The Hooley-Huxley contour method for problems in number fields III: Frobenian functions

Coleman, M.D.

2001

MIMS EPrint: **2006.129**

ISSN 1749-9097

The Hooley-Huxley Contour Method for Problems in Number Fields III: Frobenian Functions

M D Coleman

In the earlier papers of this series, [1] and [2], we applied the Hooley-Huxley contour method, as described in [9], to sums of arithmetic functions defined on the integral ideals of a number field K, say. The contour method allows the restriction of the sums to small regions of ideals, $\mathcal{S}\left(x,\psi_0,\ell\right)$, defined below. In [2] we considered multiplicative functions that are Frobenius with respect to some Galois extension L of K. That is, the functions have the same value on all unramified prime ideals whose Frobenius symbol lie in the same conjugacy class of Gal(L/K). In particular, in §2.2 of [2] we looked at when these functions are non-zero. In the present paper we introduce the ideas of Odoni, see [7] for instance, and, assuming the arithmetic functions are finite-valued, examine when these functions take a given value. It will ease reading of this paper to have [1] and [2] to hand.

Let $n=n_K=\deg K/\mathbb{Q}$, $n_L=\deg L/\mathbb{Q}$ and $n_{L/K}=\deg L/K$. Let I denote the group of fractional ideals of K and let $P=\{(\alpha)\in I:\alpha\in K^*,\alpha\succ 0\}$. Let $(\lambda_1,\lambda_2,...,\lambda_{n-1})$ be a basis for the torsion-free characters on P that satisfy $\lambda_i(\varepsilon)=1, 1\le i\le n-1$, for all units $\varepsilon\succ 0$ in $\mathcal{O}_K$, the ring of integers of K. Fixing an extension of each λ_i to a character on I then $\lambda_i(\mathfrak{a}), 1\le i\le n-1$ are defined for all fractional ideals $\mathfrak{a}$. So for such ideals of K we can define $\psi\left(\mathfrak{a}\right)=\left(\psi_j\left(\mathfrak{a}\right)\right)\in\mathbb{T}^{n-1}$ by $\lambda_j\left(\mathfrak{a}\right)=e^{2\pi i\psi_j(\mathfrak{a})}$. Then we define our small region of integral ideals as

$$\mathcal{S}\left(x,\psi_0,\ell\right)=\Big\{\mathfrak{a}\ \lhd\mathcal{O}_K:x\left(1-\ell\right)\le N\mathfrak{a}\ \le x\left(1+\ell\right),\left|\psi_j\left(\mathfrak{a}\right)-\psi_{0j}\right|_{\mathbb{T}}\le\ell,$$
$$1\le j\le n-1\}$$

for $0<\ell<1/2,\psi_0\in\mathbb{T}^{n-1}$. This differs from the definition in [1] and [2] in that we have not excluded ideals with prime divisors that ramify in L.

Let Θ be a Frobenius multiplicative function with respect to $G=$ Gal(L/K) and with values in some finite commutative monoid $M=\{\gamma_1,...,\gamma_t\}$, say. (See[7], §6D). So if the unramified prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ satisfy $[(L/K)/\mathfrak{p}]=[\left(L/K\right)/\mathfrak{q}]$ then $\Theta\left(\mathfrak{p}^n\right)=\Theta\left(\mathfrak{q}^n\right)$ for all $n\ge 1$.

In our main result we give an asymptotic result for

$$\Theta\left(\mathcal{S},\gamma\right):=\left|\{\mathfrak{a}\in\mathcal{S}(x,\psi_0,\ell):\Theta(\mathfrak{a})=\gamma\}\right|$$

for any $\gamma\in M$. Let $\Theta(C)$ denote the value taken by all unramified primes with Frobenius symbol in the conjugacy class C. Further, given $\gamma\in M$ define

$$\alpha(\gamma)=\sum\nolimits'\frac{|C|}{|G|}$$

where the sum runs over all conjugacy classes C for which $\Theta(C)$ occurs in some factorization of γ.

Theorem 1 *Let $\varepsilon > 0$ be given and assume that ℓ satisfies*

$$\exp\left(-R(x)\right) > \ell > \begin{cases} x^{-5(1-\varepsilon)/12n_K} & \text{if } L/K \text{ abelian} \\ x^{-3(1-\varepsilon)/2(n_L+3n_K)} & \text{otherwise} \end{cases} \tag{1}$$

where $R(x) = \kappa_1(\log x)^{1/3}(\log\log x)^{-1/3}$ for some constant κ_1. Then $\Theta\left(\mathcal{S},\gamma\right)$ is a finite sum (over i say) of expansions

$$\frac{(2\ell)^{n_K}x}{(\log x)^{1-\alpha_i}}\sum_{j=0}^{J(x)}\frac{Q_{ij}(\log\log x)}{(\log x)^j} + O(\ell^{n_K}x\exp(-R(x))) \tag{2}$$

where $J(x) = \kappa_2(\log x)^{1/3}(\log\log x)^{-4/3}$ for some constant κ_2, $\alpha_i \in \mathbb{C}$ and $Q_{ij}(X)$ are polynomials. In all cases $|\alpha_i| \leq \alpha(\gamma)$ and if $\alpha_i = \alpha(\gamma)$ for some i then $Q_{ij}(X)$ is of degree zero and in fact a real number, so no loglog factors occur in that asymptotic expansion.

A version of this result can be given with the truncation of the series in (2) at any $J \leq c\log x$ along with the inclusion of an appropriate error term depending on J. Such a result is seen in Theorem 6 of [2] and just like there we can give an upper bound for the $Q_{ij}(X)$ in (2), this time of the form $\ll \Gamma(j+3)(2c_0)^{-j}X^c$ where c and the implied constant depend on the module M.

