6-TORSION AND INTEGRAL POINTS ON QUARTIC THREEFOLDS

STEPHANIE CHAN, PETER KOYMANS, CARLO PAGANO, AND EFTHYMIOS SOFOS

Abstract. We prove matching upper and lower bounds for the average of the 6-torsion of class groups of quadratic fields. Furthermore, we count the number of integer solutions on an affine quartic threefold.

Contents

1. Introduction

One of the main invariants of class groups of quadratic fields $\mathbb{Q}(\sqrt{D})$ is the size $h_n(D)$ of their n-torsion. It has been investigated by several mathematicians: By the work of Gauss [16] in 1801 the average of $h_2(D)$ for $D < 0$ is a constant multiple of $\log |D|$ when ordering the number fields by $-D$. Davenport and Heilbronn [8] proved in 1971 that $h_3(D)$ has a constant average, while, Fouvry and Klüners [11, 12] in 2007 showed that $h_4(D)$ is on average a constant multiple of $\log |D|$. The influential work of Smith [22] in 2017 established the complete distribution of $h_{2^k}(D)$. There are no other values of n for which the right order of magnitude is known. For general n, there is work on bounds for $h_n(D)$ on average by Soundararajan [23], Heath-Brown–Pierce [17], Frei–Widmer [14] and Koymans–Thorner [20].

The Cohen–Lenstra conjectures [7] predict that $h_n(D)$ is of constant average for n odd and is $\log |D|$ on average for n even. Let $\mathcal{D}^+(X)$ and $\mathcal{D}^-(X)$ be the set of respectively positive and negative fundamental discriminants with absolute value up to X. In this paper we establish the right order of magnitude for the 6-torsion:

Theorem 1.1. *For all $X \geqslant 5$ we have*

$$X \log X \ll \sum_{D \in \mathcal{D}^+(X)} h_6(D) \ll X \log X \qquad \text{and} \qquad X \log X \ll \sum_{D \in \mathcal{D}^-(X)} h_6(D) \ll X \log X.$$

Remark 1.2 (Idea of the proof of Theorem 1.1)**.** Using the Davenport–Heilbronn parametrisation we turn the sum $\sum_D h_6(D)$ into an average of the function $2^{\omega(m)}$ over the values m assumed by a polynomial in 4 variables, where the integer vectors lie in a subset of $\mathbb{R}^4$ with spikes. This average is a special instance of sums of the following form:

$$\sum_{a \in \mathcal{A}} f(c_a) \chi(c_a),$$

where

- $\mathcal{A}$ is a countable set,
- $\chi : \mathcal{A} \to [0, \infty)$ is any function of finite support,

2020 *Mathematics Subject Classification.* 11N37 (primary), 11R29, 11D45 (secondary).

- c_a is an "equidistributed" sequence of positive integers,
- f is a non-negative arithmetic function being multiplicative or more general.

In our companion paper [6] we prove upper bounds for such sums; here we provide its applications.

1.1. **Applications to arithmetic statistics.** The following is a more general version of Theorem 1.1 on mixed moments:

Theorem 1.3. *Fix any $s > 0$. Then for all $X \geqslant 5$ we have*

$$X(\log X)^{2^s-1} \ll \sum_{D\in\mathcal{D}^+(X)} h_2(D)^s h_3(D) \ll X(\log X)^{2^s-1}$$

and

$$X(\log X)^{2^s-1} \ll \sum_{D\in\mathcal{D}^-(X)} h_2(D)^s h_3(D) \ll X(\log X)^{2^s-1},$$

where the implied constant depends at most on s.

1.2. **Applications to Diophantine equations.** We count the number of integer solutions of certain Diophantine equations, examples of which are the quartic affine threefold

$$x_1^2x_2^2 + x_3^2 + x_4^2 = N$$

and the affine quartic fourfold $x_1^2x_2^2+x_3^2x_4^2+x_5^2 = N$. More generally, our work will cover

$$(x_1 \cdots x_k)^2 + x_{k+1}^2 + x_{k+2}^2 = N, \tag{1.1}$$

whose number of variables is roughly half the degree of the equation.

For $N \in \mathbb{N}$ let

$$L(1, \chi_{-N}) = \sum_{m=1}^{\infty} \left(\frac{-N}{m}\right)\frac{1}{m} \qquad \text{and} \qquad \mathfrak{b}(N) = \prod_{p\mid N}\left(1 + \left(\frac{-1}{p}\right)\frac{1}{p}\right).$$

Theorem 1.4. *Fix $k \in \mathbb{N}$ and let N range through positive square-free integers $3 \pmod 8$.*

- *The number of $\mathbf{x} \in \mathbb{Z}^{k+2}$ satisfying (1.1) is*
$$\asymp \mathfrak{b}(N)^{k-1}L(1, \chi_{-N})N^{\frac{1}{2}}(\log N)^{k-1},$$
where the implied constant depends only on k.
- *The number of $\mathbf{x} \in \mathbb{Z}^{2k+1}$ satisfying*
$$(x_1 \cdots x_k)^2 + (x_{k+1} \cdots x_{2k})^2 + x_{2k+1}^2 = N$$
is $\asymp \mathfrak{b}(N)^{2(k-1)}L(1, \chi_{-N})N^{\frac{1}{2}}(\log N)^{2(k-1)}$, where the implied constant depends only on k.
- *The number of $\mathbf{x} \in \mathbb{Z}^{3k}$ satisfying*
$$(x_1 \cdots x_k)^2 + (x_{k+1} \cdots x_{2k})^2 + (x_{2k+1} \cdots x_{3k})^2 = N$$
is $\asymp \mathfrak{b}(N)^{3(k-1)}L(1, \chi_{-N})N^{\frac{1}{2}}(\log N)^{3(k-1)}$, where the implied constant depends only on k.

The upper bound in the first case follows from earlier work of Henriot [18, Theorem 3]. All cases of Theorem 1.4 are special cases of the more general Theorem 4.1, which allows us to put general multiplicative weights on the integer solutions x_i of

$$x_1^2 + x_2^2 + x_3^2 = N.$$

Its proof is given in §4.1 and is based on Theorem 2.4 and deep estimates of Duke [9] for the Fourier coefficients of cusp forms. It is worth mentioning that matching upper and lower bounds for the number of solutions of $x_1^2 + x_2^2 + p^2 = N$, ($x_1, x_2 \in \mathbb{Z}, p$ prime), were given by Friedlander and Iwaniec [15, Theorem 14.5] on the assumption of the Generalized Riemann hypothesis and the Elliott–Halberstam conjecture.

