ERROR ESTIMATES FOR THE DAVENPORT-HEILBRONN THEOREMS

KARIM BELABAS, MANJUL BHARGAVA, AND CARL POMERANCE

Abstract. We improve the known remainder terms for the theorems of Davenport and Heilbronn on the density of discriminants of cubic fields and average 3-torsion in the class group of quadratic fields. This proves analytic continuation of the related Dirichlet series to the left of the line $\Re(s) = 1$.

1. Introduction

The goal of this note is to prove the following theorems:

Theorem 1.1. *For any $\rho < 1/20$, the number of isomorphism classes of cubic fields whose discriminant Δ satisfies $0 < \Delta < X$ is*

$$\frac{1}{12\zeta(3)}X + O(X^{1-\rho}), \tag{1}$$

and the number of isomorphism classes of cubic fields whose discriminant Δ satisfies $0 < -\Delta < X$ is

$$\frac{1}{4\zeta(3)}X + O(X^{1-\rho}). \tag{2}$$

Theorem 1.2. *Let Δ denote the discriminant of a quadratic field, and $r_3(\Delta)$ the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{\Delta})$, that is, $r_3(\Delta) := \dim_{\mathbb{F}_3} \mathrm{Cl}(\Delta) \otimes_{\mathbb{Z}} \mathbb{F}_3$. For any $\rho < 1/20$, we have*

$$\sum_{0<\Delta<X} (3^{r_3(\Delta)} - 1) = \frac{1}{3} \sum_{0<\Delta<X} 1 + O(X^{1-\rho}) \tag{3}$$

and

$$\sum_{0<-\Delta<X} (3^{r_3(\Delta)} - 1) = \sum_{0<-\Delta<X} 1 + O(X^{1-\rho}). \tag{4}$$

The main terms in both these theorems are due to Davenport and Heilbronn [12]. A remainder estimate $O(X \exp(-c\sqrt{\log X}))$ for some $c > 0$ appeared in [3]. It has been conjectured that (1), (2), and possibly (3), (4) hold with $\rho = 1/6$, in fact with an explicit second term in $X^{5/6}$; see Roberts [17].

Let $\xi(s) := \sum_K |\mathrm{disc}\, K|^{-s}$ where K runs over the isomorphism classes of cubic fields. Cohen [7] asks whether the Dirichlet series ξ can be analytically continued even to the line $\Re(s) = 1$. Theorem 1.1 proves analytic continuation to $\Re(s) > 19/20$ with a simple pole at $s = 1$.

Remark 1.3. Using Fourier techniques, it is possible to reduce slightly the error terms as in [1, 4]. But we cannot hope to beat even $\rho = 1/16$ by taking Lemmas 2.9 and 2.10 as a starting point, which are a legacy from Davenport's papers (see Remark 2.11). Thus, obtaining $\rho = 1/6$ will require improving this analysis.

1991 *Mathematics Subject Classification.* 11R11, 11R29, 11R45.

Acknowledgments: This work was initiated at the "Explicit Methods in Number Theory" conference in Oberwolfach's math institute (July 2003), organized by H. Cohen, H. W. Lenstra Jr., and D. Zagier. We would like to thank the institute for its hospitality. The second author is supported by a Long-Term Prize Fellowship from the Clay Mathematics Institute.

2. Cubic fields

Throughout this note, p denotes a prime number, q a squarefree positive integer, $\omega(n)$ is the number of distinct prime divisors of n and μ is the Möbius function, so that $\mu(n) = (-1)^{\omega(n)}$ for a squarefree n and 0 otherwise.

2.1. **Sketch.** An order is a ring $\mathcal{O}$ which is both an integral domain and a free $\mathbb{Z}$-module of finite rank (hence contains a copy of $\mathbb{Z}$). Its field of fractions $K = \mathrm{Frac}(\mathcal{O})$ is a number field, which has a maximal order $\mathcal{O}_K$. The *index* of an order is $(\mathcal{O}_K : \mathcal{O})$, the cardinality of the finite abelian group $\mathcal{O}_K/\mathcal{O}$.

