LEOPOLDT'S CONJECTURE AND ARITHMETIC STATISTICS

DAVID E. ROHRLICH

ABSTRACT. We observe that Leopoldt's conjecture is equivalent to a simple statement in arithmetic statistics. This observation then leads to a comparison of traditional and nontraditional counting functions.

We begin with an illustrative problem. Let $\widehat{\mathbb{Z}}$ be the compact topological ring of adelic integers, isomorphic to the direct product over all primes p of the p-adic integer rings $\mathbb{Z}_p$, and let $\widehat{\mathbb{Q}}$ be the unique $\widehat{\mathbb{Z}}$-extension of $\mathbb{Q}$ inside some fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Put $\Gamma = \mathrm{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q})$ and let X be the set of characters of Γ. Characters are understood here to be complex-valued and one-dimensional, so that X consist of continuous homomorphisms $\chi : \Gamma \to \mathbb{C}^\times$. By the *order* of χ we mean as usual the smallest positive integer n such that $\chi^n = 1$. Since $\widehat{\mathbb{Z}}$, hence Γ, is procyclic, there are only finitely many $\chi \in X$ of a given order n. In fact the number of such characters is the number of characters of $\mathbb{Z}/n\mathbb{Z}$ of order n, namely $\varphi(n)$, where φ is the Euler totient function. Let $\alpha(x)$ be the number of $\chi \in X$ of order $\leqslant x$. The problem is to determine the asymptotic behavior of $\alpha(x)$.

The solution is straightforward. From the preceding remarks it follows that

$$\alpha(x) = \sum_{n \leqslant x} \varphi(n),$$

but the right-hand side is $3x^2/\pi^2 + O(x^\delta)$ with $\delta < 2$ by a theorem of Dirichlet (in fact $O(x^\delta)$ can be replaced by $O(x \log x)$, a result of Mertens). In particular, $\alpha(x) \sim 3x^2/\pi^2$.

The preceding example rests on the uniqueness of the $\widehat{\mathbb{Z}}$-extension of $\mathbb{Q}$ and hence on the fact that Leopoldt's conjecture holds for $\mathbb{Q}$. In the case of an arbitrary number field K we shall prove that Leopoldt's conjecture for K is equivalent to a statement similar to $\alpha(x) \sim 3x^2/\pi^2$ (Theorem 1). The equivalence is rather formal, with little arithmetic content, but it accentuates our main theme, which is the distinction between traditional and nontraditional arithmetic statistics. The relation $\alpha(x) \sim 3x^2/\pi^2$ is an instance of the latter, because the counting function $\alpha(x)$ is nontraditional. Indeed the elements $\chi \in X$ may be viewed as characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by composition with the quotient map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \Gamma$, so the traditional way of counting them would be to enumerate them by conductor. But instead we have enumerated them by their order. For arbitrary characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ the latter approach is not even possible, because for every $n \geqslant 2$ there are infinitely many characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of order n. But for characters of Γ, enumeration by the order is legitimate, and therefore two questions arise: What happens if we use the *traditional* enumeration by conductor – what asymptotic do we get then? And over number fields, does the traditional enumeration have a connection to Leopoldt's conjecture also?

Only the first question will be considered here. Let us say that a counting function β has *traditional asymptotics* if there are real numbers a, b and c with $c > 0$ such that $\beta(x) \sim cx^a(\log x)^b$ as x goes to infinity. The terminology is meant to reflect the fact that historically, the asymptotic behavior of counting functions in number theory does tend to be of this type. For example:

(i) If $\rho(x)$ is the number of lattice points inside a circle of radius $\sqrt{x}$ then $\rho(x) \sim \pi x$.
(ii) If $\pi(x)$ is the number of primes $\leqslant x$ then $\pi(x) \sim x/\log x$.
(iii) If $\delta(x)$ is the number of ordered pairs of positive integers (d, n), where $d|n$ and $n \leqslant x$, then $\delta(x) \sim x \log x$.
(iv) If $\alpha(x)$ is the number of ordered pairs of positive integers (m, n) where m is relatively prime to n and $n \leqslant x$, then $\alpha(x) \sim 3x^2/\pi^2$, as recalled above.
(v) If $\lambda(x)$ is the number of integers $\leqslant x$ which can be written as the sum of two squares then $\lambda(x) \sim cx/\sqrt{\log x}$ for some $c > 0$.