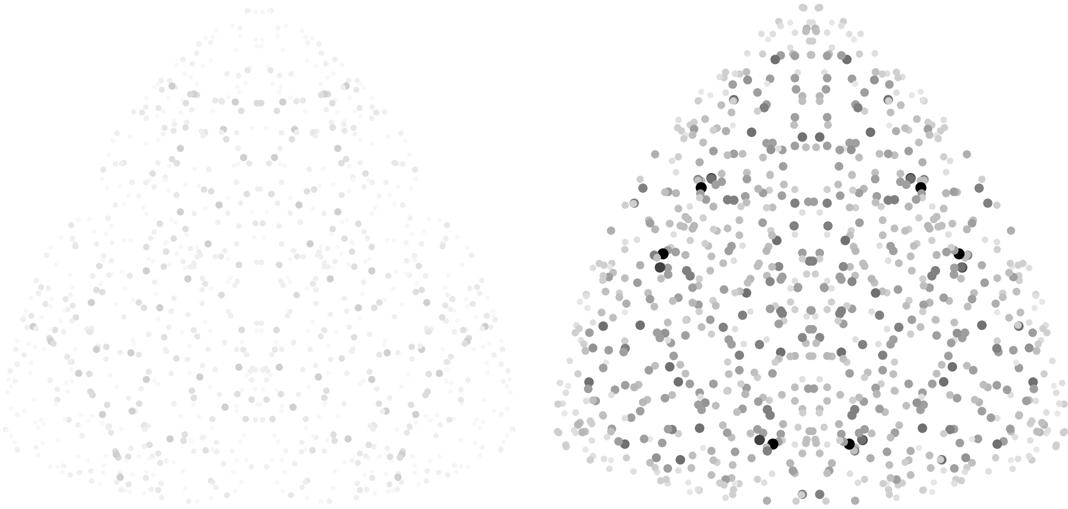

FIGURE 1.1. Weighted points on the sphere for $N = 1716099$ and $N = 1707035$

Remark 1.5 (Bias)**.** The term $L(1, \chi_{-N})N^{1/2}$ corresponds to the number of terms in the sum by a classical result of Gauss, whereas, $(\log N)^{k-1}$ is the average of the k-th divisor function. The shape of $\mathfrak{b}(N)$ is biased towards integers N having many prime divisors $p \equiv 1 \pmod 4$ below $\log N$.

The bias is illustrated in the three-dimensional plots in Figure 1.1. They depict points $\mathbf{x} \in \mathbb{N}^3$ with $\sum_{i=1}^3 x_i^2 = N$, where each $\mathbf{x}$ is colored based on the magnitude of $\prod_{i=1}^3 \tau(x_i)$. The equations respectively have 960 and 936 solutions in $\mathbb{N}^3$. Among the six primes that divide 1716099, only one is $1 \pmod 4$. However, in the factorization of 1707035, four primes are involved, and all except one are $1 \pmod 4$.

Notation. For a non-zero integer m define $\Omega(m) := \sum_{p|m} v_p(m)$, where v_p is the standard p-adic valuation. Define $P^+(m)$ to be the largest prime factor of a positive integer m with the convention $P^+(1) = 1$. Throughout the paper we shall also make use of the convention that when iterated logarithm functions $\log t, \log\log t$, etc., are used, the real variable t is assumed to be sufficiently large to make the iterated logarithm well-defined.

Acknowledgements. The work started during the research stay of SC, PK and CP during the workshop *Problèmes de densité en Arithmétique* at CIRM Luminy in 2023. We would like to thank the organisers Samuele Anni, Peter Stevenhagen and Jan Vonk. We thank Levent Alpöge, Robert J. Lemke Oliver and Frank Thorne for useful discussions on §3.1. PK gratefully acknowledges the support of Dr. Max Rössler, the Walter Haefner Foundation and the ETH Zürich Foundation. Part of the work of SC was supported by the National Science Foundation under Grant No. DMS-1928930, while the author was in residence at the MSRI in Spring 2023.

Structure of the paper. In §2 we recall the necessary results from [6]. Sections 3.1-3.2 respectively contain the proofs of Theorems 1.1 and 1.3 on the 6-rank. Sections 4.1-4.5 contain the proof of Theorem 4.1 on sums of three squares; it generalises Theorem 1.4.

2. Prerequisite lemmas

In this section we recall the required bounds proved in [6].

Definition 2.1 (Density functions)**.** Fix $\kappa, \lambda_1, \lambda_2, B, K > 0$. Then we introduce the set $\mathcal{D}(\kappa, \lambda_1, \lambda_2, B, K)$ of multiplicative functions $h : \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ by the properties

- for all $B < w < z$ we have
$$\prod_{\substack{p \text{ prime} \\ w \leqslant p < z}} (1 - h(p))^{-1} \leqslant \left(\frac{\log z}{\log w}\right)^{\kappa} \left(1 + \frac{K}{\log w}\right), \tag{2.1}$$
- for every prime $p > B$ and integers $e \geqslant 1$ we have
$$h(p^e) \leqslant \frac{B}{p}, \tag{2.2}$$
- for every prime p and $e \geqslant 1$ we have
$$h(p^e) \leqslant p^{-e\lambda_1 + \lambda_2}. \tag{2.3}$$

Let $\mathcal{A}$ be an infinite set and for each $T \geqslant 1$ let $\chi_T : \mathcal{A} \to [0, \infty)$ be such that
$$\{a \in \mathcal{A} : \chi_T(a) > 0\} \text{ is finite for every } T \geqslant 1. \tag{2.4}$$
We also assume that
$$\lim_{T \to +\infty} \sum_{a \in \mathcal{A}} \chi_T(a) = +\infty. \tag{2.5}$$
Assume that we are given a sequence of strictly positive integers $(c_a)_{a \in \mathcal{A}}$ indexed by $\mathcal{A}$ and denoted by $\mathfrak{C} := \{c_a : a \in \mathcal{A}\}$. We are interested in sums of the form
$$\sum_{a \in \mathcal{A}} \chi_T(a) f(c_a),$$
where f is an arithmetic function.

We will need the following notion of 'equidistribution' of the values of the integer sequence c_a in arithmetic progressions. For a non-zero integer d and any $T \geqslant 1$, let
$$C_d(T) = \sum_{\substack{a \in \mathcal{A} \\ c_a \equiv 0 (\mathrm{mod}\ d)}} \chi_T(a).$$

Definition 2.2 (Equidistributed sequences)**.** We say that $\mathfrak{C}$ is equidistributed if there exist positive real numbers $\theta, \xi, \kappa, \lambda_1, \lambda_2, B, K$ with $\max\{\theta, \xi\} < 1$, a function $M : \mathbb{R}_{\geqslant 1} \to \mathbb{R}_{\geqslant 1}$ and a function $h_T \in \mathcal{D}(\kappa, \lambda_1, \lambda_2, B, K)$ such that
$$C_d(T) = h_T(d) M(T) \left\{1 + O\left(\prod_{\substack{B < p \leqslant M(T) \\ p \nmid d}} (1 - h_T(p))^2\right)\right\} + O(M(T)^{1-\xi}) \tag{2.6}$$
for every $T \geqslant 1$ and every $d \leqslant M(T)^{\theta}$, where the implied constants are independent of d and T.

It is worth emphasizing that in this definition the constants $\theta, \xi, \kappa, \lambda_1, \lambda_2, B, K$ are all assumed to be independent of T. For example, the bound $h_T(p^e) = O(1/p)$ in (2.2) holds with an implied constant that is independent of e, p as well as T. From now on we shall write M for $M(T)$.

Definition 2.3 (A class of functions)**.** Fix $A \geqslant 1, \epsilon > 0, C > 0$. The set $\mathcal{M}(A, \epsilon, C)$ of functions $f : \mathbb{N} \to [0, \infty)$ is defined by the property that for all coprime m, n one has
$$f(mn) \leqslant f(m) \min\{A^{\Omega(n)}, Cn^{\epsilon}\}.$$

We are now ready to state the main result in [6].