This result generalises Theorem 3 of [6] which gives an asymptotic result (but without truncation) for $\{1 \leq n \leq x,\ (n,E) = 1,\ \Theta(n) = \gamma\}$ where Θ is multiplicative and Frobenius with respect to some extension $L/\mathbb{Q}$ unramified outside E. As Odoni describes in [6] his result was discovered during work on coefficients of modular forms. We can apply our result to the same problems and in particular we give the following result on Ramanujan's tau function, τ.

Corollary 1 *Let $m > 691$ be prime and $b \in \mathbb{N}$ be coprime to m. Then for*

$$1 > \frac{\log h}{\log x} > 1 - \frac{3}{2((m^2-1)(m^2-m)+3)}$$

we have

$$\begin{aligned} &|\{x < n < x+h, \tau(n) \equiv b (\mathrm{mod}\, m)\}| \qquad (3)\\ = \quad &\frac{h}{\phi(m)\Gamma(1-\beta)(\log x)^\beta}\sum_{j=0}^{J(x)}\frac{c_j}{(\log x)^j} + O_m(h\exp(-R(x)))\end{aligned}$$

where $\beta = m/(m^2-1)$ and c_0 is independent of m.

Summing over $1 \leq b \leq m-1$ we recover corollary 3 of [2]. Of course it is unnecessary to introduce Groessencharacters to prove Theorem 2 but later in the paper we give an application to ranges of ideals (see [8]) that uses the full force of Theorem 1.

Proof of Theorem 1 From sections 4 and 5 of [1] and the references therein it can be seen that $\Theta(\mathcal{S},\gamma)$ differs from

$$\frac{1}{2\pi i}\sum_{\|\overrightarrow{\mathbf{m}}\|<W} a_{\overrightarrow{\mathbf{m}}} e^{2\pi i\,\overrightarrow{\mathbf{m}}.\boldsymbol{\psi}_0}\int_{c-iW}^{c+iW}\tilde{g}(s)\sum_{\substack{\Theta(\mathfrak{a})=\gamma\\ \mathfrak{a}\ \lhd\mathcal{O}_K}}\frac{\lambda^{\overrightarrow{\mathbf{m}}}(\mathfrak{a})}{N\mathfrak{a}^s}ds \qquad (4)$$

by an amount that can be made arbitrarily small at the cost of demanding x is sufficiently large. Here $\overrightarrow{\mathbf{m}}\in(\mathbb{N}\cup\{0\})^{n-1}$, $\|\overrightarrow{\mathbf{m}}\|=\max_{1\le i\le n-1}m_i$, $c>1$, and $a_{\overrightarrow{\mathbf{m}}}$ and $\tilde{g}(s)$ are weights while $W=c(\log x)^4/\ell$. To deal with the condition $\Theta(\mathfrak{a})=\gamma$ we look at all t-tuples $\boldsymbol{\nu}=(\nu_1,...,\nu_t)$ of non-negative integers such that $\gamma_1^{v_1}...\gamma_t^{v_t}=\gamma$. It might be that for some i, $v_i=0$ in all these vectors. In this case we let $\mathcal{A}=\mathcal{A}(\gamma)$ be the set of i for which this doesn't happen, cardinality a, say and consider all vectors written without adornment to be a-tuples indexed by $\mathcal{A}$, so now $\boldsymbol{\nu}=(\nu_i)_{i\in\mathcal{A}}$. We follow Odoni, see [7] for example, by introducing the formal power series over such $\boldsymbol{\nu}$,

$$G(\gamma,\mathbf{z})=\sum_{\mathbf{v}\ge\mathbf{0}}{}^{'}\mathbf{z}^{\mathbf{v}},$$

where $\mathbf{z}=(z_i)_{i\in\mathcal{A}}$ and $\mathbf{z}^{\mathbf{v}}=\prod_{i\in\mathcal{A}}z_i^{\nu_i}$. Then the idea of Odoni is to use Hadamard's convolution of power series which gives

$$\sum_{\substack{\Theta(\mathfrak{a})=\gamma\\ \mathfrak{a}\ \lhd\mathcal{O}_K}}\frac{\lambda^{\overrightarrow{\mathbf{m}}}(\mathfrak{a})}{N\mathfrak{a}^s}=\frac{1}{(2\pi i)^a}\int\underset{|z_j|=\rho,\,j\in\mathcal{A}}{...}\int\Lambda(s,\overrightarrow{\mathbf{m}},\mathbf{z}^{-1})G(\gamma,\mathbf{z})\prod_{j\in\mathcal{A}}\frac{dz_j}{z_j}, \qquad (5)$$

where $0<\rho<1$, $\mathbf{z}^{-1}$denotes the vector $(z_j^{-1})_{j\in\mathcal{A}}$, and

$$\Lambda(s,\overrightarrow{\mathbf{m}},\mathbf{z})=\prod_{\mathfrak{p}}\left\{1+\sum_{j\in\mathcal{A}}z_j\sum_{\substack{\Theta(\mathfrak{p}^n)=\gamma_j\\ n\ge1}}\frac{\lambda^{\overrightarrow{\mathbf{m}}}(\mathfrak{p}^n)}{N\mathfrak{p}^{ns}}\right\}. \qquad (6)$$

To find the regions of $\overrightarrow{\mathbf{m}},\mathbf{z}$ and s for which this Euler product is defined we expand formally the product over unramified primes in (6) as a Dirichlet series to get

$$\sum_{\mathfrak{a}}\frac{\mathbf{z}^{\mathbf{f}(\mathfrak{a})}\lambda^{\overrightarrow{\mathbf{m}}}(\mathfrak{a})}{N\mathfrak{a}^s}, \qquad (7)$$

where the sum is over integral ideals divisible by no ramified primes and

$$\begin{aligned} f_j(\mathfrak{a}) &= \left|\left\{\mathfrak{p}^n\|\mathfrak{a},\Theta(\mathfrak{p}^n)=\gamma_j\right\}\right| \\ &= \omega_j(\mathfrak{a}) \end{aligned}$$