The *content* of $\mathcal{O}$ is the largest integer c such that $\mathcal{O}/\mathbb{Z} \cong c \cdot (\mathcal{O}'/\mathbb{Z})$ for some order $\mathcal{O}'$. If c is the content of $\mathcal{O}$, the "principal part" $\mathcal{O}'$ is then unique. An order $\mathcal{O}$ is *primitive* if its content is 1.

We call an order of $\mathbb{Z}$-rank 3 a *cubic order*: it is an order in a cubic number field. The crux of the method is the following result.

Theorem 2.1 (Delone-Faddeev [13])**.** *The isomorphism classes of cubic orders are in bijection with the classes of irreducible integral binary cubic forms modulo* $\mathrm{GL}(2,\mathbb{Z})$*. The bijection preserves discriminant and content. In particular, it associates primitive orders to primitive forms.*

We recall that $\mathrm{GL}(2,\mathbb{R})$ acts on the space of binary forms via

$$(\gamma \cdot F)(x,y) = (\det \gamma)^{-1} F\big((x,y)\cdot\gamma\big).$$

Instead of cubic fields, we count the isomorphism classes of their maximal orders, which are associated to certain orbits of classes of cubic forms. Davenport and Heilbronn [12] gave a local characterization of these "maximal" classes (see also [5, 6]). Via reduction theory for binary cubics, we are eventually reduced to counting integral points in a semi-algebraic set, satisfying suitable congruences.

2.2. **Orders of large index.** Let $\mathcal{N}^{\pm}(q,X)$ denote the number of isomorphism classes of cubic orders of index divisible by q, whose discriminant Δ satisfies $0 < \pm\Delta < X$, respectively. We need a rough upper bound for $\mathcal{N}^{\pm}(q,X)$.

Lemma 2.2 (Davenport [10, 11])**.** *We have* $\mathcal{N}^{\pm}(1,X) = O(X)$*.*

Lemma 2.3. *For a fixed order* $\mathcal{O}$ *and* $n \in \mathbb{Z}_{>0}$*, let*

$$\mathrm{Ord}(\mathcal{O},n) := \{\mathcal{O}' \subset \mathcal{O} \colon (\mathcal{O} : \mathcal{O}') = n,\ \mathcal{O}' \text{ is an order}\}$$

and $\psi(\mathcal{O},n) := \#\,\mathrm{Ord}(\mathcal{O},n)$*. Then* $n \mapsto \psi(\mathcal{O},n)$ *is a multiplicative function.*

Proof. If $(a,b) = 1$, the map

$$\mathrm{Ord}(\mathcal{O},a) \times \mathrm{Ord}(\mathcal{O},b) \to \mathrm{Ord}(\mathcal{O},ab),$$

where $(A,B) \mapsto A \cap B$, is a bijection. □

Lemma 2.4. *Let* $\mathcal{O}$ *be a fixed cubic order and* q *a squarefree integer coprime to the content of* $\mathcal{O}$*. The number of suborders of* $\mathcal{O}$ *with index* q *is bounded by* $3^{\omega(q)}$*.*

Proof. Since $n \mapsto \psi(\mathcal{O}, n)$ is multiplicative, we can assume that $q = p$ is prime. Let F be a representative of the class of forms associated to $\mathcal{O}$. The suborders of prime index p of $\mathcal{O}$ are associated to the roots of F in $\mathbb{P}^1(\mathbb{F}_p)$. More precisely, if $\mathcal{O} = \langle 1, u, v\rangle_{\mathbb{Z}}$, a suborder $\mathcal{O}' = \langle 1, u', v'\rangle_{\mathbb{Z}}$ of index p in $\mathcal{O}$ is given by $(u', v') = (u, v)M$, where $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} p & b \\ 0 & 1 \end{smallmatrix}\right)$, for some $0 \le b < p$. This submodule is a subring if and only if $F \circ M \equiv 0 \pmod{\det M}$. This amounts to $(b : 1)$ or $(1 : 0)$ being a root of F. There are at most $\deg(F) = 3$ roots since the content of F is coprime to q, hence $F \not\equiv 0 \pmod{p}$. □

The assumption on the content is necessary: if it is divisible by a prime p, then all $p + 1$ sub-modules of index p of $\mathcal{O}$ are subrings.

