Canadian Mathematical Society
Conference Proceedings
Volume 7 (1987)

A VARIANT OF THE BOMBIERI-VINOGRADOV THEOREM

M. Ram Murty[1] and V. Kumar Murty[2]

INTRODUCTION. Let a,q, be positive integers with $1 \leq a < q$, $(a,q) = 1$. Denote by $\pi(x,q,a)$ the number of primes $p \leq x$, satisfying $p \equiv a \pmod q$. We know from the classical result of Dirichlet [3, ch. 22] that

$$\pi(x,q,a) \sim \frac{1}{\phi(q)} \pi(x)$$

where ϕ is Euler's totient function. Estimates of the size of the error term

$$\pi(x,q,a) - \frac{1}{\phi(q)} \pi(x)$$

are of great importance in applications. It is known that the Riemann Hypothesis for all Dirichlet L-functions implies that

$$\pi(x,q,a) = \frac{1}{\phi(q)} \pi(x) + O(x^{\frac{1}{2}} (\log qx))$$

The celebrated theorem of Bombieri [1] and Vinogradov [30] shows unconditionally that this estimate holds on the average. It states that for any $A > 0$, there is a $B = B(A) > 0$ so that

$$(0.1) \qquad \sum_{q \leq Q} \max_{y \leq x} \max_{(a,q)=1} \left|\pi(y,q,a) - \frac{1}{\phi(q)} \pi(y)\right| \ll \frac{x}{(\log x)^A}$$

where $Q = x^{\frac{1}{2}} (\log x)^{-B}$ and we write $f \ll g$ to mean $|f/g|$ is bounded.

The purpose of this paper is to prove a variant of this theorem where a non-abelian splitting condition is introduced. More precisely, let K be a number field. Suppose that it is Galois over $\mathbb{Q}$ with group $G = \mathrm{Gal}(K/\mathbb{Q})$. Let C be a conjugacy class in G. With a and q as above, denote by $\pi_C(x,q,a)$ the number of primes $p \leq x$ which are unramified in K, which satisfy $(p,K/\mathbb{Q}) = C$, and $p \equiv a \pmod q$. (Here, $(p,K/\mathbb{Q})$ is the Artin symbol of p in G). From the

1 Research partially supported by NSERC grant U0237
2 Research partially supported by NSERC grant U0373

Chebotarev density theorem [12], we know that

$$\pi_C(x,q,a) \sim \delta(C,q,a)\ \pi(x)$$

for some density $\delta(C,q,a) \geq 0$. Let ζ_q denote a primitive q-th root of unity. If K and $\mathbb{Q}(\zeta_q)$ are disjoint, then

$$\delta(C,q,a) = \frac{|C|}{|G|} \cdot \frac{1}{\phi(q)} \tag{0.2}$$

(For any finite set S, we write $|S|$ for its cardinality). Our aim is to prove, for any A > 0, an estimate of the form

$$\sum_{q \leq Q} \max_{(a,q)=1} \max_{y \leq x} |\pi_C(y,q,a) - \delta(C,q,a)\ \pi(y)| \ll \frac{x}{(\log x)^A} \tag{0.3}$$

with $Q = x^{\alpha - \epsilon}$, $\epsilon > 0$ and the sum is over q such that $K \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$. Here, α will depend on G and C and satisfy

$$\alpha \geq \min\left(\frac{2}{|G|}, \frac{1}{2}\right)$$

For a precise description of α, see §7. (We remark that with more care, we can even take $Q = x^{\alpha}(\log x)^{-B}$, $B = B(A) > 0$). If we assume (AC) that the L-functions attached to all abelian twists of the non-trivial irreducible characters of G are entire, then we can prove (0.3) with a larger value of α. Indeed, set

$$\delta = \max_{\chi \neq 1} |\chi(1) - 2|$$

where the maximum is over the irreducible characters of G. Then, assuming (AC), we can take $\alpha = \min(\frac{1}{\delta}, \frac{1}{2})$. In particular, if $\delta \leq 2$, we have (0.3) with $\alpha = \frac{1}{2}$. The groups G which satisfy $\delta \leq 2$ can be classified (using results of the type [5, theorem 24.6]).

Our motivation for studying estimates of the form (0.3) comes from the observation that non-abelian analogues of the Bombieri-Vinogradov theorem would have interesting arithmetical consequences. For example, let $\pi_q(x)$ denote the number of primes $p \leq x$ which split completely in the Kummer extension $L_q = \mathbb{Q}(\zeta_q, \sqrt[q]{2})$. It is well-known [19] that an estimate of the form

$$\sum_{q \leq Q} |\pi_q(x) - \frac{1}{q(q-1)}\pi(x)| \ll \frac{x}{(\log x)^2}$$

(with Q about $x^{1/2}$) would suffice to imply Artin's primitive root conjecture.

Let f be a cusp form of weight $k \geq 2$ for the congruence subgroup $\Gamma_0(N)$, $N \geq 1$. Suppose that f is an eigenform for the Hecke operators T_p,

($p \nmid N$, p prime). Write $f = \sum_{n \geq 1} a_n e^{2\pi i n z}$ for the Fourier expansions at $i\infty$.

For each prime ℓ, let $\pi_\ell(x)$ denote the number of primes $p \leq x$ satisfying $a_p \equiv 0 \pmod{\ell}$. It is well-known [20] that there is a Galois extension $K_\ell/\mathbb{Q}$ such that the condition $a_p \equiv 0 \pmod{\ell}$ is equivalent to the condition that p has a certain splitting type in K. An estimate of the form

$$\sum_{\ell \leq Q} |\pi_\ell(x) - \frac{1}{\ell}\pi(x)| \ll \frac{x}{(\log x)^2}$$

with Q a power of exp((log x)/(log log x)) would suffice to imply the normal order (and even the statistical distribution) of the number of prime divisors of a_p and a_n. It would also imply lower bounds for a_p valid for a set of p of density 1 (cf. [20], [21]).

The need for an estimate of the precise form (0.3) arose in the problem of determining which rings of S-integers in a number field K possess a Euclidean algorithm. The connection between the two problems is explained in detail in [9]. For other variants of the Bombieri-Vinogradov theorem, see Huxley [10], Wilson [32] and Motohashi [17].

Besides the original argument of Bombieri [1], there are proofs of (0.1) given by Gallagher [6] and Vaughan [31]. Moreover, much work has been done recently by Bombieri, Iwaniec and Friedlander [3] to prove (0.1) with a larger value of Q. Our approach to (0.3) will be an adaptation of the methods of Gallagher [6] and Ramachandra [23]. The paper is self-contained, and in general, we attempt to make explicit the dependence of constants on the number field K. The first three sections contain various preliminaries. The proof of the main theorem is given in sections 4-6, and the last section contains an application to the problem of the least prime whose Artin symbol lies in a given conjugacy class.

Table of Contents

Notation If K is a number field, n_K denotes the degree $[K:\mathbb{Q}]$ of $K/\mathbb{Q}$ and d_K denotes the absolute value of the discriminant of $K/\mathbb{Q}$.

1. Character Sums

1.1 Let G be a finite group and C a conjugacy class of G. Let $\delta_C : G \to \{0,1\}$ denote the characteristic function of C. In terms of characters, we have

$$\delta_C = \frac{|C|}{|G|} \sum_{\eta} \bar{\eta}(g_C)\eta$$

where g_C is any element of C, and the sum is over all irreducible characters η of G. Let H be any subgroup of G such that $H \cap C \neq \phi$. Take $g_C \in H \cap C$ and let C_H denote the conjugacy class of g_C in H. Then

$$\delta_C = \lambda \operatorname{Ind}_H^G \delta_{C_H}$$

where $\delta_{C_H} : H \to \{0,1\}$ is the characteristic function of C_H and $\lambda = |C| \cdot |H| / |G| \cdot |C_H|$. Now, let χ be any character of G. Then by Mackey's induction theorem [24, p. 57] we have

$$\delta_C \otimes \chi = \lambda \operatorname{Ind}_H^G (\delta_{C_H} \otimes \chi|_H) \tag{1.1.1}$$

1.2 Suppose G = Gal(L/F) with $L \supseteq F$, where L, F are number fields. Let k be a non-negative integer, and let ξ be a class function. Define

$$\psi_k(L/F, \xi, x) = \frac{1}{k!} \sum_{Nv^m \leq x} (\log Nv)\left(\log \frac{x}{Nv^m}\right)^k \xi(\sigma_v^m) \tag{1.2.1}$$

where the sum is over powers of places v of F unramified in L, σ_v denotes a Frobenius element at v and N denotes $\text{Norm}_{F/\mathbb{Q}}$. It is convenient to include ramified primes also in this sum. This is done by extending ξ in the usual way. Let v be a place of F and w a place of L above v. Let D_w and I_w denote the decomposition and inertia group at w (respectively). Then $\sigma_w \in D_w/I_w$. We set

$$\xi(\sigma_v^m) = \frac{1}{|I_w|} \sum \xi(g)$$

where the sum is over all elements $g \in D_w$ whose image in D_w/I_w is σ_w^m. A different choice of w conjugates D_w and I_w and thus leaves the above sum unchanged. With this, we let $\tilde{\psi}_k(L/F, \xi, x)$ denote the sum in (1.2.1), now taken over all v^m, v a place of F and $Nv^m \leq x$. We have

$$\psi_k(L/F,\xi,x) = \tilde{\psi}_k(L/F,\xi,x) + O\left(\|\xi\| \frac{(\log x)^{k+1}}{k!}\left\{\frac{1}{|G|}\log d_L + n_F x^{\frac{1}{2}}\right\}\right) \tag{1.2.2}$$

where $\|\xi\| = \sup_{g \in G} |\xi(g)|$. The proof is almost the same as in

Serre [25, Proposition 7] and is omitted.