Of course these formulas are all classical: Example (i), or the problem of bounding the associated error term, is the Gauss circle problem; (ii) is the prime number theorem of Hadamard and de la Vallée Poussin; (iii) and (iv) are due to Dirichlet and (v) to Landau. For a contemporary example one can cite Malle's conjecture on the enumeration of Galois groups [5], which again predicts an asymptotic of the type $cx^a(\log x)^b$. The key point here is that the nontraditional counting function $\alpha(x)$ of the first paragraph has traditional asymptotics.

We can also consider a slightly weaker notion. Given functions f and g with nonnegative values, write $f(x) \ll g(x)$ for $f(x) = O(g(x))$, and $f(x) \asymp g(x)$ for $f(x) \ll g(x) \ll f(x)$. We say that $\beta(x)$ has *traditional growth* if $\beta(x) \asymp x^a(\log x)^b$ for some a and b.

In particular, let $\beta(x)$ be the number of elements $\chi \in X$ of *conductor* $\leqslant x$. By applying standard tauberian theorems and also a result of de Bruijn [3], who appeals to an unusual tauberian theorem of Hardy and Ramanujan [4], we shall prove that $\beta(x)$ does not have traditional growth (Theorem 2). In summary, the nontraditional counting function $\alpha(x)$ has traditional asymptotics, but the traditional counting function $\beta(x)$ does not even have traditional growth.

This is not a new phenomenon. In [8], Sarnak shows that if equivalence classes of primitive indefinite binary quadratic forms are enumerated by the size of the associated fundamental totally positive unit – a decidedly nontraditional means of enumeration – then the resulting asymptotics are traditional, but the best that one can say about the traditional method of enumeration, namely by discriminant, is that an asymptotic result is known only for the *product* of the class number and the totally positive fundamental unit (Siegel [10]), not for the class number alone. See also [9] and papers of Raulf [6], [7]. A more recent illustration of the phenomenon at issue is provided by the work of Ambrose [1] and Zelinski [11]. Let K be any number field other than $\mathbb{Q}$ or an imaginary quadratic field. The results of [1] and [11] strongly suggest that when one-dimensional characters of $\mathrm{Gal}(\overline{K}/K)$ are enumerated by conductor then the resulting counting function does not have traditional growth.

Returning to $\beta(x)$ and the two questions about it raised earlier, we point out that not only is the second question (about a possible connection to Leopoldt's conjecture) unanswered, but to some extent the first is as well. We shall prove that $\beta(x)$ has nontraditional growth, but the precise growth rate remains a mystery.

1. Leopoldt's conjecture

In this section we fix a number field $K \subset \overline{\mathbb{Q}}$. The notations Γ, X, and α introduced below retain their original meaning if $K = \mathbb{Q}$.

Put $d = [K : \mathbb{Q}]$. Thus $d = r_1 + 2r_2$, where r_1 is the number of field embeddings $\sigma : K \hookrightarrow \mathbb{C}$ with $\sigma(K) \subset \mathbb{R}$ and r_2 is half the number of field embeddings $\sigma : K \hookrightarrow \mathbb{C}$ with $\sigma(K) \not\subset \mathbb{R}$. Let $\widehat{K}$ be the compositum of all $\widehat{\mathbb{Z}}$-extensions of K inside $\overline{\mathbb{Q}}$, or equivalently, the compositum of all $\mathbb{Z}_p$-extensions of K as p varies over primes. Put $\Gamma = \mathrm{Gal}(\widehat{K}/K)$ and

$$\nu = r_2 + 1.$$

By the theory of $\mathbb{Z}_p$-extensions of number fields, we have

$$\Gamma \cong \prod_p \mathbb{Z}_p^{\nu_p} \tag{1}$$

with $\nu \leqslant \nu_p \leqslant d$. Leopoldt's conjecture is the assertion that $\nu_p = \nu$ for all p.