Remark 2.5. A formula of Datskovsky and Wright [8] asserts that the generating function for the orders of index n in a fixed maximal cubic order $\mathcal{O}_K$ is

$$\eta_K(s) := \sum_{n\ge 1} \psi(\mathcal{O}_K, n) n^{-s} = \frac{\zeta_K(s)}{\zeta_K(2s)} \zeta(3s-1)\zeta(2s), \tag{5}$$

where ζ_K is the Dedekind zeta function of the cubic number field K. Conversely, (5) can be proven using elementary arguments analogous to the above. If $\mathcal{O} = \mathcal{O}_K$, the bound in Lemma 2.4 is sharp if and only if all prime divisors of q split completely in K. This is proven either from (5) or a direct argument as above, using the fact that the splitting of F mod p mirrors the splitting of p in K.

Remark 2.6. Shintani [18, 19] proved that

$$\sum_{\mathcal{O}} |\operatorname{disc} \mathcal{O}|^{-s} = \sum_{K} |\operatorname{disc} K|^{-s} \eta_K(2s) \qquad (\Re(s) > 1)$$

has an analytic continuation to $\mathbb{C}$, with simple poles at $s = 1$ and $s = 5/6$, where $\mathcal{O}$ and K run through the isomorphism classes of cubic orders and fields respectively.

Lemma 2.7. *For q a squarefree integer, we have*

$$\mathcal{N}^{\pm}(q, X) = O(X \cdot 3^{\omega(q)}/q^2).$$

Proof. Among the classes of orders counted by $\mathcal{N}(q, X)$, let $\mathcal{N}_0(q, X)$ denote the number of *primitive* orders. Let $\mathcal{O}$ be such a primitive order. An overorder $\mathcal{O}'$ such that $(\mathcal{O}' : \mathcal{O}) = q$ has discriminant $\operatorname{disc} \mathcal{O}' = q^{-2} \operatorname{disc} \mathcal{O}$. By Lemma 2.2 there are $O(X/q^2)$ such orders $\mathcal{O}'$, all of them primitive. Hence $\mathcal{N}_0(q, X) = O(3^{\omega(q)} X/q^2)$ by Lemma 2.4.

In the general case, $\mathcal{O}$ has a content c and there is a unique primitive order $\mathcal{O}'$ such that $c(\mathcal{O}'/\mathbb{Z}) \cong (\mathcal{O}/\mathbb{Z})$, so that

$$\mathcal{N}(q, X) = \sum_{c\ge 1} \mathcal{N}_0(q/(c^2, q), X/c^4) = O\left(\frac{3^{\omega(q)}}{q^2} X \sum_{c\ge 1} \frac{(c^2, q)^2}{c^4} \right).$$

Since q is squarefree, $(c^2, q) = (c, q) \le c$ and the last sum is $O(1)$. □

2.3. **Orders of small index.** Davenport obtained a much more precise result than Lemma 2.2. Unfortunately he was not counting orders but classes of binary cubic forms modulo $\Gamma := \mathrm{SL}(2, \mathbb{Z})$, *not* modulo $\mathrm{GL}(2, \mathbb{Z})$ as we need them. Using reduction theory for binary cubics originating in Hermite [15] and Mathews-Berwick [16], he obtained a bijection between classes (modulo Γ) of forms of discriminant Δ, $0 < \pm\Delta < X$, and integer points in semi-algebraic sets $C_X^{\pm} \subset \mathbb{R}^4$, up to $O(X^{3/4+\varepsilon})$ points corresponding to reducible forms, for any $\varepsilon > 0$. (See [1, §3] for the precise definition of $C_X^{\pm}$.) A point $(a, b, c, d) \in \mathbb{Z}^4$, with $a > 0$, is associated to the Γ-class of $ax^3 + bx^2y + cxy^2 + dy^3$. Davenport then proceeded to count these integer points.

A variant of Davenport's procedure for classes and reduction modulo $\mathrm{GL}(2,\mathbb{Z})$ was used in [2]. Let $D_X^{\pm}$ denote the set of points $(a,b,c,d) \in C_X^{\pm}$ such that $b \geq 0$ and $d > 0$ if $b = 0$.