1.3 We can write the class function ξ as a linear combination

$$\xi = \sum a_\eta \eta$$

where η ranges over the irreducible characters of G and $a_\eta \in \mathbb{C}$. Let $L(s,\eta)$ denote the Artin L-series attached to η. Then

$$\tilde{\psi}_k(L/F, \xi, x) = \frac{1}{2\pi i} \sum_\eta a_\eta \int_{(2)} \frac{L'}{L}(s,\eta) \frac{x^s}{s^{k+1}} ds$$

where the integration is on the line $\mathrm{Re}(s) = 2$.

1.4 Let K be a Galois extension of $\mathbb{Q}$, and $1 \leq a$, $q \in \mathbb{Z}$, $a < q$, $(a,q) = 1$. We use the above observations with $L = K(\zeta_q)$, where ζ_q is a primitive q-th root of 1, and $F = \mathbb{Q}$. Suppose that $K \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$. Then we know that $G = \mathrm{Gal}(K(\zeta_q)/\mathbb{Q})$ has a splitting

$$G \simeq \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) .$$

Every element g of G can thus be written as (g_1, g_2) in an obvious way. Every conjugacy class of G is of the form (C_1, C_2) where C_1 is a class of $\mathrm{Gal}(K/\mathbb{Q})$ and C_2 a class of $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. Fix an identification $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \simeq (\mathbb{Z}/q)^\times$. We use the same letter to denote the image of a under $\mathbb{Z} \to \mathbb{Z}/q$. Let $\delta_{a,q}: G \to \{0,1\}$ be defined by $\delta_{a,q}(g) = \begin{cases} 1 \text{ if } g_2 = a \\ 0 \text{ otherwise} \end{cases}$.

Fix a conjugacy class C in $\mathrm{Gal}(K/\mathbb{Q})$ and let $\xi = \xi(C,a,q) = \delta_C \otimes \delta_{a,q}$. Thus ξ is the characteristic function of the class $(C,\{a\})$. Explicitly, we have

$$\psi_k(K(\zeta_q)/\mathbb{Q},\xi,x) = \frac{1}{k!} \sum_{\substack{p^m \leq x \\ p \nmid d_K \\ p^m \equiv a(q) \\ \sigma_{p^m} \in C}} (\log p)(\log(\frac{x}{p^m}))^k$$

Our aim is to show that given $A > 0$, there is a suitable choice of Q_1 so that

$$(1.4.1) \qquad \sum_{q \leq Q_1}{}' \max_{(a,q)=1} \max_{y \leq x} |\psi_0(K(\zeta_q)/\mathbb{Q}, \xi(C,a,q),y) - \delta(C,a,q)y| << \frac{x}{(\log x)^A}$$

The prime on the summation indicates that we range only over those q satisfying $K \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$.

1.5 We transform the sum of (1.4.1) in several ways. The first observation is that it suffices to prove an estimate with ψ_0 replaced by ψ_k for some large k. We sketch the argument as it is similar to Gallagher [6]. Write $\psi_k(x)$ for $\psi_k(K(\zeta_q)/\mathbb{Q}, \xi(C,a,q),x)$ for simplicity. Define $\tilde{\psi}_k(x)$ in a similar way. Then, we have

$$\psi_{k+1}(x) = \int_1^x \psi_k(t) \cdot \frac{dt}{t}$$

and for any $\alpha > 0$, we have by the mean value theorem,

$$\frac{1}{\alpha}\int_{e^{-\alpha}x}^{x} \psi_k(t)\frac{dt}{t} \leq \psi_k(x) \leq \frac{1}{\alpha}\int_x^{e^{\alpha}x} \psi_k(t)\frac{dt}{t}.$$

Thus

$$\max_{y\leq x}|\psi_k(y) - \delta(C,a,q)y| \ll \frac{1}{\alpha}\max_{y\leq e^{\alpha}x}|\psi_{k+1}(y) - \delta(C,a,q)y| + \alpha\delta(C,a,q)x.$$

Choosing $\alpha = (\log x)^{-A/2}$, we deduce that

$$\sum_{q\leq Q_1}{}' \max_{(a,q)=1}\max_{y\leq x}|\psi_k(y) - \delta(C,a,q)y|$$

$$\ll (\log x)^{A/2}\sum_{q\leq Q_1}{}' \max_{(a,q)=1}\max_{y\leq e^{\alpha}x}|\psi_{k+1}(y) - \delta(C,a,q)y| + \frac{x\log Q_1}{(\log x)^{A/2}}.$$

Moreover, (1.2.2) shows that replacing ψ with $\tilde{\psi}$ on the right introduces an additional contribution of

$$\ll \frac{(\log x)^{k+2+\frac{A}{2}}}{(k+1)!} Q_1\left\{\frac{1}{n_K}\log d_K + \log q + x^{\frac{1}{2}}\right\}$$

1.6 We have a decomposition

$$\tilde{\psi}_k(x) = \tilde{\psi}_k(K(\zeta_q)/\mathbb{Q}, \xi(C,a,q),x) = \frac{1}{\phi(q)}\sum\overline{\chi}(a)\,\psi_k(K(\zeta_q)/\mathbb{Q}, \delta_C\otimes\chi, x)$$

where the sum is over charcters χ of $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. The trivial character contributes a term

$$\frac{1}{\phi(q)}\tilde{\psi}_k(K(\zeta_q)/\mathbb{Q}, \delta_C, x) = \frac{1}{\phi(q)}\tilde{\psi}_k(K/\mathbb{Q}, \delta_C, x)$$

From the effective Chebotarev density theorem [12], we have

$$\tilde{\psi}_k(K/\mathbb{Q}, \delta_C, x) = \frac{|C|}{n_K} x + O(x^\beta \frac{1}{k!}(\log x)^k)$$

$$+ O(x \frac{1}{k!}(\log x)^k \exp(-c\, n_K^{-\frac{1}{2}} (\log x)^{\frac{1}{2}}))$$

where c is a positive absolute constant and β is a possible Siegel zero of $K/\mathbb{Q}$. (The implied constants are absolute). Using the bound

$$\beta < \max(1 - \frac{1}{4 \log d_K}, 1 - \frac{c_1}{d_K^{1/n_K}})$$

of Stark [28] we deduce that for $\log Q_1 << \log x$,

(1.6.1)
$$\sum_{q \leq Q_1}' \max_{(a,q)=1} \max_{y \leq x} |\tilde{\psi}_k(y) - \delta(C,a,q)y|$$

$$= \sum_{q \leq Q_1} \frac{1}{\phi(q)} \sum_{\chi \neq 1} \max_{y \leq x} |\tilde{\psi}_k(K(\zeta_q)/\mathbb{Q}, \delta_C \otimes \chi, y)|$$

$$+ O(\frac{1}{k!} x(\log x)^{k+1} \exp(-cn_K^{-\frac{1}{2}} (\log x)^{\frac{1}{2}}))$$

(Here the implied constant depends on the field K).

It is convenient to include only primitive characters $\chi \pmod q$ (ie. characters which do not factor through $Gal(\mathbb{Q}(\zeta_{q_1})/\mathbb{Q})$ for some proper divisor q_1 of q). This is easily done by observing that if $\chi \pmod q$ is induced by character $\chi_1 \pmod{q_1}$ with $q_1 | q$, $q_1 \neq q$, then

$$|\tilde{\psi}_k(K(\zeta_q)/\mathbb{Q}, \delta_C \otimes \chi, x) - \tilde{\psi}_k(K(\zeta_q)/\mathbb{Q}, \delta_C \otimes \chi_1, x)|$$

$$\leq \frac{1}{k!} \sum_{p^m | q/q_1} (\log p)(\log \frac{x}{p^m})^k << \frac{1}{k!} (\log x)^k \log(\frac{q}{q_1})$$

Moreover, we have

$$\sum_{\substack{q_1 | q \\ q \leq Q_1}} \frac{1}{\phi(q)} << \frac{\log Q_1}{\phi(q_1)}$$

Using $\log Q_1 << \log x$, we deduce that the first term on the right hand side of (1.6.1) is

$$(1.6.2) \qquad \ll (\log x) \sum_{1<q\le Q_1}{}' \max_{y\le x} \frac{1}{\phi(q)} \sum_{\chi}{}^{*} |\tilde{\psi}_k(K(\zeta_q)/\mathbb{Q}, \delta_C \otimes \chi, y)|$$

$$+ O(\frac{1}{k!} Q_1 (\log x)^{k+1})$$

where the asterisk on the sum indicates that we only include primitive $\chi \pmod q$.