Now let X be the set of characters of Γ, and write $\alpha(x)$ for the number of $\chi \in X$ of order $\leqslant x$. We will reformulate Leopoldt's conjecture as a statement about the asymptotic growth of $\alpha(x)$. To do so, let $a(n)$ be the number of $\chi \in X$ of order n, so that

$$\alpha(x) = \sum_{n \leqslant x} a(n). \tag{2}$$

In view of the self-duality of finite abelian groups, $a(n)$ is also the number of elements of $\Gamma/n\Gamma$ of order n. Hence it follows from (1) that $a(n)$ is a multiplicative function of n and that

$$a(p^k) = p^{k\nu_p} - p^{(k-1)\nu_p} \tag{3}$$

for $k \geqslant 1$. In particular, $a(n) \leqslant n^d$, whence the Dirichlet series and Euler product

$$\sum_{n \geqslant 1} a(n) n^{-s} = \prod_p (1 + \sum_{k \geqslant 1} a(p^k) p^{-ks}) \tag{4}$$

converge for $\Re(s) > d + 1$. Denote the left-hand side by $A(s)$ and put

$$A_p(s) = 1 + \sum_{k \geqslant 1} a(p^k) p^{-ks},$$

so that $A(s) = \prod_p A_p(s)$. Inserting (3) in $A_p(s)$ and summing, we obtain

$$A_p(s) = 1 + (1 - p^{-\nu_p}) \frac{p^{\nu_p - s}}{1 - p^{\nu_p - s}}$$

and thus

$$A_p(s) = \frac{1 - p^{-s}}{1 - p^{\nu_p - s}}. \tag{5}$$

Therefore

$$A(s) = \zeta(s)^{-1} \cdot \prod_p (1 - p^{\nu_p - s})^{-1}, \tag{6}$$

where $\zeta(s)$ is the Riemann zeta function. The rationale for introducing $A(s)$ is apparent from (2): It is the Dirichlet series with summatory function $\alpha(x)$, so from its analytic properties one can deduce the asymptotic behavior of $\alpha(x)$ via a tauberian theorem.

Theorem 1. *Put $\rho = \nu + 1 = r_2 + 2$ and $\kappa = (\rho\zeta(\rho))^{-1}$. Then $\nu_p = \nu$ for all p, or in other words, Leopoldt's Conjecture holds for K, if and only if $\alpha(x) \sim \kappa x^\rho$.*

Proof. If $\nu_p = \nu$ for all p then (6) becomes $A(s) = \zeta(s-\nu)/\zeta(s)$. So $A(s)$ has a simple pole at $s = \rho = \nu + 1$ with residue $1/\zeta(\rho)$ and is otherwise holomorphic in the region $\Re(s) > 1$. Thus it follows from Theorem 7.7 of [2] that $\alpha(x) \sim \kappa x^\rho$.

Conversely, suppose that $\nu_p \geqslant \nu + 1$ for some prime p. We will show that the relation $\alpha(x) \sim \kappa x^\rho$ does not hold. We consider three cases:

Case 1: There is a prime p such that $\nu_p \geqslant \nu + 2$.
Case 2: There is a unique prime p such that $\nu_p \geqslant \nu + 1$.
Case 3: There are distinct primes p and q such that $\nu_p, \nu_q \geqslant \nu + 1$.

Of course Cases 2 and 3 cover all possibilities, but it is convenient to consider Case 1 also. The awkwardness of the argument that follows arises from the fact that $A_p(s)$ has infinitely many poles on the line $\Re(s) = \nu_p$, rendering the usual tauberian method inapplicable in some spots.

Case 1: Given $x \gg p$, put $\ell(x) = \lfloor \log_p x \rfloor$, where $\log_p(x) = (\log x)/(\log p)$. Then

$$\sum_{k=0}^{\ell(x)} a(p^k) = p^{\ell(x)\nu_p}$$

by (3). But $\alpha(x)$ is an upper bound for the left-hand side while $p^{\ell(x)} > x/p$. So $\alpha(x) \gg x^{\nu_p}$. Since $\nu_p \geqslant \rho + 1$, this lower bound for $\alpha(x)$ contradicts the relation $\alpha(x) \sim \kappa x^\rho$.