Lemma 2.8. *Let $\varepsilon > 0$. Up to $O(X^{3/4+\varepsilon})$ points corresponding to reducible forms, the integer points in $D_X^{\pm} \subset C_X^{\pm}$ are in one-to-one correspondence with the cubic orders of discriminant Δ, $0 < \pm\Delta < X$. We have*

$$\left|C_X^{\pm}\right| = 2\left|D_X^{\pm}\right| + O(X^{1/2}).$$

Proof. We have $\mathrm{GL}(2,\mathbb{Z})/\Gamma = \{1,\sigma\}$ with $\sigma = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, which stabilizes $C_X^{\pm}$ and acts as $\sigma \cdot (a,b,c,d) = (a,-b,c,-d)$. The number of Γ-classes is twice the number of $\mathrm{GL}(2,\mathbb{Z})$-classes up to the fixed points of σ, which are the $(a,0,c,0) \in C_X^{\pm} \cap \mathbb{Z}^4$. For $(a,b,c,d) \in C_X^{\pm}$, we have $a = O(X^{1/4})$ and $ac^3 = O(X)$ (see [10, 11]), hence the number of fixed points is dominated by

$$\sum_{a=O(X^{1/4})} \left(1 + (X/a)^{1/3}\right) = O(X^{1/2}).$$

□

Lemma 2.9. *For $\rho > 0$, the "cusp"*

$$\left\{(a,b,c,d) \in D_X^{\pm} \colon a < X^{1/4-3\rho}\right\} \tag{6}$$

contains $O(X^{1-\rho})$ points.

Proof. For the cusp

$$\left\{(a,b,c,d) \in C_X^{\pm} \colon a < X^{1/4-3\rho}\right\},$$

which is a superset of (6), this is proven in Davenport [10, 11]. See also [1, Lemme 3.11]. □

Let $\rho > 0$, which shall be chosen at the end to minimize accumulated error terms. And for each positive squarefree integer q, let $\mathcal{N}^{\pm}(q,X,\rho)$ count the orders with index divisible by q that are associated to points outside the cusp (6).

Lemma 2.10. *For any $\rho > 0$, we have*

$$\mathcal{N}^{\pm}(1,X,\rho) = K^{\pm}X + O(X^{3/4+3\rho}),$$

where $K^- = 3K^+ = \zeta(2)/4$.

Proof. The analogous result is proven in [10, 11] for Γ-classes. There are half as many $\mathrm{GL}(2,\mathbb{Z})$-classes up to $O(X^{1/2})$ points, which are absorbed in the remainder term, as are the $O(X^{3/4+\varepsilon})$ points corresponding to reducible forms. □

Remark 2.11. Taking $\rho = 1/16$ in these two lemmas, one obtains

$$\mathcal{N}^{\pm}(1,X) = K^{\pm}X + O(X^{15/16}).$$

By studying the Dirichlet series from Remark 2.6, Shintani [18, 19] proved that [1]

$$\mathcal{N}^{\pm}(1,X) = K^{\pm}X + \lambda^{\pm}X^{5/6} + O(X^{2/3+\varepsilon}),$$

for certain $\lambda^{\pm} \neq 0$. This could provide a better starting point. In fact, Datskovsky and Wright [9] used Shintani's ideas to generalize Davenport and Heilbronn's results. Though promising, their method currently does not appear to generalize to $\mathcal{N}^{\pm}(q,X)$ as we shall need.

Further

[1] More exactly, Shintani counted Γ-classes of cubic forms, hence twice that quantity up to the $O(X^{1/2})$ points from Lemma 2.8.

Lemma 2.12. *For q a squarefree integer, we have*

$$\mathcal{N}^{\pm}(q,X,\rho)=\nu(q)\mathcal{N}^{\pm}(1,X,\rho)+O\big(\nu(q)(q^2X^{3/4+3\rho}\log X+q^6X^{1/4+3\rho}+q^8)\big),$$

where ν is a multiplicative function defined by

$$\nu(p)=1-(1-p^{-3})(1-p^{-2})=p^{-2}+p^{-3}-p^{-5}$$

for p prime. Hence $\nu(q)=O(q^{-2}\log q)$.