1.7 Now let H' be a subgroup of $G_1 = \mathrm{Gal}(K/\mathbb{Q})$ with $H' \cap C \neq \phi$. Set $H = H' \times \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. Using (1.1.1), (1.3) and the invariance of L-series under induction, we deduce that in the above sum, we may replace

$$\tilde{\psi}_k(K(\zeta_q)/\mathbb{Q}, \delta_C \otimes \chi, y) \quad \text{by} \quad \lambda \cdot \tilde{\psi}_k(K(\zeta_q)/M, \delta_{C_{H'}} \otimes \chi|_H, y)$$

where $\lambda = |C|\cdot|H'| / |C_{H'}| \cdot |G_1|$ and M is the subfield of $K(\zeta_q)$ fixed by H. (Note that M is also the subfield of K fixed by H' and so does not depend on q). Moreover, we have

$$\tilde{\psi}_k(K(\zeta_q)/M, \delta_{C_{H'}} \otimes \chi|_H, y) = \frac{|C_{H'}|}{|H'|} \sum_{\omega} \bar{\omega}(g_C)\, \tilde{\psi}_k(K(\zeta_q)/M, \omega \otimes \chi, y)$$

where ω ranges over the irreducible characters of H' and $g_C \in H' \cap C$. We deduce from these observations that

$$(1.7.1) \qquad \sum_{1<q\le Q_1}{}' \frac{1}{\phi(q)} \max_{y\le x} \sum_{\chi}{}^{*} |\tilde{\psi}_k(K(\zeta_q)/\mathbb{Q}, \delta_C \otimes \chi, y)|$$

$$\le \frac{|C|}{|G_1|} |H'| \max_{\omega} \left\{ \sum_{1<q\le Q_1}{}' \frac{1}{\phi(q)} \max_{y\le x} \sum_{\chi}{}^{*} |\tilde{\psi}_k(K(\zeta_q)/M, \omega \otimes \chi, y)| \right\}$$

Finally, decomposing the interval $(1,Q_1]$ into $O(\log Q_1)$ intervals of the form $(\frac{Q}{2}, Q]$, we find that the expression in large parentheses is

$$\ll (\log Q_1) \max_{Q\le Q_1} \max_{y\le x} \frac{\log\log Q}{Q} \sum_{1<q\le Q} \sum_{\chi}{}^{*} |\tilde{\psi}_k(K(\zeta_q)/M, \omega \otimes \chi, y)|$$

Summarizing the discussion of the previous paragraphs, we have proved the following.

<u>(1.8) Proposition</u>

$$\sum_{q\le Q_1}{}' \max_{(a,q)=1} \max_{y\le x} |\psi_k(K(\zeta_q)/\mathbb{Q}, \xi(C,a,q), y) - \delta(C,a,q)y|$$

$$\ll \frac{|C|}{|G_1|} |H'| \ell^2 \cdot \ell_2 \max_{\omega} \max_{Q\le Q_1} \max_{y\le x} \frac{1}{Q} \sum_{1<q\le Q} \sum_{\chi}{}^{*} |\tilde{\psi}_k(K(\zeta_q)/M, \omega \otimes \chi, y)| + E$$

where $\ell = \log x$, $\ell_2 = \log\log x$ and

$$E \ll \frac{1}{k!}(\log x)^{k+1} x \exp(-cn_K^{-\frac{1}{2}}(\log x)^{\frac{1}{2}}) + \frac{1}{k!}(\log x)^{k+1} Q_1$$

$$+ \frac{1}{k!}(\log x)^{k+1} Q_1 \{\frac{1}{n_K}\log d_K + \log q + x^{\frac{1}{2}}\} .$$

We recall that

$$\tilde{\psi}_k(L(\zeta_q)/M, \omega \otimes \chi, x) = \frac{1}{k!} \sum_{Nv^m \leq x} (\log Nv)(\log \frac{x}{Nv^m})^k \omega(\sigma_v^m)\, \chi(Nv^m)$$

where v runs over primes of M.

1.9 We observe that if μ and ν are two irreducible characters of a finite Galois group $G = Gal(L/F)$, and F_μ, F_ν are their Artin conductors then the Artin conductor $F_{\mu\otimes\nu}$ of $\mu \otimes \nu$ satisfies $F_{\mu\otimes\nu} \mid F_\mu^{\nu(1)} F_\nu^{\mu(1)}$ (cf. for example, Martinet [16, p. 80]). This fact will be used repeatedly.

2. Phragmén-Lindelöf Theorem

2.1 We write $s = \sigma + it$. Let $f(s)$ be a function regular in a vertical strip $c \leq \sigma \leq d$ and satisfying in this strip a growth condition

$$|f(s)| \ll e^{|s|^\delta} \tag{2.1.1}$$

for a positive constant δ. Suppose that there are positive constants C, D, α, β and a constant Q satisfying

$$\begin{aligned} |f(c+it)| &\leq C|Q+c+it|^\alpha \\ |f(d+it)| &\leq D|Q+d+it|^\beta \end{aligned} \tag{2.1.2}$$

The Phragmén-Lindelöf theorem gives an estimate for $f(s)$ when $c \leq \sigma \leq d$. We shall need it in the following sharp form given by Rademacher [22].

2.2 Proposition For $c \leq \sigma \leq d$, and f satisfying (2.1.1) and (2.1.2), we have

$$|f(s)| \leq (C\,|Q+s|^\alpha)^{\frac{d-\sigma}{d-c}} (D\,|Q+s|^\beta)^{\frac{\sigma-c}{d-c}}$$

2.3 We apply this in the study of a general class of Dirichlet series. Let $L(s)$ be a Dirichlet series satisfying the following properties. First, we require

(i) $L(s) = \prod_p L_p(s)$ for $\sigma > 1$, where L_p is a polynomial in p^{-s}. The product is over all finite primes. Denote by m_p the degree of L_p in p^{-s}.

(ii) There is a positive integer $d = d(L)$ with $m_p \leq d$ for all p and $m_p = d$ for all but finitely many p.

Let us write

$$L_p(s) = \prod_{i=1}^{m_p} (1 - \pi_i\, p^{-s})^{-1}$$

where $\pi_i = \pi_{i,p} \in \mathbb{C}$ and $|\pi_i| = 1$. Define

$$L_p^v(s) = \prod_{i=1}^{m_p} (1 - \bar{\pi}_i\, p^{-s})^{-1}$$

and set $L^v(s) = \prod_p L_p^v(s)$. Let A be a positive real number and a,b non-negative integers with $a + b \le d$. Set

$$\Lambda(s) = A^{s/2} (\pi^{-s/2} \Gamma(\tfrac{s}{2}))^a (\pi^{-(s+1)/2} \Gamma(\tfrac{s+1}{2}))^b L(s)$$

$$\Lambda^v(s) = A^{s/2} (\pi^{-s/2} \Gamma(\tfrac{s}{2}))^a (\pi^{-(s+1)/2} \Gamma(\tfrac{s+1}{2}))^b L^v(s) .$$

Suppose that

(iii) $\Lambda(s)$ and $\Lambda^v(s)$ have an analytic continuation to the entire complex plane except possibly for a pole at $s = 0$ or 1.

(iv) $\Lambda(s) = w\, \Lambda^v(1 - s)$ with $w \in \mathbb{C}$ $|w| = 1$.

2.4 Proposition Under the assumtions (i) - (iv) above, we have for $0 \le \sigma \le 1$,

$$|L(\sigma + it)| \le (A(|t| + 2)^d)^{\frac{1-\sigma}{2}} (\log[A(|t| + 2)^d])^d$$

PROOF From (i), we see that for $\in > 0$,

$$|L(1 + \in + it)| \le \zeta(1 + \in)^d$$

where ζ denotes the usual Riemann zeta function. By (iv) and Stirling's formula,

$$|L(-\in + it)| \le A^{\frac{1}{2}+\in} (|t| + 2)^{d(\frac{1}{2}+\in)} \zeta(1 + \in)^d$$

By Proposition (2.2), we have

$$|L(\sigma + it)| \le \zeta(1 + \in)^d (A(|t| + 2)^d)^{\frac{1-\sigma+\in}{2}}$$

valid for $-\frac{1}{2} \le -\in \le \sigma \le 1+\in \le \frac{3}{2}$. Choose $\in = (\log[A(|t| + 2)^d])^{-1}$.

The result follows on noting that $\zeta(1+\in) \ll \in^{-1}$.

We note two interesting consequences of Proposition (2.4). These will not be needed in the remainder of the paper.

2.5 Let f be a holomorphic cusp form of integral weight k for a congruence subgroup of $SL_2(\mathbb{Z})$. Write L(s,f) for its associated L-series. For any Dirichlet character χ, $f \otimes \chi$ is the twist of f by χ. The Shimura correspondence [26] attaches to f a cusp form F of weight $\frac{1}{2}(k+1)$ with the following property. Write

$$F(z) = \sum_{n=1}^{\infty} C(n)e^{2\pi inz}$$

for the Fourier expansion at ∞. There is a constant Ω such that for any fundamental discriminant D of a quadratic field.

$$C(|D|)^2 = \Omega|D|^{\frac{k-1}{2}} L(\tfrac{k}{2}, f \otimes \chi)$$

where $\chi(n) = (\frac{D}{n})$ is the Kronecker symbol. The analog of the Ramanujan conjecture (cf. the discussion in Goldfeld-Hoffstein-Patterson [8, p. 154]) is

$$C(|D|) \ll_\in |D|^{\frac{k-1}{4}+\in}$$

for every $\in > 0$. We see from Proposition (2.4) that

$$C(|D|) \ll |D|^{\frac{k}{4}} (\log |D|)^2 \tag{2.5.1}$$

This is slightly sharper than the estimate $|D|^{\frac{k}{4}+\in}$ stated in [8, p. 154]) Iwaniec [11] has recently obtained a significant improvement of (2.5.1) where the exponent $\frac{k}{4}$ is replaced by $\frac{k}{4} - \frac{1}{28}$.