Case 2: We may assume that $\nu_p = \nu + 1 = \rho$, else we are in Case 1. Let $A^*(s)$ be the Euler product $A(s)$ with the Euler factor at p removed. Since p is the unique prime for which $\nu_p \neq \nu$, we have

$$A^*(s) = \frac{\zeta(s-\nu)}{\zeta(s)} \cdot \frac{1 - p^{\nu - s}}{1 - p^{-s}}.$$

Put $c = (p-1)/(p - p^{-\nu})$. Then $A^*(s)$ has a simple pole at $s = \nu + 1 = \rho$ with residue $c/\zeta(\rho)$ and is otherwise holomorphic in the region $\Re(s) > 1$. Therefore, putting

$$\alpha^*(x) = \sum_{\substack{n \leqslant x \\ p \nmid n}} a(n),$$

we have $\alpha^*(x) \sim c\kappa x^\rho$. In particular, $\alpha^*(x) \gg x^\rho$. With $\ell(x)$ as in Case 1, we have

$$\alpha(x) = \sum_{k=0}^{\ell(x)} a(p^k)\alpha^*(x/p^k)$$

and consequently, our lower bound for $\alpha^*(x)$ gives

$$\alpha(x) \gg x^\rho + \sum_{k=1}^{\ell(x)} (p^{k\rho} - p^{(k-1)\rho})(x/p^k)^\rho$$

by (3). Since $(p^{k\rho} - p^{(k-1)\rho}) = (1 - p^{-\rho})p^{k\rho}$, we conclude that $\alpha(x) \gg \ell(x)x^\rho$, whence $\alpha(x) \gg (\log x)x^\rho$. Again, this inequality is incompatible with the relation $\alpha(x) \sim \kappa x^\rho$.

Case 3: We may assume that $\nu_p = \nu_q = \nu+1 = \rho$, else we are in Case 1. Suppose that $q < p$. Given $x \gg p$, let $\ell(x) = \lfloor \log_p x \rfloor$ as before and $\lambda(x) = \lfloor \log_q x \rfloor$. Then

$$\sum_{j=1}^{\lambda(x)} \sum_{k=0}^{\ell(x/q^j)} a(q^j p^k) = \sum_{j=1}^{\lambda(x)} (q^{j\rho} - q^{(j-1)\rho}) \cdot (1 + \sum_{k=1}^{\ell(x/q^j)} (p^{k\rho} - p^{(k-1)\rho}))$$

by (3) and the multiplicativity of $a(n)$. The left-hand side is bounded above by $\alpha(x)$, so we have

$$\alpha(x) \geqslant \sum_{j=1}^{\lambda(x)} (q^{j\rho} - q^{(j-1)\rho}) p^{\rho\ell(x/q^j)}$$

Since $(q^{j\rho} - q^{(j-1)\rho}) = (1 - q^{-\rho}) q^{j\rho}$, we find that

$$\alpha(x) \gg \sum_{j=1}^{\lambda(x)} q^{j\rho} p^{\rho\ell(x/q^j)}. \tag{7}$$

Now $\ell(x/q^j) = \lfloor \log(x/q^j)/\log p \rfloor$, so $p^{\rho\ell(x/q^j)} \gg (x/q^j)^\rho$, whence (7) gives

$$\alpha(x) \gg \lambda(x) x^\rho \gg (\log x) x^\rho.$$

As before, this lower bound is incompatible with the relation $\alpha(x) \sim \kappa x^\rho$. □

2. Arithmetic statistics

We return to the notation of the introduction. Thus $\widehat{\mathbb{Q}}$ is the unique $\widehat{\mathbb{Z}}$-extension of $\mathbb{Q}$ inside $\overline{\mathbb{Q}}$ and X is the set of characters of the group $\Gamma = \mathrm{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q})$. But this time we consider the traditional counting function

$$\beta(x) = \sum_{n \leqslant x} b(n), \tag{8}$$

where $b(n)$ is the number of characters in X of *conductor* n.

We claim that for odd primes p,

$$b(p^k) = \begin{cases} (p-1)p^{k-2} & \text{if } k \geqslant 2, \\ 1 & \text{if } k = 0, \\ 0 & \text{if } k = 1. \end{cases} \tag{9}$$

Indeed if χ is a nontrivial character of the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and the conductor of χ is p^k then $k \geqslant 2$ and the order of χ is p^{k-1}. Hence the number of such characters is $\varphi(p^{k-1})$. The reasoning is the same for $p = 2$, except that the first layer of the $\mathbb{Z}_2$-extension of $\mathbb{Q}$ is the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ of conductor 8. Thus

$$b(2^k) = \begin{cases} 2^{k-3} & \text{if } k \geqslant 3, \\ 1 & \text{if } k = 0, \\ 0 & \text{if } k = 1 \text{ or } k = 2. \end{cases} \tag{10}$$

Since the multiplicativity of $b(n)$ is immediate from its definition, (9) and (10) determine $b(n)$ uniquely.

