ACTA ARITHMETICA
125.3 (2006)

Non-abelian number fields with very large class numbers

by

Ryan C. Daileda (Hanover, NH)

1. INTRODUCTION

1.1. Background and motivation. Let K be a number field and denote by H its group of ideal classes. Since H is finite an interesting question one may ask is how its size, the *class number* of K, denoted by h, varies as K varies in some natural family of number fields. This question is in general very difficult to answer. As an example, an unproven conjecture of Gauss is that there are infinitely many real quadratic number fields with $h = 1$. Here we will be interested in the opposite extreme. That is, we want to study how large h can possibly be as K varies.

Littlewood [13] addresses this question in one of the simplest cases, for K an imaginary quadratic field. His work makes use of the class number formula for imaginary quadratic fields:

$$h = |d|^{1/2}\pi^{-1}L(1,\chi),$$

where d is the discriminant of K, χ is a certain quadratic Dirichlet character mod $|d|$ and $L(s,\chi)$ is the associated Dirichlet L-function. Assuming the generalized Riemann hypothesis (GRH) for all such $L(s,\chi)$, Littlewood is able to prove that for imaginary quadratic number fields

$$h \le c|d|^{1/2}\log\log|d| \tag{1}$$

for some absolute constant c. To show that his estimate is sharp he goes on to prove, still assuming GRH, that there are imaginary quadratic number fields with arbitrarily large discriminant d for which

$$h \ge c|d|^{1/2}\log\log|d| \tag{2}$$

for some absolute constant c ([1]). The key to his argument is the fact that, under GRH, $\log L(1,\chi)$ can be approximated by a relatively short sum over

2000 *Mathematics Subject Classification*: Primary 11R29; Secondary 11M26, 11F12.

([1]) The constant c is not necessarily the same at each occurrence.

primes ([2]):

$$\log L(1,\chi) = \sum_{p\le(\log|d|)^{1/2}} \chi(p)p^{-1} + O(1). \tag{3}$$

After showing that there are arbitrarily large discriminants for which $\chi(p) = 1$ for enough primes, the result follows from the asymptotic

$$\sum_{p\le x} p^{-1} = \log\log x + O(1). \tag{4}$$

Under the assumption of GRH, Littlewood's method can be used to show that for a real quadratic field of discriminant d we have

$$h \le cd^{1/2}\left(\frac{\log\log d}{\log d}\right)$$

with an absolute constant c. Montgomery and Weinberger [15] show that the analogue of Littlewood's result (2) holds unconditionally for real quadratic fields. They prove that there exist real quadratic fields with arbitrarily large discriminant d, whose class numbers satisfy

$$h \ge cd^{1/2}\left(\frac{\log\log d}{\log d}\right),$$

by substituting for GRH a zero density estimate for Dirichlet L-functions. They make use of the fact that the approximation (3) holds provided $L(s,\chi)$ has no zeros near $s = 1$, then apply the zero density estimate to show that such L-functions exist in sufficient abundance.

Duke [4, 5] proves analogous results for more general number fields. After formulating the problem of extreme class numbers rather generally, he proves [5] that there are abelian cubic number fields with arbitrarily large discriminant d satisfying

$$h \ge cd^{1/2}\left(\frac{\log\log d}{\log d}\right)^2 \tag{5}$$

for an absolute constant c. As in the work of Montgomery and Weinberger, Duke is able to make use of a zero density estimate for Dirichlet L-functions since the class number formula for abelian cubic fields gives

$$h = \frac{d^{1/2}}{4R}\,|L(1,\chi)|^2,$$

where R is the regulator of the field and χ denotes a certain primitive Dirichlet character. The primary difference between this and the imaginary quadratic case is the presence of the regulator in the class number formula, which arises from the presence of an infinite unit group in the cubic case.

([2]) Littlewood actually uses a more elaborate approximation to get good explicit constants in (1) and (2).

To deal with this, Duke must construct an abundance of number fields for which the value of $\chi(p)$ can be forced to be 1 for enough primes *and* for which the size of the regulator can be controlled. The result (5) shows that Duke's [5] bound

$$h \le cd^{1/2}\left(\frac{\log\log d}{\log d}\right)^2$$

provided by GRH is sharp, up to the constant.

Duke [4] conditionally extends these results to certain classes of non-abelian fields. Specifically, for a fixed $n \ge 2$, he considers the set $\mathcal{K}_n$ of number fields K of degree n over $\mathbb{Q}$ that are totally real and whose Galois closures have S_n as their Galois group. The class number formula for $K \in \mathcal{K}_n$ states that

$$h = \frac{d^{1/2}}{2^{n-1}R}\,L(1,\chi),$$

where d is the discriminant of K, R is the regulator and $L(s,\chi) = \zeta_K(s)/\zeta(s)$ is an Artin L-function. Under the assumptions that these Artin L-functions are entire (Artin's conjecture) and satisfy GRH, it can be shown that for $K \in \mathcal{K}_n$,

$$h \le cd^{1/2}\left(\frac{\log\log d}{\log d}\right)^{n-1}$$

with an absolute constant c. To show this estimate is sharp, Duke is able to produce, still under the assumptions of entirety and GRH for Artin L-functions, fields $K \in \mathcal{K}_n$ with arbitrarily large discriminant d for which

$$h \ge cd^{1/2}\left(\frac{\log\log d}{\log d}\right)^{n-1}. \tag{6}$$

Here the constant c depends only on n. Note that for $n = 2$, this is just a restatement of the Montgomery and Weinberger result. There are two main ingredients to Duke's construction. The first consists of finding fields in $\mathcal{K}_n$ for which R is relatively small. Duke then proves an analogue for Artin L-functions of Littlewood's result, that if $L(s,\chi)$ is entire and satisfies GRH then

$$\log L(1,\chi) = \sum_{p \le (\log N)^{1/2}} \chi(p)p^{-1} + O(1), \tag{7}$$

where N is the conductor of χ and the implied constant depends only on n, the degree of χ. The remainder of his argument is to show that $\chi(p)$ can be forced to be $n-1$ for enough primes, for arbitrarily large values of d. The result follows as above after an application of (4).

1.2. Statement of results. In this paper we will establish an unconditional version of Duke's result for $\mathcal{K}_3$. Specifically we will prove

THEOREM 1. *There exists an absolute constant $c > 0$ so that there are totally real non-abelian cubic number fields with arbitrarily large discriminant d satisfying*

$$h \geq cd^{1/2}\left(\frac{\log\log d}{\log d}\right)^2.$$

To prove this theorem we apply the technique of Montgomery and Weinberger, and use a zero density estimate to replace the need for GRH. The approach we use is suggested in the final section of [5]. Specifically, we prove an estimate for the total number of zeros of certain families of automorphic L-functions near $s = 1$ (Theorem 5). It should be noted that in order to apply this theorem we may only consider families of fields whose Artin L-functions are known to be automorphic. This is one reason why we have been able to make Duke's result unconditional only in the case $n = 3$. However, along the same lines we are able to prove the following result, which extends Theorem 1 to the case of cubic fields with negative discriminant, which we henceforth refer to as *complex cubic fields*.

THEOREM 2. *There exists an absolute constant $c > 0$ so that there are complex cubic number fields with arbitrarily large discriminant d satisfying*

$$h \geq c|d|^{1/2}\frac{(\log\log|d|)^2}{\log|d|}. \tag{8}$$

As in the totally real case, Theorem 2 shows that the bound for h provided by GRH

$$h \leq c|d|^{1/2}\frac{(\log\log|d|)^2}{\log|d|}$$

is essentially sharp. Duke [5] suggested a conditional proof (based on Littlewood's technique) for this bound; we supply the details in Proposition 3 below.

There are only two possible signatures for cubic number fields, depending on the sign of the discriminant. Theorems 1 and 2 treat each case in complete generality. However, in the case of negative discriminant we can prove a specialized result for a certain subclass of fields, namely the *pure cubic* fields. These are cubic fields of the form $\mathbb{Q}(\sqrt[3]{r})$, $r \in \mathbb{Q}$. The upper bound on the class number of such fields provided by GRH is slightly stronger than that deduced above for general complex cubic fields. As with complex cubic fields, we show in Proposition 3 that under the assumption of GRH we have

$$h \leq c|d|^{1/2}\frac{\log\log|d|}{\log|d|}$$

for pure cubic fields with an absolute implied constant c. That this bound is essentially sharp follows from the next result.

THEOREM 3. *There exists an absolute constant $c > 0$ so that there are pure cubic number fields with arbitrarily large discriminant d satisfying*

$$h \geq c|d|^{1/2} \frac{\log\log|d|}{\log|d|}. \tag{9}$$

We remark that Theorem 3 can be proven using existing zero density estimates (e.g. those due to Huxley [10], etc.) for families of L-functions of Hecke characters defined over a fixed number field, while the proofs of Theorems 1 and 2 require a zero density estimate such as that of Theorem 5. This is due to the fact that the method of Montgomery and Weinberger we use requires us to estimate the number of zeros of a certain family of L-functions of Hecke characters defined on quadratic fields. These quadratic fields are all the same for pure cubic fields, but must vary in general if we are to force the class number to be as large as allowed by GRH ([3]). It is in applicability to the case of varying field of definition that our zero density estimate supersedes its predecessors.

2. L-FUNCTIONS

The primary goal of this section is the proof of Theorem 5, which gives an upper bound for the total number of zeros near $s = 1$ of the L-functions of a certain family of automorphic representations. For L-functions with completely multiplicative coefficients, techniques based on sieve methods for proving such theorems are well established (see [9, 14]). In order to apply these techniques to the L-functions of automorphic representations, which do not have completely multiplicative coefficients, we replace them by new L-series. These new series share the zeros of the originals, but have coefficients with the desired multiplicativity property. After proving a sieve inequality analogous to that established by Duke and Kowalski [6] for the new L-series, we use well known machinery to obtain the zero density theorem.

2.1. Preliminaries. In this section we recall the basic definitions and theorems that we will need later. Throughout, $s = \sigma + it$ will denote a complex variable.

We begin with Artin L-functions. Let K/k be a finite Galois extension of number fields and let π be a finite-dimensional complex representation of $G(K/k)$. For a prime $\mathfrak{p}$ of k let $D_\mathfrak{p}$, $I_\mathfrak{p}$ and $\sigma_\mathfrak{p}$ denote the decomposition group, inertia group and Frobenius element, respectively, of any prime $\mathfrak{P}$ of K over $\mathfrak{p}$. If V is the space of π then let $V^{I_\mathfrak{p}}$ denote the subspace of vectors

([3]) In general, if we hold the associated quadratic field fixed, the GRH conditional upper bound on the class number of a non-abelian cubic number field is smaller than that mentioned above. See the proof of Lemma 9.

fixed by $I_\mathfrak{p}$. Define

$$L_\mathfrak{p}(s,K/k,\pi)=\det(I-\pi(\sigma_\mathfrak{p})|_{V^{I_\mathfrak{p}}}N(\mathfrak{p})^{-s})^{-1}.$$

The Artin L-function associated to π is then

$$L(s,K/k,\pi)=\prod_\mathfrak{p}L_\mathfrak{p}(s,K/k,\pi).$$

The factors $L_\mathfrak{p}(s,K/k,\pi)$ are all of the form

$$\prod_{i=1}^n(1-\alpha_i(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}$$

where n is the dimension of π and $|\alpha_i(p)|\leq 1$ for all p and i. In fact, since G is finite it is clear from their definition that the $\alpha_i(\mathfrak{p})$ are roots of unity or 0. This implies that the Euler product defining $L(s,K/k,\pi)$ converges uniformly on $\sigma\geq\sigma_0>1/2$ to a holomorphic function.

For the remainder of this section we set $k=\mathbb{Q}$. Expand the Euler product as a Dirichlet series

$$L(s,K/\mathbb{Q},\pi)=\sum_{m=1}^\infty\lambda(m)m^{-s}.$$

It is immediate that $\lambda(p)=\sum_i\alpha_i(p)$ for all primes p. In particular, we find that for p unramified in K, $\lambda(p)=\mathrm{Tr}(\pi(\sigma_p))$.

As is well known, an Artin L-function has a meromorphic continuation to all of $\mathbb{C}$. The Artin conjecture asserts that if π does not contain the trivial representation then $L(s,K/\mathbb{Q},\pi)$ is actually entire. While this is not known to be true in general, it will hold for the L-functions we consider.

An Artin L-function also satisfies a functional equation relating its value at s to the value of a related function at $1-s$. To state it we first define

$$L_\mathbb{R}(s)=\pi^{-s/2}\Gamma(s/2).$$

Let $\chi=\mathrm{Tr}\circ\pi$ be the character of π. If τ is the element of $G(K/\mathbb{Q})$ corresponding to complex conjugation then we set

$$n^+=\frac{\chi(1)+\chi(\tau)}{2},\qquad n^-=\frac{\chi(1)-\chi(\tau)}{2}$$

and

$$L_\infty(s,K/\mathbb{Q},\pi)=L_\mathbb{R}(s)^{n^+}L_\mathbb{R}(s+1)^{n^-}.$$

The completed L-function $\Lambda(s,K/\mathbb{Q},\pi)=L_\infty(s,K/\mathbb{Q},\pi)L(s,K/\mathbb{Q},\pi)$ then satisfies the functional equation

$$\Lambda(1-s,K/\mathbb{Q},\pi)=\varepsilon_\pi N^{s-1/2}\Lambda(s,K/\mathbb{Q},\widetilde{\pi}). \tag{10}$$

Here N is an integer, the *conductor* of π, ε_π is a complex number of absolute value 1 and $\widetilde{\pi}$ is the representation contragredient to π. The *Generalized Rie-*

mann Hypothesis (GRH) is the assertion that all of the zeros of $\Lambda(s, K/\mathbb{Q}, \pi)$ lie on the line $\sigma = 1/2$.

We now turn to automorphic L-functions. By a *cuspidal automorphic representation* of $\mathrm{GL}(2)$ over $\mathbb{Q}$ we will mean an irreducible unitary representation of $\mathrm{GL}(2, \mathbb{A}_{\mathbb{Q}})$ that occurs in the right regular representation of $\mathrm{GL}(2, \mathbb{A}_{\mathbb{Q}})$ on the space $L_0^2(\mathrm{GL}(2, \mathbb{Q}) \setminus \mathrm{GL}(2, \mathbb{A}_{\mathbb{Q}}), \omega)$ of cusp forms, where ω is a unitary character (the so-called *central character*) of $Z(\mathrm{GL}(2, \mathbb{A}_{\mathbb{Q}}))$ that is trivial on $\mathbb{Q}^\times$. See [1, 7] for notation and additional background. While this is not the most general definition (see [7]), it is sufficient for our applications. For us, the most relevant piece of information regarding a cuspidal automorphic representation π is the fact that it decomposes as a restricted tensor product of local representations π_v of $\mathrm{GL}(2, \mathbb{Q}_v)$, where v runs over the places of $\mathbb{Q}$. The factor π_∞ will be called the *infinite part* of π.