Proof. Up to the change from Γ-classes to $\mathrm{GL}(2,\mathbb{Z})$-classes, this is [1, Prop. 4.4] with $m=q^2$ (resp. $4q^2$) if q is odd (resp. even), using for $s(m)$ one of the densities computed by Davenport-Heilbronn [12]. □

Corollary 2.13. *Let q be a squarefree integer such that $q=O(X^{1/8})$. Then*

$$\mathcal{N}^{\pm}(q,X,\rho)=\nu(q)\mathcal{N}^{\pm}(1,X,\rho)+O(X^{3/4+3\rho}\log^2 X).$$

2.4. **Maximal orders.**

Theorem 2.14. *The number of isomorphism classes of cubic fields whose discriminant Δ satisfies $0<\pm\Delta<X$ is*

$$\frac{K^{\pm}}{\zeta(2)\zeta(3)}X+O(X^{19/20}\log^2 X). \tag{7}$$

Proof. By inclusion-exclusion, the number of classes of *maximal* orders, whose discriminant Δ satisfies $0<\pm\Delta<X$ is

$$\sum_{q\geq 1}\mu(q)\mathcal{N}^{\pm}(q,X) \;=\; \sum_{q\geq 1}\mu(q)\mathcal{N}^{\pm}(q,X,\rho) \;+\; O(X^{1-\rho}),$$

where we count the points belonging to the cusp separately to improve later error terms. We sum up to $Q=O(X^{1/8})$ using Corollary 2.13, and truncate the tail using Lemma 2.7 in the form

$$\mathcal{N}^{\pm}(q,X,\rho)\leq\mathcal{N}^{\pm}(q,X)=O(X3^{\omega(q)}/q^2).$$

Leaving alone the $O(X^{1-\rho})$ term for the time being, we obtain

$$\begin{aligned}\sum_{q\leq Q}\Big(\mu(q)\nu(q)\mathcal{N}^{\pm}(1,X,\rho)+O(X^{3/4+3\rho}\log^2 X)\Big)+\sum_{q>Q}\mathcal{N}^{\pm}(q,X,\rho)\\ =\mathcal{N}^{\pm}(1,X,\rho)\prod_p(1-\nu(p))\\ +O\Big(QX^{3/4+3\rho}\log^2 X\Big)+\sum_{q>Q}O\left(\mathcal{N}^{\pm}(q,X,\rho)+\nu(q)\mathcal{N}^{\pm}(1,X,\rho)\right).\end{aligned}$$

As

$$\prod_p(1-\nu(p))=\frac{1}{\zeta(2)\zeta(3)}\quad\text{and}\quad\sum_{q>Q}\frac{3^{\omega(q)}}{q^2}=O(Q^{-1}\log^2 Q),$$

we finally obtain

$$\frac{K^{\pm}}{\zeta(2)\zeta(3)}X+O(X^{1-\rho}+QX^{3/4+3\rho}\log^2 X+XQ^{-1}\log^2 Q).$$

We now choose $Q=X^{\rho}$, then ρ such that $X^{1-\rho}=X^{3/4+3\rho+\rho}$, i.e., $\rho=1/20$. (Note that with these choices $Q=O(X^{1/8})$.) □

3. 3-ranks

We follow the same general strategy as above. Let p be an odd prime (resp. $p = 2$); an integer $\Delta \equiv 0, 1 \pmod 4$ is *fundamental at* p if it satisfies $p^2 \nmid \Delta$ (resp. $\Delta \not\equiv 0, 4 \pmod{16}$). An integer $\Delta \equiv 0, 1 \pmod 4$ is a *fundamental discriminant* if it is fundamental at all primes. In other words, it is either 1 or the discriminant of a quadratic field. This provides a link between cubic orders and 3-ranks of quadratic fields:

Lemma 3.1 (Hasse [14])**.** *The number of isomorphism classes of cubic orders whose discriminant Δ is fundamental is $(3^{r_3(\Delta)} - 1)/2$.*

Remark 3.2. More generally, let K a cubic field with discriminant d_K and $k := \mathbb{Q}(\sqrt{d_K})$. Then d_K is fundamental at p if and only if the places above p in k are unramified in the cyclic cubic extension Kk/k.

