. Inst. Hautes Études Sci.*, 134:1–116, 2021.
- [NT21b] J. Newton and J. A. Thorne. Symmetric power functoriality for holomorphic modular forms, II. *Publ. Math. Inst. Hautes Études Sci.*, 134:117–152, 2021.
- [Rad60] H. Rademacher. On the Phragmén–Lindelöf theorem and some applications. *Math. Z.*, 72:192–204, 1959/1960.
- [RS62] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6(1):64–94, 1962.
- [RT17] J. Rouse and J. Thorner. The explicit Sato–Tate conjecture and densities pertaining to Lehmer-type questions. *Trans. Amer. Math. Soc.*, 369(5):3575–3604, 2017.
- [SD73] H. P. F. Swinnerton-Dyer. On l -adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math., Vol. 350, pages 1–55. Springer, Berlin, 1973.
- [Ser73] J.-P. Serre. Congruences et formes modulaires [d’après H. P. F. Swinnerton-Dyer]. In *Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416*, pages 319–338. Lecture Notes in Math., Vol. 317. 1973.
- [Ser76] J.-P. Serre. Divisibilité de certaines fonctions arithmétiques. *Enseign. Math. (2)*, 22(3-4):227–260, 1976.
- [Ser81] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.
- [Ser85] J.-P. Serre. Sur la lacunarité des puissances de η . *Glasgow Math. J.*, 27:203–221, 1985.
- [Sil09] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
- [Tit30] E. C. Titchmarsh. A divisor problem. *Rendiconti del Circolo Matematico di Palermo (1884-1940)*, 54(1):414–429, 1930.
- [TZ17] J. Thorner and A. Zaman. An explicit bound for the least prime ideal in the Chebotarev density theorem. *Algebra Number Theory*, 11(5):1135–1197, 2017.
- [TZ18] J. Thorner and A. Zaman. A Chebotarev variant of the Brun–Titchmarsh theorem and bounds for the Lang–Trotter conjectures. *Int. Math. Res. Not. IMRN*, (16):4991–5027, 2018.
- [TZ19] J. Thorner and A. Zaman. A unified and improved Chebotarev density theorem. *Algebra Number Theory*, 13(5):1039–1068, 2019.
- [Wan90] D. Q. Wan. On the Lang–Trotter conjecture. *J. Number Theory*, 35(3):247–268, 1990.
- [Wei83] A. Weiss. The least prime ideal. *J. Reine Angew. Math.*, 338:56–94, 1983.
- [Zyw15] D. Zywina. Bounds for the Lang–Trotter conjectures. In *SCHOLAR—a scientific celebration highlighting open lines of arithmetic research*, volume 655 of *Contemp. Math.*, pages 235–256. Amer. Math. Soc., Providence, RI, 2015.

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY
Email address: danielhu@princeton.edu

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY
Email address: hiyer@college.harvard.edu

DEPARTMENT OF MATHEMATICS, WILLIAMS COLLEGE
Email address: aes7@williams.edu