Theorem 2.4. *Let $\mathcal{A}$ be an infinite set and for each $T \geqslant 1$ define $\chi_T : \mathcal{A} \to [0, \infty)$ to be any function such that both* (2.4) *and* (2.5) *hold. Take a sequence of strictly positive integers $\mathfrak{C} = (c_a)_{a\in\mathcal{A}}$. Assume that $\mathfrak{C}$ is equidistributed with respect to some positive constants $\theta, \xi, \kappa, \lambda_1, \lambda_2, B, K$ and functions $M(T)$ and $h_T \in \mathcal{D}(\kappa, \lambda_1, \lambda_2, B, K)$ as in Definition 2.2. Fix any $A > 1$ and assume that f is a function such that for every $\epsilon > 0$ there exists $C > 0$ for which $f \in \mathcal{M}(A, \epsilon, C)$, which is introduced in Definition 2.3. Assume that there exists $\alpha > 0$ and $\widetilde{B} > 0$ such that for all $T \geqslant 1$ one has*

$$\sup\{c_a : a \in \mathcal{A}, \chi_T(a) > 0\} \leqslant \widetilde{B} M^{\alpha}, \tag{2.7}$$

where $M = M(T)$ is as in Definition 2.2. Then for all $T \geqslant 1$ we have

$$\sum_{a\in\mathcal{A}} \chi_T(a) f(c_a) \ll M \prod_{B<p\leqslant M} (1 - h_T(p)) \sum_{a\leqslant M} f(a) h_T(a),$$

where the implied constant is allowed to depend on $\alpha, A, B, \widetilde{B}, \theta, \xi, K, \kappa$, λ_i, the function f and the implied constants in (2.6)*, but is independent of T and M.*

The following result is inspired by [24, Théorème 1.1] that has the upper bound assumptions [24, (i),(ii),(iii),(v), pages 591-592] and a lower bound assumption [24, (iv), page 592]. We have no lower bound assumption but our upper bound assumption is less general than [24, (i),(ii),(iii),(v), pages 591-592].

Lemma 2.5. *Fix any $k \in \mathbb{N}$ and assume that f is a multiplicative function satisfying $0 \leqslant f(p^e) \leqslant \tau(p^e)^k p^{-e}$ for all $e \geqslant 1$ and primes p. Then for all $x \geqslant 2$ we have*

$$\sum_{n\leqslant x} f(n) \asymp \exp\left(\sum_{p\leqslant x} f(p)\right),$$

where the implied constants depend at most on k.

Proof. The upper bound is evident. For the lower bound our plan is to prove that there exists $\delta = \delta(k) \in (0, 1)$ such that

$$\exp\left(\sum_{p\leqslant x^{\delta}} f(p)\right) \ll \sum_{n\leqslant x} f(n). \tag{2.8}$$

This is clearly sufficient since

$$\sum_{x^{\delta}<p\leqslant x} f(p) \ll_k \sum_{x^{\delta}<p\leqslant x} \frac{1}{p} \ll_k 1.$$

To prove (2.8) we start by noting that for each $y \in [2, x]$ one has

$$\sum_{n\leqslant x} f(n) \geqslant \sum_{\substack{n\leqslant x\\ P^+(n)\leqslant y}} f(n)\mu(n)^2 = \sum_{P^+(n)\leqslant y} f(n)\mu(n)^2 - \sum_{\substack{n>x\\ P^+(n)\leqslant y}} f(n)\mu(n)^2.$$

Since there exists $C(k) > 0$ such that

$$\sum_{P^+(n)\leqslant y} f(n)\mu(n)^2 \geqslant C(k) \exp\left(\sum_{p\leqslant y} f(p)\right),$$

it suffices to show that

$$\sum_{\substack{n>x\\ P^+(n)\leqslant y}} f(n)\mu(n)^2 \leqslant \frac{C(k)}{2} \exp\left(\sum_{p\leqslant y} f(p)\right).$$

We will see that this holds when $y = x^\delta$, where δ is a small positive constant that depends on k. Define $\sigma = 1/\log y$ so that by Rankin's trick we have

$$\sum_{\substack{n>x\\ P^+(n)\leqslant y}} f(n)\mu(n)^2 \leqslant x^{-\sigma} \sum_{P^+(n)\leqslant y} f(n)\mu(n)^2 n^\sigma$$

$$=x^{-\sigma}\prod_{p\leqslant y}(1+f(p)p^\sigma) \leqslant x^{-\sigma}\exp\left(\sum_{p\leqslant y} f(p)p^\sigma\right).$$

Since $\mathrm{e}^t \leqslant 1+\mathrm{e}\cdot t$ for $0\leqslant t\leqslant 1$, we see that $p^\sigma \leqslant 1+\mathrm{e}\cdot\sigma\log p$ for all primes $p\leqslant y$, hence, the sum inside the exponential is at most

$$\sum_{p\leqslant y} f(p) + O\left(\sigma\sum_{p\leqslant y} f(p)\log p\right) \leqslant \sum_{p\leqslant y} f(p) + O\left(\sigma\sum_{p\leqslant y}\frac{\log p}{p}\right) = \sum_{p\leqslant y} f(p)+O(1).$$

Hence, there exists a positive constant $C_1(k)$ such that

$$\sum_{\substack{n>x\\ P^+(n)\leqslant y}} f(n)\mu(n)^2 \leqslant C_1(k)x^{-\sigma}\exp\left(\sum_{p\leqslant y} f(p)\right).$$

Denote $C_2(k) = C(k)/(2C_1(k))$. We want to make sure that $x^{-\sigma}\leqslant C_2(k)$; this can be achieved by taking $y = x^\delta$ with $\delta = \max\{1/2, (-\log C_2(k))^{-1}\}$. This is because we have $x^\sigma = \mathrm{e}^{1/\delta}$ due to $y = x^\delta$. □

3. Arithmetic statistics

3.1. **6-torsion.** Here we prove Theorems 1.1 using Theorem 2.4. This has an assumption related to a level of distribution result. Similar results have been obtained by [3, Theorem 1.2], [10, Section 6] and [21, Theorem 2.1]. Here we use the one by Belabas [2, Théorème 1.2]. Let g_1 be the multiplicative function defined as

$$g_1(p^e) = \begin{cases} p/(p+1), & \text{if } p\geqslant 2 \text{ and } e=1\\ 0, & \text{if } p>2 \text{ and } e\geqslant 2\\ 4/3, & \text{if } p=2 \text{ and } e=2\\ 4/3, & \text{if } p=2 \text{ and } e=3\\ 0, & \text{if } p=2 \text{ and } e\geqslant 4.\end{cases}$$

It is not difficult to see that

$$\prod_{p\leqslant X}\Big(1-\frac{g_1(p)}{p}\Big)\sum_{a\leqslant X}2^{\omega(a)}\frac{g_1(a)}{a} \leqslant \prod_{p\leqslant X}\Big(1-\frac{g_1(p)}{p}\Big)\sum_{a\leqslant X}2^{\omega(a)}\frac{4}{3a} \ll \log X. \tag{3.1}$$

Lemma 3.1. *Fix any $\epsilon>0$. Then for all $q\in\mathbb{N}$ and $X\geqslant 2$ with $q<X^{\frac{1}{15}-\epsilon}$ we have*

$$\sum_{\substack{D\in\mathcal{D}^+(X)\\ q\mid D}}(h_3(D)-1) = \frac{1}{\pi^2}\frac{g_1(q)}{q}X + O\left(\frac{X}{q(\log X)^2(\log\log X)^{2-\epsilon}} + X^{\frac{15}{16}+\epsilon}q^{-\frac{1}{16}}\right)$$

and

$$\sum_{\substack{D\in\mathcal{D}^-(X)\\ q\mid D}}(h_3(D)-1) = \frac{3}{\pi^2}\frac{g_1(q)}{q}X + O\left(\frac{X}{q(\log X)^2(\log\log X)^{2-\epsilon}} + X^{\frac{15}{16}+\epsilon}q^{-\frac{1}{16}}\right),$$

where the implied constants are independent of q and X.