Given functions $f(x)$ and $g(x)$ which go to infinity with x, we say that g *grows faster* than $f(x)$, or that f *grows more slowly* than g, if $f(x) = o(g(x))$, in other words if $\lim_{x\to\infty} f(x)/g(x) = 0$. The following statement implies that $\beta(x)$ has nontraditional growth, as asserted in the introduction.

Theorem 2. *The function $\beta(x)$ grows faster than $x\log^m x$ for every positive integer m but more slowly than $x^{1+\varepsilon}$ for every $\varepsilon > 0$.*

As a first step toward proving the theorem, we consider the set $\mathcal{N}$ of positive integers n such that $b(n) \neq 0$. It follows from (9) and (10) that $n \in \mathcal{N}$ if and only if two conditions hold:

(i) $2|n \Rightarrow 8|n$.
(ii) If p is an odd prime, then $p|n \Rightarrow p^2|n$.

Given (i), we can of course omit the word *odd* in (ii). By the *radical* of a positive integer n we mean the product of the distinct prime factors of n, where the empty product is understood to be 1. Denote the radical of n by $\mathrm{rad}(n)$, and put

$$\mathrm{rad}^*(n) = \begin{cases} \mathrm{rad}(n) & \text{if } n \text{ is odd,} \\ 2\,\mathrm{rad}(n) & \text{if } n \text{ is even.} \end{cases} \tag{11}$$

We claim that

$$b(n) = \begin{cases} \varphi(n)/\mathrm{rad}^*(n) & \text{if } n \in \mathcal{N}, \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

It suffices to observe that both sides are multiplicative and that by (9) and (10) they agree if n is a prime power.

We are now in a position to derive the upper bound in Theorem 2 from a result of de Bruijn [3]. By (12),

$$\beta(x) = \sum_{\substack{n\leqslant x\\ n\in\mathcal{N}}} \varphi(n)/\mathrm{rad}^*(n). \tag{13}$$

Since $\varphi(n) \leqslant n$ and $\mathrm{rad}(n) \leqslant \mathrm{rad}^*(n)$, it follows that

$$\beta(x) \leqslant x \sum_{n\leqslant x} \mathrm{rad}(n)^{-1}, \tag{14}$$

where the sum now runs over all positive integers $n \leqslant x$. Call this sum $\gamma(x)$, so that (14) becomes

$$\beta(x) \leqslant x\gamma(x). \tag{15}$$

By Theorem 1 of [3], $\log\gamma(x) \sim \ell(x)$, where $\ell(x) = \sqrt{8\log x}/\sqrt{\log\log x}$ for $x > e$. In particular we have, say, $\log\gamma(x) < 2\ell(x)$ for large x, so that $\beta(x) < xe^{2\ell(x)}$ by (15). But $e^{2\ell(x)}$ grows more slowly than x^ε for every $\varepsilon > 0$.

We now turn to the lower bound in Theorem 2. The proof involves four Dirichlet series, to be denoted $D_k(s)$, $D(s)$, $Z(s)$, and $D_{\mathbf{k}}(s)$.

Let $\mathcal{S}$ be the set of square-free odd positive integers, and observe that if $n \in \mathcal{S}$ and $k \geqslant 2$ then $n^k \in \mathcal{N}$. For $\Re(s) > 1$ consider the Dirichlet series

$$\sum_{n\in\mathcal{S}} \varphi(n)n^{k-2}n^{-ks} = \prod_{p\neq 2}(1 + (p-1)p^{k-2}p^{-ks}). \tag{16}$$

We denote this Dirichlet series $D_k(s)$ and write $\delta_k(s)$ for the associated summatory function:

$$\delta_k(x) = \sum_{\substack{n^k\leqslant x\\ n\in\mathcal{S}}} \varphi(n)n^{k-2}. \tag{17}$$

It follows from (9) that if $n \in \mathcal{S}$ then $b(n^k) = \varphi(n)n^{k-2}$, whence $\delta_k(x) \leqslant \beta(x)$.