2.6 The second application is to the residue of the Dedekind zeta function. Let $L/\mathbb{Q}$ be a number field. Landau [14] showed that there is a constant $C > 0$ so that

$$\operatorname*{res}_{s=1} \zeta_L(s) \leq C^{n_L} (\log d_L)^{n_L - 1} \tag{2.6.1}$$

Siegel [27] obtained sharp values for C. We are interested in the power of $\log d_L$. Suppose there is a subfield $K \subseteq L$ satisfying

(i) L/K is Galois

(ii) for every non-trivial character of Gal(L/K), the associated Artin L-series is entire.

(For example, K = L satisfies these conditions).

Then

$$\frac{\operatorname{res}_{s=1} \zeta_L(s)}{\operatorname{res}_{s=1} \zeta_K(s)} \leq \prod_{\chi} (\log A_\chi + \chi(1) \log 2)^{\chi(1)}$$

where $A_\chi = d_K^{\chi(1)} \operatorname{Norm}_{L/Q}(F_\chi)$, and χ ranges over the non-trivial irreducible characters of Gal(L/K). By the conductor-discriminant formula,

$$\log(d_L/d_K) = \sum_{\chi} \chi(1) \log A_\chi$$

Thus, we get (using the arithmetic mean-geometric mean inequality and (2.6.1)),

$$\operatorname{res}_{s=1} \zeta_L(s) \leq C^{n_K} (\log d_K)^{n_K - 1} 2^n \prod_{\chi}(\log A_\chi)^{\chi(1)}$$

$$\leq C^{n_K} \cdot 2^n (\log d_K)^{n_K - 1} \left(\frac{\log(d_L/d_K)}{n}\right)^n$$

where $n = \sum \chi(1)$. This is an improvement over (2.6.1) whenever K is a proper subfield of L. In particular, if $L/\mathbb{Q}$ is Galois, we deduce that for some absolute constant $C > 0$.

$$\operatorname{res}_{s=1} \zeta_L(s) \leq C^{n_L} \cdot (\log d_L)^{\frac{n_L}{2}+1}$$

by taking a subfield K of L such that L/K is cyclic of prime order.

<u>2.7 Remark</u> It would be of interest to know whether the power of the logarithm in Proposition (2.4) can be reduced.

3. Zero-free regions

<u>3.1</u> Let L/F be a Galois extension of number fields and χ be an abelian character of $G = \operatorname{Gal}(L/F)$. We shall need a zero-free region for the Artin L-series $L(s,\chi)$. Let F_χ denote the Artin conductor of χ and set $A_\chi = d_F N_{F/Q}(F_\chi)$.

<u>3.2 Lemma</u> For $\sigma > 1$,

$$-\operatorname{Re} \frac{\zeta_F'}{\zeta_F}(s) < \operatorname{Re}\left(\frac{1}{s} + \frac{1}{s-1}\right) + \frac{1}{2} \log \left(\frac{d_F}{2^{2r_2} \pi^{n_F}}\right) + \frac{r_1}{2} \operatorname{Re}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right) + r_2 \operatorname{Re}\frac{\Gamma'}{\Gamma}(s)$$

where $n_F = r_1 + 2r_2$ and r_1 is the number of real embeddings of F. This is part of Lemma 3 in Stark [28].

3.3 Lemma For $\sigma > 1$, and non-trivial χ,

$$-\mathrm{Re}\, \frac{L'}{L}(s,\chi) < C_1 \mathcal{L} - \sum_{\rho} \mathrm{Re}\left(\frac{1}{s-\rho}\right)$$

where $C_1 > 0$ is an absolute constant, the sum is over all zeroes ρ of $L(s,\chi)$ with $0 < \mathrm{Re}\,\rho < 1$, and $\mathcal{L} = \frac{1}{2}\log A_\chi + n_F\,(|t| + 2)$.

Proof We just sketch the proof. Set

$$\Lambda(s,\chi) = A_\chi^{s/2}\, \mathbf{\Gamma}(s)\, L(s,\chi)$$

where $\mathbf{\Gamma}(s)$ is a product of n_F Γ-factors. We have the functional equation

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

with $w \in \mathbb{C}$, $|w| = 1$, and also the Hadamard factorization

$$\Lambda(s,\chi) = e^{a+bs} \prod_{\rho} \left(1-\frac{s}{\rho}\right) e^{s/\rho}$$

where $a = a(\chi)$, $b = b(\chi)$ are complex numbers and the product is over all zeroes ρ of $\Lambda(s,\chi)$ (equivalently, over all zeroes ρ of $L(s,\chi)$ with $0 < \mathrm{Re}\,\rho < 1$). By logarithmically differentiating both sides and using $\mathrm{Re}\, b = -\sum_{\rho} \mathrm{Re}(1/\rho)$, we find

$$-\mathrm{Re}\, \frac{L'}{L}(s,\chi) = \frac{1}{2}\log A_\chi - \sum \mathrm{Re}\left(\frac{1}{s-\rho}\right) + \mathrm{Re}\frac{\mathbf{\Gamma}'}{\mathbf{\Gamma}}(s)$$

For $\sigma > 1$,

$$\mathrm{Re}\frac{\mathbf{\Gamma}'}{\mathbf{\Gamma}}(s) \ll n_F \log(|t| + 2)$$

by Stirling's formula. This proves the lemma.

3.4 Proposition There is an absolute constant $C > 0$ such that $L(s,\chi)$ has at most one zero in the region

$$1 - \frac{C}{\mathcal{L}} \leq \sigma \leq 1$$

If this zero β exists, then it is real and simple and χ is a character of order 1 or 2.

Proof For $\sigma > 1$, we have for non-trivial χ,

$$(3.4.1)\quad 3\left(-\frac{L'}{L}(\sigma,\chi_0)\right) + 4\left(-\mathrm{Re}\frac{L'}{L}(\sigma+it,\chi)\right) + \left(-\mathrm{Re}\frac{L'}{L}(\sigma+2it,\chi^2)\right) \geq 0$$

where χ_0 is the principal character mod F_χ. Then,

$$-\frac{L'}{L}(\sigma,\chi_0) = \sum_{(\mathfrak{p},F_\chi)=1} (\log N\mathfrak{p})(N\mathfrak{p})^{-n s} \leq -\frac{\zeta_F'}{\zeta_F}(\sigma)$$

and by lemma (3.2), we deduce that for $\sigma = 1 + \frac{C_2}{\mathcal{L}}$,

$$-\frac{L'}{L}(\sigma,\chi_0) < \frac{1}{\sigma-1} + C_3\mathcal{L} \tag{3.4.2}$$

where C_2, C_3 are positive absolute constants. Next, for $\sigma > 1$,

$$\mathrm{Re}\left(\frac{1}{s-\rho}\right) = \frac{\sigma-\beta}{|s-\rho|^2} \geq 0$$

and so, Lemma (3.3) implies that for any zero ρ of $L(s,\chi)$ with $0 < \mathrm{Re}\,\rho < 1$,

$$-\mathrm{Re}\,\frac{L'}{L}(s,\chi) < C_1\mathcal{L} - \mathrm{Re}\left(\frac{1}{s-\rho}\right) \tag{3.4.3}$$

Suppose that χ^2 is not the principal character. Let χ_1 be the primitve character inducing χ^2 mod F_χ. Then

$$\left|\frac{L'}{L}(s,\chi^2) - \frac{L'}{L}(s,\chi_1)\right| \leq \sum_{\gamma|F_\chi} \frac{(\log N\gamma)(N\gamma)^{-\sigma}}{(1-(N\gamma)^{-\sigma})} \leq \mathcal{L}$$

combining this with (3.4.3),

$$-\mathrm{Re}\,\frac{L'}{L}(s,\chi^2) < C_4\mathcal{L} \tag{3.4.4}$$

Using (3.4.2)-(3.4.4) in (3.4.1), we deduce that if $\rho = \beta + i\gamma$, $\sigma = 1 + \frac{C_2}{\mathcal{L}}$ and $t = \gamma$, then

$$\frac{3}{\sigma-1} - \frac{4}{\sigma-\beta} + C_5\mathcal{L} \geq 0$$

ie

$$\beta \leq 1 + \frac{C_2}{\mathcal{L}} - \frac{4\,C_2}{(3+C_2C_5)\mathcal{L}}$$

Choosing $C_2 < 1/C_5$ shows that for an absolute $C > 0$,

$$\beta \leq 1 - \frac{C}{\mathcal{L}}$$

If χ^2 is principal, Lemma (3.2) implies that

$$-\mathrm{Re}\,\frac{L'}{L}(s,\chi^2) < \mathrm{Re}\left(\frac{1}{\sigma-1+it}\right) + C_3$$

We deduce that $\beta < 1 - \frac{C}{\mathcal{L}}$ if $|\gamma| \geq C_6/\mathcal{L}$ for some $C_6 > 0$. The usual arguments show that if $|\gamma| < C_6/\mathcal{L}$, then $\gamma = 0$, and that there is at most one such zero and that it is simple (cf. [4, pp. 92-93]).