Proof. This follows from [2, Théorème 1.2] and the remark immediately thereafter. □

We are now ready to begin the proof of Theorem 1.1. The lower bounds follow from $h_6(D) \geqslant h_2(D)$ and genus theory. This idea for the lower bound was further exploited and investigated in [13, Section 5]. For the upper bounds, we use Theorem 2.4 with

$$\mathcal{A} = \{D \text{ fundamental discriminant}\},\ \chi_T(D) = (h_3(D)-1)\mathbb{1}_{|D|\leqslant T}(D),\ c_D = |D|.$$

We let $h(q) = g_1(q)/q$ and f be the multiplicative function $f(n) = 2^{\omega(n)}$. Lemma 3.1 shows that the level of distribution assumption in Definition 2.2 is satisfied with

$$M(T) = \frac{4}{\pi^2}T,\quad \theta = \frac{1}{30} \quad \text{and} \quad \xi = \frac{1}{32}.$$

Let $h_n^+(D)$ be the size of the n-torsion subgroup of the narrow class group. We have $h_n(D) \leqslant h_n^+(D)$. Since $h_2^+(D) = 2^{\omega(D)-1}$ and $h_6^+(D) = h_2^+(D)h_3^+(D)$, we obtain

$$\sum_{D\in\mathcal{D}^+(X)} h_6^+(D) + \sum_{D\in\mathcal{D}^-(X)} h_6^+(D)$$

$$= \sum_{D\in\mathcal{D}^+(X)} h_2^+(D) + \sum_{D\in\mathcal{D}^-(X)} h_2^+(D) + \sum_{D\in\mathcal{D}^+(X)\cup\mathcal{D}^-(X)} (h_3(D)-1)\, h_2^+(D).$$

The first two sums are readily estimated as $O(X\log X)$. For the final sum, the application of Theorem 2.4 and (3.1) yields

$$\sum_{D\in\mathcal{D}^+(X)\cup\mathcal{D}^-(X)} (h_3(D)-1)\, h_2^+(D) = \sum_{D\in\mathcal{A}} \chi_X(D) f(c_D) \ll X\log X.$$

3.2. **Proof of Theorem 1.3.** The proof is as that of Theorem 1.1 with the only difference being that (3.1) must be replaced by the bound

$$\sum_{a\leqslant X} \frac{2^{s\omega(a)}}{a} \ll (\log X)^{2^s}.$$

4. Diophantine equations

4.1. **Three squares.** Denote $L(1,\chi_{-N}) = \sum_{m=1}^\infty \left(\frac{-N}{m}\right) m^{-1}$, where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol. A theorem of Gauss states that for positive square-free $N \equiv 3 \pmod 8$ one has

$$\sharp\{\mathbf{x}\in\mathbb{Z}^3 : x_1^2+x_2^2+x_3^2 = N\} = \frac{8}{\pi}L(1,\chi_{-N})N^{1/2}.$$

The main result of this section allows to put multiplicative weights on each variable. For $N\in\mathbb{N}$ and an arithmetic function f we define

$$c_f(N) := \prod_{p|N}\left(1 + \left(\frac{-1}{p}\right)\frac{(f(p)-1)}{p}\right). \tag{4.1}$$

Theorem 4.1. *Fix any $s>0, \alpha_1,\alpha_2,\alpha_3 \in \{0,1\}$ and let $\alpha = \sum_{i=1}^3 \alpha_i$. Assume that $f:\mathbb{N}\to[0,\infty)$ is a multiplicative function such that $f(ab)\leqslant \tau(a)^s f(b)$ holds for all $a,b\in\mathbb{N}$. Then for all positive square-free integers $N\equiv 3 \pmod 8$ we have*

$$\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3\\ x_1^2+x_2^2+x_3^2=N}} \prod_{i=1}^3 f(|x_i|)^{\alpha_i} \ll L(1,\chi_{-N})N^{1/2}c_f(N)^\alpha \exp\left(\alpha\sum_{p\leqslant N}\frac{f(p)-1}{p}\right),$$

where the implied constant is independent of N.

If, in addition, for each $L \geqslant 1$ one has $\inf\{f(m) : \Omega(m) \leqslant L\} > 0$, then for all positive square-free integers $N \equiv 3 \pmod 8$ we have

$$\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3\\ x_1^2+x_2^2+x_3^2=N}} \prod_{i=1}^{3} f(|x_i|)^{\alpha_i} \gg L(1,\chi_{-N}) N^{1/2} c_f(N)^{\alpha} \exp\left(\alpha \sum_{p\leqslant N} \frac{f(p)-1}{p}\right),$$

where the implied constant is independent of N.

The proof requires arguments that use the fact that the coordinates x_i behave independently. In §4.3 we transform the sums into ones where $\prod_{i=1}^3 f(|x_i|)$ is replaced by $f(\prod_{i=1}^3 |x_i|)$. Subsequently, in §4.4 we prove the required level of distribution for the transformed sums by using work of Duke [9]. Finally, in §4.5 we prove Theorem 4.1.

4.2. **Input from cusp forms.** The main result in this subsection is Lemma 4.4; it regards the number of solutions of $x_1^2 + x_2^2 + x_3^2 = N$, with each x_i divisible by an arbitrary integer d_i. This is closely related to work of Brüdern–Blomer [4, Lemma 2.2] in the case where each d_i is square-free. The proof of Lemma 4.4 combines the work of Duke [9] with that of Jones [19]. We recall [9, Theorem 2, Equation (3)]:

Lemma 4.2 (Duke)**.** *There exists a positive constant κ such that for every positive definite quadratic integer ternary form q and every square-free integer N one has*

$$\sharp\{\mathbf{x}\in\mathbb{Z}^3 : q(\mathbf{x}) = N\} = \kappa L(1,\chi_{q,N}) \mathfrak{S}(q,N)\frac{\sqrt{N}}{\sqrt{D}} + O(D^6 N^{1/2-1/30}),$$

where the implied constant is absolute, D is the determinant of the matrix $(\partial^2 q/\partial x_i \partial x_j)$, $\chi_{q,N}$ is the Dirichlet character $\chi_{q,N}(m) = (\frac{-2D\mathrm{disc}(\mathbb{Q}(\sqrt{N}))}{m})$ and

$$\mathfrak{S}(q,N) := \prod_{p\mid 2D} \lim_{\lambda\to\infty} \frac{\sharp\left\{\mathbf{x}\in(\mathbb{Z}/p^\lambda\mathbb{Z})^3 : q(\mathbf{x}) \equiv N \left(\mathrm{mod}\ p^\lambda\right)\right\}}{p^{2\lambda}}.$$

Note that the definition of $\mathfrak{S}$ in [9, Equation (4)] involves a finite value of λ, however, this is equivalent since these densities stabilise owing to the fact that N is square-free. We now specify the constant κ. When $q = \sum_{i=1}^3 x_i^2$ we have $D = 8$, hence,

$$\sharp\{\mathbf{x}\in\mathbb{Z}^3 : x_1^2+x_2^2+x_3^2 = N\} = \frac{\kappa\mathcal{N}(16^3)}{2\sqrt{2}}\sqrt{N}\sum_{m=1}^{\infty}\left(\frac{-4N}{m}\right)\frac{1}{m} + O(N^{1/2-1/30}),$$

where $\mathcal{N}(m) = \sharp\{\mathbf{x}\in(\mathbb{Z}/m\mathbb{Z})^3 : x_1^2+x_2^2+x_3^2 \equiv N \pmod m\} m^{-2}$.