Next, $D(s)$ is the Dirichlet series

$$\sum_{n\in\mathcal{S}} \varphi(n)n^{-s} = \prod_{p\neq 2}(1 + (p-1)p^{-s}). \tag{18}$$

It is introduced here to facilitate the calculations: Referring to (16), we see that

$$D_k(s) = D(ks - k + 2). \tag{19}$$

Using (18), we define a branch of $\log D(s)$ for $\Re(s) > 2$ by

$$\log D(s) = \sum_{p\neq 2}(p-1)p^{-s} + \sum_{p\neq 2}\sum_{n\geqslant 2}(-1)^{n-1}\frac{(p-1)^n p^{-ns}}{n}$$

so that

$$\log D(s) = \sum_{p\neq 2} p^{1-s} - \sum_{p\neq 2} p^{-s} + \sum_{p\neq 2}\sum_{n\geqslant 2}(-1)^{n-1}\frac{(p-1)^n p^{-ns}}{n}. \tag{20}$$

The middle sum converge absolutely for $\Re(s) > 1$, while the double sum converges absolutely at least for $\Re(s) > 3/2$: Indeed if $\Re(s) = 3/2 + \varepsilon$ with $\varepsilon > 0$ then

$$|(p-1)^n p^{-ns}/n| < p^{n(1-s)} = p^{-n(1/2+\varepsilon)},$$

whence

$$|\sum_{n\geqslant 2}(-1)^{n-1}(p-1)^n p^{-ns}/n| < \frac{p^{-1-2\varepsilon}}{1 - p^{-(1/2+\varepsilon)}}.$$

The right-hand side is bounded by $cp^{-1-2\varepsilon}$, where c is a constant independent of p. For example, we can take $c = 1/(1 - 2^{-(1/2+\varepsilon)})$. It follows that the double sum is convergent for $\Re(s) > 3/2$ as claimed. Returning to (20), we conclude that

$$\log D(s) = \sum_{p\neq 2} p^{1-s} + f(s), \tag{21}$$

where $f(s)$ is holomorphic in the region $\Re(s) > 3/2$.

Next we put $Z(s) = (1 - 2^{1-s})\zeta(s-1)$ and

$$\log Z(s) = \sum_{p\neq 2} p^{1-s} + \sum_{p\neq 2}\sum_{n\geqslant 2}\frac{p^{n(1-s)}}{n}$$

for $\Re(s) > 2$. Again, the double sum converges absolutely in the region $\Re(s) > 3/2$, because if $s = 3/2 + \varepsilon$ with $\varepsilon > 0$ then

$$|p^{n(1-s)}/n| \leqslant p^{-n(1/2+\varepsilon)},$$

whence

$$|\sum_{n\geqslant 2} p^{n(1-s)}/n| \leqslant cp^{-1-2\varepsilon}$$

with $c = 1/(1 - 2^{-(1/2+\varepsilon)})$ as before. Thus

$$\log Z(s) = \sum_{p\neq 2} p^{1-s} + g(s), \tag{22}$$

where $g(s)$ is holomorphic in the region $\Re(s) > 3/2$.

Finally, we subtract (22) from (21) and exponentiate both sides of the resulting equation. We obtain $D(s) = Z(s)e^{h(s)}$, where $h(s)$ is $f(s) - g(s)$ and thus is holomorphic in the region $\Re(s) > 3/2$. To recover $D_k(s)$, precompose the functions

D, Z, and h with $s \mapsto ks - k + 2$, which maps the region $\Re(s) > 1$ bijectively onto the region $\Re(s) > 2$ and and the region $\Re(s) > 1 - 1/(2k)$ bijectively onto the region $\Re(s) > 3/2$. Recalling (19), we obtain

$$D_k(s) = (1 - 2^{-(ks-k+1)})\zeta(ks - k + 1)e^{h(ks-k+2)}.$$

Note that the pole at $s = 1$ of $\zeta(ks - k + 1)$ gives a pole of $D_k(s)$, because the residue $e^{h(2)}/(2k)$ is nonzero. We summarize these facts as follows:

Proposition 1. *The holomorphic function $D_k(s)$, initially defined for $\Re(s) > 1$, extends to a meromorphic function in the region $\Re(s) > 1 - 1/(2k)$ having a simple pole at $s = 1$ and no other singularities.*

Recalling (17), we can now deduce that $\delta_k(x) \sim \kappa x$, where $\kappa > 0$ is the residue of $D_k(s)$ at $s = 1$. And since $\beta(x) \geqslant \delta_k(x)$ we obtain $\beta(x) \gg x$. But for the stronger assertion in Theorem 2 we need to go one step further.