in the notation of [2]. The series (7) is a particular instance of $F(s,\overrightarrow{\mathbf{m}},\mathbf{z}\ )$ from [2], with $\theta\equiv1$, and $f_j=\omega_j$ for all $j\in\mathcal{A}$, in the notation of that paper. So we can quote from [2] that the series and, since the product over ramified primes in (9) is a finite product, that $\Lambda(s,\overrightarrow{\mathbf{m}},\mathbf{z})$ are defined for all $\overrightarrow{\mathbf{m}}$, $\mathbf{z}$ and $\operatorname{Re} s > 1$. But further, from [2] equation (4) we can also deduce the result that

$$\begin{aligned}\Lambda(s,\overrightarrow{\mathbf{m}},\mathbf{z}) &= \Lambda_0(s,\overrightarrow{\mathbf{m}},\mathbf{z})\prod_{C}\prod_{\chi} L(s,\chi_E\lambda^{\overrightarrow{\mathbf{m}}}_{E/K})^{\alpha(C,\chi,\mathbf{z})} \qquad (8)\\ &= \Lambda_0(s,\overrightarrow{\mathbf{m}},\mathbf{z})L(s,\overrightarrow{\mathbf{m}},\mathbf{z}),\end{aligned}$$

say. Here $\Lambda_0(s,\overrightarrow{\mathbf{m}},\mathbf{z})$ converges absolutely and uniformly for all $\overrightarrow{\mathbf{m}}$, for all $||\mathbf{z}|| < A$ for any given A and when $\operatorname{Re} s \geq \sigma_1$, for any $\sigma_1 > 1/2$. The first product in (8) is over conjugacy classes C of G. For each class, C, we choose an element $g \in C$ and then the second product is over irreducible characters of $\langle g\rangle$, the cyclic group generated by g. The L-functions in the product are defined by

$$\sum_{a}\frac{\chi_E\,(a)\,\lambda^{\overrightarrow{\mathbf{m}}}(N_{E/K}a)}{N_E a^s}, \quad \text{for} \quad \operatorname{Re} s > 1, \qquad (9)$$

where E is the fixed field of $\langle g\rangle$, χ_E is the character on G induced by χ on $\langle g\rangle$ but considered as a character on the narrow ideal classes mod$^{\times}\mathfrak{f}$ of E for some conductor $\mathfrak{f}$ and the sum is over integral ideals of E prime to $\mathfrak{f}$. Finally, the exponents $\alpha(C,\chi,\mathbf{z})$ in (8) are given by $|C|\,\bar{\chi}(g)\mathbf{z}_C/\,|G|$, where $\mathbf{z}_C$ is the value of $\mathbf{z}^{\mathbf{f}(\mathfrak{p})}$ for any prime ideal satisfying $[L/K)/\mathfrak{p}] = C$. Note that a component $z_i, i \in \mathcal{A}$, can only arise as one of these $\mathbf{z}_C$ if there exists a *single* power of a prime $\mathfrak{p}$ such that $\Theta(\mathfrak{p}) = \gamma_i$. Let $\mathcal{B} \subseteq \mathcal{A}$ denote this set of i and let $\mathbf{x}^*$ denote a vector indexed by $\mathcal{B}$, so $\mathbf{x}^* = (x_i)_{i\in\mathcal{B}}$. Then we can write $L(s,\overrightarrow{\mathbf{m}},\mathbf{z}^*)$ in place of $L(s,\overrightarrow{\mathbf{m}},\mathbf{z})$ and further

$$\begin{aligned}L(s,\overrightarrow{\mathbf{m}},\mathbf{z}^*) &= \prod_{i\in\mathcal{B}}\left(\prod_{C\sim i}\prod_{\chi}L(s,\chi_E,\lambda^{\overrightarrow{\mathbf{m}}}_{E/K})^{\alpha(C,\chi,\mathbf{1})}\right)^{z_i} \qquad (10)\\ &= \prod_{i\in\mathcal{B}}(L_i(s,\overrightarrow{\mathbf{m}}))^{z_i}\end{aligned}$$

say, where $C \sim i$ if $[(L/K)\,/\mathfrak{p}] = C$ implies $\Theta\,(\mathfrak{p}) = \gamma_i$.

To evaluate the integrals in (5) we need to quote from p.390 of [7] where it is shown that

$$G(\gamma,\mathbf{z}) = \frac{P(\gamma,\mathbf{z})}{\Pi_{j\in\mathcal{A}}\left(1 - z_j^{c_j}\right)}$$

for some polynomial $P(\gamma,\mathbf{z}\ )$ and constants $c_j, j \in \mathcal{A}$. The poles of $G(\gamma,\mathbf{z})$ are separable so the circles of integration in (4) can be moved, one by one, to circles $|z_j| = \rho', \rho' > 1$. Then, for each subset $\mathcal{U} \subseteq \mathcal{A}$ we obtain a number of terms of the form

$$\frac{1}{(2\pi i)^u}\int\ldots\int_{\substack{z_j=\rho'\\ j\in\mathcal{U}}}\Lambda(s,\overrightarrow{\mathbf{m}},\mathbf{z}_{\mathcal{U}}^{-1})G_{\mathcal{U}}(\gamma,\mathbf{z}_{\mathcal{U}})\prod_{j\in\mathcal{U}}\frac{dz_j}{z_j}. \qquad (11)$$