3.5 Finally, we need an analogue of Siegel's theorem giving a bound for the possible real zero in Proposition (3.4). We adapt a method of Stark [28]. Thus, let χ be a real character of G of conductor F_χ. Let N/F be the extension defined by it. We suppose that χ is not the trivial character, so that N is quadratic over F. As before, we write $A = A_\chi = d_F(NF_\chi)$. We may view χ as a quadratic Hecke character of F.

3.6 The Brauer-Siegel theorem implies that as we range over a set of quadratic Hecke characters χ of F with $NF_\chi \to \infty$, we have

$$L(1,\chi) > \frac{C(\varepsilon)}{C_1^{n_F} (\log d_F)^{n_F}} \cdot \frac{1}{A_\chi^{\varepsilon}} \tag{3.6.1}$$

where $\varepsilon > 0$ is arbitrary, $C_1 > 0$ is an absolute constant, and $C(\varepsilon) > 0$ depends only on ε. Indeed, if we let R denote the residue of $\zeta_N(s)$ at $s = 1$ and r the residue of $\zeta_F(s)$ at $s = 1$, then $R = L(1,\chi)r$. The Brauer-Siegel theorem states that for any $\varepsilon > 0$,

$$R > C(\varepsilon)/d_N^{\varepsilon} .$$

Also, we have by (2.6.1) that

$$r \leq (C_1 \log d_F)^{n_F} .$$

Since $d_N = d_F^2 \, NF_\chi$, we conclude that (3.6.1) holds. This implies that the exceptional zero of Proposition (3.4) satisfies

$$\beta \leq 1 - \frac{c(\varepsilon)}{(C_1 \log d_F)^{n_F} A_\chi^{\varepsilon}} .$$

This can be refined using the following result of Stark [28, Lemma 10].

3.7 Lemma Suppose there is a sequence of fields

$$Q = M_0 \subset M_1 \subset M_2 \subset \dots \subset M_t = M$$

such that for $1 \leq i \leq t$, M_i/M_{i-1} is normal. Suppose there is a real β in the range

$$1 - \frac{1}{16 \log d_M} \leq \beta < 1$$

such that $\zeta_M(\beta) = 0$. Then there is a quadratic field $S \subseteq M$ with $\zeta_S(\beta) = 0$. We shall use this to prove the following.

3.8 Proposition Let $\varepsilon > 0$ and χ as in (3.5). Let J denote the normal closure of F over $\mathbb{Q}$. Then

$$\beta \leq \max\left(1 - \frac{C(\varepsilon)}{(d_J^2 A)^{\varepsilon}} , 1 - \frac{1}{16 n_J \log(d_J^2 A)} \right)$$

Proof We may assume that β satisfies

$$1 - \frac{1}{16 n_J \log(d_J^2 A)} \leq \beta < 1 . \tag{3.8.1}$$

Then, the composition JN is Galois over N and so, by a well-known result of Aramata-Brauer, $\zeta_{JN}(\beta) = 0$. Moreover,

$$d_{JN} \leq d_J^{2n_F} d_N^{n_J} \leq (d_J^2 A)^{n_J} \tag{3.8.2}$$

and so (3.8.1) implies that

$$1 - \frac{1}{16 \log d_{JN}} \leq \beta < 1 .$$

Finally, $JN \supseteq J \supseteq \mathbb{Q}$ is a normal tower, and so, by Lemma (3.7), there is a quadratic subfield S of JN with $\zeta_S(\beta) = 0$. By the classical Siegel theorem (see for example [4, section 21] or Goldfeld [7]) there is a constant $C(\varepsilon) > 0$ so that

$$\beta \leq 1 - \frac{C(\varepsilon)}{d_S^{\varepsilon}}$$

Now,

$$d_{JN} \geq d_S^{n_{JN}/2} \geq d_S^{n_J/2} .$$

Hence,

$$\beta \leq 1 - \frac{C(\varepsilon)}{d_{JN}^{2\varepsilon/n_J}} .$$

Combining this with (3.8.2) and replacing ε by $\varepsilon/2$ proves the result.

4. Gallagher's Method

4.1 Suppose we have a Dirichlet series

$$L(s) = \sum a_n n^{-s}$$

for $\sigma = \mathrm{Re}(s) > 1$. For any Dirichlet character χ, set

$$L(s,\chi) = \sum a_n \chi(n) n^{-s}$$

(We are thus departing from the notation used in earlier sections for Artin L-functions). Suppose that all the $L(s,\chi)$ satisfy the hypotheses (i)-(iv) of (2.3). Write A for the conductor of L(s) and A_χ for the conductor of $L(s,\chi)$. We assume that

(4.1.1) $$A_\chi \ll Aq^d$$

if q = conductor of χ. Let us also write

$$\frac{1}{L(s,\chi)} = \sum b_n \chi(n) n^{-s}$$

$$-\frac{L'}{L}(s,\chi) = \sum \Lambda(n)\, c_n\, \chi(n) n^{-s}$$

for $\sigma > 1$. Let $z > 0$ be a parameter to be specified later. For any Dirichlet character χ, define

$$F_z(s,\chi) = \sum_{n \le z} \Lambda(n)\, \chi(n)\, c_n n^{-s}$$

$$G_z(s,\chi) = \sum_{n > z} \Lambda(n)\, \chi(n)\, c_n n^{-s}$$

$$M_z(s,\chi) = \sum_{n \le z} b_n\, \chi(n)\, n^{-s}$$

We use an identity of Gallagher as modified by Bombieri [2]

$$(4.1.1) \qquad -\frac{L'}{L}(s,\chi) = G_z(1 - LM_z) + F_z(1 - LM_z) - L'M_z$$

4.2 Let k be a positive integer and define for any $C > 1$,

$$\psi_k(x,\chi) = \frac{1}{2\pi i} \int_{(C)} -\frac{L'}{L}(s,\chi) \frac{x^s}{s^{k+1}}\, ds$$

(Again, this is a slight departure from the notation of section 1). Our aim in the next few paragraphs will be to obtain estimates for

$$\sum_{1 < q \le Q} \sum_{\chi}{}^{*} |\psi_k(x,\chi)|$$

Here, the inner sum ranges over primitive characters $\chi (\mathrm{mod}\ q)$.
We have from (4.1.1)

$$(4.2.1) \qquad \psi_k(x,\chi) = \frac{1}{2\pi i} \int_{(C)} G_z(1 - LM_z) \frac{x^s}{s^{k+1}}\, ds \; +$$

$$+ \frac{1}{2\pi i} \int_{(C)} F_z(1 - LM_z) \frac{x^s}{s^{k+1}}\, ds - \frac{1}{2\pi i} \int_{(C)} L'M_z \frac{x^s}{s^{k+1}}\, ds$$

4.3 Since F_z and M_z are Dirichlet polynomials and L, L' are analytic for all s, we can move the line of integration in the second and third terms of the above expression, into the critical strip. Using the inequality $2|ab| \le |a|^2 + |b|^2$ repeatedly, and taking $C = 1 + \frac{1}{\log x}$, $k > \frac{d}{4}$, we obtain

$$(4.3.1) \qquad \sum_{1 < q \le Q} \sum_{\chi}{}^{*} |\psi_k(x,\chi)| \ll x \sum_{q \le Q} \sum_{\chi}{}^{*} \int_{(C)} (|G_z|^2 + |1 - LM_z|^2) \frac{|ds|}{|s|^{k+1}}$$

$$+ x^{\frac{1}{2}} \sum_{q \le Q} \sum_{\chi}{}^{*} \int_{(\frac{1}{2})} (1 + |F_z|^2 + |M_z|^2 + |F_z M_z|^2 + |L|^2 + |L'|^2) \frac{|ds|}{|s|^{k+1}}$$

Most of these terms can be handled by the large sieve inequality of Gallagher. We briefly review how this is done.

4.4 Lemma (Gallagher) If $\sum |A_n| < \infty$ and $T \geq 1$, we have

$$\sum_{1 < q \leq Q} \sum_{\chi}^{*} \int_{-T}^{T} \Big| \sum_{n=1}^{\infty} A_n \chi(n) n^{it} \Big|^2 dt \ll \sum_{n=1}^{\infty} |A_n|^2 (n + Q^2 T)$$

(see for example, Bombieri [2, p. 30]).