Lemma 4.3. *For any integer $N \equiv 3 \pmod 8$ and $t \geqslant 3$, the number of solutions of $x_1^2+x_2^2+x_3^2 \equiv N \pmod{2^t}$ is 4^t.*

Proof. Since $N \equiv 3 \pmod 8$ every x_i must be odd. Let x_1, x_2 run through all odd elements $\pmod{2^t}$ and then count the number of x_3 for which $x_3^2 \equiv a \pmod{2^t}$, where $a \equiv N - x_1^2 - x_2^2 \pmod{2^t}$. Here $N \equiv 3 \pmod 8$, hence, $a \equiv 1 \pmod 8$. Now we use the following fact: for $t \geqslant 3$ and each $a \in \mathbb{Z}/2^t\mathbb{Z}$ with $a \equiv 1 \pmod 8$, the number of solutions of $x^2 \equiv a \pmod{2^t}$ is 4. This gives a total number of solutions $2^{t-1}\cdot 2^{t-1}\cdot 4 = 4^t$. □

In particular, $\mathcal{N}(16^3) = 1$. We obtain

$$\sharp\{\mathbf{x}\in\mathbb{Z}^3 : x_1^2+x_2^2+x_3^2 = N\} = \frac{\kappa}{2\sqrt{2}}\sqrt{N}\sum_{m=1}^{\infty}\left(\frac{-4N}{m}\right)\frac{1}{m} + O(N^{1/2-1/30}).$$

By [1, Theorem B, page 99] this equals $\frac{16}{\pi}\mathcal{L}\sqrt{N}$, where $\mathcal{L} := \sum_{m=1}^{\infty}\left(\frac{-4N}{m}\right)\frac{1}{m}$. By Siegel's theorem we have $\mathcal{L} \gg N^{-1/60}$, hence, $\kappa = 32\sqrt{2}/\pi$ is deduced from

$$\frac{\kappa}{2\sqrt{2}} - \frac{16}{\pi} = O\left(\frac{1}{N^{1/30}\mathcal{L}}\right) = O\left(\frac{1}{N^{1/60}}\right).$$

Lemma 4.4. *For each* $\mathbf{c} \in \mathbb{N}^3$ *and positive square-free* $N \equiv 3 \pmod 8$ *we have*

$$\sharp\left\{\mathbf{x} \in \mathbb{Z}^3 : \sum_{i=1}^{3}(c_i x_i)^2 = N\right\} = \frac{8}{\pi}L(1,\chi_{-N})h_N(\mathbf{c})N^{1/2} + O((c_1c_2c_3)^{12}N^{1/2-1/30}),$$

where the implied constant is absolute, $h_N(\mathbf{c})$ *is given by*

$$\frac{2^{\sharp\{p|c_1c_2c_3\}}}{c_1c_2c_3}\prod_{p|c_1c_2c_3}\left(1-\frac{\left(\frac{-N}{p}\right)}{p}\right)\mathbb{1}((4.2)-(4.4))\prod_{\substack{p|c_1c_2c_3\\ p \text{ divides exactly one } c_i}} 2^{-\mathbb{1}(p\nmid N)}\left(1-\frac{1}{p}\left(\frac{-1}{p}\right)\right)$$

and

$$2 \nmid c_1c_2c_3, \tag{4.2}$$

$$\gcd(c_1,c_2,c_3) = 1, \tag{4.3}$$

$$p \text{ divides exactly two } c_i \Rightarrow \left(\frac{N}{p}\right) = 1, \tag{4.4}$$

$$p \mid N, p \text{ divides exactly one } c_i \Rightarrow p \equiv 1 \pmod 4. \tag{4.5}$$

Proof. We use Lemma 4.2 with $q = \sum_{i=1}^{3} c_i^2 x_i^2$ so that $D = 8(c_1c_2c_3)^2$. Let us note that $\mathrm{disc}(\mathbb{Q}(\sqrt{N})) = 4N$, hence, the character $\chi_{q,N}(m)$ is given by

$$\left(\frac{-2\cdot 8(c_1c_2c_3)^2\cdot 4N}{m}\right) = \left(\frac{-N}{m}\right)\mathbb{1}(\gcd(2c_1c_2c_3,m)=1).$$

Therefore, the value of the corresponding L-function at 1 is

$$\prod_{p\nmid 2c_1c_2c_3}\frac{1}{\left(1-\frac{\left(\frac{-N}{p}\right)}{p}\right)} = \frac{L(1,\chi_{-N})}{2}\prod_{\substack{p|c_1c_2c_3\\ p\neq 2}}\left(1-\frac{\left(\frac{-N}{p}\right)}{p}\right).$$

To work out the term $\mathfrak{S}$ we use the work of Jones [19]. In the terminology of [19, Theorem 1.3] we take $Q = \sum_{i=1}^{3}(c_ix_i)^2, m = N$. When $p \neq 2$ divides exactly one of the c_i, say, c_3, then we take $a = c_1^2, b_1 = 0$ and [19, Equation (1.5)] shows that the p-adic factor in $\mathfrak{S}$ equals

$$\mathbb{1}(p \mid N)2\left(1-\frac{1}{p}\right)\mathbb{1}(p \equiv 1 \pmod 4) + \mathbb{1}(p \nmid N)\left(1-\frac{1}{p}\left(\frac{-1}{p}\right)\right).$$

If p divides exactly two of the c_i's, say c_2 and c_3 then by taking $a = c_1^2$ in [19, Equation (1.4)] shows that the p-adic factor in $\mathfrak{S}$ becomes 2 or 0, according to whether $(\frac{N}{p}) = 1$ or not. Finally, since N is square-free, there is no prime p that divides every c_i since that would imply that p^2 divides N. Further, by Lemma 4.3 the 2-adic density equals 1. □

4.3. **Transformation.** To transform the sums in Theorem 4.1 a preliminary step is to show that for most integer solutions of $x_1^2 + x_2^2 + x_3^2 = N$ the common divisors of each pair (x_i, x_j) are typically small. In Lemma 4.5 we show that these divisors are frequently smaller than any fixed power of N, while in Lemmas 4.6-4.7 we show that these divisors are smaller than a power of $\log N$. The latter task combines equidistribution in the form of Lemma 4.4 with a "level-lowering" mechanism that is grounded on work of Brady [5].

Lemma 4.5. *Fix any $s>0$ and $\delta\in(0,1/6)$. Then for any positive square-free integer $N\equiv 3 \pmod 4$ we have*

$$\sum_{c>N^\delta}\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3, c\mid(x_1,x_2)\\ x_1^2+x_2^2+x_3^2=N}} (\tau(x_1)\tau(x_2)\tau(x_3))^s \ll N^{1/2-\delta/2}L(1,\chi_{-N}),$$

where the implied constant depends at most on δ and s.