Here $u = |\mathcal{U}|$, $(\mathbf{z}_{\mathcal{U}})_j$ is a c_j-th root of unity if $j \notin \mathcal{U}$ and $G_{\mathcal{U}}(\gamma, \mathbf{z}_{\mathcal{U}})$ is the residue of $G(\gamma, \mathbf{z})$ at these roots. If we first consider the special case when the numerator $P(\gamma, \mathbf{z})$ of $G(\gamma, \mathbf{z})$ is a monomial, then it is easily seen on changing variables to $w_j = 1/z_j$ for all $j \in \mathcal{U}$ that if the poles at infinity of $G_{\mathcal{U}}(\gamma, \mathbf{z}_{\mathcal{U}})$ at $z_j, j \in \mathcal{U}$, are of sufficiently large order then the integrals, now around the origin, give derivatives, with respect to these w_j, of the integrand which are then evaluated at $w_j = 0$ for all $j \in \mathcal{U}$. This in turn gives a sum of derivatives of $\Lambda(s, \overrightarrow{\mathbf{m}}, \mathbf{w}_{\mathcal{U}})$ say, where for $j \notin \mathcal{U}$ we have $(\mathbf{w}_{\mathcal{U}})_j = (\mathbf{z}_{\mathcal{U}})_j^{-1}$, a c_j-th root of unity. The general $P(\gamma, \mathbf{z})$ is just a sum of monomials and so (11), and thus (5), are linear sums of

$$\frac{\partial^{\mathbf{k}}}{\partial \mathbf{w}^{\mathbf{k}}} \Lambda(s, \overrightarrow{\mathbf{m}}, \mathbf{w})$$

evaluated at $\mathbf{w} = \boldsymbol{\eta}$ where η_j is either 0 or a c_j-th root of unity in which case we must have $k_j = 0$. From (8) and (10) we see that (5) is, in fact, a finite linear sum over $(\mathbf{k}, \boldsymbol{\eta})$ of terms

$$L(s, \overrightarrow{\mathbf{m}}, \mathbf{k}^*, \boldsymbol{\eta}^*) := L(s, \overrightarrow{\mathbf{m}}, \boldsymbol{\eta}^*) \prod_{i \in \mathcal{B}} (\log L_i \left(s, \overrightarrow{\mathbf{m}}\right))^{k_i} \tag{12}$$

with coefficients $\kappa(s, \overrightarrow{\mathbf{m}}, \mathbf{k}, \boldsymbol{\eta})$, say, that are holomorphic in $\operatorname{Re} s > 1/2$ and uniformly bounded for all $\overrightarrow{\mathbf{m}}$ and $\operatorname{Re} s \geq 1/2 + \delta$ for any $\delta > 0$. The product of L-functions occurring in (12) is of exactly the form to which we can apply the Hooley-Huxley method though none of our previous applications have all the features of (12). In [1] the Hooley-Huxley method is applied to integrals containing products as in (12) though the L-functions occurring have only $E = K$. In [2] we have L-functions of the type (9) but with no logarithms of L-functions. Nonetheless the methods of [2] give the following version of part of Theorem 1 of [1]. Let $\mathcal{C}_0 = \{s \in \mathbb{C} : |s - 1| = c_0, s \neq 1 - c_0\}$ traversed in the anti-clockwise direction. Here c_0 is chosen such that no $L(s, \overrightarrow{\mathbf{0}}, \mathbf{k}^*, \boldsymbol{\eta}^*)$ that appears in (5) has a singularity on the boundary or interior of the circle $s - 1 = 3c_o$. Then

$$\Theta\left(\mathcal{S}, \gamma\right) - I(x, \ell) \ll x \ell^{n_K} \exp(-R(x))$$

for ℓ satisfying (1) and where

$$I(x, \ell) = \frac{(2\ell)^{n_K - 1}}{2\pi i} \int_{x(1-\ell)}^{x(1+\ell)} \int_{\mathcal{C}_0} y^{s-1} \sum_{\mathbf{k}, \boldsymbol{\eta}} \kappa(s, \overrightarrow{\mathbf{0}}, \mathbf{k}, \boldsymbol{\eta}) L(s, \overrightarrow{\mathbf{0}}, \mathbf{k}^*, \boldsymbol{\eta}^*) ds dy. \tag{13}$$

The terms of the inner double sum can be written as

$$\left(\frac{1}{s-1}\right)^{\alpha(\boldsymbol{\eta}^*)} \left(\log\left(\frac{1}{s-1}\right)\right)^{k^*} H(s, \mathbf{k}, \boldsymbol{\eta})$$

where

$$\alpha(\boldsymbol{\eta}^*) = \sum_{i \in \mathcal{B}} \eta_i \sum_{C \sim i} \frac{|C|}{|G|}, \qquad k^* = \sum_{i \in \mathcal{B}} k_i,$$

and $H\left(s,\mathbf{k},\boldsymbol{\eta}\right)$ is analytic in $|s-1|\leq 3c_0$.

If $\boldsymbol{\eta}^*=\mathbf{1}$, then necessarily $\mathbf{k}^*=\mathbf{0}$ and there are no logarithmic terms in (12). In this case the integrals in (13) have been evaluated in [2] giving an expansion of the form (2), with no $\log\log$ factors and with main term $c(2\ell)^n x(\log x)^{-(1-\alpha)}$ where

$$\alpha=\alpha(\gamma)=\sum_{i\in\mathcal{B}}\sum_{C\sim i}\frac{|C|}{|G|},$$

which reduces to the form given in the statement of the Theorem. Note the constant $c=c(\gamma)$ might be 0 since, if $\mathcal{B}\neq\mathcal{A}$, it might happen that

$$\sum_{\substack{\mathbf{k},\boldsymbol{\eta}\\ \boldsymbol{\eta}^*=\mathbf{1}^*}}\kappa(1,\overrightarrow{\mathbf{0}},\mathbf{k},\boldsymbol{\eta})=0.$$

If $c\neq 0$ the $\boldsymbol{\eta}^*=\mathbf{1}$ contribution will give the dominant term. For the cases when $\boldsymbol{\eta}^*\neq\mathbf{1}^*$ we have $\operatorname{Re}\alpha(\boldsymbol{\eta}^*)<\operatorname{Re}\alpha(\mathbf{1}^*)<1$ where the strict inequality follows from the definition of $\mathcal{B}$ which ensures that $\sum_{C\sim i}|C|/|G|\neq 0$ for each $i\in\mathcal{B}$. We can use the ideas of [1] to estimate the inner integrals of (13). In fact, since Re $\alpha(\boldsymbol{\eta}^*)<1$ the integral on a circle such as $\mathcal{C}_0$ tends to zero as the radius of the circle tends to 0. Thus we are left with an integral along the real axis, which we interchange with the integral over y. Then each $(\mathbf{k},\boldsymbol{\eta})$ in the summation in (13) contributes

$$(2\ell)^{n_K}\int_0^{c_0}\frac{x^{1-r}}{r^\alpha}\sum_{a+b=k^*}\binom{k^*}{a}\left(\log\frac{1}{r}\right)^a H_b(1-r,\mathbf{k},\boldsymbol{\eta})k(\ell,r)dr. \tag{14}$$