4.5 Using this, we find that

$$\sum_{1 < q \leq Q} \sum_{\chi}^{*} \int_{C-i}^{C+i} |G_z|^2 \frac{|ds|}{|s|^{k+1}} \ll \sum_{n > z} \frac{\Lambda(n)^2 \, |C_n|^2}{n^{2C}} (n + Q^2)$$

$$\ll d^2 (\log x)^3 (1 + \frac{Q^2}{z})$$

since $|C_n| \leq d$. Moreover, for any integer $j > 1$,

$$\sum_{1 < q \leq Q} \sum_{\chi}^{*} \int_{C-(j+1)i}^{C-ji} + \int_{C+ji}^{C+(j+1)i} \ll \frac{1}{j^{k+1}} \sum_{1 < q \leq Q} \sum_{\chi}^{*} \int_{C-(j+1)i}^{C+(j+1)i} |G_z|^2 \, |ds|$$

$$\ll \frac{1}{j^k} d^2 (\log x)^3 (1 + \frac{Q^2}{z})$$

Take $k \geq 2$, and sum over j to deduce that

$$\sum_{1 < q \leq Q} \sum_{\chi}^{*} \int_{(C)} |G_z|^2 \frac{|ds|}{|s|^{k+1}} \ll d^2 (\log x)^3 (1 + \frac{Q^2}{z}) \tag{4.5.1}$$

Next,

$$1 - LM_z = - \sum_{n > z} \sum_{\substack{e|n \\ e \leq z}} b_e \, a_{\frac{n}{e}} \, \chi(n) \, n^{-s}$$

It is easy to see that $b_{p^\alpha} = 0$ if $\alpha > d$ and for $\alpha \leq d$, $|b_{p^\alpha}| \leq \binom{d}{\alpha}$. Also, $|a_n| \leq \tau_d(n)$ where $\tau_j(n)$ represents the number of ways of writing n as an unordered product of j integers. Therefore,

$$\Big| \sum_{\substack{e|n \\ e \leq z}} b_e \, a_{n/e} \Big| \leq \tau_{d+1}(n) \, \tau(n)^d$$

where $\tau(n) = \tau_2(n)$ is the usual divisor function. Hence,

$$(4.5.2)\qquad \sum_{1<q\leq Q} \sum_{\chi}^{*} \int_{(C)} |1-LM_z|^2 \frac{|ds|}{|s|^{k+1}} \ll \sum_{n>z} \frac{\tau_{d+1}(n)^2 \tau(n)^{2d}}{n^{2C}} (n+Q^2)$$

$$\ll (\log x)^{(d+1)^2 2^{2d}} ((d+1)^2 2^{2d})! \, (1+\frac{Q^2}{z})$$

The other sums are handled similarly, and we obtain

$$\sum_{1<q\leq Q} \sum_{\chi}^{*} \int_{(\frac{1}{2})} (1+|F_z|^2+|M_z|^2+|F_zM_z|^2) \frac{|ds|}{|s|^{k+1}}$$

$$\ll 2^{2d} d^2 \sum_{n\leq z^2} \frac{(\log n)^2 \tau(n)^4}{n} (n+Q^2)$$

$$(4.5.3)\qquad \ll 2^{2d} d^2 (Q^2+z^2)(\log z)^{17}$$

All of the implied constants are absolute. It remains only to treat

$$(4.5.4)\qquad \sum_{1<q\leq Q} \sum_{\chi}^{*} \int_{(\frac{1}{2})} (|L|^2+|L'|^2) \frac{|ds|}{|s|^{k+1}}$$

At this point, we depart from the method used in the proof of the classical Bombieri-Vinogradov theorem since we do not have an approximate functional equation for L in which the dependence on the field and conductor is explicit. In principle, it should be possible to derive such an estimate, but in fact it is more convenient to use a method of Ramachandra to estimate (4.5.4) more directly. This is discussed in the next section. (The referee points out that it may also be possible to generalize Vaughan's proof [31] which does not use the approximate functional equation).

5. Mean Value Estimates

5.1 We use a method of Ramachandra [23]. Write

$$L(s,\chi) = \theta(s,\chi)\, L^{V}(1-s,\bar{\chi})$$

where

$$\theta(s,\chi) = A_{\chi}^{\frac{1}{2}-s}\, \gamma_{\chi}(1-s)/\gamma_{\chi}(s)$$

and

$$\gamma_{\chi}(s) = (\pi^{-\frac{s}{2}} \Gamma(\tfrac{s}{2}))^{a_{\chi}} (\pi^{-(s+1)/2} \Gamma(\tfrac{s+1}{2}))^{b_{\chi}}$$

Here, a_χ and b_χ are non-negative integers satisfying $a_\chi + b_\chi = d$. We deduce from Stirling's formula that

(5.1.1) $$\theta(s,\chi) << (A_\chi(|t|+2)^d)^{\frac{1}{2}-\sigma}$$

for $-\frac{3}{4} \le \sigma < 1$, as $|t| \to \infty$.

5.2 For any $U > 0$, we have

(5.2.1) $$L(s,\chi) = \sum_{n=1}^{\infty} a_n \chi(n) e^{-n/U} n^{-s} - \frac{1}{2\pi i} \int_{(C_1)} L(s+w,\chi) U^w \Gamma(w) dw$$

where $C_1 = -\frac{1}{2} - \frac{1}{\log V}$. Here, U and V are parameters to be specified.

For $\mathrm{Re}(s+w) < 0$, we can write

$$L(s+w,\chi) = \theta(s+w,\chi) \sum_{n=1}^{\infty} \bar{a}_n \bar{\chi}(n) n^{s+w-1}$$

We split the sum into two parts corresponding to $n > U$ and $n \le U$. Substituting into the integral in (5.2.1) we get

$$L(s,\chi) = \sum_{n=1}^{\infty} a_n \chi(n) e^{-n/U} n^{-s} - \frac{1}{2\pi i} \int_{(C_1)} \theta(s+w,\chi) \sum_{n>U} \bar{a}_n \overline{\chi(n)} n^{s+w-1} U^w \Gamma(w) dw$$

$$- \frac{1}{2\pi i} \int_{(C_1)} \theta(s+w,\chi) \sum_{n \le U} a_n \chi(n) n^{s+w-1} U^w \Gamma(w) dw$$

5.3 We move the second integral to the line $C_2 = -\frac{1}{\log V}$ and apply the Cauchy-Schwartz inequality to both sides. Using (5.1.1), we deduce that

(5.3.1) $$\int_{-T}^{T} |L(\tfrac{1}{2}+it,\chi)|^2 dt << \int_{-T}^{T} \Big| \sum_{n=1}^{\infty} a_n \chi(n) e^{-n/U} n^{-\frac{1}{2}+it} \Big|^2 dt$$

$$+ \left(\frac{A_\chi T^d}{U}\right)^{-2C_1} \int_{-\infty}^{\infty} \int_{-T}^{T} \Big| \sum_{n>U} \bar{a}_n \overline{\chi(n)} n^{-1-\frac{1}{\log V}+i(y+t)} \Big|^2 \Gamma(C_1+iy)^2 dt\, dy$$

$$+ \left(\frac{A_\chi T^d}{U}\right)^{-2C_2} \int_{-\infty}^{\infty} \int_{-T}^{T} \Big| \sum_{n \le U} \bar{a}_n \overline{\chi(n)} n^{-\frac{1}{2}-\frac{1}{\log V}+i(y+t)} \Big|^2 \Gamma(C_2+iy)^2 dt\, dy$$

Summing both sides over primitive characters $\chi \pmod q$ and $q \leq Q$, we can write the right hand side of (5.3.1) as $\sum_1 + \sum_2 + \sum_3$. From Lemma 4.4, we see that

$$\sum_1 \ll \sum_{n=1}^{\infty} |a_n|^2 e^{-2n/U} n^{-1}(n+Q^2T) \ll (U+Q^2T)(\log U)^{d^2} .$$

We choose

$$V = U = (AQ^d T^d)^{\frac{1}{2}}$$

Then,

$$\sum_2 \ll (AQ^d T^d)^{\frac{1}{2}} \left(\sum_{n>U} \frac{|a_n|^2}{n^{2+(2/\log V)}} (n+Q^2T) \right)$$

$$\ll (AQ^d T^d)^{\frac{1}{2}} \left(1 + \frac{Q^2T}{U}\right)(\log U)^{d^2} = (U + Q^2T)(\log U)^{d^2}$$

Similarly,

$$\sum_3 \ll \sum_{n \leq U} |a_n|^2 n^{-1-\frac{2}{\log V}} (n + Q^2T)$$

$$\ll (U + Q^2T)(\log U)^{d^2}$$

Summarizing, we have

$$(5.3.2) \qquad \sum_{q \leq Q} \sum_{\chi}{}^{*} \int_{-T}^{T} |L(\tfrac{1}{2}+it,\chi)|^2 \, dt \ll (U + Q^2T)(\log U)^{d^2} .$$

5.4 Proposition (2.4) implies that

$$\int_T^{\infty} |L(\tfrac{1}{2}+it,\chi)|^2 \frac{dt}{t^{k+1}} \ll \int_T^{\infty} (AQ^d t^d)^{\frac{1}{2}} (\log AQ^d t^d)^{2d} \frac{dt}{t^{k+1}}$$

$$\ll \frac{(AQ^d)^{\frac{1}{2}} d^{2d} (\log AQ^d)^{2d} (\log T)^{2d}}{T^{k-\frac{1}{2}d}} .$$

Summing over primitive $\chi \pmod q$ and $q \leq Q$ yields

$$\sum_{q\leq Q}\sum_{\chi}{}^{*}\int_{T}^{\infty}|L(\tfrac{1}{2}+it,\chi)|^{2}\frac{dt}{t^{k+1}} << \frac{(d\log A)^{2d}A^{\frac{1}{2}}\cdot Q^{\frac{d}{2}+2}(\log Q)^{2d}(\log T)^{2d}}{T^{k-\frac{1}{2}d}}$$

Let $\frac{1}{4} > \in > 0$. We choose $T = Q^{\in/d}$ and $k = \frac{d}{2}(1+\frac{d}{\in})$. Then, we get

$$\sum_{q\leq Q}\sum_{\chi}{}^{*}\int_{T}^{\infty}|L(\tfrac{1}{2}+it,\chi)|^{2}\frac{dt}{t^{k+1}} << Q^{2}(\log Q)^{4d}\quad(\in d\log A)^{2d}A^{\frac{1}{2}}$$