Proof. Since $c^2\mid x_1^2+x_2^2=N-x_3^2$, we obtain the upper bound

$$\ll_{\epsilon,s} N^\epsilon \sum_{c>y}\sum_{\substack{|x_3|\leqslant N^{1/2}\\ c^2\mid N-x_3^2}} r_2(N-x_3^2) \ll_\epsilon N^{2\epsilon}\sum_{c>y}\sharp\{|x_3|\leqslant N^{1/2}: c^2\mid N-x_3^2\}.$$

We shall now split in two ranges: $N^\delta<c\leqslant N^{1/2-\delta}$ and $c>N^{1/2-\delta}$. For the second range we write $D=(N-x_3^2)/c^2$ and note that $D\leqslant N^{2\delta}$. Swapping summation thus leads to

$$\sum_{c>N^{1/2-\delta}}\sharp\{|x_3|\leqslant N^{1/2}: c^2\mid N-x_3^2\}\leqslant \sum_{1\leqslant D\leqslant N^{2\delta}}\sharp\{c,x_3\in\mathbb{Z}: N=x_3^2+Dc^2\}.$$

Since $D>0$, the unit group of $\mathbb{Q}(\sqrt{-D})$ is bounded independently of D. From the theory of binary quadratic forms we can then infer that

$$\sharp\{c,x_3\in\mathbb{Z}: N=x_3^2+Dc^2\}\ll\sum_{m\mid N}\left(\frac{D}{m}\right)\ll_\epsilon N^\epsilon,$$

where the implied constant depends only on ϵ. This gives the overall bound

$$\ll N^{3\epsilon+2\delta}\ll N^{4\epsilon+2\delta}L(1,\chi_{-N})$$

by Siegel's estimate. Using $\delta<1/6$ we see that $2\delta<1/2-\delta$, thus, taking $\epsilon=\delta/8$ gives the bound $N^{1/2-\delta/2}L(1,\chi_{-N})$, which is satisfactory.

We next deal with the first range. Splitting in progressions we get

$$\sharp\{|x_3|\leqslant N^{1/2}: c^2\mid N-x_3^2\}\leqslant\sum_{\substack{t\in\mathbb{Z}/c^2\mathbb{Z}\\ c^2\mid N-t^2}}\left(\frac{N^{1/2}}{c^2}+1\right)\ll N^\epsilon\left(\frac{N^{1/2}}{c^2}+1\right).$$

Summing over the range $N^\delta<c\leqslant N^{1/2-\delta}$ this gives $\ll N^{1/2-\delta+\epsilon}$, which is acceptable upon choosing a suitably small value for ϵ. □

The two next proofs use that the range $c>N^\delta$ has been dealt with.

Lemma 4.6. *Fix arbitrary $s>0$ and let $\beta=60(100s-1)/7$. For any $\mathbf{c}\in\mathbb{N}^3$ and positive square-free integer $N\equiv 3 \pmod 8$ we have*

$$\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3, c_i\mid x_i\forall i\\ x_1^2+x_2^2+x_3^2=N}} (\tau(x_1)\tau(x_2)\tau(x_3))^s \ll L(1,\chi_{-N})N^{1/2}(\log\log N)^2(\log N)^{3\cdot 2^{\beta+1}}\prod_{i=1}^3\frac{\tau(c_i)^{\beta+3}}{c_i}$$
$$+N^{1/2-1/100}(c_1c_2c_3)^{12},$$

where the implied constant depends at most on β and s.

Proof. The function $H(\delta)=\delta\log_2(\delta^{-1})+(1-\delta)\log_2(1-\delta)^{-1}$ satisfies $H(7/6000)>1/100$. Taking $\delta=7/6000$ we see that the assumption $7\beta+60=6000s$ allows us to use [5, Theorem 4]. This yields the following bound for the sum over $\mathbf{x}$ in the lemma:

$$\ll_{\beta,s}\sum_{\substack{\mathbf{d}\in\mathbb{N}^3\\ d_i\leqslant N^{\delta/2}\forall i}}(\tau(d_1)\tau(d_2)\tau(d_3))^\beta\sharp\{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3: x_1^2+x_2^2+x_3^2=N, [c_i,d_i]\mid x_i\forall i\},$$

where $[\cdot,\cdot]$ denotes the least common multiple. By Lemma 4.4 this can be bounded by

$$\ll \sum_{\substack{\mathbf{d}\in\mathbb{N}^3\\ d_i\leqslant N^{\delta/2}\forall i}} \Big(\prod_{i=1}^3 \tau(d_i)^\beta\Big)(\log\log N)^2\Big(L(1,\chi_{-N})N^{1/2}\prod_{i=1}^3\frac{\tau([c_i,d_i])}{[c_i,d_i]} + N^{1/2-1/30}\prod_{i=1}^3 [c_i,d_i]^{12}\Big),$$

where we used the following standard bound for $t=c_1c_2c_3$,

$$\prod_{p|t}\left(1+\frac{1}{p}\right) \ll \prod_{p|t}\left(1-\frac{1}{p}\right)^{-1} = \frac{t}{\phi(t)} \ll \log\log t. \tag{4.6}$$

Using $[c_i,d_i]\leqslant c_id_i$ we can see that the second part of this sum is

$$\ll N^{1/2-1/30}\prod_{i=1}^3 c_i^{12}\left(\sum_{d\leqslant N^{\delta/2}}\tau(d)^\beta d^{12}\right)^3 \ll N^{1/2-1/30+19.5\delta}(\log N)^{3(2^\beta-1)}\prod_{i=1}^3 c_i^{12},$$

which is $\ll N^{1/2-1/30+20\delta}\prod c_i^{12}$. Our choice $\delta=7/6000$ makes sure that this is $\ll N^{1/2-1/100}\prod c_i^{12}$. The first part of the sum is $\ll L(1,\chi_{-N})(\log\log N)^2N^{1/2}\prod\mathcal{S}(c_i)$, where

$$\mathcal{S}(c) := \sum_{d\leqslant N}\tau(d)^\beta\frac{\tau([c,d])}{[c,d]} \leqslant \frac{\tau(c)}{c}\sum_{d\leqslant N}\tau(d)^{\beta+1}\frac{\gcd(c,d)}{d}.$$

Writing $m=\gcd(c,d)$ and $d=mt$, the sum over d can be seen to be at most

$$\sum_{m|c} m\sum_{\substack{d\leqslant N\\ m|d}}\frac{\tau(d)^{\beta+1}}{d} \leqslant \sum_{m|c}\tau(m)^{\beta+1}\sum_{t\leqslant N}\frac{\tau(t)^{\beta+1}}{t} \ll \tau(c)^{\beta+2}(\log N)^{2^{\beta+1}}.$$

□

Lemma 4.7. *Fix any positive A and s. Then for any positive square-free $N\equiv 3 \pmod 8$ we have*

$$\sum_{c>(\log N)^A}\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3, c|(x_1,x_2)\\ x_1^2+x_2^2+x_3^2=N}} (\tau(x_1)\tau(x_2)\tau(x_3))^s \ll_{A,s} L(1,\chi_{-N})N^{1/2}(\log N)^{\rho(s)-A/2},$$

where $\rho(s)=6\cdot 2^{(6000s-60)/7}$ and the implied constant depends at most on A and s.