Here

$$k(\ell,r)=\frac{(1+\ell)^{1-r}-(1-\ell)^{1-r}}{2\ell}\ll 1$$

and

$$H_b(s,\mathbf{k},\boldsymbol{\eta})=\frac{H(s,\mathbf{k},\boldsymbol{\eta})}{s}\frac{\left((i\pi)^b e^{i\pi\alpha}-(-i\pi)^b e^{-i\pi\alpha}\right)}{2\pi i}$$

The situation can now be compared with the proof of Theorem 5 of [1]. Since $H_b(1-s,\mathbf{k},\boldsymbol{\eta})$ is analytic for $|s|<3c_0$ it can be expanded as a power series and truncated as

$$H_b(1-r,\mathbf{k},\boldsymbol{\eta})=\sum_{j=0}^{J}\alpha_j r^j+O\left(\left(\frac{r}{2c_0}\right)^{J+1}\right) \tag{15}$$

for $r<2c_o$ and some $\alpha_j=\alpha_j(b,\mathbf{k},\boldsymbol{\eta})\ll(1/2c_0)^j$. Multiplied through by $(\log 1/r)^a$ from (14) we have then, in (15), a special case of equation (12) in [1]. Compared to equation (11) in [1] the integrals in (14) are complicated by the $r^{-\alpha}$ factor but since $|\alpha|<1$ this is easily dealt with. So each term in (14) can be evaluated as

$$\sum_{j=0}^{J(x)}(2\ell)^{n_K}x\frac{Q_{aj}(\log_2 x)}{(\log x)^{j-\alpha+1}}+O(\ell^{n_K}x\exp(-R(x)))$$

with $J(x)$ and $R(x)$ as in Theorem 1. Here $Q_{aj}(X)$ is a polynomial of degree at most a. ■

Note (i) The way in which (14) is evaluated is to complete the integral to ∞ and then to consider it to be the difference of two integrals who integrands differ in having $(x(1+\ell))^{1-r}$ in one and $(x(1-\ell))^{1-r}$ in the other. This difference, which we might write as $(2\ell)^{-1}(I(x(1+\ell)) - I(x(1-\ell)))$, will have a main term that is independent of ℓ and an error which, if ℓ is sufficiently small, for instance $\exp(-R(x)) > \ell$, can be absorbed into the error in (2). If ℓ is larger than this then the numerators of each term in the sum in (2) will depend on both ℓ and $\log\log x$. This reaches its extreme when ℓ is a constant, for instance $\ell = 1/2$, when we get an expansion as in (2) but with $Q_{ij}(X)$ different to those in (2). As we saw in §2.4 [2] when ℓ is constant we can deduce (2) with $R(x) = \kappa_1(\log x)^{3/5}(\log\log x)^{-1/5}$ and $J(x) = \kappa_2(\log x)^{3/5}(\log\log x)^{-6/5}$.

(ii) In the proof of Theorem 1 above a new version of part of Theorem 1 of [1] is given. A similar version of the remaining part of that theorem can be proved by the methods of [2]. So, for

$$\exp\left(-R(x)\right) > \ell > \begin{cases} x^{-5(1-\varepsilon)/6n_K} & \text{if } L/K \text{ abelian} \\ x^{-3(1-\varepsilon)/(n_L+3n_K)} & \text{otherwise} \end{cases}$$

we can say that

$$\int_{\mathbb{T}^{n_K-1}} \int_X^{2X} \left|\Theta\left(\mathcal{S},\gamma\right) - I(x,\ell)\right|^2 d\psi_0 dx \ll X^3 \ell^{n_K} \exp(-R(X)).$$

Then, with m and b as in Corollary 1 but with

$$1 > \frac{\log h}{\log x} > 1 - \frac{3}{((m^2-1)(m^2-m)+3)}$$

we have for almost all x that $|\{x < n < x+h, \tau(n) \equiv b \pmod{m}\}|$ has an expansion as in (3).

Proof of Corollary 1 In this case $M = \mathbb{Z}/m\mathbb{Z}$. Since $b \neq 0$, we can never have 0 in any factorization of b unlike any other element of M, hence $\mathcal{A} = (\mathbb{Z}/m\mathbb{Z})^*$ and $a = m-1$.

In [3] it is shown that there exists a field extension K_m of $\mathbb{Q}$ and an irreducible two-dimensional complex linear representation $\rho : \mathrm{Gal}(K_m/\mathbb{Q}) \to GL_2(\mathbb{Z}/m\mathbb{Z})$ such that, for primes p unramified in K_m, $Tr\rho([(K_m/\mathbb{Q})/p]) = \tau(p)(\bmod\, m)$. Further, if $m > 691$ the map ρ is a bijection. Not only does this imply $\deg K_m = (m^2-1)(m^2-m)$ but also that every possible value of $\tau(n)(\bmod\, m)$ is attained with n prime. Thus $\mathcal{B} = \mathcal{A}$ in the notation earlier. So it remains to examine $G(b,\mathbf{z})$ where $\mathbf{z}$ is an $m-1$-tuple.

