QUATERNIONIC ARTIN REPRESENTATIONS OF $\mathbb{Q}$

DAVID E. ROHRLICH

Abstract. Isomorphism classes of dihedral Artin representations of $\mathbb{Q}$ can be counted asymptotically using Siegel's asymptotic averages of class numbers of binary quadratic forms. Here we consider the analogous problem for quaternionic representations. While an asymptotic formula is out of our reach in this case, we show that the asymptotic behavior in the two cases is quite different.

Two asymptotic relations in Galois theory can serve as our point of departure. The first pertains to $\vartheta^{\mathrm{di}}(x)$, the number of isomorphism classes of dihedral Artin representations of $\mathbb{Q}$ with conductor $\leqslant x$: The relation we have in mind is

$$\vartheta^{\mathrm{di}}(x) \sim \frac{\pi}{36\zeta(3)^2}\, x^{3/2} \tag{1}$$

for $x \to \infty$. This follows from Siegel's work on average values of class numbers of binary quadratic forms (see formulas (2) and (22) of [21] and Theorem 2 of [20]). The second relation arises in Klüners' work [12] on Malle's conjecture [15]. Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, a number field $k \subset \overline{\mathbb{Q}}$, and a finite group G, and write $Z(k, G; x)$ for the number of Galois extensions K of k inside $\overline{\mathbb{Q}}$ such that $\mathrm{Gal}(K/k) \cong G$ and the absolute norm of the relative discriminant of K/k is $\leqslant x$. Klüners considers the case where G is dicyclic of order $4m$. For $m = 3$ or m a power of 2 he shows that $Z(k, G; x) \sim x^a$ with $a = 1/(2m)$, while for primes $m \geqslant 5$ he obtains

$$x^a \ll Z(\mathbb{Q}, G; x) \ll x^{a+\varepsilon}, \tag{2}$$

where $\varepsilon > 0$ is arbitrary. He remarks that the asymptotic equality $Z(k, G; x) \sim x^a$ would follow also for primes $m \geqslant 5$ if one had better bounds on m-ranks of ideal class groups than are presently known.

This note is situated at the crossroads of (1) and (2). On the one hand, we count Artin representations ordered by conductor as in (1) rather than number fields ordered by discriminant as in (2). On the other hand, the Galois groups underlying our Artin representations are dicyclic as in (2) rather than dihedral as in (1), and we obtain only upper and lower bounds rather than an asymptotic equality. It should be added, however, that our lower bound depends in the first instance on an unproven conjecture of Erdős as extended to number fields by Ambrose. It is only thanks to Ambrose's work [2] in the direction of his conjecture that we are able to give an unconditional lower bound at all.

To state our result precisely we make some definitions. We begin by introducing the relevant finite groups, which have a presentation of the form

$$Q_{4m} = \langle a, b | a^{2m} = 1, a^m = b^2, bab^{-1} = a^{-1} \rangle$$

with $m \geqslant 2$. Thus for $m = 2$ we have the quaternion group Q_8, for m a power of 2 the generalized quaternion groups, and for arbitrary $m \geqslant 2$ the groups which are sometimes also included under the heading "generalized quaternion groups"

(cf. [16], p. 72) but more often referred to as the dicyclic groups Dic_m. In this note we shall use the term *quaternionic representation* to mean an irreducible two-dimensional monomial symplectic representation of a finite group. It is a fact that the image of every such representation is isomorphic to $Q_{4m} = \mathrm{Dic}_m$ for some $m \geqslant 2$. Conversely, the faithful irreducible representations of these groups are all two-dimensional, monomial, and symplectic. The term *quaternionic representation* is modeled on *dihedral representation*, and we recover a characterization of the latter if in the preceding three sentences we replace "symplectic" by "orthogonal" and the groups $Q_{4m} = \mathrm{Dic}_m$ ($m \geqslant 2$) by the dihedral groups D_{2m} ($m \geqslant 3$).

Now let $\vartheta^{\mathrm{qu}}(x)$ be the number of isomorphism classes of quaternionic Artin representations of $\mathbb{Q}$ of conductor $\leqslant x$. It is beyond our reach to prove that

$$x^{1-\varepsilon} \ll \vartheta^{\mathrm{qu}}(x) \ll x/\log x \qquad (x \geqslant 2) \tag{3}$$

for every $\varepsilon > 0$, but thanks to Ambrose's result [2] we have at least:

Theorem. *If $\varepsilon > 1/(4\sqrt{e}) = .15163\ldots$, then* (3) *holds.*

As we have already indicated, the validity of (3) for all $\varepsilon > 0$ does follow from the conjecture of Erdős and Ambrose, which we now describe.

There are actually two versions. Fix a number field k and a real number $\delta > 0$, and let $\pi_{k,\delta}(x)$ be the number of prime ideals $\mathfrak{p}$ of k of absolute norm $\leqslant x$ such that every prime divisor ℓ of $\mathbf{N}\mathfrak{p} - 1$ satisfies $\ell < x^\delta$ (note that this last inequality is vacuous unless $\delta < 1$). The case $k = \mathbb{Q}$ of the following conjecture is attributed to Erdős on p. 704 of [1], albeit without any bibliographical reference:

Conjecture A. *For all number fields k and real numbers $\delta > 0$,*

$$\pi_{k,\delta}(x) \gg x/(\log x) \qquad (x \geqslant 2), \tag{4}$$

where the implicit constant depends on k and δ.

I do not know whether a statement of Conjecture A for $k = \mathbb{Q}$ can be found in Erdős's published work, but his engagement with the underlying issue is evident already in his result, proved in 1935, that if $k = \mathbb{Q}$ then there exists a number $\delta < 1$ such that (4) is satisfied ([7], p. 212, Lemma 4). Since the same is true for any number field (in other words, given k there exists $\delta < 1$ such that (4) is satisfied; cf. [18], p. 385, Proposition 1), it seems natural to extend his conjecture to arbitrary number fields. In fact Ambrose [2] has already done so, except that he extends a slightly weaker form of Erdős's conjecture stated for example on p. 390 of [14]:

Conjecture B. *For all number fields k and real numbers $\gamma, \delta > 0$,*

$$\pi_{k,\delta}(x) \geqslant x/(\log x)^{1+\gamma} \tag{5}$$

provided x is sufficiently large, where "sufficiently large" depends on k, γ, and δ.

This formulation (for $k = \mathbb{Q}$) seems to be favored in the literature, probably because better values of δ can be obtained for (5) than for (4); compare Pomerance [17] with Balog [4], Friedlander [8], and Baker and Harman [3]. In any case, Conjecture B suffices for our application. Indeed let $\mathcal{K}$ be the set of real quadratic fields K inside some fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ such that the discriminant of K is a product of distinct primes congruent to 1 mod 4. The lower bound in (3) follows for all $\varepsilon > 0$ if we know that (5) holds for some $K \in \mathcal{K}$, some $\gamma > 0$, and all $\delta > 0$.

But even if we grant the conjecture in its strongest form, we do not obtain an asymptotic equality as in (1). There are two obstacles. The first is the difficulty of separating class numbers from fundamental units in real quadratic fields. This issue does not arise in connection with (1) because when one counts ring class characters of quadratic fields, the imaginary quadratic fields predominate. True, Siegel's formula for positive discriminants has the same order of growth as for negative discriminants, namely a constant times $x^{3/2}$, but when one removes the log of the fundamental unit by partial summation then the contribution of the positive discriminants is only $x^{3/2}/\log x$. By contrast, quaternionic Artin representations of $\mathbb{Q}$ can be induced only from real quadratic fields, and therefore the shallowness of our method can no longer be hidden in an error term.

The second obstacle is that the ray class characters that we are counting – we call them "conjugate-symplectic" characters – form a *coset* of the group of ring class characters (to a given modulus, of a given field), and in general it seems difficult to predict whether this coset is *nonempty*, or in other words, whether a single conjugate-symplectic character to the given modulus exists. This problem does happen to have an easy solution if $K \in \mathcal{K}$, a fact on which our lower bound for $\vartheta^{\mathrm{qu}}(x)$ depends.

The referee has asked whether other classes of Artin representations can be treated by the methods of this note. As Ambrose's result is very general – the estimate (5) holds for $\gamma = 1$, $\delta > 1/(2\sqrt{e})$, and all abelian number fields k – one could try to count all irreducible monomial Artin representations of $\mathbb{Q}$ induced from abelian number fields k of a given degree n. The case $n = 2$ is considered in [20] and an asymptotic equality comparable to (1) is obtained. But there again we are taking advantage of the fact that the imaginary quadratic fields predominate. For $n \geqslant 3$ there is no escape: If $[k : \mathbb{Q}] \geqslant 3$ then k has units of infinite order, and an asymptotic equality by the methods of this paper is out of the question. On the other hand, it may be possible to obtain upper and lower bounds as in (3), but as n increases so does the challenge of controlling the units.

The referee has also suggested that an outline of the paper would be helpful. We begin in §1 with some elementary group-theoretic remarks about conjugate-symplectic characters. In §2 we transfer the discussion to the setting of number fields, observing in particular that conjugate-symplectic characters do not exist for imaginary quadratic fields. Ring class numbers are introduced in §3 and are used in §4 to define a Dirichlet series $B(s)$ and its associated summatory function $\beta(x)$. A tauberian theorem then gives an asymptotic formula for $\beta(x)$, which is combined in §5 with an elementary lower bound for fundamental units to give the upper bound for $\vartheta^{\mathrm{qu}}(x)$ in (3). In §6 we turn our attention to the lower bound. After verifying in §7 that the contribution of the quadratic ring class characters is negligible, we count ring class characters of arbitrary order in §8. Our method is crude in the sense that we are limited to ring class characters of a fixed $K \in \mathcal{K}$, but granting this limitation, we deduce our lower bound for $\vartheta^{\mathrm{qu}}(x)$ from Ambrose's theorem [2] via a method of Luca and Sankaranarayanan [14]. While [14] is a vast improvement on the naïve approach in §2 of [18], here we have the additional complication that imprimitive characters must be excluded. Largely as a result of this complication, §8 occupies more than a quarter of the paper.