We say an order is fundamental at p if its discriminant is. Let $\mathcal{M}^{\pm}(q, X)$ be the number of isomorphism classes of cubic orders $\mathcal{O}$ whose discriminant Δ satisfies $0 < \pm\Delta < X$ and is *not* fundamental at any prime divisor of q.

Lemma 3.3. *Let q be a squarefree positive integer. The number of isomorphism classes of* maximal *cubic orders $\mathcal{O}_K$ whose discriminants satisfy $0 < \pm\Delta < X$ and which are not fundamental at any prime divisor of q is $O(X \cdot 3^{\omega(q)}/q^2)$.*

Proof. This is due to

$$\sum_{0<\pm\Delta<X} 3^{r_3(\Delta)} = O(X),$$

which follows from Lemmas 2.2 and 3.1, and a classical inequality bounding the 3-rank of the ring class group modulo q of $\mathbb{Q}(\sqrt{\Delta})$ by $\omega(q)+r_3(\sqrt{\Delta})+O(1)$, already used by Davenport and Heilbronn [12]. See Datskovsky and Wright [9] for a (more general) proof yielding $4^{\omega(q)}$ instead of $3^{\omega(q)}$. □

We are now in the position to prove the analogue of Lemma 2.7:

Lemma 3.4. *For q a squarefree integer, we have*

$$\mathcal{M}^{\pm}(q, X) = O(X \cdot 6^{\omega(q)}/q^2). \tag{8}$$

Proof. Let $\mathcal{O}$ be an order contained in a maximal order $\mathcal{O}_K$. Then $\mathcal{O}$ fails to be fundamental at p if and only if $\mathrm{disc}(\mathcal{O}_K)$ is not fundamental at p, or p divides the index $(\mathcal{O}_K : \mathcal{O})$.

Let a, b, c be three integers such that $abc = q$, hence pairwise coprime. We want to count the number of (isomorphism classes of) orders $\mathcal{O}$ such that

- $|\mathrm{disc}(\mathcal{O})| < X$,
- c divides the content of $\mathcal{O}$,
- b divides the index of $\mathcal{O}$ in its maximal order $\mathcal{O}_K$,
- $\mathcal{O}_K$ is not fundamental at any prime divisor of a.

Let cd be the content of such an $\mathcal{O}$, $I = bc^2de$ its index, for some integers $d, e \geq 1$. (Note that b and $(cd)^2$ divide the index, but we may have $(b, d) > 1$; on the other hand, $(b, c) = 1$ and b is squarefree.) The maximal order $\mathcal{O}_K$ containing $\mathcal{O}$ has discriminant less than X/I^2 in absolute value, so there are

$$O(X \cdot 3^{\omega(a)}/(aI)^2)$$

possibilities for $\mathcal{O}_K$ by Lemma 3.3. Let $\Omega(I)$ denote the number of prime divisors of I, counted with multiplicity. Applying repeatedly Lemma 2.4, each of these (primitive) maximal orders contains at most $3^{\Omega(I)}$ *primitive* suborders of index I.

Summing over d and e, we obtain $O(X \cdot 3^{\Omega(abc^2)}/(abc^2)^2)$ orders, that is

$$O(X \cdot 3^{\omega(q)}/q^2 \cdot 3^{\omega(c)}/c^2).$$

There are $3^{\omega(q)}$ ways to write $q = abc$ since q is squarefree, which would yield $9^{\omega(q)}$ instead of $6^{\omega(q)}$ in (8). We instead estimate

$$\sum_{\substack{a,b,c \\ abc=q}} \frac{3^{\omega(c)}}{c^2} = \sum_{c|q} \frac{3^{\omega(c)}}{c^2} 2^{\omega(q/c)} = O(2^{\omega(q)}).$$