Obviously $G(b,\mathbf{z}) = H(b,\mathbf{z})/\Pi_{i=1}^{p-1}(1-z_i^{a_i})$ where a_i is the order of $i \bmod m$ and

$$H(b,\mathbf{z}) = \sum_{\substack{\Pi_{i=1}^{p-1} i^{c_i} \equiv b (\bmod m) \\ 0 \le c_i < a_i}} \mathbf{z}^{\mathbf{c}}.$$

Then

$$
\begin{aligned}
z_b H(1,\mathbf{z}) &= \sum_{\substack{\Pi_{i=1}^{p-1} i^{c_i} \equiv b (\mathrm{mod} m) \\ 0 \le c_i < a_i, i \ne b \\ 1 \le c_b \le a_b}} \mathbf{z}^{\mathbf{c}} \\
&= H(b,\mathbf{z}) + \sum_{\substack{\Pi_{i=1}^{p-1} i^{c_i} \equiv b (\mathrm{mod} m) \\ 0 \le c_i < a_i, i \ne b \\ c_b = a_b}} \mathbf{z}^{\mathbf{c}} - \sum_{\substack{\Pi_{i=1}^{p-1} i^{c_i} \equiv b (\mathrm{mod} m) \\ 0 \le c_i < a_i, i \ne b \\ 1 = c_b}} \mathbf{z}^{\mathbf{c}} \\
&= H(b,\mathbf{z}) + (z_b^{a_b} - 1) g(b, \mathbf{z}^{(b)})
\end{aligned}
$$

say, where $\mathbf{z}^{(b)} = (z_i)_{i \ne b}$. Thus

$$
G(b,\mathbf{z}) = \frac{z_b H(1,\mathbf{z})}{\prod_{i=1}^{p-1}(1 - z_i^{a_i})} + \frac{g(b,\mathbf{z}^{(b)})}{\prod_{i=1, i\ne b}^{p-1}(1 - z_i^{a_i})}.
$$

There are no poles at infinity so no $\log\log$ terms in any of the asymptotic expansions that arise. The main contribution, which, because $\mathcal{B} = \mathcal{A}$ has a non-zero coefficient, arises from the pole at $\mathbf{z} = \mathbf{1}$. The residue of $G(b,\mathbf{z})$ at $\mathbf{z} = \mathbf{1}$ is $H(1,\mathbf{1})/\Pi_{i=1}^{p-1} a_i$. Yet $H(1,\mathbf{1})$ is the number of solutions of $\Pi_{i=1}^{p-1} i^{c_i} \equiv 1 (\mathrm{mod}\, m), 0 \le c_i < a_i$. Let k be a primitive root mod m. Then for any choices of $c_i, i \ne k, 0 \le c_i < a_i$ we can uniquely solve $\Pi_{i \ne k} i^{c_i} k^{c_k} \equiv 1 (\mathrm{mod}\, m)$ for c_k. All solutions of $\Pi_{i=1}^{p-1} i^{c_i} \equiv 1 (\mathrm{mod}\, m)$ arise in this way. So $H(1,\mathbf{1}) = \Pi_{i \ne k} a_i = \frac{1}{m-1} \Pi_{i=1}^{p-1} a_i$ and hence the residue equals $1/(m-1)$. Finally, the exponent, β, of the logarithm in (3) is the proportion of the elements of $Gal(K_m/\mathbb{Q})$ that have trace zero under the map ρ. By a simple counting argument this is $m/(m^2-1)$ as given. ■

An application of Theorem 1, when K is not necessarily $\mathbb{Q}$, is to the *range* of ideals. Let $\mathfrak{f}$ be an integral ideal in L and denote by $\mathcal{A}(L,\mathfrak{f})$, or just $\mathcal{A}$, the narrow ideal class group $(\mathrm{mod}^\times \mathfrak{f})$. Let $H(\mathfrak{f})$ be the class field $(\mathrm{mod}^\times \mathfrak{f})$, that is the maximal Abelian extension of L ramified only at $\mathfrak{f}$, and let F/K be the Galois hull of H/K. For ideals $\mathfrak{a}_1 \lhd \mathcal{O}_K$ define the range to be

$$
R(\mathfrak{a}_1) = \left\{ [\mathfrak{a}_2] : \mathfrak{a}_2 \lhd \mathcal{O}_L,\ \mathfrak{a}_2 + \mathfrak{f} = \mathfrak{O}_L, N_{L/K}\mathfrak{a}_2 = \mathfrak{a}_1 \right\}
$$

where $[\mathfrak{a}_2]$ is the narrow ideal class, $(\mathrm{mod}^\times \mathfrak{f})$, containing $\mathfrak{a}_2$. So $R(\mathfrak{a}_1) = \emptyset$ if $\mathfrak{a}_1$ is not co-prime to $N_{L/K}\mathfrak{f}$. This definition of the range of an ideal is given in §3 of [5] though the definition of the range of a rational integer is given in [4]. As noted in [5] the function R is multiplicative, Frobenius with respect to F/K and takes values in the power set of $\mathcal{A}$. The power set $2^{\mathcal{A}}$ is a commutative moniod on defining $XY = \{xy : x \in X, y \in Y\}$ for all non-empty $X, Y \in 2^{\mathcal{A}}$ and $XY = \emptyset$ if either X or Y empty. So from Theorem 1 we deduce

Corollary 2 *Assume ℓ satisfies*

$$
\exp(-R(x)) > \ell > \begin{cases} x^{-5(1-\varepsilon)/12 n_K} & \text{if } F/K \text{ abelian} \\ x^{-3(1-\varepsilon)/2(n_F + 3n_K)} & \text{otherwise.} \end{cases} \tag{16}
$$

Then for $R^* \in 2^{\mathcal{A}}, R^* \neq \emptyset$

$$|\{\mathfrak{a}_1 \in \mathcal{S}(x, \psi_0, \ell) : R(\mathfrak{a}_1) = R^*\}| \tag{17}$$

has an asymptotic expansion of the form (2) with $\alpha(R^*)$ no larger than ∂, the Dirichlet density of prime ideals $\mathfrak{p} \lhd \mathcal{O}_K$ for which $R(\mathfrak{p}) \neq \emptyset$.