1. Conjugate-symplectic characters

We recall a few facts about group representations. The groups we have in mind are finite or perhaps profinite, and if we are thinking of the latter then terms like *abelianization* should be interpreted in the category of topological groups. But we consider only continuous finite-dimensional representations over $\mathbb{C}$, and as all such representations of profinite groups factor through representations of finite groups, it will suffice to discuss the latter. One-dimensional characters will often be referred to simply as characters, and the trivial one-dimensional character of any group will be denoted 1.

Given a finite group G and a subgroup H, we let $\mathrm{tran}_{G/H} : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ be the transfer, where the superscript "ab" denotes abelianization. If $\xi : H \to \mathbb{C}^\times$ is a one-dimensional character then $\mathrm{ind}_H^G \xi$ denotes the representation of G induced by ξ. Since one-dimensional characters of a group factor through its abelianization, we may view ξ and $\det \circ \mathrm{ind}_H^G \xi$ as characters of H^{ab} and G^{ab} respectively, and according to a standard formula,

$$\det \circ \mathrm{ind}_H^G \xi = (\mathrm{sign}_{G/H}) \cdot (\xi \circ \mathrm{tran}_{G/H}),$$

where $\mathrm{sign}_{G/H}$ is the sign character of the permutation representation of G on the cosets of H. In particular, if $[G : H] = 2$, as we shall henceforth assume, then we deduce a necessary and sufficient condition for $\mathrm{ind}_H^G \xi$ to be symplectic: Since a two-dimensional symplectic representation is simply a two-dimensional representation with trivial determinant, the equality

$$\xi \circ \mathrm{tran}_{G/H} = \mathrm{sign}_{G/H} \tag{6}$$

is precisely the condition at issue. We call a character ξ of H satisfying (6) *conjugate-symplectic*. Thus:

Proposition 1. *Let G be a finite group, H a subgroup of index two, and $\xi : H \to \mathbb{C}^\times$ a one-dimensional character. Then $\mathrm{ind}_H^G \xi$ is symplectic if and only if ξ is conjugate-symplectic.*

Next consider an element $g \in G \smallsetminus H$, so that g represents the nonidentity coset of H. For any character ξ of H, let ξ^g be the character $h \mapsto \xi(ghg^{-1})$. We say that ξ is *conjugate-self-dual* if

$$\xi^g = \xi^{-1}. \tag{7}$$

Applying Mackey's criterion and Frobenius reciprocity, we deduce:

Proposition 2. *Suppose that ξ is conjugate-self-dual. Then $\mathrm{ind}_H^G \xi$ is irreducible if and only if ξ has order $\geqslant 3$. Furthermore, if $\mathrm{ind}_H^G \xi$ is irreducible then ξ and ξ^{-1} are precisely the characters of H which induce $\mathrm{ind}_H^G \xi$.*

Proposition 2 applies in particular to conjugate-symplectic characters, for they are easily seen to be conjugate-self-dual. So are *conjugate-orthogonal* characters, namely those for which

$$\xi \circ \mathrm{tran}_{G/H} = 1. \tag{8}$$

The following statement is an immediate consequence of the definitions:

Proposition 3. *The set of conjugate-symplectic characters of H, if nonempty, is a coset of the group of conjugate-orthogonal characters of H.*

Remark. The analogue of Proposition 1 is false for conjugate-orthogonal characters because necessity fails. Indeed if G is cyclic of order 4 and ξ is the quadratic character of the subgroup H of index 2 then $\mathrm{ind}_H^G \xi = \psi \oplus \psi^{-1}$, where ψ is either of the quartic characters of G. Hence $\mathrm{ind}_H^G \xi$ is both orthogonal and symplectic. By Proposition 1, ξ satisfies (6) and thus does not satisfy (8).

2. Conjugate-symplectic characters of real quadratic fields

All number fields are understood to be subfields of some fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Thus if k is a number field then an Artin representation of k is a continuous finite-dimensional complex representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$, or what amounts to the same thing, a representation of $\mathrm{Gal}(K/k)$ for an appropriate finite Galois extension K of k. Given any finite extension K of k, Galois or not, we write $\mathrm{tran}_{K/k}$ for the transfer from $\mathrm{Gal}(\overline{\mathbb{Q}}/k)^{\mathrm{ab}}$ to $\mathrm{Gal}(\overline{\mathbb{Q}}/K)^{\mathrm{ab}}$, and if ξ is an Artin representation of K then we put $\mathrm{ind}_{K/k}\xi = \mathrm{ind}_H^G \xi$ with $G = \mathrm{Gal}(\overline{\mathbb{Q}}/k)$ and $H = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$.

The conductor of an Artin representation ρ of k is an ideal $\mathfrak{q}(\rho)$ of the ring of integers $\mathcal{O}_k$ of k, and we denote the absolute norm of $\mathfrak{q}(\rho)$ by $q(\rho)$. Thus if K is a finite extension of k and ξ a one-dimensional character of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ then

$$q(\mathrm{ind}_{K/k}\xi) = d_{K/k} q(\xi), \tag{9}$$

where $d_{K/k}$ is the absolute norm of the relative discriminant ideal of K/k. Of course if $k = \mathbb{Q}$ then $\mathcal{O}_k = \mathbb{Z}$ and $\mathfrak{q}(\rho) = q(\rho)\mathbb{Z}$, and we refer to $q(\rho)$ itself as the conductor of ρ. Furthermore (9) becomes

$$q(\mathrm{ind}_{K/\mathbb{Q}}\xi) = d_K q(\xi), \tag{10}$$

where d_K is $d_{K/\mathbb{Q}}$, in other words, the absolute value of the discriminant of K.

Now let K be a quadratic field, and write $\mathrm{sign}_{K/\mathbb{Q}}$ for the quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Adapting (6) and (8) to the present setting, we call a character ξ of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ *conjugate-symplectic* or *conjugate-orthogonal* if

$$\xi \circ \mathrm{tran}_{K/\mathbb{Q}} = \mathrm{sign}_{K/\mathbb{Q}} \tag{11}$$

or

$$\xi \circ \mathrm{tran}_{K/\mathbb{Q}} = 1 \tag{12}$$

respectively. Then Proposition 1 gives:

Proposition 4. *The two-dimensional monomial symplectic Artin representations of* $\mathbb{Q}$ *are precisely the representations* $\mathrm{ind}_{K/\mathbb{Q}}\xi$*, where* K *is a quadratic field and* ξ *is a conjugate-symplectic character of* $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$.

In contrast to conjugate-orthogonal characters, which exist for every quadratic field K, conjugate-symplectic characters do not exist if K is imaginary:

Proposition 5. *If* K *is a quadratic field and* ξ *is a conjugate-symplectic character of* $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ *then* K *is real.*

Proof. Suppose that K is imaginary, and let $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be complex conjugation relative to some embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. The definition of the transfer gives $\mathrm{tran}_{K/\mathbb{Q}}(g) = g^2 = 1$, whence $\mathrm{sign}_{K/\mathbb{Q}}(g) = 1$ by (11), contradicting the fact that g represents the nontrivial coset of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. □

Given a number field k, let $\mathbb{A}_k$ denote the adele ring of k. Idele class characters of k will be viewed as continuous homomorphisms $\xi : \mathbb{A}_k^\times \to \mathbb{C}^\times$ which are trivial on $k^\times$. We retain the notations $\mathfrak{q}(\xi)$ and $q(\xi)$ for the conductor and absolute norm of the conductor of an idele class character ξ, and we use Artin reciprocity to identify characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ with idele class characters of k of finite order.

In particular, if K is a quadratic field then we may view $\mathrm{sign}_{K/\mathbb{Q}}$ as an idele class character of $\mathbb{Q}$. Given another idele class character ξ of K of finite order, we say that ξ is *conjugate-symplectic* or *conjugate-orthogonal* if

$$\xi|\mathbb{A}_\mathbb{Q}^\times = \mathrm{sign}_{K/\mathbb{Q}} \tag{13}$$

or

$$\xi|\mathbb{A}_\mathbb{Q}^\times = 1 \tag{14}$$

respectively, these identities being the counterparts to (11) and (12) under Artin reciprocity. It follows easily from (14) (or see [19], p. 471) that if ξ is conjugate-orthogonal then $\mathfrak{q}(\xi) = q\mathcal{O}_K$ for some rational integer $q \geqslant 1$.

To describe $\mathfrak{q}(\xi)$ in the conjugate-symplectic case, let $x \mapsto x'$ be the nonidentity automorphism of K over $\mathbb{Q}$, and extend $x \mapsto x'$ to $\mathbb{A}_K$ by identifying $\mathbb{A}_K$ with $\mathbb{A}_\mathbb{Q} \otimes_\mathbb{Q} K$. A nonzero integral ideal $\mathfrak{q}$ of K will be called *invariant* if $\mathfrak{q} = \mathfrak{q}'$. Since a conjugate-symplectic idele class character ξ is conjugate-self-dual – in other words, satsfies the identity $\xi(x') = \xi(x)^{-1}$ for $x \in \mathbb{A}_K^\times$ – it is clear at least that $\mathfrak{q}(\xi)$ is invariant. To go further, let us write invariant ideals $\mathfrak{q}$ in the form

$$\mathfrak{q} = m \prod_{\mathfrak{p}|p|d_K} \mathfrak{p}^{a_p}, \tag{15}$$

where $m \geqslant 1$ is a rational integer relatively prime to d_K and $\mathfrak{p}$ runs over the ramified prime ideals of K, with $p = \mathbf{N}\mathfrak{p}$ and $a_p \geqslant 0$. For each prime $p|d_K$, put

$$\nu_{K,p} = \begin{cases} 1 & \text{if } p \text{ is odd} \\ 3 & \text{if } p = 2 \text{ and } d_K \equiv 4 \bmod 8 \\ 5 & \text{if } p = 2 \text{ and } d_K \equiv 0 \bmod 8, \end{cases} \tag{16}$$

and consider the following conditions on the exponents a_p in (15):

(i) $a_p \geqslant \nu_{K,p}$.
(ii) If $a_p > \nu_{K,p}$ then a_p is even.