Let π be a cuspidal automorphic representation of $\mathrm{GL}(2)$ over $\mathbb{Q}$ and let $L(s, \pi)$ denote the finite part of the L-function of π. Then $L(s, \pi)$ is given by the degree 2 Euler product

$$L(s, \pi) = \prod_p (1 - \alpha_1(p)p^{-s})^{-1}(1 - \alpha_2(p)p^{-s})^{-1},$$

which converges absolutely and uniformly for $\sigma = \operatorname{Re} s$ sufficiently large (below we will see just how large). The parameters in each local factor are determined by the finite local factors π_v alluded to above.

As is well known, $L(s, \pi)$ has analytic continuation to the entire complex plane and satisfies a functional equation relating its value at s to its value at $1 - s$. The infinite part of π determines complex numbers μ_1, μ_2 with $\operatorname{Re} \mu_j > -1/2$, so that if

$$L_\infty(s, \pi) = L_{\mathbb{R}}(s + \mu_1)L_{\mathbb{R}}(s + \mu_2)$$

and we set

$$\Lambda(s, \pi) = L_\infty(s, \pi)L(s, \pi) \tag{11}$$

then

$$\Lambda(s, \pi) = \varepsilon_\pi q^{1/2-s} \Lambda(1 - s, \widetilde{\pi}). \tag{12}$$

Here ε_π is a complex number of absolute value 1, q is an integer called the *conductor* of π and $\widetilde{\pi}$ is the representation contragredient to π (see [11]). For our purposes, it is enough to know that the local parameters defining $\Lambda(s, \widetilde{\pi})$ are the complex conjugates of those defining $\Lambda(s, \pi)$ (see [21]). It is well known that $\Lambda(s, \pi)$ is an entire function of order 1, the zeros ϱ of Λ satisfying $0 \le \operatorname{Re} \varrho \le 1$.

Using the functional equations together with the Phragmén–Lindelöf convexity principle [18] one can readily deduce the following bounds, valid in the region $\sigma < 1$.

LEMMA 1. *Let $L/\mathbb{Q}$ be a finite Galois extension and let π be an n-dimensional complex representation of $G(L/\mathbb{Q})$. If N is the conductor of π and the associated Artin L-function $L(s, L/\mathbb{Q}, \pi)$ satisfies Artin's conjecture then*

$$|L(s, L/\mathbb{Q}, \pi)| \ll_n N^{3/4-\sigma/2}|1+s|^{n(3/4-\sigma/2)}$$

for all $-1/2 \le \sigma \le 3/2$.

LEMMA 2. *Let π be a cuspidal automorphic representation of* GL(2) *over $\mathbb{Q}$ with conductor q. Let $L(s, \pi)$ be the associated L-function and suppose that there is a $c < 1/2$ so that*

$$|\alpha_i(p)| \le p^c \tag{13}$$

for all i, p. Then for $-1/2 \le \sigma \le 3/2$ we have

$$L(s, \pi) \ll_\infty (1/2-c)^2 q^{3/4-\sigma/2}|s+3/2|^{3/2-\sigma}.$$

The notation means that the implied constant depends only on the infinite part of π.

As one may take $c = 3/10$ (see [21]) we see that this lemma holds for all cuspidal automorphic π, and we can in fact ignore the factor dependent on c. However, we will only be applying this lemma to L-functions satisfying the Ramanujan–Petersson conjecture so that we may in fact take $c = 0$.

We will make use of the following general results on the vertical distribution of the zeros of $\Lambda(s, \pi)$, where π is a cuspidal automorphic representation of GL(2) over $\mathbb{Q}$. They can be proven in the same way as the analogous results for Dirichlet L-functions [3].

PROPOSITION 1. *Let π be a cuspidal automorphic representation of* GL(2) *over $\mathbb{Q}$ with conductor q. Then for any $t \in \mathbb{R}$ the zeros $\varrho = \beta + i\gamma$ of $\Lambda(s, \pi)$ satisfy*

$$\#\{\varrho : |t-\gamma| < 1\} \ll \log(q(|t|+m)),$$

where $m \ge 2$ is a constant depending only on the infinite part of π and the implied constant is absolute.

COROLLARY 1. *Let π be a cuspidal automorphic representation of* GL(2) *over $\mathbb{Q}$ with conductor q. Then for any $T \ge 1/2$ the zeros $\varrho = \beta + i\gamma$ of $\Lambda(s, \pi)$ satisfy*

$$\#\{\varrho : |\gamma| \le T\} \ll T\log((T+m)q),$$

where $m \ge 2$ is a constant depending only on the infinite part of π and the implied constant is absolute.

2.2. Sieve inequalities. As above, let π denote a cuspidal automorphic representation of GL(2) over $\mathbb{Q}$ and let $L(s, \pi)$ denote the finite part of the

L-function of π:

$$L(s,\pi) = \prod_p (1-\alpha_1(p)p^{-s})^{-1}(1-\alpha_2(p)p^{-s})^{-1}.$$

We suppose that π satisfies the Ramanujan–Petersson conjecture:

$$|\alpha_i(p)| \le 1$$

for all i, p. Writing $L(s,\pi)$ as a Dirichlet series

$$L(s,\pi) = \sum_{n=1}^{\infty} \lambda_\pi(n) n^{-s},$$

we let

$$L_{\mathrm{c}}(s,\pi) = \prod_{p \ge K} (1-\lambda_\pi(p)p^{-s})^{-1}$$

where K is a constant whose value will be chosen later. If we write $L_{\mathrm{c}}(s,\pi)$ as a Dirichlet series

$$L_{\mathrm{c}}(s,\pi) = \sum_{n=1}^{\infty} l_\pi(n) n^{-s}$$

then $l_\pi(p) = \lambda_\pi(p)$ for $p \ge K$ and $l_\pi(p) = 0$ for $p < K$. Note that whereas the coefficients of $L(s,\pi)$ are multiplicative, those of $L_{\mathrm{c}}(s,\pi)$ are *completely* multiplicative. This will be important. The functions L and L_{c} are related through the following lemma.

LEMMA 3. *Let $L(s,\pi)$ and $L_{\mathrm{c}}(s,\pi)$ be as above. Then for sufficiently large K there is an Euler product*

$$H(s,\pi) = \prod_p H_p(s,\pi)$$

which converges uniformly and absolutely for $\sigma \ge \sigma_0 > 1/2$ satisfying

$$L_{\mathrm{c}}(s,\pi) = H(s,\pi)L(s,\pi).$$

Moreover, on $\sigma > 1/2$ the function $H(s,\pi)$ is free from zeros and satisfies the bound

$$H(s,\pi) \ll_K (\sigma - 1/2)^{-2}.$$

Proof. To simplify notation, we omit π in what follows and write $X = p^{-s}$. We define the local factors as follows. Let

$$H_p(s) = \begin{cases} (1-\alpha_1(p)X)(1-\alpha_2(p)X) & \text{for } p < K, \\ \dfrac{(1-\alpha_1(p)X)(1-\alpha_2(p)X)}{1-\lambda(p)X} & \text{for } p \ge K. \end{cases}$$

Note that we need K to be large enough to ensure that the denominator of this expression does not vanish for $\sigma > 1/2$. Since the local factors of H are just the quotients of the local factors of L and L_{c}, the equality $L_{\mathrm{c}}(s) = H(s)L(s)$ is a formal consequence of the definitions.

To prove the convergence properties of $H(s)$, note first that for $p > K$,

$$H_p(s) = 1 + \frac{\alpha_1\alpha_2 X^2}{1-(\alpha_1+\alpha_2)X}$$

since $\lambda(p) = \alpha_1(p) + \alpha_2(p)$. Now if K is sufficiently large, the Ramanujan–Petersson conjecture (which we have assumed to be true) gives

$$\left|\frac{\alpha_1\alpha_2 X^2}{1-(\alpha_1+\alpha_2)X}\right| \leq 2|X|^2$$

for all $\sigma > 1/2$. The convergence properties as stated above then follow.

The bound for H is easily deduced from the following more general statement. If $H(s) = \prod_p H_p(s)$ and there is a $C > 0$ so that $|H_p(s)| \leq 1 + Cp^{-2\sigma}$ for all p and $\sigma > 1/2$ then

$$|H(s)| \ll (\sigma - 1/2)^{-C},$$

the implied constant depending only on C. To prove this, note that

$$1 + Cp^{-2\sigma} = \frac{1+Cp^{-2\sigma}}{(1+p^{-2\sigma})^C}\,(1-p^{-4\sigma})^C(1-p^{-2\sigma})^{-C}.$$

The first two terms give rise to Euler products which are bounded for $\sigma > 1/2$ and the last term yields $\zeta(2\sigma)^C$. ∎

This lemma provides the analytic continuation of $L_{\mathrm{c}}(s,\pi)$ to $\sigma > 1/2$, and shows that the zeros of L_{c} in this region coincide with those of L.

In [6] it is shown that the coefficients $\lambda_\pi(n)$ of the L-functions of certain families of automorphic representations satisfy a sieve inequality. Their proof is based on the analytic properties of the L-functions, and given the relationship between L and L_{c} it is not surprising that we can modify their proof to give the analogous sieve inequality for the coefficients $l_\pi(n)$. However, as in the case of Dirichlet L-functions, in order to prove our zero density theorem we require a more general inequality that sieves not only over a family of representations but also over a collection of points.

To be specific, for $Q > 0$ we let $S(Q)$ denote a family of cuspidal automorphic representations of GL(2) over $\mathbb{Q}$ that have the same infinite part (for all Q), satisfy the Ramanujan–Petersson conjecture and have conductors bounded by Q. Let $T, \delta > 0$ and for each $\pi \in S(Q)$ let $\mathcal{S}(\pi)$ be a set of real numbers satisfying:

- $|t - t'| \geq \delta$ for distinct $t, t' \in \mathcal{S}(\pi)$;
- $|t| \leq T$ for all $t \in \mathcal{S}(\pi)$.

We denote by $\mathcal{S}$ the set of all pairs (π, t) with $\pi \in S(Q)$ and $t \in \mathcal{S}(\pi)$. The cardinality of a finite set A is denoted by $|A|$. If $a = (a_i)_I$ is a finite sequence of complex numbers indexed by I we denote by $\|a\|$ the L^2-norm of a. The result that we require is the following.

THEOREM 4. *Let everything be as above and assume that*

$$|S(Q)| = O(Q^d)$$

for some $d > 0$ and that $T \geq \max\{1, \delta\}$. Then, if K is sufficiently large, there exists a constant $E > 2$ such that if $\beta > 2(d+1)$ and $N > Q^\beta$ then for any $\varepsilon > 0$, $F > 1$ we have

$$\sum_{(\pi,t)\in\mathcal{S}} \Big| \sum_{n\leq N} a_n l_\pi(n) n^{it} \Big|^2 \ll_{\varepsilon,F} N^{1+\varepsilon}(\delta^{-F} + T^E\delta^{-1})\|a\|^2$$

for any sequence $a = (a_n)_{1\leq n\leq N}$ of complex numbers.

Proof. The inequality we seek to prove is equivalent to the estimate

$$\|T_{N,Q}\|^2 \ll_\varepsilon N^{1+\varepsilon}(\delta^{-F} + T^E\delta^{-1})$$

for the norm of the linear operator

$$T_{N,Q} : \mathbb{C}^N \to \mathbb{C}^{|\mathcal{S}|}, \qquad (a_n)_{1\leq n\leq N} \mapsto \Big(\sum_{n\leq N} a_n l_\pi(n) n^{it} \Big)_{(\pi,t)\in\mathcal{S}}.$$

By general theory the norm of $T_{N,Q}$ is the same as the norm of the conjugate of its adjoint

$$\overline{T^*_{N,Q}} : \mathbb{C}^{|\mathcal{S}|} \to \mathbb{C}^N, \qquad (\alpha_{(\pi,t)})_{(\pi,t)\in\mathcal{S}} \mapsto \Big(\sum_{(\pi,t)\in\mathcal{S}} \alpha_{(\pi,t)} l_\pi(n) n^{it} \Big)_{1\leq n\leq N}.$$

Choosing a smooth, compactly supported $\psi : [0,\infty) \to [0,1]$ satisfying $\psi(x) = 1$ for $x \in [0,1]$ we find that for any $\alpha \in \mathbb{C}^{|\mathcal{S}|}$,

$$\|\overline{T^*_{N,Q}}(\alpha)\|^2 \leq \sum_{n\geq 1} \Big| \sum_{(\pi,t)\in\mathcal{S}} \alpha_{(\pi,t)} l_\pi(n) n^{it} \Big|^2 \psi(n/N).$$

Expanding the square and swapping the order of summation gives

$$\|\overline{T^*_{N,Q}}(\alpha)\|^2 \leq \sum_{(\pi,t)\in\mathcal{S}} \sum_{(\pi',t')\in\mathcal{S}} \alpha_{(\pi,t)} \overline{\alpha_{(\pi',t')}} S_N(\pi, \pi', t - t')$$

where

$$S_N(\pi, \pi', t) = \sum_{n\geq 1} l_\pi(n) \overline{l_{\pi'}(n)} \psi(n/N) n^{it}.$$

By Lemma 1 of [6],

$$\|\overline{T^*_{N,Q}}(\alpha)\|^2 \leq \max_{(\pi,t)\in\mathcal{S}} \sum_{(\pi',t')\in\mathcal{S}} |S_N(\pi, \pi', t - t')|$$

so that we are reduced to studying the $S_N(\pi, \pi', t)$.

If $\widehat{\psi}(s)$ denotes the Mellin transform of ψ,

$$\widehat{\psi}(s) = \int_0^\infty \psi(t) t^s \frac{dt}{t},$$

then by Mellin inversion

$$\psi(t) = \frac{1}{2\pi i} \int\limits_{(3)} \widehat{\psi}(s) t^{-s}\, ds$$

where the integral is taken over the line $\sigma = 3$. Consequently we get the integral representation

$$S_N(\pi, \pi', t) = \frac{1}{2\pi i} \int\limits_{(3)} \sum_{n \geq 1} (l_\pi(n)\overline{l_{\pi'}(n)} n^{-s+it}) \widehat{\psi}(s) N^s\, ds.$$

If we set

$$L_{\mathrm{b}}(s, \pi_1, \pi_2) = \sum_{n \geq 1} l_{\pi_1}(n) l_{\pi_2}(n) n^{-s}$$

then

$$S_N(\pi, \pi', t) = \frac{1}{2\pi i} \int\limits_{(3)} L_{\mathrm{b}}(s - it, \pi, \widetilde{\pi}') \widehat{\psi}(s) N^s\, ds. \tag{14}$$

We will bound this integral by studying the analytic properties of $L_{\mathrm{b}}(s, \pi_1, \pi_2)$. This we will do by relating it to the Rankin–Selberg L-function $L(s, \pi_1 \otimes \pi_2)$ (see [1, 2]) through the next lemma.