□

Theorem 1.2 is now proven as in the previous section, starting from

$$\begin{aligned} \sum_{0<\pm\Delta<X} 1 &= \frac{3}{\pi^2} X + O(X^{1/2}), \\ \sum_{0<\pm\Delta<X} (3^{r_3(\Delta)} - 1)/2 &= \sum_{q \geq 1} \mu(q) \mathcal{M}^{\pm}(q, X), \end{aligned}$$

and the analogue of Lemma 2.12:

Lemma 3.5. *For q a squarefree integer, we have*

$$\mathcal{M}^{\pm}(q, X, \rho) = \tau(q) \mathcal{N}^{\pm}(1, X, \rho) + O\big(\tau(q)(q^2 X^{3/4+3\rho} \log X + q^6 X^{1/4+3\rho} + q^8)\big),$$

where τ is a multiplicative function defined by

$$\tau(p) = 1 - (1 - p^{-2})^2 = 2p^{-2} - p^{-4}$$

for p prime, hence $\tau(q) = O(q^{-2} 2^{\omega(q)})$.

References

[1] K. Belabas, Crible et 3-rang des corps quadratiques, *Ann. de l'Inst. Fourier* **46** (1996), pp. 909–949.

[2] K. Belabas, A fast algorithm to compute cubic fields, *Math. Comp.* **66** (1997), pp. 1213–1237.

[3] K. Belabas, On the mean 3-rank of quadratic fields, *Compositio Mathematica* **118** (1999), pp. 1–9.

[4] K. Belabas & E. Fouvry, Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier, *Duke Math. J.* **98** (1999), no. 2, pp. 217–268.

[5] K. Belabas, On quadratic fields with high 3-rank, *Math. Comp.*, to appear.

[6] M. Bhargava, A simple proof of the Davenport-Heilbronn theorem, 1999, preprint.

[7] H. Cohen, Constructing and counting number fields, in *Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002)*, Higher Ed. Press, 2002, pp. 129–138.

[8] B. Datskovsky & D. J. Wright, The adelic zeta function associated to the space of binary cubic forms. II. Local theory, *J. Reine Angew. Math.* **367** (1986), pp. 27–75.

[9] B. Datskovsky & D. J. Wright, Density of discriminants of cubic extensions, *J. Reine Angew. Math.* **386** (1988), pp. 116–138.

[10] H. Davenport, On the class number of binary cubic forms (i), *J. Lond. Math. Soc.* **26** (1951), pp. 183–192, errata *ibid* **27** (1951), p. 512.

[11] H. Davenport, On the class number of binary cubic forms (ii), *J. Lond. Math. Soc.* **26** (1951), pp. 192–198.

[12] H. Davenport & H. Heilbronn, On the density of discriminants of cubic fields (ii), *Proc. Roy. Soc. Lond. A* **322** (1971), pp. 405–420.

[13] B. N. Delone & D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, vol. 10, American Mathematical Society, 1964.

[14] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Zeitschrift.* **31** (1930), pp. 565–582.

[15] C. Hermite, Sur la réduction des formes cubiques à deux indéterminées, *C.R. Acad. Sci. Paris* **48** (1859), pp. 351–357.

[16] G.-B. Mathews, On the reduction and classification of binary cubics which have a negative discriminant, *Proc. London Math. Soc.* **10** (1912), pp. 128–138.

[17] D. P. Roberts, Density of cubic field discriminants, *Math. Comp.* **70** (2001), no. 236, pp. 1699–1705.
[18] T. Shintani, On Dirichlet series whose coefficients are class numbers of integral binary cubic forms, *J. Math. Soc. Japan* **24** (1972), pp. 132–188.
[19] T. Shintani, On zeta-functions associated with the vector space of quadratic forms, *J. Fac. Sci. Univ. Tokyo, Sec. Ia* **22** (1975), pp. 25–66.

Université Paris-Sud, Département de Mathématiques, F-91405 Orsay, France
E-mail address: Karim.Belabas@math.u-psud.fr

Department of Mathematics, Princeton University, Princeton, NJ 08544, USA
E-mail address: bhargava@math.princeton.edu

Department of Mathematics, Dartmouth College, Hanover, NH 03784, USA
E-mail address: carlp@math.dartmouth.edu