The set of invariant ideals of K which satisfy (i) and (ii) for each $p|d_K$ will be denoted $\mathcal{Q}_K$. We also write $\mathfrak{d}_K$ for the different ideal of K.

Proposition 6. *If $\mathfrak{q} \in \mathcal{Q}_K$ then $\mathfrak{d}_K|\mathfrak{q}$. If ξ is conjugate-symplectic then $\mathfrak{q}(\xi) \in \mathcal{Q}_K$.*

Proof. The first statement is immediate from (i). For the second, put $\mathfrak{q} = \mathfrak{q}(\xi)$, fix $p|d_K$, and let $\xi_\mathfrak{p}$ be the component of ξ at the prime ideal $\mathfrak{p}$ above p. Then the exponent a_p in (15) is $a(\xi_\mathfrak{p})$, the exponent of the conductor of $\xi_\mathfrak{p}$. In other words, $a(\xi_\mathfrak{p}) = 0$ if $\xi_\mathfrak{p}$ is unramified and otherwise $a(\xi_\mathfrak{p})$ is the smallest integer $n \geqslant 1$ such that $\xi_\mathfrak{p}$ is trivial on $1 + \mathfrak{p}^n\mathcal{O}_\mathfrak{p}$, where $\mathcal{O}_\mathfrak{p}$ is the completion of $\mathcal{O}_K$ at $\mathfrak{p}$.

We must show that the integer $a_p = a(\xi_\mathfrak{p})$ satisfies (i) and (ii) above. For simplicity, put $\kappa = \mathrm{sign}_{K/\mathbb{Q}}$, and let κ_p be the component of κ at p. Since p divides d_K, the character κ_p is ramified, in other words $\kappa_p|\mathbb{Z}_p^\times \neq 1$. Hence it follows from (13) that $\xi_\mathfrak{p}|\mathcal{O}_\mathfrak{p}^\times \neq 1$, so $\xi_\mathfrak{p}$ is ramified also. Thus $a(\xi_p) \geqslant 1$. We now consider cases according as p is odd, or $p = 2$ and $d_K \equiv 4 \bmod 8$, or $p = 2$ and $d_K \equiv 0 \bmod 8$.

Suppose first that p is odd. We have just verified (i). If the integer $n = a(\xi_p)$ is odd but > 1 then $n-1$ is even and $\geqslant 2$. Furthermore $\xi_{\mathfrak{p}}$ is nontrivial on $1+\mathfrak{p}^{n-1}\mathcal{O}_{\mathfrak{p}}$ and hence on $1+p^{(n-1)/2}\mathbb{Z}_p$, because the latter group represents all cosets of the former modulo $1+\mathfrak{p}^n\mathcal{O}_{\mathfrak{p}}$. From (13) we deduce that κ_p is nontrivial on $1+p^{(n-1)/2}\mathbb{Z}_p$. This is a contradiction, because $(n-1)/2 \geqslant 1 = a(\kappa_p)$.

Next suppose that $p=2$ and $d_K \equiv 4 \bmod 8$. Then $\xi_{\mathfrak{p}}(3) = \kappa_2(3) = -1$ by (13), and since $3 = 1+2 \in 1+\mathfrak{p}^2$ we obtain $a(\xi_{\mathfrak{p}}) \geqslant 3$. Thus (i) holds. If the integer $n = a(\xi_p)$ is odd but > 3 then $n-1$ is even and $\geqslant 4$. Since $a(\kappa_2) = 2$ we see from (13) that $\xi_{\mathfrak{p}}$ is trivial on $1+2^{(n-1)/2}\mathbb{Z}_2$, a contradiction since this group represents the cosets of $1+\mathfrak{p}^{n-1}\mathcal{O}_{\mathfrak{p}}$ modulo $1+\mathfrak{p}^n\mathcal{O}_{\mathfrak{p}}$.

Finally, if $p=2$ and $d_K \equiv 0 \bmod 8$ then $\xi_{\mathfrak{p}}(5) = \kappa_2(5) = -1$, and since $5 = 1+4 \in 1+\mathfrak{p}^4$ we deduce that $a(\xi_{\mathfrak{p}}) \geqslant 5$. Again, (i) follows, and (ii) is verified as in the previous cases. □

3. Ring class numbers

Given a real quadratic field K and an invariant ideal $\mathfrak{q}$ of K, we let $[\mathfrak{q}]$ be the largest positive rational integer q such that $q|\mathfrak{q}$. If $\mathfrak{q}$ is written as in (15), then

$$[\mathfrak{q}] = m \prod_{p|d_K} p^{[a_p/2]}, \tag{17}$$

where the integer part $[t]$ of a real number t is defined as the greatest integer $\leqslant t$. It follows that if a rational integer divides $\mathfrak{q}$, then it divides $[\mathfrak{q}]$.

With $\mathfrak{q}$ still denoting an arbitrary invariant ideal of K, let $H^{\mathrm{orth}}_{K/\mathbb{Q}}(\mathfrak{q})$ be the group of conjugate-orthogonal idele class characters of K of conductor dividing $\mathfrak{q}$. If $\mathfrak{q} = q\mathcal{O}_K$ with an integer $q \geqslant 1$ then we also write $H^{\mathrm{orth}}_{K/\mathbb{Q}}(q)$. As we have already remarked, the conductor of a conjugate-orthogonal character has the form $q\mathcal{O}_K$ for some integer $q \geqslant 1$; thus $H^{\mathrm{orth}}_{K/\mathbb{Q}}(\mathfrak{q}) = H^{\mathrm{orth}}_{K/\mathbb{Q}}([\mathfrak{q}])$. Nonetheless, by Proposition 3 it is still the case that the set $H^{\mathrm{symp}}_{K/\mathbb{Q}}(\mathfrak{q})$ of conjugate-symplectic idele class characters of K of conductor dividing $\mathfrak{q}$ is either empty or a coset of $H^{\mathrm{orth}}_{K/\mathbb{Q}}(\mathfrak{q})$.

It is sometimes convenient to identify idele class characters of finite order with characters of ray class groups. In particular, $H^{\mathrm{orth}}_{K/\mathbb{Q}}(q)$ can be identified with the dual of the *narrow ring class group of K to the modulus $q\mathcal{O}_K$*, the order of which is denoted here by $h^{\mathrm{nar}}_{K/\mathbb{Q}}(q)$. Since $H^{\mathrm{symp}}_{K/\mathbb{Q}}(\mathfrak{q})$ is either empty or a coset of $H^{\mathrm{orth}}_{K/\mathbb{Q}}(\mathfrak{q})$, we have

$$|H^{\mathrm{symp}}_{K/\mathbb{Q}}(\mathfrak{q})| \leqslant h^{\mathrm{nar}}_{K/\mathbb{Q}}([\mathfrak{q}]), \tag{18}$$

and equality holds unless the left-hand side is 0. Put

$$\alpha(x) = \sum_K \sum_{\substack{\mathfrak{q}\in\mathcal{Q}_K \\ d_K\mathbf{N}\mathfrak{q}\leqslant x}} h^{\mathrm{nar}}_{K/\mathbb{Q}}([\mathfrak{q}]), \tag{19}$$

where the outer sum runs over real quadratic fields K and the inner sum runs over ideals $\mathfrak{q} \in \mathcal{Q}_K$ for which the stated inequality holds.

Proposition 7. $\vartheta^{\mathrm{qu}}(x) \leqslant \alpha(x)$.

Proof. By Propositions 4 and 5, every two-dimensional monomial symplectic Artin representation of $\mathbb{Q}$ has the form $\mathrm{ind}_{K/\mathbb{Q}}\xi$ for some real quadratic K and some conjugate-symplectic idele class character of K, and by Proposition 6, $\mathfrak{q}(\xi) \in \mathcal{Q}_K$.

The number of conjugate-symplectic ξ with $\mathfrak{q}(\xi)$ equal to a fixed $\mathfrak{q} \in \mathcal{Q}_K$ is bounded by the left-hand side of (18) and hence by the right-hand side as well. Finally, if $\rho = \mathrm{ind}_{K/\mathbb{Q}}\xi$ and $\mathfrak{q}(\xi) = \mathfrak{q}$ then $q(\rho) = d_K\mathbf{N}\mathfrak{q}$ by (10). □

4. A Dirichlet series

As before, K denotes a real quadratic field. We fix an embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$ and hence of K in $\mathbb{R}$. Given a rational integer $q > 0$, let $\mathcal{O}_{K,q}$ be the order $\mathbb{Z} + q\mathcal{O}_K$ of K and let $\epsilon^+_{K,q}$ be the fundamental totally positive unit of $\mathcal{O}_{K,q}$. The counting function $\alpha(x)$ becomes more tractable if the term corresponding to a pair $(K, \mathfrak{q})$ is weighted by $\log \epsilon^+_{K,q}$, where $q = [\mathfrak{q}]$. Thus initially we attempt to estimate

$$\beta(x) = \sum_K \sum_{\substack{\mathfrak{q} \in \mathcal{Q}_K \\ d_K\mathbf{N}\mathfrak{q} \leqslant x}} h^{\mathrm{nar}}_{K/\mathbb{Q}}([\mathfrak{q}]) \log \epsilon^+_{K,[\mathfrak{q}]} \tag{20}$$

rather than $\alpha(x)$. We also put

$$B_K(s) = \sum_{\mathfrak{q} \in \mathcal{Q}_K} (h^{\mathrm{nar}}_{K/\mathbb{Q}}([\mathfrak{q}]) \log \epsilon^+_{K,[\mathfrak{q}]})(d_K\mathbf{N}\mathfrak{q})^{-s} \tag{21}$$

and $B(s) = \sum_K B_K(s)$, so that $B(s) = \sum_{n \geqslant 1} b(n)n^{-s}$ with

$$b(n) = \sum_K \sum_{\substack{\mathfrak{q} \in \mathcal{Q}_K \\ d_K\mathbf{N}\mathfrak{q} = n}} h^{\mathrm{nar}}_{K/\mathbb{Q}}([\mathfrak{q}]) \log \epsilon^+_{K,[\mathfrak{q}]}. \tag{22}$$

It follows that $\beta(x) = \sum_{n \leqslant x} b(n)$, and we can hope to deduce the asymptotic behavior of $\beta(x)$ from the analytic behavior of $B(s)$ via a tauberian theorem.