Lemma 4. *Let π_1 and π_2 be cuspidal automorphic representations of* $\mathrm{GL}(2)$ *over $\mathbb{Q}$ satisfying the Ramanujan–Petersson conjecture. If K in the definition of $L_{\mathrm{c}}(s, \pi_i)$ is taken sufficiently large (independently of the π_i) then there exists an Euler product*

$$H(s, \pi_1, \pi_2) = \prod_p H_p(s, \pi_1, \pi_2)$$

so that $L_{\mathrm{b}}(s, \pi_1, \pi_2) = H(s, \pi_1, \pi_2) L(s, \pi_1 \otimes \pi_2)$. Moreover, $H(s, \pi_1, \pi_2)$ is holomorphic on $\sigma > 1/2$ and for any $\varepsilon > 0$ satisfies the bound

$$H(s, \pi_1, \pi_2) \ll_\varepsilon [q_1, q_2]^\varepsilon (\sigma - 1/2)^{-A},$$

where q_i is the conductor of π_i, for some $A > 0$.

We will return to the proof of this lemma shortly. For now we note that, as above, it provides the continuation of L_{b} to $\sigma > 1/2$ since the Rankin–Selberg L-function is known to have such a continuation. Indeed, in our situation it is known [1, 2] that $L(s, \pi \otimes \widetilde{\pi}')$ is holomorphic on $\sigma > 1/2$ unless $\pi = \pi'$, in which case it has a simple pole at $s = 1$.

We now shift the contour in the representation (14) to the line $\sigma = 1/2 + c$, where c is a positive constant to be chosen later. Since $\widehat{\psi}$ is rapidly decreasing on vertical strips and $L(s, \pi \otimes \widetilde{\pi}')$ is of at most polynomial growth (we will see why shortly), the lemma shows that shifting the contour is permissible. If we let R_π denote the value of the residue of $L(s, \pi \otimes \widetilde{\pi})$ at

$s = 1$ then we find that

$$S_N(\pi, \pi', t) = \delta(\pi, \pi')H(1, \pi, \widetilde{\pi})\widehat{\psi}(1 + it)N^{1+it}R_\pi + \frac{1}{2\pi i}\int\limits_{(1/2+c)} L_{\mathrm{b}}(s - it, \pi, \widetilde{\pi}')\widehat{\psi}(s)N^s\, ds.$$

Since $H(1, \pi, \widetilde{\pi}) \ll Q^{2\varepsilon}$, $\widehat{\psi}(1 + it)$ decreases more rapidly than any power of t, and $R_\pi \ll Q^\varepsilon$ (this follows from the Ramanujan–Petersson conjecture), we find that the first term above is $\ll NQ^\varepsilon|t|^{-F}$ for any $F > 0$. As to the integral, from the functional equation for $L(s, \pi \otimes \widetilde{\pi}')$ and the Phragmén–Lindelöf principle it follows that

$$L(1/2 + c + it, \pi \otimes \widetilde{\pi}') \ll Q^{1-2c}|t|^E$$

for some $E > 0$ (the value of E depends only on the infinite parts of the π's). Using the bound for H provided by the lemma and the rapid decay of $\widehat{\psi}$ on the line we get the bound

$$\ll c^{-A}N^{1/2+c}Q^{1-2c+\varepsilon}|t|^{E+1}$$

for the integral. If $N > Q^\beta$ and we take $c = (\log N)^{-1}$ then this is

$$\ll N^{1/2+1/\beta+\varepsilon}|t|^{E+1}.$$

Applying these estimates we find that for any $(\pi, t) \in \mathcal{S}$,

$$\begin{aligned}\sum_{(\pi',t')\in\mathcal{S}} &|S_N(\pi, \pi', t - t')| \\ &\ll NQ^\varepsilon + \sum_{\substack{t'\in\mathcal{S}(\pi)\\ t'\neq t}} |t - t'|^{-F} + N^{1/2+1/\beta+\varepsilon}\sum_{\pi'\in S(Q)}\sum_{t'\in\mathcal{S}(\pi')} |t - t'|^{E+1} \\ &\ll N^{1+\varepsilon/\beta}(\delta^{-F} + 1) + N^{1/2+(d+1)/\beta+\varepsilon}T^{E+1}(T\delta^{-1} + 1) \\ &\ll N^{1+\varepsilon}(\delta^{-F} + T^{E+1}(T\delta^{-1} + 1)) \ll N^{1+\varepsilon}(\delta^{-F} + T^{E+2}\delta^{-1})\end{aligned}$$

provided $F > 1$ and $\beta > 2(d + 1)$. ∎

Proof of Lemma 4. Because both L and L_{b} have Euler product representations, we proceed locally. As before, we write $X = p^{-s}$ and omit p from our notation when it will cause no confusion. The Euler factor for the Rankin–Selberg L-function at a prime p that is unramified for both π_1 and π_2 is given by

$$L_p(s)^{-1} = \prod_{\substack{i=1,2\\ j=1,2}} (1 - \alpha_{1i}\alpha_{2j}X),$$

and at a ramified prime by

$$L_p(s)^{-1} = \prod_{1\le i\le m} (1-\beta_i X)$$

where the β_i are complex numbers and $m \le 4$. The Euler factors of the function L_{b} are given by

$$L_{\mathrm{b},p}(s)^{-1} = 1 - \lambda_{\pi_1}(p)\lambda_{\pi_2}(p)X = 1 - (\alpha_{11}(p)+\alpha_{12}(p))(\alpha_{21}(p)+\alpha_{22}(p))X$$

for $p \ge K$ and by $L_{\mathrm{b},p}(s) = 1$ for $p < K$.

We now set $H_p(s) = L_{\mathrm{b},p}(s)/L_p(s)$ for all primes. That $L_{\mathrm{b}}(s) = H(s)L(s)$ is then a formal consequence of this definition, so it only remains to verify the stated properties of H. We first note that for unramified $p > K$,

$$H_p(s) = 1 + \frac{X^2 f(X)}{1-(\alpha_{11}+\alpha_{12})(\alpha_{21}+\alpha_{22})X},$$

where $f(X)$ is a polynomial of degree at most 2 whose coefficients are polynomials in the α's. For $\sigma > 1/2$ the Ramanujan–Petersson conjecture gives

$$|1-(\alpha_{11}+\alpha_{12})(\alpha_{21}+\alpha_{22})X| \ge 1 - 4p^{-1/2} \ge 1/2$$

provided $K \ge 17$. Thus

$$\frac{X^2 f(X)}{1-(\alpha_{11}+\alpha_{12})(\alpha_{21}+\alpha_{22})X} \ll |X|^2|f(X)|.$$

The Ramanujan–Petersson conjecture again shows that for $\sigma > 1/2$ we have $|f(X)| \ll 1$. Consequently the Euler product converges uniformly and absolutely for $\sigma \ge \sigma_0 > 1/2$ and therefore represents a holomorphic function on $\sigma > 1/2$.

To bound H we apply the same reasoning as in Lemma 3 to the unramified primes, since we have just shown that $|H_p(s)| \le 1 + Ap^{-2\sigma}$ for $p \ge K$ (it is easy to compensate for the fact that this may not hold for finitely many primes: this will simply introduce another constant in the bound that depends on K). It remains to deal with the ramified primes. Since we are dealing with representations of GL(2), $L(s, \pi_1 \otimes \pi_2)$ is the L-function of an automorphic form on GL(4). This is a case of Langlands functoriality due to Ramakrishnan [20]. Consequently at the ramified places we may use the well known bound $|\beta_i(p)| < p^{1/2}$. Thus, for any ramified p we have

$$|H_p(s)| \le 2 \prod_{1\le i\le m} (1 + p^{1/2}p^{-\sigma}) \le 2^5 = C_1.$$

So for the product over the ramified primes we have

$$\Big| \prod_{p|[q_1,q_2]} H_p(s) \Big| \le \prod_{p|[q_1,q_2]} C_1 \ll_\varepsilon [q_1,q_2]^\varepsilon$$

since the number of primes dividing an integer n is $O(\log n/\log\log n)$ (this is an easy consequence of an argument in Chapter 22 of [8]). ∎

We now wish to replace the sets $\mathcal{S}(\pi)$ of real numbers by sets of complex numbers and prove an analogous sieve inequality. To be specific, for each $\pi \in S(Q)$ we now let $\mathcal{S}(\pi)$ be a set of complex numbers $s = \sigma + it$ and suppose that there exist $T, \delta > 0$ and $\sigma_0 > 1/2$ so that

- $|t - t'| \geq \delta$ for distinct $s, s' \in \mathcal{S}(\pi)$;
- $|t| \leq T$ for all $s \in \mathcal{S}(\pi)$;
- $\sigma \geq \sigma_0$ for all $s \in \mathcal{S}(\pi)$.

As before, let $\mathcal{S}$ be the set of all pairs (π, s) with $\pi \in S(Q)$ and $s \in \mathcal{S}(\pi)$.

COROLLARY 2. *Let everything be as above and assume that*

$$|S(Q)| = O(Q^d)$$

for some $d > 0$ and that $T \geq \max\{1, \delta\}$. Then, if K is sufficiently large, there exists a constant $E > 2$ such that if $\beta > 2(d+1)$ and $N > Q^\beta$ then for any $\varepsilon > 0$, $F > 1$ we have

$$\sum_{(\pi,s)\in\mathcal{S}} \Big| \sum_{n\leq N} a_n l_\pi(n) n^{-s} \Big|^2 \ll_{\varepsilon,F} N^{1+\varepsilon}(\delta^{-F} + T^E\delta^{-1}) \sum_{n\leq N} |a_n|^2 n^{-2\sigma_0}$$

for any sequence $a = (a_n)_{1\leq n\leq N}$ of complex numbers.

Proof. We use the identity

$$\sum_{n=1}^{N} a_n n^{-s} = a_1(1 - N^{\sigma_0-\sigma}) + N^{\sigma_0-\sigma} \sum_{n=1}^{N} a_n n^{-(\sigma_0+it)} + (\sigma - \sigma_0) \int_2^N \Big(\sum_{2\leq n\leq u} a_n n^{-(\sigma_0+it)} \Big) u^{-\sigma+\sigma_0-1}\, du$$

to remove dependence on the real part and apply the theorem. See Chapter 7 of [14] for the details. We end up with

$$\sum_{(\pi,s)\in\mathcal{S}} \Big| \sum_{n\leq N} a_n l_\pi(n) n^{-s} \Big|^2 \ll Q^d T\delta^{-1}|a_1|^2 + N^{1+\varepsilon}(\delta^{-F} + T^E\delta^{-1}) \log\log N \sum_{n\leq N} |a_n|^2 n^{-2\sigma_0},$$

which gives the result provided $\beta > 2(d+1)$. ∎

2.3. A zero density estimate. We are now in a position to prove our theorem on the zeros of families of automorphic L-functions. Our development here closely follows that of [9]. For an automorphic representation π, $\sigma > 1/2$ and $T > 0$ let $N(\sigma, T, \pi)$ denote the number of zeros of $L(s, \pi)$

in the rectangle $R(\sigma,T)=[\sigma,1]\times[-T,T]$. We aim to obtain a non-trivial upper bound for

$$\sum_{\pi\in S(Q)} N(\sigma,T,\pi).$$

As proven in the preceding section, the zeros of $L(s,\pi)$ and $L_{\mathrm{c}}(s,\pi)$ in any such rectangle coincide, so it is sufficient to work with the latter.

Since $L_{\mathrm{c}}(s,\pi)$ has completely multiplicative coefficients, if we set

$$M_X(s,\pi)=\sum_{n\le X}\mu(n)l_\pi(n)n^{-s}$$

then

$$L_{\mathrm{c}}(s,\pi)M_X(s,\pi)=1+\sum_{n>X}a_nl_\pi(n)n^{-s}\quad\text{where}\quad a_n=\sum_{\substack{d\mid n\\ d\le X}}\mu(d).$$

Applying Mellin inversion to $\Gamma(s)$ we obtain

$$\frac{1}{2\pi i}\int\limits_{(3)} L_{\mathrm{c}}(s+w,\pi)M_X(s+w,\pi)\Gamma(w)Y^w\,dw = e^{-1/Y}+\sum_{n>X}a_nl_\pi(n)n^{-s}e^{-n/Y}.$$

We take s to be a zero $\varrho=\beta+i\gamma$ of $L_{\mathrm{c}}(s,\pi)$ with $1/2<\beta$, and shift the contour of integration to the line $\operatorname{Re}w=1/2-\beta+c$, where c is a small positive constant whose exact value will be chosen later. Because $L_{\mathrm{c}}(\varrho,\pi)=0$, we pick up no residues in shifting the contour. Our formula thus becomes

$$\frac{1}{2\pi i}\int\limits_{(1/2-\beta+c)} L_{\mathrm{c}}(s+w,\pi)M_X(s+w,\pi)\Gamma(w)Y^w\,dw = e^{-1/Y}+\sum_{n>X}a_nl_\pi(n)n^{-s}e^{-n/Y}. \tag{15}$$

Since the Ramanujan–Petersson conjecture implies that $|\lambda_\pi(p)|\le 2$, from the complete multiplicativity of l_π it follows that

$$|l_\pi(n)|\le\prod_{p\mid n}2^{v_p(n)}\le n.$$

Consequently

$$\Big|\sum_{n>lY}a_nl_\pi(n)n^{-\varrho}e^{-n/Y}\Big|\le\sum_{n>lY}\sum_{\substack{d\mid n\\ d\le X}}n^{1-\beta}e^{-n/Y}\ll Y^{3/2}e^{-l}(l+1)\log Y$$

provided $l>1$ and $X\le Y$. To obtain this estimate, reverse the order of summation and approximate the resulting inner sum by an integral. If we

take $l = 2\log Y$ then in fact the above is

$$\ll Y^{-1/2}(\log Y)^2.$$

The upshot of this is that we have

$$\Big|\sum_{n>lY} a_n l_\pi(n) n^{-\varrho} e^{-n/Y}\Big| < \frac{1}{6}$$

for all sufficiently large Y. Likewise, $e^{-1/Y} \geq 5/6$ for all sufficiently large Y. Thus, from (15) we conclude that for all sufficiently large Y,

$$\Big|\sum_{X<n\leq lY} a_n l_\pi(n) n^{-\varrho} e^{-n/Y}\Big| \geq \frac{1}{3} \tag{16}$$

or

$$\Big|\int_{(1/2-\beta+c)} L_{\mathrm{c}}(s+w,\pi) M_X(s+w,\pi)\Gamma(w) Y^w\, dw\Big| \geq \frac{2\pi}{3}. \tag{17}$$

This gives us a means of detecting zeros of $L_{\mathrm{c}}(s,\pi)$ in $R(\sigma,T)$. To estimate the total number of zeros, we sum the quantities on the left hand sides of (16) and (17) over (almost) all of the zeros, then bound the resulting sums using the sieve inequality of the preceding section. Zeros that satisfy (16) are said to be of *class* (i) and those that satisfy (17) are said to be of *class* (ii). We will treat each class of zeros separately.