Proof. Fix any $\delta>0$. By Lemma 4.5 we can discard the contribution of $c>N^\delta$. For the remaining c we employ Lemma 4.6 with β defined by $7\beta+60=6000s$. We obtain

$$\ll \sum_{(\log N)^A<c\leqslant N^\delta}\left(L(1,\chi_{-N})N^{1/2}(\log\log N)^2(\log N)^{3\cdot 2^{\beta+1}}\frac{\tau(c)^{2\beta+6}}{c^2} + N^{1/2-1/100}c^{24}\right)$$

$$\ll L(1,\chi_{-N})N^{1/2}(\log N)^{3\cdot 2^{\beta+1}-A/2} + N^{1/2-1/100+25\delta}.$$

Choosing sufficiently small δ and using Siegel's bound we obtain

$$N^{-1/100+25\delta} \ll N^{-1/1000} \ll L(1,\chi_{-N})(\log N)^{3\cdot 2^{\beta+1}-A/2}.$$

□

Define for $N,m_1,m_2,m_3\in\mathbb{N}$ the function

$$\mathcal{R}_{\mathbf{m}}(N) := \sum_{\substack{\mathbf{y}\in(\mathbb{Z}\setminus\{0\})^3:\sum_i(m_jm_ky_i)^2=N\\ \gcd(y_i,y_j)=1\forall i\neq j}} f(y_1^{\alpha_1}y_2^{\alpha_2}y_3^{\alpha_3}).$$

Lemma 4.8. *Fix any $A>0$. In the setting of Theorem 4.1 we have*

$$\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3\\ x_1^2+x_2^2+x_3^2=N}} \prod_{i=1}^3 f(x_i)^{\alpha_i} \ll \sum_{\substack{\mathbf{m}\in\mathbb{N}^3,(4.7)\\ \max m_i\leqslant(\log N)^A}} \mathcal{R}_{\mathbf{m}}(N)\prod_{i=1}^3 \tau(m_i)^{2s} + \frac{L(1,\chi_{-N})N^{1/2}}{(\log N)^{A/2-\rho(s)}},$$

where $\rho(s)$ is as in Lemma 4.7, the implied constant depends at most on s,A and

$$\gcd(m_i,2m_j)=1\forall i\neq j \quad p\mid m_1m_2m_3 \Rightarrow \left(\frac{N}{p}\right)=1. \tag{4.7}$$

Proof. By our assumption $f\leqslant\tau^s$ and Lemma 4.7 we may write the sum over $\mathbf{x}$ as

$$\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3, x_1^2+x_2^2+x_3^2=N\\ \gcd(x_i,x_j)\leqslant(\log N)^A\forall i\neq j}} \prod_{i=1}^3 f(x_i)^{\alpha_i} + O(L(1,\chi_{-N})N^{1/2}(\log N)^{-A/2+\rho(s)}).$$

For $\{i,j,k\}=\{1,2,3\}$ we let $m_i=\gcd(x_j,x_k)$ so that the m_i are coprime in pairs due to $\gcd(x_1,x_2,x_3)=1$ that can be inferred from the fact that N is square-free and $N=\sum_i x_i^2$. Hence, letting $y_i:=x_i/(m_jm_k)$ we see that $m_i=\gcd(x_j,x_k)$ is equivalent to $1=\gcd(m_ky_j,m_jy_k)$. We obtain

$$\sum_{\substack{\mathbf{m}\in\mathbb{N}^3\\ \gcd(m_i,m_j)=1\forall i\neq j\\ m_i\leqslant(\log N)^A\forall i}} \sum_{\substack{\mathbf{y}:\sum_i(m_jm_ky_i)^2=N\\ \gcd(y_i,y_j)=1\forall i\neq j}} \prod_{i=1}^3 f(m_jm_ky_i)^{\alpha_i} + O(L(1,\chi_{-N})N^{1/2}(\log N)^{-A/2+\rho(s)}).$$

We omitted the condition $\gcd(y_i,m_i)=1$ as it is implied by the fact that N is square-free and a sum of integer multiples of m_i^2 and y_i^2. Our assumption $f(ab)\leqslant\tau(a)^sf(b)$ allows us to write

$$\prod_{i=1}^3 f(m_jm_ky_i)^{\alpha_i}\leqslant\prod_{i=1}^3\tau(m_j)^s\tau(m_k)^sf(y_i)^{\alpha_i}=f(y_1^{\alpha_1}y_2^{\alpha_2}y_3^{\alpha_3})\prod_{i=1}^3\tau(m_i)^{2s},$$

since the y_i are pairwise coprime and f is multiplicative. The condition that each prime divisor p of m_i must satisfy $(\frac{N}{p})=1$ comes from the fact that each m_i divides two of the coefficients of $\sum_i(m_jm_ky_i)^2$ and is coprime to the third. Finally, if one of the m_i is even, then 4 divides $N-(m_jm_ky_i)^2$, which is impossible owing to $N\equiv 3 \pmod 4$. □

4.4. **Level of distribution.** Throughout this subsection $\mathbf{m}$ is a fixed vector in $\mathbb{N}^3$ satisfying (4.7). For positive integers d,N define

$$C_d(N):=\sharp\left\{\mathbf{y}\in\mathbb{Z}^3: \begin{array}{l}(m_2m_3y_1)^2+(m_1m_3y_2)^2+(m_1m_2y_3)^2=N,\\ \gcd(y_i,y_j)=1\forall i\neq j,\quad d\mid y_1y_2y_3\end{array}\right\}.$$

The main result is Lemma 4.11; it gives a level of distribution result for $C_d(N)$ that will subsequently be fed into Theorem 2.4 to bound $\mathcal{R}_{\mathbf{m}}(N)$.

We start with a sieving argument that deals with the coprimality of the y_i.

Lemma 4.9. *Keep the setting of Theorem 4.1 and fix any $\delta\in(0,1/9)$. For all $\mathbf{m}$ as in (4.7) and all $d\in\mathbb{N}$ we have*

$$C_d(N)=\sum_{\substack{\mathbf{d}\in\mathbb{N}^3,d=d_1d_2d_3\\ \gcd(d_i,d_j)=1\forall i\neq j\\ \gcd(d_i,m_i)=1\forall i}} \sum_{\substack{\mathbf{b}\in\mathbb{N}^3,\max b_i\leqslant N^{\delta_i}\forall i\\ \gcd(b_i,b_j)=1\forall i\neq j\\ \gcd(b_i,d_im_j)=1\forall i\neq j}} \mu(b_1)\mu(b_2)\mu(b_3)C_{\mathbf{b},d}(N)+O(N^{1/2-\delta/400}L(1,\chi_{-N})),$$

where $\delta_1=\delta/100,\delta_2=\delta/10,\delta_3=\delta$, the quantity $C_{\mathbf{b},d}(N)$ is given by

$$\sharp\{\mathbf{t}\in\mathbb{Z}^3: N=(m_2m_3[d_1,b_2b_3]t_1)^2+(m_1m_3[d_2,b_1b_3]t_2)^2+(m_1m_2[d_3,b_1b_2]t_3)^2\}$$

and the implied constant depends at most on δ.