The same estimate holds if we change the range of integration on the left to $(-\infty, -T)$. Summarizing, we have proved that

$$(5.4.1)\qquad \sum_{q\leq Q}\sum_{\chi}{}^{*}\int_{(\frac{1}{2})}|L(s,\chi)|^{2}\frac{|ds|}{|s|^{k+1}} <<$$

$$<< (\log A)^{d^2}(\log Q)^{d\max(4,d)}(d+\in)^{d^2}\{Q^{2+\frac{\in}{d}}+A^{\frac{1}{2}}Q^{\frac{d+\in}{2}}+Q^{2}A^{\frac{1}{2}}\}$$

5.5 An estimate for the the term in (4.5.4) involving $L'(s,\chi)$ is obtained in a similar fashion. We begin with

$$L(s,\chi) = \sum_{n=1}^{\infty} a_n\chi(n)e^{-n/U}n^{-s} - \frac{1}{2\pi i}\int_{(C_1)}\theta(s+w,\chi)\,L^{v}(1-s-w,\bar{\chi})\,U^{w}\Gamma(w)dw$$

and differentiate with respect to s. We obtain

$$L'(s,\chi) = -\sum a_n\chi(n)e^{-n/U}(\log n)n^{-s} - \frac{1}{2\pi i}\int_{(C_1)}\theta'(s+w,\chi)\,L^{v}(1-s-w,\bar{\chi})\,U^{w}\Gamma(w)dw$$

$$+\frac{1}{2\pi i}\int_{(C_1)}\theta(s+w,\chi)\,L^{v'}(1-s-w,\bar{\chi})\,U^{w}\Gamma(w)dw$$

We then proceed as before with the last integral, decomposing the Dirichlet series for $L^{v'}$ at U. There is essentially no change in the previous calculation. For the first integral, we note that

$$\theta'(s+w,\chi) = \theta(s+w,\chi)\frac{\theta'}{\theta}(s+w,\chi) .$$

From Stirling's formula,

$$\frac{\theta'}{\theta}(s+w,\chi) << d(\log(|t+y|+2) + \frac{1}{|s+w|})$$

where $s = \frac{1}{2} + it$, $w = C_1 + iy$. Thus the second integral is a magnification by a factor of $O(d \log U)$ of the integral in (5.2.1). Finally, the Phragmén-Lindelöf estimate for $L'(s,\chi)$ is a magnification of the estimate for $L(s,\chi)$ by a factor of $(\log(A(|t| + 2)^d))^d$. Putting all these observations together, we deduce that

(5.5.1) $$\sum_{q \le Q} \sum_{\chi}^{*} \int_{(\frac{1}{2})} |L'(s,\chi)|^2 \frac{|ds|}{|s|^{k+1}} <<$$

$$<< (\log A)^{d(d+2)} (\log Q)^{d(d+2)} (d+\epsilon)^{d(d+2)} \{ Q^{2+\frac{\epsilon}{d}} + A^{\frac{1}{2}} Q^{\frac{d+\epsilon}{2}} + Q^2 A^{\frac{1}{2}} \}$$

5.6 We put together all the estimates of the previous two sections. Using (4.2.1), (4.3.1), (4.5.1), (4.5.3), (5.4.1), (5.5.1) we see that

$$\sum_{q \le Q} \sum_{\chi}^{*} |\psi_k(x,\chi)| << ((d+1)^2 2^{2d})!\ x(\log x)^{(d+1)^2 2^{2d}} (1 + \frac{Q^2}{z})$$

$$+ x^{\frac{1}{2}} 2^{2d} d^2 (Q^2 + z^2)(\log z)^{17} + (d+\epsilon)^{d(d+2)} x^{\frac{1}{2}} ((\log A)(\log Q))^{d(d+2)} .$$

$$\cdot \{ Q^{2+\frac{\epsilon}{d}} + A^{\frac{1}{2}} Q^{\frac{d+\epsilon}{2}} + Q^2 A^{\frac{1}{2}} \} .$$

We chose $z = Q(\log x)^{\gamma}$ with $\gamma > (d+1)^2 2^{2d} + D$. Let $\ell = \log x$ and suppose that

(5.6.1) $$\ell^{\gamma} \le Q \le \min(x^{\frac{1}{2}} \ell^{-(2\gamma + 17 + D)}, x^{\frac{1}{2} - \epsilon}, x^{\frac{1}{d-2} - \epsilon})$$

Then, we deduce that

(5.6.2) $$\frac{1}{Q} \sum_{q \le Q} \sum_{\chi}^{*} |\psi_k(x,\chi)| << C_d\, x(\log x)^{-D}$$

where

$$C_d = \max((d+1)^2 2^{2d})!, (d+\epsilon)^{d(d+2)} A^{\frac{1}{2}} (\log A)^{d(d+2)}) .$$

We remark that this estimate is valid for any Dirichlet series $L(s)$ satisfying the conditions at the beginning of (4.1). Notice that if $d \le 4$, we can take $Q = x^{\frac{1}{2} - \epsilon}$.

6. Estimates for the Initial Range

To take care of the range $Q \le (\log x)^{\gamma}$, we must specialize to the following case. Let L/F be an abelian extension of number fields, with group G. Take for L(s) and Artin L-series of G. Then L(s) satisfies the hypotheses of §4 with $d = n_F = [F : \mathbb{Q}]$. Thus, under the condition (5.6.1), the estimate (5.6.2) holds. We shall need the following estimate.

6.2 Lemma Suppose that L is normal over $\mathbb{Q}$. Let $1 < q$, N be positive integers with $A_\chi \ll A_q^d \leq (\log x)^N$. Then, there are positive constants $C_1 = C_1(N)$ and

$$C_2 = C_2(L,N) = \min(d_L^{-1/N}, (32n_L \log d_L)^{-1})$$

so that for any primitive Dirichlet character $\chi(\bmod q)$,

$$|\psi_k(x,\chi)| \ll (\log A_\chi)\, x \exp(-C_1 C_2 (\log x)^{\frac{1}{2}})$$

Proof This is by the traditional method (see [12] or [18]). We have for $2 \leq T \leq x$,

$$\psi_k(x,\chi) = -\sum_{|\gamma| < T} \frac{x^\rho}{\rho^{k+1}} + O(\frac{dx(\log x)^2}{T}) .$$

Denote by $N(t,\chi)$ the number of zeroes ρ of $L(s,\chi)$ with $|t - \text{Im}\rho| \leq 1$ and $0 < \text{Re}\,\rho < 1$. We have

$$N(t,\chi) \ll \log A_\chi + d \log(|t| + 5) .$$

Hence,

$$-\sum_{|\gamma| < T} \frac{1}{\rho^{k+1}} \ll \sum_{j < T} \frac{1}{j^{k+1}} N(j,\chi) \ll \log A_\chi$$

$$\ll \log A + d \log q$$

Now using Propositions (3.4) and (3.8) and choosing

$$T = \exp(\tfrac{1}{d}((\log x)^{\frac{1}{2}} - \tfrac{1}{2}\log A_\chi))$$

and $\varepsilon = 1/2N$, the result follows.

6.3 Let $\gamma > 0$ and $U = (\log x)^\gamma$. If $q \leq U$, then Lemma (6.2) implies that for some $c = c(d,\gamma)$, and for $x \gg e^A$, and any $D > 0$, (6.3.1) $$\frac{1}{U} \sum_{q \leq U} \sum_{\chi}^{*} |\psi_k(x,\chi)| \ll U x \exp(-c(\log x)^{\frac{1}{2}}) \ll x (\log x)^{-D}$$

7. Completion of the Proof

7.1 We now return to the notation and context of section 1. Thus $K/\mathbb{Q}$ is a Galois extension with group G_1, and C is a conjugacy class in G_1. Let H' be an abelian subgroup of G_1 such that $H' \cap C \neq \phi$. Let M be the subfield of K left fixed by H'. Then, for any q, $K(\zeta_q)/M$ is abelian. Let ω be an irreducible character of H'. We appeal to the results of sections 4-6 with $L(s)$ the Artin L-series $L(s,\omega)$. Let $\in > 0$ and $D > 0$. We deduce from (5.6.2) and (6.3.1) that for $d = [M : \mathbb{Q}]$ and any

$$Q \leq \min(x^{\frac{1}{2}-\in}, x^{\frac{1}{d-2}-\in}) \overset{df}{=} Q_1$$

we have

$$\frac{1}{Q} \sum_{q \leq Q} \sum_{\chi}^{*} |\psi_k(K(\zeta_q)/M, \omega \otimes \chi, x)| \ll x(\log x)^{-D}$$

where the implied constant depends on K, $\in$ and D. Notice that this dependence can be made explicit for Q larger than a power of $(\log x)$, but not for small values of Q.

Now, proposition (1.8) implies that

$$\sum_{q \leq Q_1}{}' \max_{(a,q)=1} \max_{y \leq x} |\psi_k(K(\zeta_q)/\mathbb{Q}, \xi(C,a,q), y) - \delta(C,a,q)y| \ll x(\log x)^{3-D}$$

By the reductions of section 1, we deduce that

$$\sum_{q \leq Q_1}{}' \max_{(a,q)=1} \max_{y \leq x} |\psi_0(K(\zeta_q)/\mathbb{Q}, \xi(C,a,q), y) - \delta(C,a,q)y| \ll x(\log x)^{-D}$$

7.2 Let H be the largest abelian subgroup of G_1 with $H \cap C \neq \phi$. Let $d = [G_1 : H]$. Set

$$\eta = \begin{cases} d - 2 & \text{if} \quad d \geq 4 \\ 2 & \text{if} \quad d \leq 4 \end{cases}$$

Take an element $g \in C$ and let H_1 be the subgroup generated by g. Then $d \leq [G_1 : H_1] \leq \frac{1}{2}|G_1|$. We can now state the main result.