We begin by selecting from the collection of all zeros some well spaced representatives. From Corollary 1 we know that

$$\#\{\varrho : L(\varrho,\pi) = 0,\ 0 \leq \beta \leq 1,\ |\gamma| \leq T\} \ll T\log((T+m)q_\pi)$$

where $m \geq 2$ is a constant whose value depends only on the infinite part of π. Consequently, for each $\pi \in S(Q)$ we can choose a subset of the zeros in $R(\sigma,T)$ that have imaginary parts separated by at least 1 and that account for a proportion $\gg (T\log((T+m)Q))^{-1}$ of all of the zeros in this rectangle. We call these zeros the *representative zeros*, and denote by $R_A(\pi)$ the set of representative zeros of $L_{\mathrm{c}}(s,\pi)$ of class A. Let $\mathcal{S}_A$ denote the set of all pairs (π,ϱ) with $\pi \in S(Q)$ and $\varrho \in R_A(\pi)$.

In order to deal with the class (i) zeros effectively we must subdivide the class. To do this, write $(X, lY]$ as the union of intervals of the form $I_r = (2^r Y, 2^{r+1}Y]$, the first and last intervals instead being $(X, 2^{r_0+1}Y]$ and $(2^{r_1}Y, lY]$, respectively. By the triangle inequality we find that for any zero ϱ of class (i) there is an $r \in [r_0, r_1]$ so that

$$\Big|\sum_{n\in I_r} a_n l_\pi(n) n^{-\varrho} e^{-n/Y}\Big| \geq \frac{1}{3(r_1 - r_0 + 1)} \gg (\log Y)^{-1}.$$

A zero satisfying this inequality will be called a *class* (i, r) zero. Applying Corollary 2, we see that the representative zeros of class (i, r) number

$$\begin{aligned}
&\ll (\log Y)^2 \sum_{(\pi,\varrho)\in\mathcal{S}_{(\mathrm{i},r)}} \Big| \sum_{n\in I_r} a_n l_\pi(n) n^{-\varrho} e^{-n/Y} \Big|^2 \\
&\ll (\log Y)^2 (2^{r+1}Y)^{1+\varepsilon} T^E \sum_{n\in I_r} |a_n|^2 n^{-2\sigma} e^{-2n/Y} \\
&\ll (\log Y)^2 (2^{r+1}Y)^{1+\varepsilon} T^E \sum_{n\in I_r} d(n)^2 n^{-2\sigma} e^{-2^{r+1}} \\
&\ll (\log Y)^2 (2^{r+1}Y)^{1+\varepsilon} T^E (2^r Y)^{1-2\sigma} (\log(2^{r+1}Y))^4 e^{-2^{r+1}} \\
&\ll (\log Y)^6 Y^{2(1-\sigma)+\varepsilon} T^E (2^r)^{2(1-\sigma)+\varepsilon} (r+1)^4 e^{-2^{r+1}}.
\end{aligned}$$

Here we have used summation by parts and the inequality

$$\sum_{m\le x} d(m)^2 m^{-1} \ll (\log x)^4$$

(see [9, Chapter 2]). Note that in order to apply the corollary we must have $2^{r+1}Y > Q^\beta$ for some $\beta > 2(d+1)$, for all r in our range. This is certainly satisfied if we require $X > Q^\beta$.

Summing over all of the possible values for r we find that the number of representative zeros of class (i) is

$$\begin{aligned}
&\ll (\log Y)^6 Y^{2(\sigma-1)+\varepsilon} T^E \sum_{r\ge r_0} (2^r)^{2(1-\sigma)+\varepsilon} (r+1)^4 e^{-2^{r+1}} \\
&\ll (\log Y)^6 Y^{2(\sigma-1)+\varepsilon} T^E \Big(\sum_{r_0\le r<0} (r+1)^4 + \sum_{r\ge 0} 4^r (r+1)^4 e^{-2^{r+1}} \Big) \\
&\ll (\log Y)^{11} Y^{2(1-\sigma)+\varepsilon} T^E.
\end{aligned}$$

Here we have assumed $\varepsilon \le 1$. If we choose not to make this restriction, the final inequality is still valid, but with the implied constant dependent upon ε.

Having treated the class (i) zeros so carefully, we are allowed greater flexibility in treating the class (ii) zeros. We choose a rather simple method here. From expression (17) we see that the number of representative zeros of class (ii) is

$$\begin{aligned}
&\ll \sum_{(\pi,\varrho)\in\mathcal{S}_{(\mathrm{ii})}} \Big| \int\limits_{(1/2-\beta+c)} L_{\mathrm{c}}(s+w,\pi) M_X(s+w,\pi) \Gamma(w) Y^w \, dw \Big|^2 \\
&\ll Y^{1-2\sigma+2c} \sum_{(\pi,\varrho)\in\mathcal{S}_{(\mathrm{ii})}} \Big(\int\limits_{-\infty}^{\infty} |L_{\mathrm{c}}(1/2+c+i(t+\gamma),\pi)|^2 |\Gamma(1/2-\beta+c+it)| \, dt \Big) \\
&\quad \times \Big(\int\limits_{-\infty}^{\infty} |M_X(1/2+c+i(t+\gamma),\pi)|^2 |\Gamma(1/2-\beta+c+it)| \, dt \Big)
\end{aligned}$$

by Cauchy's inequality. Since $1/2 < \sigma \le \beta \le 1$, $|\Gamma(1/2-\beta+c+it)| \le (\sigma-1/2-c)^{-1}g(t)$, where $g(t)$ decays rapidly as $t \to \pm\infty$. By Lemma 3,

$$|L_{\mathrm{c}}(1/2+c+i(t+\gamma),\pi)| \ll c^{-2}|L(1/2+c+i(t+\gamma),\pi)|.$$

From Lemma 2 we have the bound

$$L(s,\pi) \ll q_\pi^{3/4-\sigma/2}|s+3/2|^{3/2-\sigma} \tag{18}$$

for $-1/2 \le \sigma \le 3/2$, where the implied constant depends only on the infinite part of π. So we see that

$$|L(1/2+c+i(t+\gamma),\pi)|^2 \ll q_\pi|3+i(t+\gamma)|^2$$

provided $c \le 1$. Continuing the above, we see that the number of representative zeros of class (ii) is

$$\begin{aligned}
&\ll Y^{1-2\sigma+2c}(\sigma-1/2-c)^{-2}Qc^{-4}\Big(\int_{-\infty}^{\infty}(|t|+T)^2g(t)\,dt\Big)\\
&\quad\times\Big(\int_{-\infty}^{\infty}\sum_{(\pi,\varrho)\in\mathcal{S}_{(\mathrm{ii})}}|M_X(1/2+c+i(t+\gamma),\pi)|^2g(t)\,dt\Big)\\
&\ll Y^{1-2\sigma+2c}(\sigma-1/2-c)^{-2}QT^2c^{-4}\\
&\quad\times\Big(\int_{-\infty}^{\infty}\sum_{(\pi,\varrho)\in\mathcal{S}_{(\mathrm{ii})}}|M_X(1/2+c+i(t+\gamma),\pi)|^2g(t)\,dt\Big).
\end{aligned}$$

We now apply Theorem 4 inside the integral. Note that in dealing with the class (i) zeros we have already made an assumption about the size of X that guarantees the theorem is applicable. This gives

$$\begin{aligned}
&\ll Y^{1-2\sigma+2c}X^{1+\varepsilon}(\sigma-1/2-c)^{-2}QT^2c^{-4}\\
&\quad\times\Big(\sum_{n\le X}\mu(n)^2n^{-1-2c}\Big)\int_{-\infty}^{\infty}(|t|+T)^Eg(t)\,dt\\
&\ll Y^{1-2\sigma+2c}X^{1+\varepsilon}(\sigma-1/2-c)^{-2}QT^{E+2}c^{-5}.
\end{aligned}$$

Now take $c=(\log Y)^{-1}$, and assume that Y is so large that $c\le(1/2)(\sigma-1/2)$. This is not a particularly restrictive condition since we will primarily be interested in cases where σ can be bounded away from $1/2$. We conclude that the number of representative zeros of class (ii) is

$$\ll(\sigma-1/2)^{-2}(\log Y)^5T^{E+2}QX^{1+\varepsilon}Y^{1-2\sigma}.$$

Now choose any $\beta > 2(d+1)$ and let

$$X = Q^\beta, \quad Y = Q^{\beta+1}.$$

Then the representative zeros of class (i) number

$$\ll(1+\beta)^{11}T^E(\log Q)^{11}Q^{2(\beta+1)(1-\sigma)+\varepsilon}$$

and the representative zeros of class (ii) number

$$\ll (1+\beta)^5(\sigma-1/2)^{-2}T^{E+2}(\log Q)^5Q^{2(\beta+1)(1-\sigma)+\beta\varepsilon}.$$

Adding these two and multiplying by $T\log((T+m)Q)$ (since we have counted only representative zeros) we arrive at

THEOREM 5. *Let $S(Q)$ be as above and assume that*

$$|S(Q)|\ll Q^d$$

for some $d>0$. Let $\sigma\in(1/2,1)$ and $T>1$. Then there are constants $E>5$ and $m\geq 2$ so that for any $\varepsilon>0$,

$$\sum_{\pi\in S(Q)}N(\sigma,T,\pi)\ll_\varepsilon(\sigma-1/2)^{-2}T^E\log((T+m)Q)(\log Q)^{11}Q^{(4d+6)(1-\sigma)+\varepsilon}$$

provided Q is sufficiently large.

The most important aspect of this bound it that the power of the conductor Q can be made arbitrarily small by letting σ approach 1. The same cannot be said about the power of T, however. This is a result of the fact that the T and Q aspects were not separated in the sieve inequalities of the previous section. This separation *has* been achieved for Dirichlet L-functions [9, 14], and in this respect our estimate is somewhat crude. Nevertheless, it suffices for what we have in mind. For if we assume further that T grows more slowly than any power of Q we can deduce the existence of L-functions that are zero free near $s=1$.

COROLLARY 3. *Let $S(Q)$ be as above and assume that*

$$Q^e\ll|S(Q)|\ll Q^d$$

for some $0<e<d$. Then there is a $\sigma\in(1/2,1)$ so that for all sufficiently large Q there exist $\pi\in S(Q)$ so that $L(s,\pi)$ is free from zeros in $[\sigma,1]\times[-(\log N)^2,(\log N)^2]$, N being the conductor of π. Moreover, as $Q\to\infty$ the number of such $\pi\in S(Q)$ cannot remain bounded.

Proof. Choose $\varepsilon>0$ and $1-\sigma$ so small that

$$f=(4d+6)(1-\sigma)+\varepsilon<e.$$

Taking $T=(\log Q)^2$ in Theorem 5 we find that

$$\sum_{\pi\in S(Q)}N(\sigma,(\log Q)^2,\pi)\ll Q^f.$$

The result now follows since the number of L-functions is $\gg Q^e$ and since $e>f$. ∎

2.4. Approximating $\log L(1,\pi)$**.** In this section we show that if an entire Artin L-function $L(s,\pi)$ is free from zeros near $s=1$ then $\log L(1,\pi)$ can be approximated by a short sum over primes. In particular, as the length of the sum we will be able to take a small power of the log of the conductor. This approximation will be crucial to later applications. The technique we use is not new, but we provide details for the sake of completeness. We begin with the following technical lemma.

LEMMA 5. *Let $L(s)$ be a holomorphic function on $\operatorname{Re} s > 1/2$. Let C_0, C_1, $A, T > 0$, $0 < \Delta < 1/2$, and $0 < \varepsilon < \Delta$ with $A \le T - \sqrt{\Delta^2 + 2\Delta}$. Suppose that L is free from zeros in $\Omega = \{\operatorname{Re} s > 1\} \cup \{\sigma + it : |t| \le T,\ 1-\Delta \le \sigma \le 1\}$. Finally let $f(t)$ be an increasing function and suppose that*

$$|L(2+it)| \ge C_0, \qquad |L(s)| \le f(|s|) \quad \text{for } \operatorname{Re} s > 1/2,$$
$$\left|\frac{L'(s)}{L(s)}\right| \le C_1 \quad \text{for } \operatorname{Re} s \ge 2.$$

Then

$$\frac{1}{2\pi i}\int_{(2)} \frac{L'(s+u)}{L(s+u)}\, x^s \Gamma(s)\, ds - \frac{L'(u)}{L(u)}$$
$$\ll x^2 e^{-A/2}\left(\frac{\log(f(A+5)/C_0)}{A\varepsilon^2} + C_1(A^{-1}+1)\right)$$
$$+ \frac{x^{1-\Delta+\varepsilon-u}}{\varepsilon^2(u-(1-\Delta+\varepsilon))}\int_{-A}^{A} \log\left(\frac{f(|t|+5)}{C_0}\right) dt$$

for $1-\Delta+\varepsilon < u \le 7/4-\Delta+\varepsilon$ and $x \ge 1$. The implied constant is absolute.

Proof. Since $A \le T - \sqrt{\Delta^2+2\Delta}$ we can cover the rectangle $|t| \le A$, $1-\Delta+\varepsilon \le \sigma \le 1$ with open disks $\{|s-(2+it_0)| < 1+\Delta\}$, $|t_0| \le A$, each disk lying in Ω. On any such disk

$$|s| \le (3+\Delta) + (|t_0|+1+\Delta) = |t_0| + 4 + 2\Delta$$

so that $\log|L(s)| \le \log(f(|t_0|+4+2\Delta))$, since f is increasing. As L is free from zeros on the simply connected region Ω, we may define a branch of $\log L$ there, and on any of the disks we thus have

$$\operatorname{Re}(\log L(s) - \log L(2+it_0)) \le \log\left(\frac{f(|t_0|+4+2\Delta)}{C_0}\right).$$

We now appeal to the following classical result.