Choose a vector $\mathbf{k} = (k_1, k_2, \ldots, k_m)$ where the k_μ are integers $\geqslant 2$ satisfying

$$k_1 + k_2 + \cdots + k_\mu < k_{\mu+1} \tag{23}$$

for $1 \leqslant \mu \leqslant m - 1$. We claim that the value of a subsum of the k's uniquely determines the set of summands in the subsum. Or to state the claim more formally:

Lemma. *Given a vector $\mathbf{k} = (k_1, k_2, \ldots, k_m)$ as above, suppose that*

$$k_{\mu_1} + k_{\mu_2} + \cdots + k_{\mu_i} = k_{\nu_1} + k_{\nu_2} + \cdots + k_{\nu_j} \tag{24}$$

with $\mu_1 < \mu_2 < \cdots < \mu_i$ and $\nu_1 < \nu_2 < \cdots < \nu_j$. Then $i = j$ and $\mu_l = \nu_l$ for $1 \leqslant l \leqslant i = j$.

Proof. If $\mu_i > \nu_j$ then (23) ensures that k_{μ_i} is strictly greater that the right-hand side of (24). If $\mu_i < \nu_j$ then k_{ν_j} is strictly greater than the left-hand side of (24). Therefore $\mu_i = \nu_j$, and after subtracting k_{μ_i} $(= k_{\nu_j})$ from both sides of (24) we can complete the argument by induction. □

Next we put

$$D_{\mathbf{k}}(s) = \prod_{\mu=1}^{m} D_{k_\mu}(s) \tag{25}$$

and write

$$D_{\mathbf{k}}(s) = \sum_{n \geqslant 1} d_{\mathbf{k}}(n) n^{-s}$$

and

$$\delta_{\mathbf{k}}(x) = \sum_{n \leqslant x} d_{\mathbf{k}}(n). \tag{26}$$

By Proposition 1, $D_{\mathbf{k}}(s)$ has a pole of order m at $s = 1$ and no other singularities in the region $\Re(s) > 1 - 1/(2k_m)$. Applying a standard tauberian theorem, we deduce that $\delta_{\mathbf{k}}(x) \sim \kappa x(\log x)^{m-1}$ for some positive constant κ. We shall prove that $\beta(x) \geqslant \delta_{\mathbf{k}}(x)$. Granting this, we have $\beta(x) \gg x(\log x)^{m-1}$. And since m is arbitary we can replace m by $m + 2$ and conclude that $\beta(x)$ grows faster then $x(\log x)^m$ for any m. It remains to prove:

Proposition 2. $\delta_{\mathbf{k}}(x) \leqslant \beta(x)$.

Proof. In view of the definitions (8) and (26), it suffices to show that $d_{\mathbf{k}}(n) \leqslant b(n)$ for all n. Since this is vacuously true if $d_{\mathbf{k}}(n) = 0$, we may assume that

$$n = \prod_{\mu=1}^{m} n_\mu^{k_\mu} \tag{27}$$

for some integers $n_\mu \in \mathcal{S}$. We fix a choice of such integers for which (27) holds. A key point to be proved is that only one such choice is possible.

Write the prime factorization of n as

$$n = \prod_p p^{\lambda_p}, \tag{28}$$

where the product is taken over all primes p, with $\lambda_p = 0$ for all but finitely many p. Any subtletly in verifying that $d_{\mathbf{k}}(n) \leqslant b(n)$ stems from the fact that there may be a prime p which occurs with positive exponent in (28) and which divides two different factors n_μ and n_ν with $\mu \neq \nu$. If this is not the case, in other words if the n_μ are pairwise relatively prime, then each nonzero exponent in (28) is equal to k_μ for a unique μ, and consequently

$$n_\mu = \prod_{p \in P_\mu} p^{k_\mu}$$

with $P_\mu = \{p : \lambda_p = k_\mu\}$. Thus the factors n_μ in (27) are uniquely determined by n, so that $d_{\mathbf{k}}(n)$, instead of being a *sum* of products of coefficients contributed by the series $D_{k_\mu}(s)$, is equal to a single such product:

$$d_{\mathbf{k}}(n) = \prod_{\mu=1}^{m} \varphi(n_\mu) n_\mu^{k_\mu - 2}. \tag{29}$$

And because the factors n_ν are coprime in pairs, the right-hand side of (29) is also $b(n)$. Here we are using (9) and the multiplicativity of $b(*)$ as well as the fact that the elements of $\mathcal{S}$ are odd. Thus if the n_μ are pairwise relatively prime then the desired relation $d_{\mathbf{k}}(n) \leqslant b(n)$ holds with equality.