Let χ_K be the primitive quadratic Dirichlet character corresponding to K. We recall a standard formula for $h^{\mathrm{nar}}_{K/\mathbb{Q}}(q)$ (cf. [19], p. 472):

$$h^{\mathrm{nar}}_{K/\mathbb{Q}}(q) = \frac{h^{\mathrm{nar}}_K \log \epsilon^+_K}{\log \epsilon^+_{K,q}} \cdot q \prod_{p|q}(1 - \chi_K(p)/p), \tag{23}$$

where h^{nar}_K is the narrow class number of K and $\epsilon^+_K = \epsilon^+_{K,1}$ the fundamental totally positive unit. But $h^{\mathrm{nar}}_K \log \epsilon^+_K = 2h_K \log \epsilon_K$, where h_K is the class number of K and ϵ_K the fundamental unit, and $2h_K \log \epsilon_K = L(1, \chi_K)\sqrt{d_K}$. Thus (23) becomes

$$h^{\mathrm{nar}}_{K/\mathbb{Q}}(q) \log \epsilon^+_{K,q} = L(1, \chi_K)\sqrt{d_K} \cdot q \prod_{p|q}(1 - \chi_K(p)/p). \tag{24}$$

Returning to (21), we see that

$$B_K(s) = \frac{L(1, \chi_K)\sqrt{d_K}}{d_K^s} \sum_{\mathfrak{q} \in \mathcal{Q}_K} \frac{[\mathfrak{q}] \prod_{p|[\mathfrak{q}]}(1 - \chi_K(p)/p)}{(\mathbf{N}\mathfrak{q})^s} \tag{25}$$

The next step is to express $B_K(s)$ as an Euler product.

To this end, we observe that the function $\mathfrak{q} \mapsto [\mathfrak{q}]$ is multiplicative in the sense that $[\mathfrak{q}\mathfrak{q}'] = [\mathfrak{q}][\mathfrak{q}']$ whenever $\mathfrak{q}$ and $\mathfrak{q}'$ are relatively prime invariant ideals of K. Furthermore, $[\mathfrak{q}]$ and $[\mathfrak{q}']$ are again relatively prime. Thus (25) can be written

$$B_K(s) = \frac{L(1, \chi_K)\sqrt{d_K}}{d_K^s} \prod_{p \nmid d_K} E_{K,p}(s) \cdot \prod_{p|d_K} p^{-\nu_{K,p}s + (\nu_{K,p}-1)/2} F_{K,p}(s), \tag{26}$$

where the exponents $\nu_{K,p}$ are as in (16) and the shape of the Euler factors $E_{K,p}(s)$ and $F_{K,p}(s)$ is dictated by Proposition 6 and the definition of $\mathcal{Q}_K$:

$$E_{K,p}(s) = 1 + (1 - \chi_K(p)/p) \sum_{j \geqslant 1} p^{j(1-2s)} \tag{27}$$

and

$$\begin{aligned} F_{K,p}(s) &= 1 + \sum_{j \geqslant 1} p^{j-(2j-1)s} \\ &= 1 + p^s \sum_{j \geqslant 1} p^{j(1-2s)}. \end{aligned} \tag{28}$$

Let $E_K(s)$ and $F_K(s)$ be the product of the factors $E_{K,p}(s)$ and the factors $F_{K,p}(s)$ over primes $p \nmid d_K$ and primes $p|d_K$ respectively. Then (26) becomes

$$B_K(s) = \frac{L(1,\chi_K)\sqrt{d_K} E_K(s)(d_K^\circ/d_K)F_K(s)}{(d_K d_K^\circ)^s} \tag{29}$$

with11

$$d_K^\circ = \prod_{p|d_K} p^{\nu_{K,p}}. \tag{30}$$

Note that d_K° is d_K, $2d_K$, or $4d_K$ according as d_K is odd, congruent to 4 mod 8, or congruent to 0 mod 8. Thus the denominator in (29) is essentially d_K^{2s} rather than d_K^s, as it would be in the dihedral case. The disparate growth rates of $\vartheta^{\mathrm{qu}}(x)$ and $\vartheta^{\mathrm{di}}(x)$ can be traced to this difference, and thus ultimately to the fact that $\mathfrak{d}_K|\mathfrak{q}(\xi)$ for ξ conjugate-symplectic (Proposition 6).

So far $B_K(s)$ has been treated as the formal Dirichlet series with nonnegative coefficients defined by (21), but in fact it converges for $\Re(s) > 1$. To see this, rewrite (27) and (28) as

$$E_{K,p}(s) = \frac{1 - \chi_K(p)p^{-2s}}{1 - p^{1-2s}} \tag{31}$$

and

$$F_{K,p}(s) = \frac{1 - p^{1-2s} + p^{1-s} + p^{1-s}}{1 - p^{1-2s}}. \tag{32}$$

The right-hand side of (31) is the Euler factor at p of $\zeta(2s-1)/L(2s,\chi_K)$, so $E_K(s)$ is obtained from $\zeta(2s-1)/L(2s,\chi_K)$ by removing the Euler factors at primes $p|d_K$. For such p the numerator of the right-hand side of (31) is 1; thus

$$E_K(s) = \frac{\zeta(2s-1)}{L(2s,\chi_K)} \prod_{p|d_K} (1 - p^{1-2s}). \tag{33}$$

Substituting (33) and (32) in (29), we obtain $B_K(s) = \zeta(2s-1)C_K(s)$ with

$$C_K(s) = \frac{L(1,\chi_K)\sqrt{d_K}(d_K^\circ/d_K)}{(d_K d_K^\circ)^s L(2s,\chi_K)} \prod_{p|d_K} (1 - p^{1-2s} + p^{1-s}). \tag{34}$$

Since the Dirichlet series $1/L(2s,\chi_K)$ converges absolutely for $\Re(s) > 1/2$, so does $C_K(s)$. Therefore $B_K(s)$ converges for $\Re(s) > 1$.

Next we claim that as a series of holomorphic functions, $\sum_K C_K(s)$ is normally convergent on right half-planes of the form $\Re(s) \geqslant 5/6 + \varepsilon$ for arbitrary $\varepsilon > 0$.

Indeed suppose that $\Re(s) \geqslant 5/6 + \varepsilon$. Using the estimate $|L(1, \chi_K)| < 2 + \log d_K$ (cf. [6], p. 262, Théorème 8.2) and the fact that $d_K \leqslant d_K^\circ$, we see that

$$\frac{|L(1,\chi_K)|\sqrt{d_K}}{|(d_K d_K^\circ)^s|} \leqslant \frac{2 + \log d_K}{d_K^{7/6+2\varepsilon}}. \tag{35}$$

Furthermore

$$|1/L(2s, \chi_K)| \leqslant \zeta(5/3)/\zeta(10/3) \tag{36}$$

and

$$(d_K^\circ/d_K)|\prod_{p|d_K}(1 - p^{1-2s} + p^{1-s})| \leqslant 4\prod_{p|d_K}(2 + p^{1/6}) \leqslant 4 \cdot 3^{\omega(d_K)} d_K^{1/6}, \tag{37}$$

where $\omega(n)$ is the number of distinct prime divisors of n. Together, (34), (35), (36), and (37) give

$$|C_K(s)| \ll (\log d_K) 3^{\omega(d_K)}/d_K^{1+2\varepsilon},$$

so $\sum_K C_K(s)$ is normally convergent as claimed.

To summarize, $B_K(s)$ is a Dirichlet series with nonnegative coefficients which converges for $\Re(s) > 1$, and $\sum_K C_K(s)$ converges normally on half-planes of the form $\Re(s) \geqslant 5/6 + \varepsilon$. Since $B_K(s) = \zeta(2s-1)C_K(s)$, we deduce that $\sum_K B_K(s)$ converges normally on half-planes of the form $\Re(s) \geqslant 1 + \varepsilon$. It follows (cf. [20], Proposition 1) that the formal sum $B(s) = \sum_K B_K(s)$ is a convergent Dirichlet series for $\Re(s) > 1$ and that the holomorphic function which it defines coincides with $\sum_K B_K(s)$ and therefore with $\zeta(2s-1)\sum_K C_K(s)$. Put $\varrho = \sum_K C_K(1)$. Since $\zeta(2s-1)$ has a simple pole at $s = 1$ with residue $1/2$, we obtain:

Proposition 8. *The Dirichlet series $B(s)$ is absolutely convergent for $\Re(s) > 1$ and extends as a meromorphic function to the half-plane $\Re(s) > 5/6$, its only pole in the latter region being a simple pole of order one with residue $\varrho/2$.*

A standard tauberian theorem (cf. [5], p. 154) yields the following corollary:

Corollary. $\beta(x) \sim \varrho x/2$.