LEMMA 6. *Suppose that $f(s)$ is holomorphic in $|s-s_0| < r$ and satisfies there*

$$\operatorname{Re}(f(s) - f(s_0)) \le U.$$

Then there is an absolute constant $A'>0$ so that for $|s-s_0|=r_0<r$ we have

$$|f'(s)|<\frac{A'Ur}{(r-r_0)^2}.$$

This is proven as Lemma 4 in [13] and as Carathéodory's lemma in [19]. From it we conclude that

$$\left|\frac{L'(s)}{L(s)}\right|\ll\frac{\log(f(|t_0|+5)/C_0)}{\varepsilon^2}$$

for $|s-(2+it_0)|\le 1+\Delta-\varepsilon$, $|t_0|\le A$. The implied constant is absolute.

We now turn to estimating the integral

$$\frac{1}{2\pi i}\int\limits_{(2)}\frac{L'(s+u)}{L(s+u)}\,x^s\Gamma(s)\,ds.$$

We shift the portion of the contour with $|t|\le A$ to the abscissa $\sigma=1-\Delta+\varepsilon-u$, picking up the residue $L'(u)/L(u)$ at $s=0$. Now we need to bound integrals over the contours

$$\begin{aligned}\gamma_1&:\sigma=1-\Delta+\varepsilon-u,\quad |t|\le A,\\ \gamma_2^{\pm}&:1-\Delta+\varepsilon-u\le\sigma\le 2,\quad t=\pm A,\\ \gamma_3^{\pm}&:\sigma=2,\quad \pm t\ge A.\end{aligned}$$

On γ_1 we have

$$|\Gamma(s)|\ll(u-(1-\Delta+\varepsilon))^{-1},\qquad |x^s|=x^{1-\Delta+\varepsilon-u},$$

$$\left|\frac{L'(s+u)}{L(s+u)}\right|=\left|\frac{L'(1-\Delta+\varepsilon+it)}{L(1-\Delta+\varepsilon+it)}\right|\ll\frac{\log(f(|t|+5)/C_0)}{\varepsilon^2}$$

since $|t|\le A$. Thus

$$\left|\frac{1}{2\pi i}\int\limits_{\gamma_1}\frac{L'(s+u)}{L(s+u)}\,x^s\Gamma(s)\,ds\right|\ll\frac{x^{1-\Delta+\varepsilon-u}}{\varepsilon^2(u-(1-\Delta+\varepsilon))}\int\limits_{-A}^{A}\log\left(\frac{f(|t|+5)}{C_0}\right)dt$$

and the implied constant is absolute.

By Stirling's formula and the fact that $\Gamma(s)$ has a simple pole at $s=0$ we find that

$$|\Gamma(s)|\ll A^{-1}e^{-A/2}$$

on $\gamma_2^{\pm}$. Moreover, on this contour we have $1-\Delta+\varepsilon\le\sigma+u\le 15/4$. On the part of this interval up to $\sigma+u=3$ we can use the bound

$$\left|\frac{L'(s+u)}{L(s+u)}\right|\ll\frac{\log(f(A+5)/C_0)}{\varepsilon^2},$$

and on the part of the interval with $\sigma+u>3$ (if it is not empty) we can

bound $|L'(s+u)/L(s+u)|$ by C_1. Since the length of $\gamma_2^{\pm}$ is $\ll 1$ we see that

$$\left|\frac{1}{2\pi i}\int\limits_{\gamma_2^{\pm}} \frac{L'(s+u)}{L(s+u)}\, x^s \Gamma(s)\, ds\right| \ll x^2 A^{-1} e^{-A/2}\left(\frac{\log(f(A+5)/C_0)}{\varepsilon^2} + C_1\right)$$

provided $x \geq 1$. As before, the implied constant is absolute.

Finally, on $\gamma_3^{\pm}$, Stirling's formula yields

$$|\Gamma(s)| \ll e^{-|t|/2}$$

and the L term may again be bounded by C_1. Thus

$$\left|\frac{1}{2\pi i}\int\limits_{\gamma_3^{\pm}} \frac{L'(s+u)}{L(s+u)}\, x^s \Gamma(s)\, ds\right| \ll C_1 x^2 \int\limits_A^{\infty} e^{-t/2}\, dt \ll C_1 x^2 e^{-A/2}$$

with, as usual, an absolute implied constant.

The conclusion of Lemma 5 now follows immediately. ∎

We will apply this lemma to an entire Artin L-function $L(s, L/\mathbb{Q}, \pi)$ where $L/\mathbb{Q}$ is a finite Galois extension and π is an n-dimensional complex representation of $G(L/\mathbb{Q})$ of conductor N. We drop L and $\mathbb{Q}$ from our notation for convenience. From the Euler product for $L(s,\pi)$ the following bounds are easily verified:

$$|L(2+it,\pi)| \geq \left(\frac{\zeta(4)}{\zeta(2)}\right)^n \gg_n 1, \qquad |L(s,\pi)| \leq \zeta(\sigma)^n \ \text{ for } \sigma > 1,$$

$$\frac{L'(s,\pi)}{L(s,\pi)} \ll_n 1 \ \text{ for } \sigma \geq 2.$$

From Lemma 1 we conclude that for $1/2 \leq \sigma \leq 3/2$ we have

$$|L(s,\pi)| \ll_n N^{1/2}(|s|+1)^{n/2}.$$

Therefore, we set $f(t) = C_n N^{1/2}(t+1)^{n/2}$ (for an appropriate $C_n > 0$) and conclude that $|L(s,\pi)| \leq f(|s|)$ for $\sigma \geq 1/2$. For any $0 < \delta < 1$ we set $\Delta = \delta/7$ and $\varepsilon = \delta/8$. Letting $T = (\log N)^2$ and $A = \log N$ we arrive at

Corollary 4. *Let $L/\mathbb{Q}$ be a finite Galois extension and let π be an n-dimensional complex representation of $G(L/\mathbb{Q})$ of conductor N. Let $0 < \delta < 1$. If $L(s,\pi)$ is entire and is free from zeros in the rectangle $[1-\delta/7, 1] \times [-(\log N)^2, (\log N)^2]$ and N is sufficiently large then*

$$\frac{1}{2\pi i}\int\limits_{(2)} \frac{L'(s+u,\pi)}{L(s+u,\pi)}\, x^s \Gamma(s)\, ds - \frac{L'(u,\pi)}{L(u,\pi)} \ll_n \frac{x^2}{\delta^2 N^{1/2}} + \frac{(\log N)^2}{\delta^3 x^{\delta/56}}$$

for $1 \leq u \leq 3/2$ and $x \geq 1$.

This corollary allows us to deduce our approximation to $\log L(1,\pi)$. Recall the notation $\lambda(m)$ for the coefficient of m^{-s} in the Dirichlet series expansion of $L(s,\pi)$.

PROPOSITION 2. *Let π be as above and let $0 < \delta < 1$. Suppose that $L(s,\pi)$ is free from zeros in the rectangle $[1-\delta/7, 1] \times [-(\log N)^2, (\log N)^2]$. If N is sufficiently large then for any $0 < \alpha < 112/\delta$,*

$$\log L(1,\pi) = \sum_{p \leq (\log N)^\alpha} \lambda(p) p^{-1} + O_{n,\alpha,\delta}(1).$$

Proof. Taking the logarithmic derivative of the Euler product gives

$$\frac{L'(s,\pi)}{L(s,\pi)} = -\sum_{i=1}^{n} \sum_{p} \log p \sum_{k=1}^{\infty} \alpha_i(p)^k p^{-ks}.$$

This together with Mellin inversion applied to $\Gamma(s)$ implies

$$\frac{1}{2\pi i} \int\limits_{(2)} \frac{L'(s+u,\pi)}{L(s+u,\pi)} x^s \Gamma(s)\, ds = -\sum_{i=1}^{n} \sum_{p} \log p \sum_{k=1}^{\infty} \alpha_i(p)^k p^{-ku} e^{-p^k/x}.$$

Substitution of this into the corollary and subsequent integration from $u = 1$ to $u = 3/2$ yields

$$\sum_{p} \lambda_\pi(p) p^{-1} e^{-p/x} - \log L(1,\pi) + \log L(3/2,\pi) \ll_n \frac{x^2}{\delta^2 N^{1/2}} + \frac{(\log N)^2}{\delta^3 x^{\delta/56}} + 1. \tag{19}$$

Here we have made use of the fact that $\lambda(p) = \sum_i \alpha_i(p)$.

If $y < x$ then

$$\sum_{p \leq y} p^{-1}(1 - e^{-p/x}) < 1, \qquad \sum_{p > x^2} p^{-1} e^{-p/x} \ll 1,$$

$$\sum_{y < p \leq x^2} p^{-1} e^{-p/x} = \log\left(\frac{2\log x}{\log y}\right) + O(1).$$

Furthermore, one can show that the formal logarithm of the Euler product converges, and this can be used to show that $\log L(3/2,\pi) \ll 1$. Thus (19) becomes

$$\sum_{p \leq y} \lambda_\pi(p) p^{-1} - \log L(1,\pi) \ll_n \frac{x^2}{\delta^2 N^{1/2}} + \frac{(\log N)^2}{\delta^3 x^{\delta/56}} + \log\left(\frac{2\log x}{\log y}\right) + 1.$$

We now take $x = (\log N)^{112/\delta}$, $y = (\log N)^\alpha$ with $0 < \alpha < 112/\delta$ to get the statement of the proposition. ∎

3. NUMBER FIELDS WITH LARGE CLASS NUMBERS

We begin this section with the computation of the L-functions attached to non-abelian cubic number fields and show that they come from automor-

phic representations. By constructing appropriate families of fields, we then apply the zero density estimate of Theorem 5 (specifically Corollary 3) to prove Theorems 1, 2 and 3.

3.1. Non-abelian cubic number fields. By a *non-abelian cubic number field* we will mean a field K of degree 3 over $\mathbb{Q}$ whose Galois closure $\widehat{K}$ has S_3 as its Galois group. Equivalently, $K = \mathbb{Q}(\alpha)$ where α is a root of a monic irreducible cubic polynomial $f \in \mathbb{Q}[x]$ with $\operatorname{disc}(f) \notin \mathbb{Q}^2$. Corresponding to the normal subgroup A_3 we have the associated quadratic subfield $L = \mathbb{Q}(\sqrt{\operatorname{disc}(f)})$ of $\widehat{K}$. The main result of this section is Lemma 7. It provides a factorization of the Dedekind zeta-function of a non-abelian cubic number field as a product of Riemann's zeta-function and the L-function of a cuspidal automorphic representation.

We begin by recalling the relationship between Artin L-functions and the Dedekind zeta function of a number field. Let k be a number field and let K be an extension of degree n with Galois closure $\widehat{K}$. Let $G = G(\widehat{K}/k)$ and $H = G(\widehat{K}/K)$. Letting G act by left multiplication on the coset space G/H gives rise to an n-dimensional complex (permutation) representation ϱ of G. This representation is induced from the trivial representation of H, and therefore

$$L(s, \widehat{K}/k, \varrho) = L(s, \widehat{K}/K, 1_H) = \zeta_K(s).$$

Taking $k = \mathbb{Q}$ and letting K be a non-abelian cubic number field we find that $\varrho \cong 1 \oplus \pi$, where π is the unique two-dimensional, irreducible representation of S_3, induced by any non-trivial character δ of A_3. Therefore we have

$$\begin{aligned} \zeta_K(s) &= L(s, \widehat{K}/\mathbb{Q}, \varrho) = L(s, \widehat{K}/\mathbb{Q}, 1)L(s, \widehat{K}/\mathbb{Q}, \pi) \\ &= \zeta(s)L(s, \widehat{K}/L, \delta). \end{aligned} \tag{20}$$

We aim to show that $L(s, \widehat{K}/\mathbb{Q}, s) = L(s, \widehat{K}/L, \delta)$ is automorphic, i.e. is the L-function of a cuspidal automorphic representation.

As A_3 is abelian, we know from class field theory that $L(s, \widehat{K}/L, \delta)$ is an entire Hecke L-function (see [17, Chapter VII]). In fact, if χ denotes the *Größencharakter* on L obtained by composing δ with the Artin symbol, then the conductor of χ is precisely the conductor $\mathfrak{m}$ of the extension $\widehat{K}/L$, χ is primitive and

$$L(s, \widehat{K}/L, \delta) = L(s, \chi).$$

This is in fact true for the completed L-functions as well. By Theorem 7.11 and Lemma 7.9 of [7], there is an automorphic representation $\pi(\chi)$ of GL(2) over $\mathbb{Q}$ so that

$$L(s, \chi) = L(s, \pi(\chi)),$$

this equality again holding at the level of completed L-functions as well. The infinite part of $\pi(\chi)$ depends only on the infinite part of χ (see [7, p. 144]), which depends only on the signature of L (see [17, p. 538]), hence only on the signature of K. Moreover, $\pi(\chi)$ is cuspidal provided there is no *Größencharakter* ψ of $\mathbb{Q}$ so that $\chi = \psi \circ N$ where N is the norm map

$$N : \mathbb{A}_L^\times \to \mathbb{A}_\mathbb{Q}^\times \tag{21}$$

defined by $N(\beta) = \alpha$, where for any place v of $\mathbb{Q}$,

$$\alpha_v = \prod_{w|v} N_{\mathbb{Q}_v}^{L_w}(\beta_w).$$

To show that this is indeed the case, choose any unramified prime p of $\mathbb{Q}$ whose Frobenius in $G(\widehat{K}/\mathbb{Q})$ is of order 3. The corresponding Euler factor in $L(s, \widehat{K}/\mathbb{Q}, \pi)$ is then

$$(1 + p^{-s} + p^{-2s})^{-1}.$$

That infinitely many such primes actually exist is a consequence of the Chebotarev density theorem. If $\mathfrak{P}$ and $\mathfrak{p}$ denote primes lying over p in $\widehat{K}$ and L, respectively, we have

$$1_L = \mathrm{Frob}(\mathfrak{P} \,|\, p)|_L = \mathrm{Frob}(\mathfrak{p} \,|\, p),$$

since the elements of order 3 fix L. Hence, p splits completely in L. If we assume that $\chi = \psi \circ N$ then we may also assume that p and $\mathfrak{p}$ are unramified for ψ and χ, respectively, since there are only finitely many primes ramified for each *Größencharakter*. It then follows that

$$\chi_\mathfrak{p}(\varpi_\mathfrak{p}) = \psi_p(N_{\mathbb{Q}_p}^{L_\mathfrak{p}}(\varpi_\mathfrak{p})) = \psi_p(p)$$

since $L_\mathfrak{p} = \mathbb{Q}_p$ ($\varpi_\mathfrak{p}$ is a prime element of $L_\mathfrak{p}$). As there are two primes of L lying over p, this would mean that the Euler factor corresponding to p in $L(s, \chi)$ is

$$(1 - \chi_{\mathfrak{p}_1}(\varpi_{\mathfrak{p}_1})N(\mathfrak{p}_1)^{-s})^{-1}(1 - \chi_{\mathfrak{p}_2}(\varpi_{\mathfrak{p}_2})N(\mathfrak{p}_2)^{-s})^{-1} = (1 - \psi_p(p)p^{-s})^{-2},$$

which cannot agree with $(1 + p^{-s} + p^{-2s})^{-1}$. Hence, it is not the case that $\chi = \psi \circ N$ and so $\pi(\chi)$ is cuspidal. This implies, in turn, that $L(s, \widehat{K}/L, \delta)$ is entire.