Now consider the general case. Let p be a prime dividing n. Then

$$\lambda_p = k_{\mu_1} + k_{\mu_2} + \cdots + k_{\mu_i}, \tag{30}$$

where $\{\mu_1, \mu_2, \ldots, \mu_i\}$ is the set of indices μ such that p divides n_μ. Now initially we simply fixed a choice of the n_μ for which (27) held. But λ_p is uniquely determined by n via (28). And $\mu_1, \mu_2, \ldots, \mu_i$ are uniquely determined by λ_p thanks to (30) and the lemma. In other words, $\mu_1, \mu_2, \ldots, \mu_i$ are uniquely determined by n and p, and they are characterized as the indices μ for which the square-free integer n_μ is divisible by p. Since this is true for every prime p dividing n, we conclude that the factors $n_1, n_2, \ldots, n_m$ in (27) are uniquely determined by n. We deduce as before that $d_{\mathbf{k}}(n)$ is the single product shown in (29), not a sum of such products. But this time the factors n_μ in (27) are not necessarily relatively prime in pairs.

To deal with this problem, we use the elementary fact that for arbitrary positive integers v and w,

$$\varphi(v)\varphi(w) \leqslant \varphi(vw) \tag{31}$$

and

$$\operatorname{rad}(vw) \leqslant \operatorname{rad}(v)\operatorname{rad}(w) \tag{32}$$

with equality if v and w are relatively prime. Put $\psi(v) = \varphi(v)/\mathrm{rad}(v)$. It follows from (31) and (32) that

$$\psi(v)\psi(w) \leqslant \psi(vw). \tag{33}$$

Now since the elements of $\mathcal{S}$ are square-free, (29) can be written

$$d_{\mathbf{k}}(n) = \prod_{\mu=1}^{m} \psi(n_\mu^{k_\mu}). \tag{34}$$

On the other hand, recalling once again that the elements of $\mathcal{S}$ are odd, so that the first alternative holds in (11), we see by (12) that

$$b(n) = \psi(\prod_{\mu=1}^{m} n_\mu^{k_\mu}) \tag{35}$$

The proposition follows from (33), (34), and (35). □

References

[1] C. Ambrose, *On Artin's primitive root conjecture and a problem of Rohrlich*, Math. Proc. Cambridge Philos. Soc. 157 (2014), 79–99.

[2] P. T. Bateman and H. G. Diamond, *Analytic Number Theory: An Introductory Course.* World Scientific (2004).

[3] N. G. de Bruijn, *On the number of integers $\leq x$ whose prime factors divide n*, Illinois J. Math. 6 (1962), 137 – 141.

[4] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quarterly J. Math. 48 (1917), 76-92.

[5] G. Malle, *On the distribution of Galois groups, II*, Experimental Math. 13 (2004), 129 – 135.

[6] N. Raulf, *Asymptotics of class numbers for progressions and for fundamental discriminants*, Forum Math. 21 (2009), 221–257.

[7] N. Raulf, *Limit distribution of class numbers for discriminants in progressions and fundamental discriminants*, Internat. J. of Number Thy. 12 (2016), 1237 – 1258.

[8] P. Sarnak, *Class numbers of indefinite binary quadratic forms*, J. Number Thy. 15 (1982), 229-247.

[9] P. Sarnak, *Class numbers of indefinite binary quadratic forms II*, J. Number Thy. 21 (1985), 333-346.

[10] C. L. Siegel, *The average measure of quadratic forms with given determinant and signature*, Ann. of Math. 45 (1944), 667 - 685.

[11] J. Zelinski, *Upper bounds for the number of primitive ray class characters with conductor below a given bound*, Acta Arithmetica 174 (2016) 297-308.

Department of Mathematics and Statistics, Boston University, Boston, MA 02215
E-mail address: rohrlich@math.bu.edu