5. The upper bound

To deduce an upper bound for $\vartheta^{qu}(x)$, we need a lower bound for $\epsilon^+_{K,[\mathfrak{q}]}$, where $\mathfrak{q} \in \mathcal{Q}_K$. The following elementary statement suffices for our purposes:

Proposition 9. $\epsilon^+_{K,[\mathfrak{q}]} > (d_K \mathbf{N}\mathfrak{q})^{1/4}/2$.

Proof. Put $q = [\mathfrak{q}]$ and $n = d_K \mathbf{N}\mathfrak{q}$. Since $\epsilon^+_{K,q}$ is the fundamental totally positive unit of $\mathcal{O}_{K,q}$, we can write $\epsilon^+_{K,q} = (a + bq\sqrt{d_K})/2$ with integers $a, b \geqslant 1$. Therefore $\epsilon^+_{K,q} > q\sqrt{d_K}/2$, and it suffices to show that

$$q\sqrt{d_K} \geqslant n^{1/4}. \tag{38}$$

If $d_K \geqslant \sqrt{n}$ there is nothing to prove, so we may assume that $d_K \leqslant \sqrt{n}$. Then $n = d_K \mathbf{N}\mathfrak{q} \leqslant \sqrt{n}\mathbf{N}\mathfrak{q}$ and consequently

$$\sqrt{n} \leqslant \mathbf{N}\mathfrak{q}. \tag{39}$$

But if $\mathfrak{q}$ is written as in (15) then $[\mathfrak{q}]$ $(= q)$ is as in (17), whence

$$\mathbf{N}\mathfrak{q} = m^2 \prod_{p|d_K} p^{a_p} \leqslant m^2 \prod_{p|d_K} p^{2[a_p/2]+1} \leqslant q^2 d_K. \tag{40}$$

Together, (39) and (40) give (38). □

The parallel expressions (19) and (20) for $\alpha(x)$ and $\beta(x)$ can also be written $\beta(x) = \sum_{n \leqslant x} b(n)$ and $\alpha(x) = \sum_{n \leqslant x} a(n)$, where $b(n)$ is as in (22) and

$$a(n) = \sum_K \sum_{\substack{\mathfrak{q} \in \mathcal{Q}_K \\ d_K \mathbf{N}\mathfrak{q} = n}} h^{\mathrm{nar}}_{K/\mathbb{Q}}([\mathfrak{q}]).$$

Put $A(x) = \sum_{n \leqslant x} a(n) \log n$; then

$$\alpha(x) = A(x)(\log x)^{-1} + \int_5^x \frac{A(t)}{t(\log t)^2}\, dt \tag{41}$$

by Abel summation (note that $a(n) = 0$ for $n < 5$ because $d_K \geqslant 5$ for all K). It follows from Proposition 9 that $A(x) \ll \beta(x)$ and from the corollary to Proposition 8 that $\beta(x) = O(x)$. Therefore $A(x) = O(x)$, and (41) gives:

Proposition 10. $\alpha(x) = O(x/\log x)$.

The upper bound in (3) now follows from Proposition 7:

Corollary. $\vartheta^{\mathrm{qu}}(x) = O(x/\log x)$.

6. Ring class numbers again

We now turn to the lower bound in (3). As in the introduction, we write $\mathcal{K}$ for the set of real quadratic subfields K of $\overline{\mathbb{Q}}$ such that d_K is a product of distinct primes congruent to 1 mod 4. Recall also that $\mathfrak{d}_K$ denotes the different ideal of K.

Proposition 11. *If $K \in \mathcal{K}$ then there exists a quadratic conjugate-symplectic idele class character η of K with $\mathfrak{q}(\eta) = \mathfrak{d}_K$.*

Proof. Let $\mathrm{sign}_{K/\mathbb{Q}}$ be the primitive quadratic Dirichlet character determined by K, and for each prime $p|d_K$, let χ_p be either of the two primitive quartic Dirichlet characters of conductor p. Then χ_p^2 is the Legendre symbol at p, and consequently the product $\chi = \prod_{p|d_K} \chi_p$ satisfies

$$\chi^2 = \mathrm{sign}_{K/\mathbb{Q}}. \tag{42}$$

Changing notation, we view χ and $\mathrm{sign}_{K/\mathbb{Q}}$ as idele class characters of $\mathbb{Q}$, and we define an idele class character η of K by $\eta = \chi \circ N_{K/\mathbb{Q}}$, where $N_{K/\mathbb{Q}}$ is the idelic norm. Then $\eta|\mathbb{A}_{\mathbb{Q}}^\times = \mathrm{sign}_{K/\mathbb{Q}}$ by (42), so η is conjugate-symplectic. Furthermore, as $\eta^2 = \chi^2 \circ N_{K/\mathbb{Q}}$, we see from (42) that η is quadratic. Finally, since $\eta = \chi \circ N_{K/\mathbb{Q}}$ and $\eta|\mathbb{A}_{\mathbb{Q}}^\times = \mathrm{sign}_{K/\mathbb{Q}}$, we see that η is ramified at precisely the prime divisors of $\mathfrak{d}_K$. As η is quadratic and d_K is odd it follows that $\mathfrak{q}(\eta) = \mathfrak{d}_K$. □

For the remainder of this paper, K denotes a fixed element of $\mathcal{K}$. We also write η for a fixed idele class character of K as in Proposition 11. Let $\vartheta^{\mathrm{qu},K}(x)$ be the number of isomorphism classes of quaternionic Artin representations of $\mathbb{Q}$ with conductor $\leqslant x$ *which can be induced from* K. Our argument is based on the simple remark that any lower bound for $\vartheta^{\mathrm{qu},K}(x)$ is also a lower bound for $\vartheta^{\mathrm{qu}}(x)$.

Given a nonzero ideal $\mathfrak{q}$ of $\mathcal{O}_K$, let $g(\mathfrak{q})$ be the number of conjugate-symplectic idele class characters of K of conductor $\mathfrak{q}$ and order $\geqslant 3$. In light of the formula (10) for the conductor of a monomial representation, Propositions 1, 2, and 6 give

$$\vartheta^{\mathrm{qu},K}(x) = \frac{1}{2} \sum_{\substack{\mathbf{N}\mathfrak{q} \leqslant x/d_K \\ \mathfrak{q} \in \mathcal{Q}_K}} g(\mathfrak{q}). \tag{43}$$

The coefficient $1/2$ on the right-hand side reflects the fact that if ξ has order $\geqslant 3$ then ξ and ξ^{-1} induce isomorphic representations.

As the ideals $\mathfrak{q}$ in (43) belong to $\mathcal{Q}_K$, they are divisible by $\mathfrak{d}_K$ (Proposition 6), so $\eta \in H^{\mathrm{symp}}_{K/\mathbb{Q}}(\mathfrak{q})$. Thus $H^{\mathrm{symp}}_{K/\mathbb{Q}}(\mathfrak{q})$ is nonempty, whence equality holds in (18). In fact since $H^{\mathrm{symp}}_{K/\mathbb{Q}}(\mathfrak{q})$ is nonempty it is a coset of $H^{\mathrm{orth}}_{K/\mathbb{Q}}(\mathfrak{q})$, so its elements are precisely the characters $\eta\xi$ with $\xi \in H^{\mathrm{orth}}_{K/\mathbb{Q}}(\mathfrak{q})$. In this connection we note two points.

First, $\eta\xi$ has order $\geqslant 3$ if and only if ξ does. Equivalently (Proposition 2), $\mathrm{ind}_{K/\mathbb{Q}}\eta\xi$ is irreducible if and only if $\mathrm{ind}_{K/\mathbb{Q}}\xi$ is.

Second, $\mathfrak{q}(\eta\xi) = \mathfrak{q}$ if and only if $\mathfrak{q}(\xi) = [\mathfrak{q}]$. This claim is easily verified if one keeps in mind that $\mathfrak{q} \in \mathcal{Q}_K$ and d_K is odd. Indeed if $\mathfrak{q}$ is written as in (15), so that $[\mathfrak{q}]$ is as in (17), then our claim quickly reduces to the assertion that for a prime ideal $\mathfrak{p}$ lying over a prime divisor p of d_K, we have $\mathrm{ord}_p\mathfrak{q}(\xi) = [a_p/2]$ if and only if $\mathrm{ord}_\mathfrak{p}\mathfrak{q}(\eta\xi) = a_p$. The latter equivalence is verified by considering separately the cases where $a_p = 1$ and where a_p is an even integer $\geqslant 2$.

It follows from the preceding two remarks that

$$g(\mathfrak{q}) = (h^{\mathrm{nar}}_{K/\mathbb{Q}})^*([\mathfrak{q}]) - (h^{\mathrm{nar},(2)}_{K/\mathbb{Q}})^*([\mathfrak{q}]) \tag{44}$$

where $(h^{\mathrm{nar}}_{K/\mathbb{Q}})^*(q)$ is the number of *primitive* narrow ring class characters of K of conductor $q\mathcal{O}_K$ and $(h^{\mathrm{nar},(2)}_{K/\mathbb{Q}})^*(q)$ is the number of such characters which are of order $\leqslant 2$. Combining (44) and (43), we obtain

$$\vartheta^{\mathrm{qu},K}(x) = \frac{1}{2} \sum_{\substack{\mathbf{N}\mathfrak{q} \leqslant x/d_K \\ \mathfrak{q} \in \mathcal{Q}_K}} (h^{\mathrm{nar}}_{K/\mathbb{Q}})^*([\mathfrak{q}]) - (h^{\mathrm{nar},(2)}_{K/\mathbb{Q}})^*([\mathfrak{q}]). \tag{45}$$

The next step is to replace (45) by a sum over positive integers q rather than over ideals $\mathfrak{q} \in \mathcal{Q}_K$.

Write $\mathbb{Z}^+$ for the set of positive integers. Although Proposition 11 depended on our assumption that $K \in \mathcal{K}$, the next assertion uses only the fact that d_K is odd.