Finally, equation (20) allows us to deduce the functional equation satisfied by $L(s, \widehat{K}/\mathbb{Q}, \pi)$ from those satisfied by Dedekind's ζ-functions. Comparing this with Artin's functional equation we find that the conductor of π (and of the associated cuspidal automorphic representation) is $|\mathrm{disc}(K)|$.

Lemma 7. *Let K be a non-abelian cubic number field. Then*

$$\zeta_K(s) = \zeta(s)L(s, \widehat{K}/\mathbb{Q}, \pi)$$

where $L(s, \widehat{K}/\mathbb{Q}, \pi)$ is an entire Artin L-function of degree 2 and conductor

$|\mathrm{disc}(K)|$. *In fact,* $L(s, \widehat{K}/\mathbb{Q}, \pi)$ *is the* L*-function of a cuspidal automorphic representation of* $\mathrm{GL}(2)$ *over* $\mathbb{Q}$ *whose infinite part depends only on the signature of* K.

3.2. GRH and upper bounds for h. We now deduce the upper bounds provided by GRH for class numbers of non-abelian cubic number fields. This is fairly straightforward in the general cases (those corresponding to Theorems 1 and 2) but to get the sharper result for pure cubic fields we need to refine our argument.

LEMMA 8. *Let* K *be a cubic number field and let* $L(s, \widehat{K}/\mathbb{Q}, s)$ *be the* L*-function of Lemma* 7*. If this* L*-function satisfies GRH then*

$$L(1, \widehat{K}/\mathbb{Q}, \pi) \ll (\log\log|\mathrm{disc}(K)|)^2.$$

The implied constant is absolute.

Proof. By Lemma 7, under the assumption of GRH we may apply the approximation

$$\log L(1, \widehat{K}/\mathbb{Q}, \pi) = \sum_{p \le (\log|\mathrm{disc}(K)|)^{1/2}} \lambda(p) + O(1)$$

of Proposition 2, the implied constant of the error term being now absolute. We need to bound the coefficients $\lambda(p)$. Since π is two-dimensional,

$$|\lambda_\pi(p)| \le 2 \quad \text{for all } p.$$

Thus

$$\begin{aligned}\log L(1, \widehat{K}/\mathbb{Q}, \pi) &= \sum_{p \le (\log|\mathrm{disc}(K)|)^{1/2}} \lambda_\pi(p) + O(1)\\ &\le 2 \sum_{p \le (\log|\mathrm{disc}(K)|)^{1/2}} 1 + O(1) = 2\log\log\log|\mathrm{disc}(K)| + O(1),\end{aligned}$$

which follows from the asymptotics

$$\sum_{p \le x} p^{-1} = \log\log x + O(1). \tag{22}$$

The result is immediate. ∎

LEMMA 9. *Let* $K = \mathbb{Q}(\sqrt[3]{m})$, $m \in \mathbb{Z}$ *cube-free, be a pure cubic number field and let* $L(s, \widehat{K}/\mathbb{Q}, s)$ *be the* L*-function of Lemma* 7*. If this* L*-function satisfies GRH then*

$$L(1, \widehat{K}/\mathbb{Q}, \pi) \ll \log\log|\mathrm{disc}(K)|.$$

The implied constant is absolute.

Proof. As in the previous proof, the assumption of GRH yields the approximation

$$\log L(1,\widehat{K}/\mathbb{Q},\pi)=\sum_{p\leq(\log|d_K|)^{1/2}}\lambda(p)+O(1)$$

with an absolute implied constant. Our goal is to improve upon the bound $\lambda(p)\leq 2$ used above.

We claim that for odd primes p, $\lambda(p)\leq 2$ if $p\equiv 1 \pmod 3$ and $\lambda(p)\leq 0$ if $p\equiv -1 \pmod 3$. Assuming this for the moment, we find that

$$\begin{aligned}\log L(1,\widehat{K}/\mathbb{Q},\pi)&=\sum_{p\leq(\log|d|)^{1/2}}\lambda(p)p^{-1}+O(1)\\&\leq 2\sum_{\substack{p\leq(\log|d|)^{1/2}\\p\equiv 1 \pmod 3}}p^{-1}+O(1)=\log\log\log|d|+O(1).\end{aligned}$$

Here we have used the relation

$$\sum_{\substack{p\leq x\\p\equiv 1 \pmod 3}}p^{-1}=\frac{1}{2}\log\log x+O(1). \tag{23}$$

The statement of the lemma now follows.

It remains to prove the claim. Recall that for primes p unramified in $\widehat{K}$, $\lambda(p)$ is the trace of the Frobenius element in $G(\widehat{K}/\mathbb{Q})$ at p. As π is a 2-dimensional representation with real-valued character, we have $\lambda(p)\leq|\lambda(p)|\leq 2$ for unramified primes. So our only concern is with the ramified primes and those odd primes that are congruent to -1 mod 3.

Suppose p ramifies in $\widehat{K}$. As $[\widehat{K}:\mathbb{Q}]=6$, the ramification index must be 2, 3 or 6. If it is 2, then using multiplicativity of the ramification index in towers we find that p must ramify in the quadratic subfield $\mathbb{Q}(\sqrt{\operatorname{disc}(x^3-m)})=\mathbb{Q}(\sqrt{-3})$ of $\widehat{K}$. Hence $p=3$. If the ramification index is 3 or 6 then the inertia subgroup at p, $I_p\subset S_3$, must have order at least 3, and hence must contain A_3. However, there are no vectors fixed by the image of A_3 under π. Consequently, the Euler factor is trivial, and so $\lambda(p)=0$.

Now suppose p is unramified in $\widehat{K}$, $p\neq 2,3$. If p splits completely in $\widehat{K}$, then p must also split completely in the quadratic subfield $\mathbb{Q}(\sqrt{-3})$. This means that x^2+3 must split completely mod p, which by the law of quadratic reciprocity means that $p\equiv 1 \pmod 3$. Hence, if $p\equiv -1 \pmod 3$ is unramified in $\widehat{K}$ then the Frobenius at p is not trivial and consequently has non-positive trace, i.e. $\lambda(p)\leq 0$.

Having established the claim, the proof of the lemma is complete. ∎

It is now an easy matter to deduce upper bounds on h for non-abelian cubic number fields.

PROPOSITION 3. *Let K be a non-abelian cubic number field with discriminant d_K and class number h. Assume that the L-function of Lemma 7 satisfies GRH. If K is totally real (i.e. $d_K > 0$) then*

$$h \ll d_K^{1/2} \left(\frac{\log\log d_K}{\log d_K} \right)^2.$$

If K is complex (i.e. $d_K < 0$) then

$$h \ll |d_K|^{1/2} \frac{(\log\log|d_K|)^2}{\log|d_K|}.$$

If K is, in addition, pure cubic then

$$h \ll |d_K|^{1/2} \frac{\log\log|d_K|}{\log|d_K|}.$$

In each case, the implied constant is absolute.

Proof. We use the preceding lemmas and the class number formula, which in view of (20) becomes

$$h = \frac{w|d_K|^{1/2}}{2^{r_1}(2\pi)^{r_2} R_K} L(1, \widehat{K}/\mathbb{Q}, \pi).$$

As $r_1 \geq 1$, K has at least one real embedding. Therefore ± 1 are the only roots of unity in K, so that $w = 2$. As K has no non-trivial subfields, the regulator bound of Silverman [23] gives

$$R_K \gg (\log|d_K|)^{r_1+r_2-1}.$$

The proposition now follows easily. ∎

3.3. Proofs of the theorems. For non-abelian cubic K the class number formula and (20) give

$$h = \frac{|\mathrm{disc}(K)|^{1/2}}{2^{r_1-1}(2\pi)^{r_2} R} L(1, \widehat{K}/Q, \pi)$$

for the class number h of K. Here R is the regulator of K and, as above, r_1 and $2r_2$ are the numbers of real and complex embeddings of K, respectively. There are two possibilities for the values of the r_i. Either we have $r_1 = 3$ and $r_2 = 0$, or $r_1 = r_2 = 1$. These correspond to Theorems 1 and 2, respectively.

In order to prove our theorems we must construct families of cubic fields for which $L(1, \widehat{K}/Q, \pi)$ is large and R is small, relative to d. This turns out to be much simpler to do in the pure cubic case, so we prove Theorem 3 first to demonstrate the method.

Proof of Theorem 3. The following result will be crucial to our construction.

THEOREM 6 (Nagell). *For $D \in \mathbb{Z}$ the equation*

$$x^3 + Dy^3 = 1$$

has at most one solution in integers x, y different from zero. If D is not a cube and if x_1, y_1 is a solution then $x_1 + y_1\sqrt[3]{D}$ is either the fundamental unit of $\mathbb{Q}(\sqrt[3]{D})$ or its square; the latter can happen for only finitely many values of D.

For a proof of this theorem see [12, Chapter 3]. For $n \in \mathbb{Z}^+$ let $K_n = \mathbb{Q}(\sqrt[3]{n^3-1})$. If we write $n^3 - 1 = Dm^3$ with D cube-free, then as long as $D \neq 1$, K_n is a pure cubic number field with one real and two complex embeddings with the associated quadratic field $\mathbb{Q}(\sqrt{-3})$. If we write $D = ab^2$ with ab square-free then $d_n = \operatorname{disc}(K_n) = (-3)^k a^2 b^2$ where $k = 1$ or 3 (see [12] or [16]). According to Theorem 6, $n - m\sqrt[3]{D}$ is either the fundamental unit in K_n or its square. It follows immediately that the regulator, R_n, of K_n satisfies

$$R_n \ll |\log(n + m\sqrt[3]{D})|.$$

We will only need to consider the case in which $n^3 - 1 = D$ is cube-free. In this case the regulator bound above becomes

$$R_n \ll \log D \ll \log |d_n|. \tag{24}$$

We will need to know how often $n^3 - 1$ is cube-free when n is restricted to lie in an arithmetic progression. For $q \in \mathbb{Z}^+$ and $x > 0$ we let

$$A(x; q, a) = \{1 \leq n \leq x : n \equiv a \pmod q,\ n^3 - 1 \text{ cube-free}\}$$

and $N(x; q, a) = |A(x; q, a)|$. The next result gives an asymptotics for the size of this quantity.

LEMMA 10. *Suppose that $6 \mid q$ and $(a^3 - 1, q) = 1$. Then there is a constant $1 > c_q > 9/10$, whose value is given below, so that*

$$N(x; q, a) = c_q \frac{x}{q} + O(x^{3/4}(\log x)^2).$$

Proof. Clearly

$$N(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod q}} \sum_{r^3 \mid (n^3-1)} \mu(r) = \sum_{\substack{r \leq \sqrt[3]{n^3-1} \\ (r,q)=1}} \mu(r) \sum_{\substack{n \leq x \\ n^3 - 1 \equiv 0 \pmod{r^3} \\ n \equiv a \pmod q}} 1.$$

We may assume that $(r, q) = 1$ since the condition $(a^3 - 1, q) = 1$ implies that the inner sum on the right is empty otherwise. For any $0 < y < x$ the sum over $r > y$ is

$$\leq \sum_{y < r \leq x} \sum_{\substack{n \leq x \\ n^3 - 1 \equiv 0 \pmod{r^3}}} 1 \leq \sum_{s \leq x^3/y^3} \#\{(r, n) : n^3 - sr^3 = 1\} \ll \sum_{s \leq x^3/y^3} 1 \ll \frac{x^3}{y^3}$$

by Theorem 6. Consequently

$$N(x;q,a) = \sum_{\substack{r\le y\\(r,q)=1}} \mu(r) \sum_{\substack{n\le x\\ n^3-1\equiv 0 \,(\mathrm{mod}\, r^3)\\ n\equiv a \,(\mathrm{mod}\, q)}} 1 + O(x^3/y^3). \tag{25}$$

Now let $c(m)$ denote the number of solutions mod m to $n^3-1\equiv 0 \,(\mathrm{mod}\, m)$. Then c is multiplicative and

$$c(p^k) = 2 + \left(\frac{-3}{p}\right)$$

for $k\ge 1$, $p\ne 2,3$. Thus

$$\sum_{\substack{r\le y\\(r,q)=1}} \mu(r) \sum_{\substack{n\le x\\ n^3-1\equiv 0 \,(\mathrm{mod}\, r^3)\\ n\equiv a \,(\mathrm{mod}\, q)}} 1$$

$$= \sum_{\substack{r\le y\\(r,q)=1}} \mu(r)c(r)\left(\frac{x}{r^3q} + O(1)\right) = \frac{x}{q} \sum_{\substack{r\le y\\(r,q)=1}} \mu(r)c(r)r^{-3} + O\Big(\sum_{5\le r\le y} c(r)\Big)$$

$$= \frac{x}{q} \sum_{\substack{r=1\\(r,q)=1}}^{\infty} \mu(r)c(r)r^{-3} + O\Big(x\sum_{r>y} c(r)r^{-3}\Big) + O\Big(\sum_{5\le r\le y} c(r)\Big).$$

Since $c(r)\le 3^{\omega(r)}$ and

$$\sum_{r>y} 3^{\omega(r)}r^{-3} = O(y^{-2}(\log y)^2), \qquad \sum_{r\le y} 3^{\omega(r)} = O(y(\log y)^2),$$

we see that

$$N(x;q,a) = \frac{x}{q} \sum_{\substack{r=1\\(r,q)=1}}^{\infty} \mu(r)c(r)r^{-3} + O(xy^{-2}(\log y)^2) + O(y(\log y)^2) + O(x^3y^{-3}).$$

The result follows by taking $y = x^{3/4}$ and

$$c_q = \sum_{\substack{r=1\\(r,q)=1}}^{\infty} \mu(r)c(r)r^{-3} = \prod_{p\nmid q}\left(1 - \left(2 + \left(\frac{-3}{p}\right)\right)p^{-3}\right). \ \blacksquare$$

There are now two questions we must address. The first is how often we might have two integers m,n for which both $m^3-1=E$ and $n^3-1=D$ are cube-free and $K_n=K_m$. In this case, another application of Theorem 6 shows that for all sufficiently large values of m and n we must have $m-\sqrt[3]{E} =$

$n-\sqrt[3]{D}$, since both give the fundamental unit in K_n. Subtracting m from both sides and cubing we are led to the equation

$$(n-m)^3-(D-E)-3(n-m)^2\sqrt[3]{D}+3(n-m)\sqrt[3]{D^2}=0,$$

which implies that $m=n$. Hence, sufficiently large n for which n^3-1 is cube-free give rise to distinct K_n.