Similar results have been given in [8] for $\{n \leq x : R(n) = R^*\}$ with an extension L of $\mathbb{Q}$. . The question then examined in that paper is for which R^* do we have $\alpha(R^*) = \partial$? To answer the same question for (17) we need only look at the $\ell = 1/2$ case for which we know, by note (i), that there is a result similar to Corollary 2. We do, though, also give results valid in the interval (16).

Let $\mathfrak{e}$ be the product of all prime ideals of K that ramify in L. Define $H_{\mathfrak{e}}$ to be the subgroup of $2^{\mathcal{A}}$ consisting of those classes that contain fractional ideals prime to $\mathfrak{e}$ and of norm 1. Then to prove an analogue of Theorem 1 of [8] we need look at

$$|\,\{\mathfrak{a} \in \mathcal{S}(x, \psi_0, \ell) : \mathfrak{a} + \mathfrak{e} = \mathcal{O}_K, \emptyset \neq R(\mathfrak{a}) \subseteq \alpha H_{\mathfrak{e}}\}\,|, \tag{18}$$

for any $\alpha \in \mathcal{A}$. The condition $R(\mathfrak{a}) \subseteq \alpha H_{\mathfrak{e}}$ is captured by demanding that $R(\mathfrak{a})H_{\mathfrak{e}} = \alpha H_{\mathfrak{e}}$ which in turn can be captured by a linear sum of characters of $\mathcal{A}$ that are trivial on $H_{\mathfrak{e}}$. In this way we are led to a sum over $\mathfrak{a} \in \mathcal{S}(x, \psi_0, \ell)$, $\mathfrak{a}+\mathfrak{e} = \mathcal{O}_K$, of $\chi(R(\mathfrak{a})H_{\mathfrak{e}})$. This can be estimated by Theorem 1 of [2] to give, for either $\ell = 1/2$ or ℓ satisfying (16), an asymptotic expansion for this sum as in (2), though with no log log terms. The exponent of the logarithm will be $1-\alpha_\chi$ with $\alpha_\chi = \sum_C \chi(R(C)H_{\mathfrak{e}})|C|/|G|$ in the obvious notation since $R(\mathfrak{p})$ is constant on the conjugacy classes C of $G = \mathrm{Gal}(F/K)$. So the largest value of α_χ will occur when $\chi \equiv 1$ when we get ∂. Summing over the characters of $\mathcal{A}$ we get our result for (18) of the type (2) with the largest α equal to ∂.

In fact, Theorem 1 of [2] and its extension in note (iii) of that paper can be applied to the proofs of a number of analogues of results in [8]. For instance, given $\mathfrak{a}_1 \lhd \mathcal{O}_K, \mathfrak{a}_1 + \mathfrak{e} = \mathcal{O}_K$ define

$$r(\mathfrak{a}_1) = \left|\left\{\mathfrak{a}_2 \lhd \mathcal{O}_L, \mathfrak{a}_2 + \mathfrak{f} = \mathcal{O}_L, N_{L/K}\mathfrak{a}_2 = \mathfrak{a}_1\right\}\right|$$

and

$$S(\chi, a_1) = \sum_{\substack{N_{L/K}\mathfrak{a}_2 = \mathfrak{a}_1 \\ \mathfrak{a}_2 + \mathfrak{f} = \mathcal{O}_L}} \chi(\mathfrak{a}_2)$$

where χ is a character on $\mathcal{A}$. Then Theorem 1 of [2] gives an asymptotic result for

$$\sum_{\substack{\mathfrak{a}_1 \in \mathcal{S}(x, \psi_0, \ell) \\ \mathfrak{a}_1 + \mathfrak{e} = \mathcal{O}_K}} \lambda(\mathfrak{a}_1)\,|S(\chi, \mathfrak{a}_1)|^2 \tag{19}$$

where $\lambda(\mathfrak{a}_1) = 0$ if $r(\mathfrak{a}) = 0, \lambda(\mathfrak{a}_1) = r(\mathfrak{a})^{-2}$ otherwise. This should be compared to the (weighted) sum W_χ in equation (6.6) of [8]. The $\ell = 1/2$ case of (19) is sufficient for us to follow the arguments of §6 of [8], deduce that both

$$|\{N\mathfrak{a} \leq x, \mathfrak{a} + \mathfrak{e} = \mathcal{O}_K, R(\mathfrak{a}) = \alpha H_{\mathfrak{e}}\}| \quad \text{and} \quad |\{N\mathfrak{a} \leq x, \mathfrak{a} + \mathfrak{e} = \mathcal{O}_K, \alpha \in R(\mathfrak{a})\}|$$

have the same main term as we would get for (18) when $\ell = 1/2$ and conclude that (17) has an expansion with $\alpha(R^*) = \partial$ if, and only if, R^* is a coset of $H_{\mathfrak{e}}$, a so-called $\mathfrak{e}$-maximal range. A good deal of [8] is concerned with showing that $H_{\mathfrak{e}}$ can be replaced with a subgroup that does not depend on $\mathfrak{e}$. Finally, with our analogues of Theorems 1 and 2 of [8], valid for ℓ satisfying (16) we can deduce that almost all norms in $\mathcal{S}(x, \psi_0, \ell)$, prime to $\mathfrak{e}$, have an $\mathfrak{e}$-maximal range.

Ranges have been used in other problems and for instance we can prove an analogue of Theorem 5 of [5]. Suppose $\mathcal{M}$ is a full $\mathcal{O}_K$-module in $\mathcal{O}_L$. For a principal ideal $\mathfrak{a}_1 = (\alpha) = \alpha O_K$ define $r_0(\mathfrak{a}_1)$ to be the number of principal ideals $\mathfrak{a}_2 = (\mu) = \mu O_L$, $\mu \in \mathcal{M}$ such that $\mathfrak{a}_1 = N_{L/K}\mathfrak{a}_2$. Define the conductor $\mathfrak{f}$ of $\mathcal{M}$ to be the join of all ideals of $\mathcal{O}_L$ contained in $\mathcal{M}$. Then we can define the Galois extension F/K as before.