Proposition 12. *The map from $\mathcal{Q}_K$ to $\mathbb{Z}^+$ given by $\mathfrak{q} \mapsto [\mathfrak{q}]$ is a bijection, and $\mathbf{N}\mathfrak{q} \leqslant [\mathfrak{q}]^2 d_K$.*

Proof. One readily checks that the map $\mathbb{Z}^+ \to \mathcal{Q}_K$ given by

$$q \mapsto q \cdot \prod_{\substack{\mathfrak{p}|p|d_K \\ p\nmid q}} \mathfrak{p}$$

is an inverse of $\mathfrak{q} \mapsto [\mathfrak{q}]$. Furthermore

$$\mathbf{N}\mathfrak{q} = [\mathfrak{q}]^2 \cdot \prod_{\substack{\mathfrak{p}|d_K \\ p\nmid \mathfrak{q}}} p,$$

from which the stated inequality follows. □

Put $q = [\mathfrak{q}]$ in (45) and apply Proposition 12. If $[\mathfrak{q}]^2 \leqslant x/d_K^2$ then $\mathbf{N}\mathfrak{q} \leqslant x/d_K$, and consequently we obtain

$$\vartheta^{\mathrm{qu},K}(x) \geqslant \frac{1}{2} \sum_{q^2 \leqslant x/d_K^2} (h^{\mathrm{nar}}_{K/\mathbb{Q}})^*(q) - (h^{\mathrm{nar},(2)}_{K/\mathbb{Q}})^*(q), \tag{46}$$

where q is now an arbitary positive integer. To state (46) more succinctly, put

$$\sigma(x) = \sum_{q \leqslant x} (h^{\mathrm{nar}}_{K/\mathbb{Q}})^*(q) \tag{47}$$

and

$$\tau(x) = \sum_{q^2 \leqslant x/d_K^2} (h^{\mathrm{nar},(2)}_{K/\mathbb{Q}})^*(q). \tag{48}$$

Since $\vartheta^{\mathrm{qu}}(x) \geqslant \vartheta^{\mathrm{qu},K}(x)$, we have:

Proposition 13. $2\vartheta^{\mathrm{qu}}(x) \geqslant \sigma(\sqrt{x}/d_K) - \tau(x)$.

The next step it to bound $\tau(x)$, which we want to regard as an error term.

7. Quadratic ring class characters

Let $N_{K/\mathbb{Q}} : \mathbb{A}_K^\times \to \mathbb{A}_\mathbb{Q}^\times$ be the idelic norm. The following elementary fact was pointed out to me by Dick Gross many years ago:

Lemma. *The conjugate-orthogonal idele class characters of K of order dividing 2 are precisely the characters $\chi \circ N_{K/\mathbb{Q}}$, where χ is an idele class character of $\mathbb{Q}$ of order dividing 2.*

Proof. If χ is an idele class character of $\mathbb{Q}$ such that $\chi^2 = 1$, then for $x \in \mathbb{A}_\mathbb{Q}$ we have $\chi(N_{K/\mathbb{Q}}(x)) = \chi(x^2) = 1$, so that the character $\xi = \chi \circ N_{K/\mathbb{Q}}$ is conjugate-orthogonal and also satisfies $\xi^2 = 1$. Conversely, suppose that ξ is conjugate-orthogonal, and let $x \mapsto x'$ be the automorphism of $\mathbb{A}_K$ induced by the nonidentity element of $\mathrm{Gal}(K/\mathbb{Q})$. Then $\xi(xx') = 1$ for all $x \in \mathbb{A}_K^\times$, but if in addition $\xi^2 = 1$, then $1 = \xi(xx') = \xi(x/x')$, so ξ is trivial on the kernel of $N_{K/\mathbb{Q}}$. Thus ξ factors through $N_{K/\mathbb{Q}}$ and indeed through the map $\mathbb{A}_K^\times/K^\times \to \mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times$ induced by $N_{K/\mathbb{Q}}$. In other words, there is an idele class character χ of $\mathbb{Q}$ such that $\xi = \chi \circ N_{K/\mathbb{Q}}$. Evaluating both sides on $x \in \mathbb{A}_\mathbb{Q}^\times$ we see that $\chi(x^2) = \xi(x) = 1$; thus $\chi^2 = 1$. □

Proposition 14. $\tau(x) = O(\sqrt{x})$.

Proof. Recalling (48), we may describe $\tau(x)$ as the number of primitive ring class characters ξ with $\xi^2 = 1$ and $\mathfrak{q}(\xi) = q\mathcal{O}_K$, where $q \leqslant \sqrt{x}/d_K$. Let us identify primitive ring class characters with conjugate-orthogonal idele class characters. Then the lemma enables us to write $\xi = \chi \circ N_{K/\mathbb{Q}}$ with an idele class character χ of $\mathbb{Q}$ satisfying $\chi^2 = 1$. At a prime $p \nmid d_K$, we have $\mathrm{ord}_p q(\chi) = \mathrm{ord}_p q$, and if $p | d_K$ then p is odd so $\mathrm{ord}_p q(\chi) \leqslant 1$. Thus $q(\chi)$ divides qd_K. In particular, $q(\chi) \leqslant \sqrt{x}$. hence

$$\tau(x) \leqslant \sum_{\substack{\chi^2 = 1 \\ q(\chi) \leqslant \sqrt{x}}} 1.$$

Changing our point of view again, we may think of χ as a primitive Dirichlet character. Since the number of primitive quadratic Dirichlet characters of conductor $\leqslant x$ is $O(x)$, the proposition follows. □

8. The lower bound

Fix $\varepsilon > 1/(4\sqrt{e})$. In this section we complete the proof of our main theorem by establishing the lower bound in (3). The key ingredient is Ambrose's result that (5) holds (for x sufficiently large) provided k is abelian, $\gamma = 1$, and $\delta > 1/(2\sqrt{e})$ ([2], p. 81, Theorem 2 (i)). We may assume that $\varepsilon < 1/2$, and we choose δ so that

$$1/(2\sqrt{e}) < \delta < 2\varepsilon < 1. \tag{49}$$

The method of Luca and Sankaranarayanan ([14], pp. 396-397) figures prominently in our argument, and our exposition follows theirs closely at times. But we begin with a strategem (Propositions 15 and 16 below) to ensure that the ring class characters we count are primitive.

To get started, recall that ϵ_K^+ and $\epsilon_{K,q}^+$ denote the fundamental totally positive units of $\mathcal{O}_K$ and $\mathcal{O}_{K,q}$ respectively. The positive integer n such that $(\epsilon_K^+)^n = \epsilon_{K,q}^+$ will be denoted $\nu(q)$. We also write $\omega(q)$ for the number of distinct prime divisors of q and $\varphi(q)$ and $\lambda(q)$ for the order and minimal exponent of the abelian group $(\mathbb{Z}/q\mathbb{Z})^\times$. Note that if q is divisible only by primes that split in K then $\lambda(q)$ is also the minimal exponent of the group

$$(\mathcal{O}_K/q\mathcal{O}_K)^\times \cong (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times. \tag{50}$$

Furthermore $\nu(q)$ coincides with the order of the coset of ϵ_K^+ in the quotient of $(\mathcal{O}_K/q\mathcal{O}_K)^\times$ by the naturally embedded subgroup $(\mathbb{Z}/q\mathbb{Z})^\times$, and consequently $\nu(q)$ divides $\lambda(q)$. In particular $\nu(q) \leqslant \lambda(q)$.

We seek a lower bound for $(h_{K/\mathbb{Q}}^{\mathrm{nar}})^*(q)$, the number of primitive ring class characters of conductor $q\mathcal{O}_K$. An immediate elementary lower bound is

$$(h_{K/\mathbb{Q}}^{\mathrm{nar}})^*(q) \geqslant h_{K/\mathbb{Q}}^{\mathrm{nar}}(q) - \sum_{p|q} h_{K/\mathbb{Q}}^{\mathrm{nar}}(q/p). \tag{51}$$

The following proposition refines (51) in a special case.

Proposition 15. *Let q be a product of distinct prime numbers which split in K, and suppose that $\nu(q/p) = \nu(q)$ for all prime divisors p of q. Then*

$$(h_{K/\mathbb{Q}}^{\mathrm{nar}})^*(q) \geqslant h_K^{\mathrm{nar}} \cdot (\varphi(q)/\lambda(q)) \cdot (1 - \omega(q)/\varphi(\hat{p})),$$

where $\hat{p}$ is the smallest prime dividing q.

Proof. If $\omega(q)/\varphi(\hat{p}) \geqslant 1$ then the inequality to be proved is vacuous. Hence we may assume that $\omega(q)/\varphi(\hat{p}) < 1$. Referring to (23), we see that under our hypotheses,

$$h_{K/\mathbb{Q}}^{\mathrm{nar}}(q) = h_K^{\mathrm{nar}} \cdot (\varphi(q)/\nu(q)), \tag{52}$$

and, for every prime divisor p of q,

$$h_{K/\mathbb{Q}}^{\mathrm{nar}}(q/p) = h_K^{\mathrm{nar}} \cdot (\varphi(q)/(\varphi(p)\nu(q))). \tag{53}$$

Substituting (52) and (53) into (51), we obtain

$$(h_{K/\mathbb{Q}}^{\mathrm{nar}})^*(q) \geqslant h_K^{\mathrm{nar}} \cdot (\varphi(q)/\nu(q)) \cdot (1 - \omega(q)/\varphi(\hat{p})),$$

because $\varphi(p) = p - 1 \geqslant \hat{p} - 1 = \varphi(\hat{p})$. As $\nu(q) \leqslant \lambda(q)$ the proposition follows. □

The next proposition provides an elementary way of ensuring that the condition $\nu(q/p) = \nu(q)$ is satisfied. By a *prime power* we mean a number of the form ℓ^n, where ℓ is a prime and n is a positive integer.