This brings us to our second question. Even though the fields K_n for cube-free n^3-1 are all distinct, might it be that the associated Artin L-functions $\zeta_{K_n}(s)/\zeta(s)$ coincide for different values of n? The next result shows that this cannot occur.

LEMMA 11. *Let L_i, $i=1,2$, be finite Galois extensions of $\mathbb{Q}$ both with Galois groups isomorphic to G. Let $\pi_i : G\to \mathrm{GL}_n(\mathbb{C})$, $i=1,2$, be faithful representations. Then $L(s,L_1/\mathbb{Q},\pi_1)=L(s,L_2/\mathbb{Q},\pi_2)$ implies that $L_1=L_2$.*

Proof. We will show that under the stated hypotheses the identity $L(s,L_1/\mathbb{Q},\pi_1)=L(s,L_2/\mathbb{Q},\pi_2)$ implies that the primes that split completely in L_1 also split completely in L_2. As the hypotheses are symmetric, it will then follow that a prime splits completely in L_1 if and only if it does in L_2. The conclusion is then a straightforward consequence of the Chebotarev density theorem (see p. 548 of [17]).

Writing both L-functions as Euler products and then as Dirichlet series, the hypothesis $L(s,L_1/\mathbb{Q},\pi_1)=L(s,L_2/\mathbb{Q},\pi_2)$ allows us to conclude that both functions have the same Euler factors. Suppose that p splits completely in L_1. Then the Frobenius $\sigma_{1,p}\in G(L_1/\mathbb{Q})$ of p is trivial so that

$$L_p(s,\pi_2)=L_p(s,\pi_1)=(\det(I-\pi_1(\sigma_{1,p})p^{-s}))^{-1}=(1-p^{-s})^{-n}.$$

Since π_2 is faithful, the only way $L_p(s,\pi_2)$ can have degree n is if p is unramified in L_2. Thus if $\sigma_{2,p}\in G(L_2/\mathbb{Q})$ is the Frobenius of p then

$$(1-p^{-s})^{-n}=L_p(s,\pi_2)=(\det(I-\pi_2(\sigma_{2,p})p^{-s}))^{-1}$$

so that the only eigenvalue of $\pi_2(\sigma_{2,p})$ is 1. Since the only unipotent matrix of finite order is I, we conclude that $\pi_2(\sigma_{2,p})=I$. The faithfulness of π_2 then implies that $\sigma_{2,p}$ is trivial so that p splits completely in L_2. ∎

We are now ready to prove Theorem 3. For each n for which n^3-1 is cube-free, associated to the field K_n we have the automorphic representation π_n of GL(2) over $\mathbb{Q}$ so that $\zeta_{K_n}(s)/\zeta(s)=L(s,\pi_n)$. For $x>1$ we let

$$y=\frac{1}{10}\log x,\qquad q=\prod_{p\le y}p.$$

Then $q\le x^{1/5}$. Lemma 10 shows that we have (for large x)

$$x^{4/5}\ll N(x;q,0)\le x. \tag{26}$$

For $n \in A(x;q,0)$, a direct comparison of the field and polynomial discriminants shows that the primes that divide the index of $\sqrt[3]{n^3-1}$ also divide $3(n^3-1)$. Consequently, for $p \mid q$, $p \geq 5$, the factorization of p in K_n can be determined by factoring $x^3-(n^3-1) \bmod p$. But for these primes, $n \equiv 0$, so we are reduced to factoring x^3+1. This polynomial splits completely if $p \equiv 1 \pmod 3$ and factors into linear and irreducible quadratic factors if $p \equiv -1 \pmod 3$. Thus, if $p \equiv 1 \pmod 3$ then p splits completely in $\widehat{K}_n$ and so has trivial Frobenius, and if $p \equiv -1 \pmod 3$ then p factors as a product of two distinct primes in K_n and consequently has a Frobenius of order 2.

Let $Q = 27x^6$ and

$$S(Q) = \{\pi_n : n \in A(x;q,0)\}.$$

We have shown that for sufficiently large x we have $|S(Q)| = N(x;q,0)$ so that

$$Q^{2/15} \ll |S(Q)| \ll Q^{1/6}.$$

By Corollary 3 we conclude that there is a $\sigma \in (1/2,1)$ so that for all sufficiently large Q there exist $\pi_n \in S(Q)$ so that $L(s,\pi_n)$ is zero-free in $[1-\sigma,1] \times [-(\log|d_n|)^2, (\log|d_n|)^2]$. Additionally, in the associated field K_n all primes $5 \leq p \leq (1/10)\log n$ split as described above. Since $(\log|d_n|)^{1/2} \leq (1/10)\log x$ for large x, applying Corollary 4 gives

$$\begin{aligned}\log L(1,\pi_n) &= \sum_{p \leq (\log|d_n|)^{1/2}} \lambda_{\pi_n}(p)p^{-1} + O(1) = 2 \sum_{\substack{p \leq (\log|d_n|)^{1/2} \\ p \equiv 1 \pmod 3}} p^{-1} + O(1) \\ &= \log\log\log|d_n| + O(1).\end{aligned}$$

This together with the bound (24) and the class number formula gives

$$h \gg |d_n|^{1/2} \frac{\log\log|d_n|}{\log|d_n|}$$

with an absolute implied constant. Theorem 3 now follows since as $Q \to \infty$ we must have $d_n \to \infty$ since $n \equiv 0 \pmod q$ and $q \to \infty$. ∎

Proof of Theorem 1. We now move on to the construction of an appropriate family of totally real fields. In fact, we will make use of the same family considered by Duke in his conditional version of this theorem. Let $f_t(x) = (x-t)(x-4t)(x-9t)-t$ and for $t \in \mathbb{Z}$ let K_t be the number field obtained by adjoining any fixed root of $f_t(x)$ to $\mathbb{Q}$. For square-free $t > 1$, $f_t(x)$ is an Eisenstein polynomial and hence K_t is a cubic number field. Moreover, since $\operatorname{disc}(f_t) = t^2(36t^2+1)(400t^2-27)$ is never a square, we conclude that $G(\widehat{K}_t/\mathbb{Q}) \cong S_3$. This family of cubic number fields is ideal for our purposes because the regulator of K_t can be effectively controlled. Indeed, if R_t is the regulator and d_t the discriminant of K_t, then by Proposition 1

of [4],

$$R_t \ll (\log d_t)^2. \tag{27}$$

By Lemma 7, for square-free t the Artin L-function $\zeta_{K_t}(s)/\zeta(s)$ is the L-function of an automorphic cuspidal representation π_t of $\mathrm{GL}(2)$ over $\mathbb{Q}$ with conductor d_t. We now seek to count how many distinct π_t there are. Let $A(x;q,a)$ denote the set

$$\{1 \le t \le x : t \equiv a \,(\mathrm{mod}\, q),\ t \text{ and } (36t^2+1)(400t^2-27) \text{ square-free}\}$$

and $N(x;q,a) = |A(x;q,a)|$. We have the following result concerning the size of this quantity.

LEMMA 12. *Let $C_0>0$ and suppose $210 \mid q$ and $(a(36a^2+1)(400a^2-27), q) = 1$. Then there is a constant C_1, depending only on C_0, so that if $x \ge \max\{C_0 q^4, C_1\}$ then*

$$N(x;q,a) \ge \frac{x}{8q}.$$

The proof of this lemma is similar to the proof of Lemma 10, but slightly more involved. We realize the set in question as the intersection of several other sets that are more amenable to estimation. These sets are described in the next three lemmas, all of which can be proven in the same manner as Lemma 2 of [5] (see also Lemma 1 of [15]).

LEMMA 13. *Let $q, a \in \mathbb{Z}^+$ satisfy $(a,q) = 1$ and let*

$$N_1(x;q,a) = \#\{1 \le t \le x : t \equiv a \ (\mathrm{mod}\, q),\ t \text{ square-free}\}.$$

Then for $x \ge 2$,

$$N_1(x;q,a) = c_{1,q}\,\frac{x}{q} + O(x^{1/2}),$$

where

$$c_{1,q} = \frac{6}{\pi^2}\prod_{p \mid q}(1-p^{-2})^{-1}$$

and the implied constant is absolute.

LEMMA 14. *Let $q, a \in \mathbb{Z}^+$ satisfy $(36a^2+1, q) = 1$ and suppose that $6 \mid q$. Let*

$$N_2(x;q,a) = \#\{1 \le t \le x : t \equiv a \ (\mathrm{mod}\, q),\ 36t^2+1 \text{ square-free}\}.$$

Then for $x \ge 2$,

$$N_2(x;q,a) = c_{2,q}\,\frac{x}{q} + O(x^{2/3}\log x),$$

where

$$c_{2,q} = \sum_{\substack{r \ge 1 \\ (r,q)=1}} \mu(r)c(r)r^{-2} = \prod_{p \nmid q}\left(1 - \left(1 + \left(\frac{-1}{p}\right)\right)p^{-2}\right)$$

and the implied constant is absolute.

LEMMA 15. *Let $q, a \in \mathbb{Z}^+$ satisfy $(400a^2 - 27, q) = 1$ and suppose that $30 \mid q$. Let*

$$N_3(x; q, a) = \#\{1 \le t \le x : t \equiv a \pmod q,\ 400t^2 - 27 \text{ square-free}\}.$$

Then for $x \ge 2$,

$$N_3(x; q, a) = c_{3,q}\,\frac{x}{q} + O(x^{2/3}\log x),$$

where

$$c_{3,q} = \prod_{p \nmid q}\left(1 - \left(1 + \left(\frac{3}{p}\right)\right)p^{-2}\right)$$

and the implied constant is absolute.

Proof of Lemma 12. Let $A_1(x; q, a)$ (resp. A_2, A_3) denote the set of integers considered in Lemma 13 (resp. 14, 15). For any $t \in \mathbb{Z}$ the only prime that can divide $(36t^2+1, 400t^2-27)$ is 7, since $100(36t^2+1) - 9(400t^2-27) = 7^3$. Since $7 \mid q$ the hypothesis $(a(36a^2+1)(400a^2-27), q) = 1$ implies that

$$A(x; q, a) = \bigcap_{i=1}^{3} A_i(x; q, a). \tag{28}$$

Since $210 \mid q$ it is easy to deduce from their definitions that

$$3/4 < c_{i,q} < 1 \tag{29}$$

for all i. Equations (28) and (29) together with Lemmas 13–15 now give

$$\begin{aligned} N(x; q, a) = |A(x; q, a)| &\ge \left[\frac{x}{q}\right] - \sum_{i=1}^{3}\left(\left[\frac{x}{q}\right] - N_i(x; q, a)\right) + O(1) \\ &= \frac{x}{q}\Big(1 - \sum_{i=1}^{3}(1 - c_{i,q})\Big) + O(x^{2/3}\log x) \\ &\ge \frac{x}{q}\left(1 - \frac{1}{4} - \frac{1}{4} - \frac{1}{4}\right) + O(x^{2/3}\log x) = \frac{x}{4q} + O(x^{2/3}\log x) \end{aligned}$$

and the result follows. ∎

Square-free t for which $(36t^2 + 1)(400t^2 - 27)$ is also square-free are important for the following reason. Primes dividing such t do not divide the index (see p. 61 of [16]), so we must have

$$d_t = \operatorname{disc}(f_t) = t^2(36t^2 + 1)(400t^2 - 27).$$

As a function of t, $\operatorname{disc}(f_t)$ is one-to-one. Hence distinct t will produce distinct d_t, and consequently distinct π_t. Moreover, since the index is 1, the factorization in K of any rational prime p can be determined by factoring $f_t(x) \bmod p$.

In the proof of Theorem 3 we controlled the size of the coefficients appearing in the approximation to $\log L(1,\pi_n)$ by controlling the splitting of certain primes in K_n, and this was done by knowing how the polynomial giving rise to K_n factored mod p. In order to implement this step in the current situation we need analogous information for the polynomial $f_t(x)$. We obtain this information by showing there are enough points on a certain curve over $\mathbb{Z}/p\mathbb{Z}$, provided p is sufficiently large. This requires the use of the Weil's bound (the Riemann hypothesis for curves over finite fields).

PROPOSITION 4. *Let $f_t(x)=(x-t)(x-4t)(x-9t)-t$. Then there is a $\kappa>0$ so that for all primes $p\geq\kappa$ there is at least one t_p mod p for which $f_{t_p}(x)$ splits completely in $\mathbb{F}_p[x]$.*

Proof. We reformulate the splitting of the polynomial in terms of splitting of primes in a certain number field, and reduce this problem to a certain curve having points over $\mathbb{F}_p$. For square-free $t\in\mathbb{Z}$ the polynomial $f_t(x)$ is Eisenstein and hence irreducible over $\mathbb{Q}$. For such t let α_t be a root of $f_t(x)$ and let $K_t=\mathbb{Q}(\alpha_t)$. Fix a prime p. As long as $p\nmid\operatorname{disc}(f_t)=t^2(400t^2-27)(36t^2+1)$ the splitting of p in K_t is controlled by the splitting of $f_t(x)$ in $\mathbb{F}_p[x]$. Thus, for such p we see that $f_t(x)$ splits completely in $\mathbb{F}_p[x]$ if and only if p splits completely in K_t. However, a prime splits completely in a number field if and only if it splits completely in its Galois closure. Thus, provided $p\nmid t^2(400t^2-27)(36t^2+1)$, the polynomial $f_t(x)$ will split completely in $\mathbb{F}_p$ if and only if p splits completely in $\widehat{K}_t$, the Galois closure of K_t.

The polynomial

$$h_t(x)=x^6-294t^2d(t)x^4+21609t^4d(t)^2x^2-t^2(286t^2+27)^2d(t)^3,$$

where $d(t)=t^2(400t^2-27)(36t^2+1)$, has the property that any of its roots generate $\widehat{K}_t$. Consequently, if $p\nmid\operatorname{disc}(h_t)$ (which is an integral polynomial in t of degree 120) then p splits completely in $\widehat{K}_t$ if and only if $h_t(x)$ splits completely in $\mathbb{F}_p[x]$. However, as $\widehat{K}_t$ is Galois over $\mathbb{Q}$, the inertial degrees of all primes in $\widehat{K}_t$ lying over p are the same. Hence, all of the irreducible factors of $h_t(x)$ in $\mathbb{F}_p[x]$ have the same degree (and each occurs with multiplicity 1 as the condition $p\nmid\operatorname{disc}(h_t)$ ensures that p does not ramify in $\widehat{K}_t$). Therefore, $h_t(x)$ splits completely in $\mathbb{F}_p[x]$ if and only if $h_t(x)$ has at least one root in $\mathbb{F}_p$.