7.3 Theorem Let $Q = x^{\frac{1}{\eta}-\epsilon}$. Then for any $A > 0$,

$$\sum_{q \leq Q}{}' \max_{(a,q)=1} \max_{y \leq x} \left|\pi_C(y,q,a) - \frac{|C|}{|G|\phi(q)}\pi(y)\right| << \frac{x}{(\log x)^A} .$$

The implied constant depends on K, ϵ and A.

7.4 In general, it is possible to replace η by a larger value as follows. Let

$$d^* = \min_H \max_\omega [G_1 : H]\,\omega(1)$$

where the minimum is over all subgroups H satisfying

(i) $H \cap C \neq \phi$

(ii) for every irreducible character ω of H and any non-trivial Dirichlet character χ, the Artin L-series $L(s, \omega \otimes \chi)$ is entire. The maximum is over irreducible characters of H. Then, in the def$^{\underline{n}}$ of η we can replace d with d^*.

8. The Least Prime in a Conjugacy Class

8.1 As before, let $K/\mathbb{Q}$ be a Galois extension and C a conjugacy class in $G = \mathrm{Gal}(K/\mathbb{Q})$. For $0 < a$, $q \in \mathbb{Z}$, $(a,q) = 1$, denote by $P_C(q,a)$ the least prime $p \equiv a \pmod q$, p unramified in K and $(p, K/\mathbb{Q}) = C$. Define

$$F_C(q) = \max_{(a,q)=1} P_C(q,a)$$

From the work of Lagarias-Odlyzko-Montgomery [13] it is known that there is an absolute constant $L > 0$ so that

$$F_C(q) << d_{K(\zeta_q)}^L$$

Moreover, assuming the Generalized Riemann Hypothesis, we have for every $\epsilon > 0$,

$$F_C(q) \underset{\epsilon}{<<} (\log d_{K(\zeta_q)})^{2+\epsilon}$$

Notice that $d_{K(\zeta_q)}$ can be as large as $d_K^{\phi(q)}\ q^{\phi(q)[K:\mathbb{Q}]}$. Let η be as in (7.2). As an application of the main theorem, we shall verify the following.

<u>8.2 Proposition</u> For any $\epsilon > 0$, $F_C(q) \le q^{\eta+\epsilon}$ with the possible exception of a set of q of density 0. The exceptional set depends on K, C and ϵ.

<u>Proof</u> For each $Q > 0$, set

$$S_Q = \{\tfrac{1}{2}Q \le q \le Q : F_C(q) > q^{\eta+\epsilon}\}$$

Let $x = (\frac{1}{2}Q)^{\eta+\epsilon}$. Then, for $q \in S_Q$, $\pi_C(x,q,a) = 0$ for some a(mod q). From Theorem (7.3) we deduce that

$$\frac{\log\log Q}{Q}\,|S_Q| \cdot \frac{|C|}{|G|}\,\mathrm{Li}\,x \ll \sum_{q \in S_Q} \frac{|C|}{|G|} \cdot \frac{\mathrm{Li}\,x}{\phi(q)} \ll \frac{x}{(\log x)^4}$$

Thus,

$$|S_Q| \ll \frac{|G|}{|C|}\ \frac{Q}{(\log\log Q)(\log Q)^3}$$

We therefore get

$$\{q \le Q : F_C(q) > q^{\eta+\epsilon}\} \ll \frac{|G|}{|C|} \cdot \frac{Q}{(\log Q)^2} = \underline{o}(Q)$$

<u>Remark</u> The problem of estimating F(q) seems to have first been considered by Turán [29] who showed (assuming the Lindelöf hypothesis) that $F(q) \ll q^{4+\epsilon}$ for a set of q of density 1. When $K = \mathbb{Q}$, the proposition gives $F(q) \ll q^{2+\epsilon}$ for a set of q of density 1. This can be further improved by utilising the recent work of Bombieri-Iwaniec-Friedlander [3].

<u>References</u>

1. E. Bombieri, On the Large Sieve, Mathematika, 12(1965), 201-225.

2. E. Bombieri, Le Grand Crible dans la Theorie Analytique des Nombres, Astérisque No. 18, Soc. Math. France, 1974.

3. E. Bombieri, H. Iwaniec and J. Friedlander, Primes in Arithmetic Progressions to Large Moduli, Acta Mathematica, 1986.

4. H. Davenport, Multiplicative Number Theory, second edition, Springer-Verlag, New York, 1980.

5. W. Feit, Characters of Finite Groups, Benjamin, New York, 1967.

6. P.X. Gallagher, Bombieri's Mean Value Theorem, Mathematika, 15(1968), 1-6.

7. D. Goldfeld, A Simple Proof of Siegel's Theorem, Proc. Nat. Acad. Sci. U.S.A., 71(1974)1055.

8. D. Goldfeld, J. Hoffstein and S. Patterson, On Automorphic Forms of Half-integral Weight with Applications to Elliptic Curves, in Number Theory Related to Fermat's Last Theorem, pp. 153-193, ed. N. Koblitz, Birkhauser, Boston, 1982.

9. R. Gupta, M. Ram Murty and V. Kumar Murty, The Euclidean Algorithm for S-integers, these proceedings.

10. M. Huxley, The Large Sieve Inequality for Algebraic Number Fields, III. Zero Density Results, J. London Math. Soc. (2)3(1971) 233-240.

11. H. Iwaniec, Fourier Coefficients of Modular Forms of Half-Integral Weight, to appear.

12. J. Lagarias and A. Odlyzko, Effective versions of the Chebotarev Density Theorem, pp. 409-464 in: Algebraic number fields, ed. A. Frohlich, Academic Press, New York, 1977.

13. J. Lagarias, A. Odlyzko and H. Montgomery, A Bound for the Least Prime Ideal in the Chebotarev Density Theorem, Inv. Math., 54(1979) 271-296.

14. E. Landau, Nachr. Akad. Wiss. Göttingen, (1918) 78-97, 478-488.

15. S. Lang, Algebraic Number Theory, Addison-Wesley, Reading, 1970.

16. J. Martinet, Character Theory and Artin L-functions, pp. 1-87 in: Algebraic number fields, ed. A. Fröhlich, Academic Press, New York, 1977

17. Y. Motohashi, An Induction Principle for the generalization of Bombieri's prime number theorem, Proc. Japan Academy, 52(1976) 273-275.

18. V. Kumar Murty, Explicit Formulae and the Lang-Trotter Conjecture, in Proc. Edmonton number theory conference, ed. M.V. Subbarao, Rocky Mountain J. Math. 15(1985) 535-551.

19. M. Ram Murty, On Artin's Conjecture, J. Number Theory, 16(1983) 147-168.

20. M. Ram Murty and V. Kumar Murty, Prime Divisors of Fourier Coefficients of modular forms, Duke Math. J. 51(1984) 57-76.

21. M. Ram Murty and V. Kumar Murty, An Analogue of the Erdös-Kac theorem for Fourier coefficients of modular forms, Indian J. Pure Appl. Math. 15(1984) 1090-1101.

22. H. Rademacher, On the Phragmén-Lindelöf Theorem and Some Applications, Math. Z. 72(1959) 192-204.

23. K. Ramachandra, A Simple Proof of the Mean Fourth Power Estimate for $\zeta(1/2 + it)$ and $L(1/2 + it,\chi)$, Ann. Scuola Norm. Sup. Pisa, 1(1974) 81-97.

24. J.P. Serre, Linear Representations of Finite Groups, Springer-Verlag, New York, 1977.

25. J.P. Serre, Quelques Applications du Théorème de Densité de Chebotarev, Publ. Math. IHES, 54(1982) 123-201.

26. G. Shimura, On Modular Forms of Half-Integral Weight, Ann. Math., 97(1973) 440-481.

27. C.L. Siegel, Abschätzung von Einheiten, Nachr. Akad. Wiss. Gottingen, (1969)71-86.

28. H.M. Stark, Some Effective Cases of the Brauer-Siegel Theorem, Inv. Math., 23(1974) 135-152.

29. P. Turán, On Some Recent Results in the Analytical Theory of Numbers, pp. 359-374. in Institute on number theory, ed. D.J. Lewis, Proc. Symp. Pure Math. 20, AMS, Providence, 1971.

30. A.I. Vinogradov, On the Density Conjecture for Dirichlet L-series, Izv. Akad. Nauk SSSR Ser. Mat., 29(1965) 903-934.

31. R.C. Vaughan, An Elementary method in Prime Number Theory, Acta Arithmetica, 27(1980) 111-115.

32. R. Wilson, The Large Sieve in Algebraic Number Fields, Mathematika, 16(1969) 189-204.

M. Ram Murty: Dept. of Mathematics, McGill University, Montreal, Canada

V. Kumar Murty: Dept. of Mathematics, Concordia University, Montreal, Canada