Proposition 16. *Let r be a product of distinct primes which split in K, and let $\mathcal{L}$ be a finite set of prime powers. Suppose that for each prime divisor p of r the prime powers dividing $p-1$ all belong to $\mathcal{L}$. Then there exists an integer t satisfying $0 \leqslant t \leqslant |\mathcal{L}|$ together with distinct prime divisors $p_1, p_2, \ldots, p_t$ of r if $t > 0$ such that the integer*

$$q = \begin{cases} r/(p_1 p_2 \cdots p_t), & \text{if } t > 0 \\ r, & \text{if } t = 0 \end{cases}$$

satisfies $\nu(q/p) = \nu(q)$ for all prime divisors p of q.

Proof. The proof rests on some simple algebraic remarks. As already noted, $\nu(q)$ is the order of the coset represented by ϵ_K^+ in the cokernel of the natural embedding of $(\mathbb{Z}/q\mathbb{Z})^\times$ in $(\mathcal{O}_K/q\mathcal{O}_K)^\times$. Now this embedding is simply the map on unit groups associated to the unique ring homomorphism

$$\mathbb{Z}/q\mathbb{Z} \to \mathcal{O}_K/q\mathcal{O}_K,$$

and if $\mathfrak{q}$ and $\mathfrak{q}'$ are conjugate ideals of $\mathcal{O}_K$ such that $\mathfrak{q}\mathfrak{q}' = q\mathcal{O}_K$, then (50) can likewise be described as the isomorphism on unit groups arising from the natural ring isomorphisms

$$\mathcal{O}_K/q\mathcal{O}_K \cong (\mathcal{O}_K/\mathfrak{q}) \times (\mathcal{O}_K/\mathfrak{q}') \cong (\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}). \tag{54}$$

It follows that the composition

$$(\mathbb{Z}/q\mathbb{Z})^\times \to (\mathcal{O}_K/q\mathcal{O}_K)^\times \cong (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$$

is the diagonal map Δ. Thus we have isomorphisms

$$\frac{(\mathcal{O}_K/q\mathcal{O}_K)^\times}{\text{image of } (\mathbb{Z}/q\mathbb{Z})^\times} \cong \frac{(\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times}{\Delta(\mathbb{Z}/q\mathbb{Z})^\times} \cong (\mathbb{Z}/q\mathbb{Z})^\times \cong \prod_{p|q} (\mathbb{Z}/p\mathbb{Z})^\times, \tag{55}$$

where the isomorphism in the middle sends the coset of (x, y) to xy^{-1}. Let ψ_q denote the composition (55). While ψ_q is not quite canonical – for it depends on the chosen order of $\mathfrak{q}$ and $\mathfrak{q}'$ in (54) – nonetheless, if p is a prime divisor of q and the prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ above p are ordered so that $\mathfrak{p}|\mathfrak{q}$ and $\mathfrak{p}'|\mathfrak{q}'$ then the obvious diagram with horizontal arrows ψ_q and ψ_p commutes. Thus $\nu(q)$ is just the least common multiple of the numbers $\nu(p)$ for $p|q$.

The upshot of these remarks is that $\nu(q/p) = \nu(q)$ if and only if for every $l \in \mathcal{L}$ dividing $\nu(p)$ there exists another prime divisor p_0 of q different from p such that l divides $\nu(p_0)$. Otherwise $\nu(q/p) < \nu(q)$.

The proof of the proposition is now straightforward. Indeed if $\nu(r/p) = \nu(r)$ for every prime divisor p of r then we put $t = 0$ and $q = r$ and there is nothing to prove. Otherwise let p_1 be a prime divisor of r such that $\nu(r/p_1) < \nu(r)$, and let $l_1 \in \mathcal{L}$ be a divisor of $\nu(p_1)$ which does not divide $\nu(p)$ for any $p|r_1$, where $r_1 = r/p_1$. Now we repeat our reasoning: If $\nu(r_1/p) = \nu(r_1)$ for all prime divisors p of r_1 then we put $t = 1$ and $q = r_1$. Otherwise there is a prime divisor p_2 of r_1 and an element $l_2 \in \mathcal{L}$ which divides $\nu(p_2)$ but not $\nu(p)$ for any $p|r_2$, where $r_2 = r_1/p_2 = r/(p_1 p_2)$. Note that $l_2 \neq l_1$ because l_1 does not divide $\nu(p_2)$. In fact the argument ensures that $l_1, l_2, \ldots$ are all distinct, and consequently the process stops after at most $|\mathcal{L}|$ steps. □

We must now produce a set of integers r to which Proposition 16 can be applied. As a first step, we make a simple deduction from Ambrose's theorem. Let $\mathcal{P}_\delta(x)$ be the set of prime numbers $p \leqslant x$ which split in K and for which every prime divisor ℓ of $p-1$ satisfies $\ell < x^\delta$. We write $\varpi_\delta(x)$ for the cardinality of $\mathcal{P}_\delta(x)$.

Proposition 17. *$\varpi_\delta(x) \gg x/(\log x)^2$ for $x \geqslant 2$.*

Proof. Let $\pi_K^{\mathrm{dg}2}(x)$ be the number of prime ideals of K of absolute norm $\leqslant x$ and residue class degree 2. By the prime number theorem in arithmetic progressions, $\pi_K^{\mathrm{dg}2}(x) \sim \sqrt{x}/(\log x)$. Since the number of ramified prime ideals of K is finite while $\pi_{K,\delta}(x) \gg x/(\log x)^2$ by [2], it follows that the number of split prime ideals counted by $\pi_{K,\delta}(x)$, say $\pi_{K,\delta}^{\mathrm{split}}(x)$, satisfies

$$\pi_{K,\delta}^{\mathrm{split}}(x) \sim \pi_{K,\delta}(x).$$

As $\varpi_\delta(x) = \pi_{K,\delta}^{\mathrm{split}}(x)/2$, the proposition follows. □

Recall that a positive integer j is *powerful* if the divisibility of j by a prime ℓ implies its divisibility by ℓ^2. Let $\iota(x)$ denote the number of powerful numbers $\leqslant x$. Then

$$\iota(x) = O(\sqrt{x}) \tag{56}$$

because in fact $\iota(x) \sim \zeta(3/2)\sqrt{x}/\zeta(3)$ (Golumb [10], p. 848, formulas (4) and (6)). We now follow [14], first of all by changing notation slightly (y in place of x). More importantly, we define a subset $\mathcal{P}_\delta^*(y)$ of $\mathcal{P}_\delta(y)$ to eliminate large powerful divisors of $p-1$. Choose a constant $c > 2$. Then $\mathcal{P}_\delta^*(y)$ is the set of $p \in \mathcal{P}_\delta(y)$ satisfying two conditions:

LS1. $p > y/(\log y)^c$.

LS2. If m is powerful and divides $p-1$ then $m \leqslant (\log y)^{2c}$.

Condition **LS1** excludes at most $O(y/(\log y)^{c+1})$ elements of $\mathcal{P}_\delta(y)$, and using Abel summation and (56), we see that **LS2** excludes at most

$$\sum_{\substack{(\log y)^{2c} < m \leqslant y \\ m \text{ powerful}}} y/m \ll y/(\log y)^c$$

elements. Let $\varpi_\delta^*(y)$ denote the cardinality of $\mathcal{P}_\delta^*(y)$. We conclude that

$$\varpi_\delta^*(y) = \varpi_\delta(y) - O(y/(\log y)^c),$$

and as $c > 2$, Proposition 17 gives:

Proposition 18. *$\varpi_\delta^*(y) \gg y/(\log y)^2$ for $y \geqslant 2$.*

Next let $\mathcal{R}_\delta(y)$ be the set of all products of $[y^\delta]$ distinct elements of $\mathcal{P}_\delta^*(y)$. As in [14], we will estimate $|\mathcal{R}_\delta(y)|$ by using an elementary lower bound for binomial coefficients: For positive integers $m < n$ we have

$$\binom{n}{m} \geqslant (n/m)^m, \tag{57}$$

because $(n-j)/(m-j) \geqslant n/m$ for $0 \leqslant j \leqslant m-1$. Taking $n = \varpi_\delta^*(y)$ and $m = [y^\delta]$, and referring to Propositon 18, we obtain:

Proposition 19. $|\mathcal{R}_\delta(y)| \gg e^{(1-\delta-o(1))[y^\delta]\log y}$.

Let $\mathcal{L}_\delta(y)$ be the set of all prime powers occurring as a divisor of $p-1$ for some $p \in \mathcal{P}^*_\delta(y)$. We claim that

$$|\mathcal{L}_\delta(y)| \ll y^\delta/\log y \tag{58}$$

for $y \geqslant 2$. The left-hand side is the number of pairs (ℓ, n) such that $\ell^n|(p-1)$ for some $p \in \mathcal{P}^*_\delta(y)$, and we will first estimate the number of pairs for which $n = 1$. The number of such pairs is simply bounded by the number of primes $< y^\delta$ and is therefore $\ll y^\delta/(\log y)$. On the other hand, if $n \geqslant 2$ then $\ell^n \leqslant (\log y)^{2c}$ by **LS2**, so ℓ^n is a powerful number $\leqslant (\log y)^{2c}$. Hence the number of pairs (ℓ, n) with $n \geqslant 2$ is $\ll (\log y)^c$ by (56), and (58) follows.