Combining the arguments of the preceding paragraphs, we see that for a given t mod p, if $p\nmid\operatorname{disc}(f_t)\operatorname{disc}(h_t)$ then $f_t(x)$ splits completely in $\mathbb{F}_p[x]$ if and only if $h_t(x)$ has a root in $\mathbb{F}_p$ (the splitting completely condition depends only on the residue class of t mod p, and as every residue class mod p contains infinitely many square-free integers, the square-free condition on t may be dropped). The result will follow if we can show that for all

sufficiently large p the curve $0 = h_t(x) = F(x,t)$ has points over $\mathbb{F}_p$ satisfying $p \nmid \operatorname{disc}(f_t)\operatorname{disc}(h_t)$.

Since $\operatorname{disc}(f_t)\operatorname{disc}(h_t)$ is a polynomial of fixed degree, the number of points on the curve $0 = F(x,t)$ with $p \mid \operatorname{disc}(f_t)\operatorname{disc}(h_t)$ is bounded by a constant, N. As long as $p \neq 2, 3$, $F(x,t)$ is absolutely irreducible over $\mathbb{F}_p$, and the Riemann hypothesis for curves over finite fields (see also [22, p. 92, Theorem 1A]) implies that the number of points on $F(x,t) = 0$ over $\mathbb{F}_p$ tends to infinity with p. Hence there is a $\kappa > 0$ such that for $p \geq \kappa$ the curve $F(x,t) = 0$ has more than N points over $\mathbb{F}_p$ and the result follows. ∎

We now conclude the proof of Theorem 1. Let $\kappa > 0$ and t_p for $p \geq \kappa$ be as in Proposition 4. If $p = 2,\ 3,\ 5$ or 7 is less than κ, then we choose t_p so that $\operatorname{disc}(f_{t_p}) \not\equiv 0 \pmod p$. Given x, let

$$y = \frac{1}{8}\log x, \qquad q = 210 \prod_{\kappa \leq p \leq y} p.$$

Choose $a \equiv t_p \pmod p$ for $\kappa \leq p \leq y$ and $p = 2, 3, 5, 7$. Then all primes $\kappa \leq p \leq y$ split completely in K_t for $t \in A(x; q, a)$. Let $C > 0$ be chosen so that $\operatorname{disc}(f_t) \leq Ct^6$ for $t \geq 1$. Finally, let $Q = Cx^6$ and $S(Q) = \{\pi_t : t \in A(x; q, a)\}$. Then $|S(Q)| = N(x; q, a)$. We have $(a(36a^2+1)(400a^2-27), q) = 1$ since $\operatorname{disc}(f_a) \not\equiv 0 \pmod p$ for any $p \mid q$. Since $q \ll x^{1/4}$ we may apply Lemma 12 to conclude that

$$Q^{1/8} \ll |S(Q)| \ll Q^{1/6}$$

for all sufficiently large x. Again applying Corollary 3 we conclude that there exists a $\sigma \in (1/2, 1)$ so that for all large Q there exist $\pi_t \in S(Q)$ so that $L(s, \pi_t)$ is zero-free in $[1-\sigma, 1] \times [-(\log d_t)^2, (\log d_t)^2]$. Moreover, in the associated totally real fields K_t all primes $\kappa \leq p \leq y$ split completely, so that applying Corollary 4 we get

$$\begin{aligned}\log L(1, \pi_t) &= \sum_{p \leq (\log d_t)^{1/2}} \lambda_{\pi_t}(p) p^{-1} + O(1) = 2 \sum_{\kappa \leq p \leq (\log d_t)^{1/2}} p^{-1} + O(1) \\ &= 2 \log\log\log d_t + O(1).\end{aligned}$$

Here we have used the fact that $(\log d_t)^{1/2} \leq (1/8)\log x$ for large x. Equation (27) and the class number formula now imply that

$$h \gg d_t^{1/2} \left(\frac{\log\log d_t}{\log d_t} \right)^2$$

with an absolute implied constant. The proof of Theorem 1 is now completed by noting that we can arrange that $t \to \infty$ (and hence $d_t \to \infty$) as $Q \to \infty$, since otherwise we would contradict the last statement in Corollary 3. ∎

Proof of Theorem 2. We begin again with the construction of fields. For $t \in \mathbb{Z} \setminus \{0\}$ let $f_t(x) = x^3 + tx^2 + t$ and let $K_t = \mathbb{Q}(\alpha_t)$ where α_t is the unique

real root of $f_t(x)$ (f_t has exactly one real root as $\operatorname{disc}(f_t) = -t^2(4t^2+27) < 0$). If $t > 1$ is square-free then f_t is an Eisenstein polynomial, and hence K_t is a complex cubic field. In order to bound the regulator in K_t we will need the following lemmas. The first provides us with a unit in K_t and the second allows us to compare the regulator to this unit.

LEMMA 16. *Let $t \in \mathbb{Z} \setminus \{0\}$. Then $\alpha_t^3/t \in \mathcal{O}_{K_t}^\times$.*

Proof. Since $f_t(\alpha_t) = 0$ it follows that

$$\frac{\alpha_t^3}{t} = -\alpha_t^2 - 1 \in \mathbb{Z}[\alpha_t] \subset \mathcal{O}_{K_t}.$$

It also follows that

$$\left(\frac{\alpha_t^3}{t}\right)^2 \frac{(\alpha_t+t)^3}{t} = \frac{(f_t(\alpha_t)-t)^3}{t^3} = -1.$$

Moreover

$$(\alpha_t+t)^3 \equiv \alpha_t^2(\alpha_t+t) \pmod t = f_t(\alpha_t) - t \equiv 0 \pmod t$$

so that $(\alpha_t+t)^3/t \in \mathcal{O}_{K_t}$ as well. ∎

LEMMA 17. *Let $K \subset \mathbb{R}$ be a complex cubic number field. If $\varepsilon \in \mathcal{O}_K^\times$, $\varepsilon \neq \pm 1$, then*

$$\operatorname{Reg} K \leq \big|\log|\varepsilon|\big|.$$

Proof. Suppose first that ε is the fundamental unit in K. As $\varepsilon \in \mathbb{R}$ it follows that its Galois conjugates are of the form β, $\overline{\beta}$ and satisfy $\pm 1 = N(\varepsilon) = \varepsilon|\beta|^2$. Thus

$$\operatorname{Reg} K = \left|\det\begin{pmatrix} \log|\varepsilon| & 2\log|\beta| \\ 1/3 & 2/3 \end{pmatrix}\right| = \frac{1}{3}\left|\log\frac{|\varepsilon|^2}{|\beta|^2}\right| = \big|\log|\varepsilon|\big|.$$

In general, however, we will have $\varepsilon = \pm(\varepsilon')^n$ with ε' the fundamental unit. Thus

$$\big|\log|\varepsilon|\big| \geq \big|\log|\varepsilon'|\big| = \operatorname{Reg} K. \ ∎$$

Putting these two lemmas together we find that for square-free t,

$$\operatorname{Reg} K_t \leq \big|\log|\alpha_t^3/t|\big| \ll \log|\operatorname{disc}(f_t)|. \tag{30}$$

This follows from the fact that $t = -\alpha_t^3/(1+\alpha_t^2)$.

As in the proof of Theorem 1, we will need to know how often one of the factors of $\operatorname{disc}(f_t)$ is square-free when t is restricted to lie in an arithmetic progression.

LEMMA 18. *Let $q, a \in \mathbb{Z}^+$ satisfy $(4a^2+27, q) = 1$ and suppose that $6 \mid q$. Let*

$$N_4(x; q, a) = \#\{1 \leq t \leq x : t \equiv a \pmod q,\ 4t^2+27 \text{ square-free}\}.$$

Then for $x \geq 2$,

$$N_4(x; q, a) = c_{4,q} \frac{x}{q} + O(x^{2/3} \log x)$$

where

$$c_{4,q} = \sum_{\substack{r \geq 1 \\ (r,q)=1}} \mu(r) c(r) r^{-2} = \prod_{p \nmid q} \left(1 - \left(1 + \left(\frac{-3}{p}\right)\right) p^{-2}\right)$$

and the implied constant is absolute.

As before, we refer the reader to Lemma 2 of [5] or Lemma 1 of [15] for the method of proof.

Combining this with Lemma 13 above and proceeding as in the proof of Lemma 12 we deduce the next result.

LEMMA 19. *Let* $C_0 > 0$ *and suppose* $6 \mid q$ *and* $(a(4a^2 + 27), q) = 1$. *Let*

$$N(x; q, a) = \#\{1 \leq t \leq x : t \equiv a \pmod q,\ t \text{ and } 4t^2 + 27 \text{ square-free}\}.$$

Then there exists a constant C_1, *depending only on* C_0, *such that if* $x \geq \max\{C_0 q^4, C_1\}$ *then*

$$N(x; q, a) \geq \frac{x}{16q}.$$

The formalism of the rest of the proof of Theorem 2 is now totally analogous to that of Theorem 1, and we will therefore be content to provide just a sketch. For square-free $t > 1$, K_t is a complex cubic number field and primes dividing t do not divide the index of ε_t in $\mathcal{O}_{K_t}$ (see p. 61 of [16]). Consequently, if moreover $4t^2 + 27$ is square-free it follows that $d_t = \operatorname{disc}(K_t) = \operatorname{disc}(f_t) = -t^2(4t^2 + 27)$. For such t we also have the associated automorphic representation π_t so that $\zeta_{K_t}(s)/\zeta(s) = L(s, \pi_t)$. As before, the Riemann hypothesis for curves over finite fields can be used to show that there is a $\kappa > 0$ so that for all $p \geq \kappa$ there exists $t_p \pmod p$ for which $f_{t_p}(x)$ splits completely in $(\mathbb{Z}/p\mathbb{Z})[x]$. The argument is exactly the same as before, but this time uses the polynomial

$$h_t(x) = x^6 - 6t^2 d(t) x^4 + 9t^4 d(t)^2 x^2 - t^2(2t^2 + 27)^2 d(t)^3$$

where $d(t) = \operatorname{disc}(f_t) = -t^2(4t^2 + 27)$.

Now for $x > 1$ let

$$y = \frac{1}{8} \log x, \qquad q = 6 \prod_{\kappa \leq p \leq y} p$$

so that $q \ll x^{1/4}$. Choose $C > 0$ so that $t^2(4t^2 + 27) \leq Ct^4$ for all t and let $Q = Cx^4$. Finally, choose a so that $a \equiv t_p \pmod p$ for all $\kappa \leq p \leq y$ (and $a \equiv 1 \pmod{2, 3}$ if $2, 3 < \kappa$) and let

$$S(Q) = \{\pi_t : 1 \leq t \leq x,\ t \equiv a \pmod q,\ t \text{ and } 4t^2 + 27 \text{ square-free}\}.$$

Then $|S(Q)| = N(x;q,a)$ so that by Lemma 19 we have

$$Q^{3/16} \ll |S(Q)| \ll Q^{1/4}.$$

Theorem 2 now follows from Corollaries 3 and 4, the class number formula and equation (30).

Acknowledgements. My thanks to my Ph.D. advisor, Bill Duke, for suggesting this problem to me. I also thank the referee for providing many useful comments and suggestions, especially the much simplified proof of Lemma 12 given here.

References

[1] D. Bump, *Automorphic Forms and Representations*, Cambridge Stud. Adv. Math. 55, Cambridge Univ. Press, 1998.

[2] J. W. Cogdell, *Analytic theory of L-functions for* GL_n, in: An Introduction to the Langlands Program, J. Bernstein and S. Gelbart (eds.), Birkhäuser, 2003, 197–228.

[3] H. Davenport, *Multiplicative Number Theory*, Grad. Texts in Math. 74, Springer, 2000.

[4] W. Duke, *Extreme values of Artin L-functions and class numbers*, Compos. Math. 136 (2003), 103–115.

[5] —, *Number fields with large class groups*, in: Number Theory (CNTA VII), CRM Proc. Lecture Notes 36, Amer. Math. Soc., 2004, 117–126.

[6] W. Duke and E. Kowalski, *A problem of Linnik for elliptic curves and mean value estimates for automorphic representations*, Invent. Math. 139 (2000), 1–39.

[7] S. S. Gelbart, *Automorphic Forms on Adele Groups*, Ann. Math. Stud. 83, Princeton Univ. Press, 1975.

[8] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford Univ. Press, 1960.

[9] M. N. Huxley, *The Distribution of Prime Numbers*, Oxford Univ. Press, 1972.

[10] —, *The large sieve inequality for algebraic number fields. III. Zero-density results*, J. London Math. Soc. (2) 3 (1971), 233–240.

[11] H. Iwaniec and P. Sarnak, *Perspectives on the analytic theory of L-functions*, Geom. Funct. Anal. 2000, Special Volume, Part II, 705–741.

[12] W. J. LeVeque, *Topics in Number Theory*, Vol. II, Addison-Wesley, 1956.

[13] J. E. Littlewood, *On the class number of the corpus* $P(\sqrt{-k})$, in: Collected Papers of J. E. Littlewood, Vol. II, Oxford Univ. Press, 1982, 920–934.

[14] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. 227, Springer, 1971.

[15] H. L. Montgomery and P. J. Weinberger, *Real quadratic fields with large class number*, Math. Ann. 225 (1977), 173–176.

[16] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, PWN – Polish Scientific Publishers, 1973.

[17] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[18] H. Rademacher, *On the Phragmén–Lindelöf theorem and some applications*, in: Collected Papers of Hans Rademacher, Vol. II, The Massachusetts Institute of Technology, 1974, 496–509.

[19] H. Rademacher, *Topics in Analytic Number Theory*, Grundlehren Math. Wiss. 169, Springer, 1973.

[20] D. Ramakrishnan, *Modularity of the Rankin–Selberg L-series, and multiplicity one for* SL(2), Ann. of Math. 152 (2000), 45–111, 903.

[21] Z. Rudnick and P. Sarnak, *Zeros of principal L-functions and random matrix theory. A celebration of John F. Nash, Jr.*, Duke Math. J. 81 (1996), 269–322.

[22] W. M. Schmidt, *Equations over Finite Fields*, Lecture Notes in Math. 536, Springer, 1976.

[23] J. H. Silverman, *An inequality relating the regulator and the discriminant of a number field*, J. Number Theory 19 (1984), 437–442.

Department of Mathematics
6188 Bradley Hall
Dartmouth College
Hanover, NH 03755-3551, U.S.A.
E-mail: daileda@dartmouth.edu

Received on 24.6.2005
and in revised form on 16.8.2006 (5015)