Corollary 3 *Assume ℓ satisfies (16). Then*

$$|\{\mathfrak{a}_1 \in \mathcal{S}(x, \psi_0, \ell) : r_0(\mathfrak{a}_1) > 0\}| \tag{20}$$

has an expansion as in (2) with dominant term having α equal to the Dirichlet density of the set of prime ideals $\mathfrak{p}_1$ of $\mathcal{O}_K$ expressible as $N_{L/K}\mathfrak{p}_2$ for some prime ideal $\mathfrak{p}_2$ of $\mathcal{O}_L$.

Proof Follow [5] in defining a prime ideal of $\mathcal{O}_L$ to be bad or good respectively if it divides or fails to divide $N_L\mathfrak{f}$. An ideal of $\mathcal{O}_L$ is bad or good respectively if all its prime ideal factors are bad or good. Apply the same terminology to the ideals of $\mathcal{O}_K$. Each ideal $\mathfrak{a}$ of either $\mathcal{O}_L$ or $\mathcal{O}_K$ is uniquely expressible as $\mathfrak{a} = \mathfrak{b}\mathfrak{g}$ with $\mathfrak{b}$ bad and $\mathfrak{g}$ good. Lemma 1.1 of [5] shows that if the good ideals $\mathfrak{g}$ and $\mathfrak{g}'$ of $\mathcal{O}_L$ are in the same narrow ideal class (mod$^\times$ $\mathfrak{f}$) and $\mathfrak{b}$ is a bad ideal of $\mathcal{O}_L$ such that $\mathfrak{b}\mathfrak{g} = \mu\mathcal{O}_L$, for some $\mu \in \mathcal{M}$ then $\mathfrak{b}\mathfrak{g}' = \mu'\mathcal{O}_L$, for some $\mu' \in \mathcal{M}$. Thus we can partition the set of ideals counted in (20) according to the range of the good factors of the $\mathfrak{a}_1$. For each range $R \in 2^{\mathcal{A}}$ let $\mathcal{B}_R$ be the set of bad ideals $\mathfrak{b}_1$ of $\mathcal{O}_K$ such that for all good ideals $\mathfrak{g}_1$ with $R(\mathfrak{g}_1) = R$ we have $\mathfrak{b}_1\mathfrak{g}_1 = N_{L/K}(\mu\mathcal{O}_L)$, for some $\mu \in \mathcal{M}$. Then

$$|\{\mathfrak{a}_1 \in \mathcal{S}(x, \psi_0, \ell) : r_0(\mathfrak{a}_1) > 0\}| =$$

$$= \sum_{R\in 2^{\mathcal{A}}} \sum_{\substack{\mathfrak{b}_1 \in \mathcal{B}_R \\ N\mathfrak{b}_1 \le x(1+\ell)}} |\{\mathfrak{g}_1 \in \mathcal{S}(x/N_K\mathfrak{b}_1, \psi_0 - \psi(\mathfrak{b}_1), \ell) : R(\mathfrak{g}_1) = R\}|$$

It is possible to apply Corollary 2 to each summand but it is simpler to go back to (4) and replace the Dirichlet series by

$$\sum_{R\in 2^{\mathcal{A}}} \sum_{R(\mathfrak{g}_1)=R} \frac{\lambda^{\vec{\mathbf{m}}}(\mathfrak{g}_1)}{N_K\mathfrak{g}_1^s} \sum_{\mathfrak{b}_1\in\mathcal{B}_R} \frac{\lambda^{\vec{\mathbf{m}}}(\mathfrak{b}_1)}{N_K\mathfrak{b}_1^s}.$$

Since bad ideals have only a finite number of different prime ideal factors the Dirichlet series over $\mathfrak{b}_1 \in \mathcal{B}_R$ converges and is regular for $\operatorname{Re} s > 0$. It can be absorbed into $\Lambda_0(s, \vec{\mathbf{m}}, \mathbf{z})$ of (8) that arises from the analysis of the Dirichlet series over $R(\mathfrak{g}_1) = R$. Hence by the method of proof of Theorem 1 we obtain Corollary 3. ■

When $\mathcal{M} = \mathcal{O}_K$ this is a result about the relative norms of principal integral ideals. This can be compared with the results of §2.1 of [2] concerning the relative norm of fractional and integral ideals.

References

[1] M. D. Coleman, *The Hooley-Huxley contour method for problems in number fields I: Arithmetic Functions*, J. Number Theory, **74**, (1999), 250-277.

[2] M. D. Coleman, *The Hooley-Huxley contour method for problems in number fields II: Factorization and Divisibility,* submitted to J. Number Theory.

[3] P. Deligne, J. -P. Serre, *Formes modulaires de poids 1,* Ann. scient. Ec. Norm. Sup., Série 4, **7** (1974), 507-530.

[4] R. W. K. Odoni, *On the norms of algebraic integers*, Mathematika, **22** (1975), 71-80.

[5] R. W. K. Odoni, *Representations of algebraic integers by binary quadratic forms and norm forms of full modules of extension fields,* J. Number Theory, **10**, (1978), 324-333.

[6] R. W. K. Odoni, *The distribution of integral and prime-integral values of systems of full-norm polynomials and affine-decomposable polynomials,* Mathematika **26** (1979), 80-87.

[7] R. W. K. Odoni, *Notes on the method of Frobenian functions, with applications to the coefficients of modular forms,* in: *Elementary and analytic theory of numbers,* Banach Center Publications, vol. 17, Polish Scientific Publishers, Warsaw 1985, pp. 371-403.

[8] R. W. K. Odoni, *On the distribution of norms of ideals in given ray-classes and the theory of central ray-class fields,* Acta Arith. **52** (1989), 373-397.

[9] K. Ramachandra, *Some problems of analytic number theory,* Acta Arith. **31** (1976), 313-324.