Let $\mathcal{Q}_\delta(y)$ be the set of numbers q obtained from the numbers $r \in \mathcal{R}_\delta(y)$ by applying Proposition 16 with $\mathcal{L} = \mathcal{L}_\delta(y)$. Of course the procedure in Proposition 16 involves some choices, so in principle there could be many numbers q obtained from a single r. But making an arbitrary choice among the possibilities, we obtain a well-defined function

$$\mathcal{R}_\delta(y) \longrightarrow \mathcal{Q}_\delta(y) \tag{59}$$

sending r to q, where r and q are related as in Proposition 16 with $\mathcal{L} = \mathcal{L}_\delta(y)$. Since each $q \in \mathcal{Q}_\delta(y)$ satisfies $q \leqslant r$ for some $r \in \mathcal{R}_\delta(y)$, and since each $r \in \mathcal{R}_\delta(y)$ is a product of $[y^\delta]$ primes in $\mathcal{P}^*_\delta(y)$, we have:

Proposition 20. *If $q \in \mathcal{Q}_\delta(y)$ then $q \leqslant y^{[y^\delta]} \leqslant e^{y^\delta \log y}$.*

We also have a lower bound for the cardinality of $\mathcal{Q}_\delta(y)$:

Proposition 21. *If $\delta' > \delta$ then $|\mathcal{Q}_\delta(y)| \gg e^{(1-\delta')y^\delta \log y}$.*

Proof. We will bound the fibers of the map (59). Let $\mathcal{F}_q$ be the fiber over q and put $t = [y^\delta] - \omega(q)$. If $t = 0$ then $\mathcal{F}_q = \{q\}$. Otherwise $\mathcal{F}_q$ is contained in the set of all numbers of the form $qp_1p_2\cdots p_t$, where $p_1, p_2, \dots, p_t$ are distinct elements of $\mathcal{P}^*_\delta(y)$. Thus putting $n = \varpi^*_\delta(y)$, we have

$$|\mathcal{F}_q| \leqslant \binom{n}{t} = \frac{n(n-1)\cdots(n-t+1)}{t!} \leqslant n^t$$

By the prime number theorem, $n \leqslant (1+o(1))y/\log y$, so (58) gives

$$|\mathcal{F}_q| \leqslant ((1+o(1))y/\log y)^{O(y^\delta/\log y)} \leqslant y^{O(y^\delta/\log y)}$$

for y sufficiently large. Thus

$$|\mathcal{F}_q| \leqslant e^{O(y^\delta)}.$$

Referring to Proposition 19, we deduce that

$$|\mathcal{Q}_\delta(y)| \geqslant \frac{|\mathcal{R}_\delta(y)|}{e^{O(y^\delta)}} \gg e^{(1-\delta-o(1))[y^\delta]\log y} e^{-O(y^\delta)}. \tag{60}$$

Choose δ'' so that $\delta < \delta'' < \delta'$. Since $[y^\delta] = (1+o(1))y^\delta$, we have

$$(1-\delta-o(1))[y^\delta] > (1-\delta'')y^\delta$$

for y sufficiently large. Hence the stated lower bound follows from (60). □

By construction, the elements $q \in \mathcal{Q}_\delta(y)$ satisfy the hypotheses of Proposition 15, so we can use the proposition to deduce a lower bound for $(h^{\mathrm{nar}}_{K/\mathbb{Q}})^*(q)$. Recall that we have fixed a constant $c > 2$.

Proposition 22. *Suppose that $q \in \mathcal{Q}_\delta(y)$, and let $\hat{p}$ be the smallest prime divisor of q. Assume $y \geqslant 2$.*

(a) $\varphi(\hat{p}) \gg y/(\log y)^c$.

(b) $\omega(q) = y^\delta(1 + o(1))$.

(c) $\lambda(q) \ll e^{O(y^\delta)}$.

(d) *If $\alpha > 0$ then* $\varphi(q) \gg e^{(1-\alpha)y^\delta \log y}$.

Proof. (a) Condition **LS1** gives $\hat{p} > y/(\log y)^c$, so $\varphi(\hat{p}) = \hat{p} - 1 \gg y/(\log y)^c$.

(b) Let $r \in \mathcal{R}_\delta(y)$ be a preimage of q under the map (59). Then $\omega(q) = \omega(r) - t$ with $0 \leqslant t \leqslant |\mathcal{L}_\delta(y)|$. Since $\omega(r) = [y^\delta]$, we see from (58) that

$$\omega(q) = [y^\delta] - O(y^\delta/\log y).$$

But $[y^\delta] = y^\delta(1 + o(1))$.

(c) For each prime $\ell < y^\delta$ define $n(\ell) \geqslant 0$ as follows: If ℓ does not divide $p - 1$ for any prime divisor p of q then put $n(\ell) = 0$; otherwise let $n(\ell)$ be the largest positive integer n such that ℓ^n divides $p-1$ for some prime p dividing q. Since $\lambda(q)$ is the least common multiple of the numbers $p - 1$ as p runs over prime divisors of q, we have

$$\lambda(q) = \prod_{\ell < y^\delta} \ell^{n(\ell)} \leqslant \prod_{l \in \mathcal{L}_\delta(y)} l \leqslant y^{|\mathcal{L}_\delta(y)|} \ll y^{O(y^\delta/\log y)},$$

where in the last step we have used (58).

(d) Choose α' so that $0 < \alpha' < \alpha$. The prime divisors p of q satsfy $p > y/(\log y)^c$ by **LS1**, so by (b) we have

$$q \gg (y/(\log y)^c)^{(1-\alpha')y^\delta} \gg y^{(1-\alpha')y^\delta}.$$

As $\varphi(q) \gg q/\log\log q$ (cf. [11], Theorem 328) and $y/\log\log y$ is an increasing function for large y, we deduce that

$$\varphi(q) \gg \frac{y^{(1-\alpha')y^\delta}}{\log\log(y^{(1-\alpha')y^\delta})},$$

which is $\gg y^{(1-\alpha)y^\delta}$. □

Returning to Proposition 15, and inserting the relevant estimates from Proposition 22, we see that if $q \in \mathcal{Q}_\delta(y)$ then

$$(h^{\mathrm{nar}}_{K/\mathbb{Q}})^*(q) \gg e^{(1-\alpha)y^\delta \log y - O(y^\delta)} \cdot (1 - o(1)).$$

The right-hand side is $\gg e^{(1-\alpha')y^\delta \log y}$ for every $\alpha' > \alpha$, but since $\alpha > 0$ is arbitrary, we can simply change notation and assert that

$$(h^{\mathrm{nar}}_{K/\mathbb{Q}})^*(q) \gg e^{(1-\alpha)y^\delta \log y} \tag{61}$$

for every $\alpha > 0$.

Now take $x \geqslant 2$, and as in [14], let y be the function of x defined by $x = e^{y^\delta \log y}$ (note that $y^\delta \log y$ is strictly increasing for $y > e^{-1/\delta}$). Recalling Proposition 20 as well as the definition (47) of $\sigma(x)$, we see that

$$\sigma(x) \geqslant \sum_{q \in \mathcal{Q}_\delta(y)} (h^{\mathrm{nar}}_{K/\mathbb{Q}})^*(q). \tag{62}$$

Hence (61) and Proposition 21 give $\sigma(x) \gg e^{(2-\alpha-\delta')y^\delta \log y}$ or in other words

$$\sigma(x) \gg x^{2-\alpha-\delta'}. \tag{63}$$

Here α and δ' are arbitrary numbers such that $\alpha > 0$ and $\delta' > \delta$. Thus in light of (49) we may assume that $\alpha + \delta' < 2\varepsilon$, so that (63) gives $\sigma(x) \gg x^{2(1-\varepsilon)}$. In particular, since K is fixed,

$$\sigma(\sqrt{x}/d_K) \gg x^{1-\varepsilon}. \tag{64}$$

Finally, combining (64) with Propositions 13 and 14, we obtain the lower bound in (3). By assumption, $\varepsilon > 1/(4\sqrt{e})$, but if Conjecture B were available then we would obtain (3) for all $\varepsilon > 0$.

References

[1] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math. 140 (1994), 703 – 722.

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

[3] R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith. 83 (1998), 331 – 361.

[4] A. Balog, *$p+a$ without large prime factors*, Sém. Théorie des Nombres Bordeaux (1983–84), éxposé 31.

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

[6] W. J. Ellison (en collaboration avec M. Mendès France), *Les nombers premiers*, Hermann (1975).

[7] P. Erdős, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function*, Quarterly. J. of Math. 6 (1935), 205–213.

[8] J. Friedlander, *Shifted primes without large prime factors.* In: *Number Theory and Applications*, Kluwer (1990), 393–401.

[9] D. Goldfeld and J. Hoffstein, *Eisenstein series of $\frac{1}{2}$-integral weight and the mean value of real Dirichlet L-series*, Invent. math. 80 (1985), 185–208.

[10] S. W. Golomb, *Powerful numbers*, American Math. Monthly 77 (1970), 848-852.

[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press (1979).

[12] J. Klüners, *Über die Asymptotik von Zahlkörpern mit vorgegebener Galoisgruppe*. Habilitationsschrift, Universität Kassel (2005).

[13] S. Lang, *Algebraic Number Theory*, 2nd ed., Springer GTM 110 (1994).

[14] F. Luca and A. Sankaranarayanan, *On the moments of the Carmichael λ function*, Acta Arith. 123 (2006) 389 – 398.

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

[16] J. Martinet, *Character theory and Artin L-functions*, In: *Algebraic Number Fields, Proceedings of the Durham Symposium*, A. Fröhlich ed. Academic Press (1977), 1 – 87.

[17] C. Pomerance, *Popular values of Euler's function*, Mathematika 27 (1980), 84–89.

[18] D. E. Rohrlich, *Nonvanishing of L-functions for GL(2)*, Invent. Math. 97 (1989), 381 – 403.

[19] D. E. Rohrlich, *Self-dual Artin representations* In: Automorphic Represesentations and L-Functions, edited by D. Prasad, C. S. Rajan, A. Sankaranarayanan, J., Tata Institute of Fundamental Research Studies in Math. Vol. 22 (2013), 455 – 499.

[20] D. E. Rohrlich, *Artin representations of $\mathbb{Q}$ of dihedral type*, Mathematical Research Letters 22 (2015), 1767 –1789.

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

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