Proof. Since y_i are coprime in pairs in $C_d(N)$, we can write $d = d_1d_2d_3$ where $d_i \mid y_i$ and the d_i are coprime in pairs. Then, $C_d(N)$ becomes

$$\sum_{\substack{\mathbf{d}\in\mathbb{N}^3, d=d_1d_2d_3 \\ \gcd(d_i,m_id_j)=1\forall i\neq j}} \sharp\left\{\mathbf{y}\in(\mathbb{Z}\setminus\{0\})^3 : \begin{array}{l}(m_2m_3y_1)^2+(m_1m_3y_2)^2+(m_1m_2y_3)^2=N,\\ \gcd(y_i,y_j)=1\forall i\neq j, \quad d_i\mid y_i\forall i\end{array}\right\}.$$

The condition $\gcd(d_i, m_i) = 1$ comes from the fact that N is square-free and the sum of squares equation. We now use the expression $\sum_{b_1|(y_2,y_3)} \mu(b_1)$ to detect the coprimality of y_2 and y_3. The contribution of $b_1 > N^{\delta/100}$ will then be at most

$$\tau_3(d)\sum_{b_1>N^{\delta/100}} \sharp\{\mathbf{t}\in\mathbb{Z}^3 : t_1^2+t_2^2+t_3^2=N, b_1\mid(t_2,t_3)\} \ll \tau_3(d)N^{1/2-\delta/200}L(1,\chi_{-N})$$

by Lemma 4.7. We have $d \leqslant N^3$ due to $d \mid y_1y_2y_3$, hence, the bound $\tau_3(d) \ll N^{\delta/400}$ shows that the contribution is $\ll N^{1/2-\delta/400}L(1, \chi_{-N})$. Next, we use $\sum_{b_2|(y_1,y_3)} \mu(b_2)$ to detect the coprimality of y_1 and y_3. The contribution of $b_2 > N^{\delta/10}$ is

$$\ll \tau_3(d)\sum_{\substack{b_1\leqslant N^{\delta/100} \\ b_2>N^{\delta/10}}} \sharp\{\mathbf{t}\in\mathbb{Z}^3 : t_1^2+t_2^2+t_3^2=N, b_2\mid(y_1,y_3)\} \ll \tau_3(d)N^{1/2+\delta/100-\delta/20}L(1,\chi_{-N})$$

by Lemma 4.7. This can be seen to be $\ll N^{1/2-\delta/150}L(1, \chi_{-N})$ as before. Finally, using $\sum_{b_3|(y_1,y_2)} \mu(b_3)$, we can see that the range $b_3 > N^{\delta}$ contributes

$$\ll \tau_3(d)\sum_{\substack{b_1\leqslant N^{\delta/100}, b_2\leqslant N^{\delta/10} \\ b_3>N^{\delta}}} \sharp\{\mathbf{t}\in\mathbb{Z}^3 : t_1^2+t_2^2+t_3^2=N, b_3\mid(t_1,t_2)\} \ll N^{1/2-\delta/10}L(1,\chi_{-N}).$$

We thus obtain the expression claimed in the lemma. The conditions of the form $\gcd(b_1, b_2b_3d_1m_2m_3) = 1$ in the lemma come from the fact that N is square-free. Finally, the vectors $\mathbf{t}$ having $t_i = 0$ for some i contribute at most

$$\ll \tau_3(d)N^{\delta_1+\delta_2+\delta_3}r_2(N) \ll N^{2\delta},$$

which is acceptable by the assumption $\delta < 1/9$. □

We next apply Lemma 4.4. Denote

$$b = b_1b_2b_3, \quad m = m_1m_2m_3 \quad \text{and} \quad \mathfrak{C}_d := \prod_{\substack{p\equiv 3 \pmod 4 \\ p\mid(d,N)}} p.$$

Lemma 4.10. *Keep the setting of Lemma 4.9 and fix any $\varpi > 0$. For all $d \in \mathbb{N}$ and $\mathbf{m} \in \mathbb{N}^3$ as in* (4.7) *with the additional restriction* $\max m_i \leqslant (\log N)^{\varpi}$ *we have*

$$C_d(N) = \frac{8}{\pi}L(1,\chi_{-N})N^{1/2}M_1M_2 + O(d^{12}N^{1/2+\max\{50\delta-1/30,-\delta/800\}}(\log N)^{100\varpi}L(1,\chi_{-N})),$$

where the implied constant depends at most on δ and ϖ. Here

$$M_1 = \frac{\mathbb{1}(2\nmid d)}{d}\frac{2^{\omega(m)}}{m^2}\prod_{p\mid m}\left(1-\frac{1}{p}\left(\frac{-1}{p}\right)\right)$$

and

$$M_2=\sum_{\mathbf{b}\in\mathbb{N}^3}2^{\sharp\{p|b:p\nmid m\}}\frac{\mu(b)}{b^2}2^{\sharp\{p|d:p\nmid bm\}}\prod_{p|b,p\nmid m}\left(1-\frac{1}{p}\left(\frac{-1}{p}\right)\right)\frac{2^{\sharp\{p|(d,b)\}}}{2^{\sharp\{p|d:p\nmid bmN\}}}$$
$$\times\gcd(d,b)3^{\sharp\{p|d:p\nmid bm\}}2^{\sharp\{p|d,p|m,p\nmid b\}}\prod_{\substack{p|d\\p\nmid bm}}\left(1-\frac{1}{p}\left(\frac{-1}{p}\right)\right)\left(1-\frac{1}{p}\left(\frac{-N}{p}\right)\right),$$

where the sum is over $\mathbf{b}$ *satisfying the further conditions*

$$\mathfrak{C}_d\mid b_1b_2b_3m,\gcd(b_i,2b_jm_j)=1\forall i\neq j,$$

and $(\frac{N}{p})=1$ *for all primes* $p\mid b_1b_2b_3$ *with* $p\nmid m$.

Proof. We employ Lemma 4.4 with $c_i=m_jm_k[d_i,b_jb_k]$ to estimate $C_d(N)$ in Lemma 4.9. The error term is

$$\ll\tau_3(d)d^{12}N^{1/2-1/30}(\log N)^{100\varpi}\prod_{i=1}^{3}\sum_{b\leqslant N^{\delta_i}}b^{24}\ll d^{12}N^{1/2-1/30+50\delta}(\log N)^{100\varpi}L(1,\chi_{-N})$$

by Siegel's bound and $\tau_3(d)\ll N^{\delta-\delta_1-\delta_2}L(1,\chi_{-N})$ that is implied by $d\leqslant N^3$.

To deal with the main term let us recall that the m_i are pairwise coprime and use the coprimality conditions on the b_i,d_i to see that (4.3) is always met. Denote $b:=b_1b_2b_3$. Note that a prime p divides exactly two of the c_i if and only if $p\mid bm$. In addition, p divides exactly one of c_i if and only if p divides d but not bm. We get the main term

$$\frac{8}{\pi}L(1,\chi_{-N})N^{1/2}\frac{\mathbb{1}(2\nmid m)}{m^2}\mathfrak{K}\prod_{p|m}\left(1-\frac{1}{p}\left(\frac{-N}{p}\right)\right),$$

where $\mathfrak{K}$ is the sum

$$\sum\nolimits^{*}2^{\omega(mb)}\frac{\mu(b_1)\mu(b_2)\mu(b_3)}{(b_1b_2b_3)^2}\prod_{\substack{p|b_1b_2b_3\\p\nmid m}}\left(1-\frac{1}{p}\left(\frac{-N}{p}\right)\right)\frac{\mathbb{1}(2\nmid d)2^{\sharp\{p|d:p\nmid bm\}}}{d}\mathfrak{F}(d)$$
$$\times\mathbb{1}(p\mid(d,N),p\nmid bm\Rightarrow p\equiv1\ (\mathrm{mod}\ 4))\prod_{\substack{p|d\\p\nmid bm}}\left(1-\frac{1}{p}\left(\frac{-1}{p}\right)\right)\left(1-\frac{1}{p}\left(\frac{-N}{p}\right)\right)\left(\frac{1}{2}\right)^{\mathbb{1}(p\nmid N)}$$

with $\sum^*$ taken over $\mathbf{b}\in\mathbb{N}^3$ satisfying $b_i\leqslant N^{\delta_i}$ for all i, $\gcd(b_i,2b_jm_j)=1$ for all $i\neq j$, and, with the further property that each prime divisor p of b that does not divide m must satisfy $(\frac{N}{p})=1$. The multiplicative function $\mathfrak{F}(d)$ is defined as

$$\sum_{\mathbf{d}\in\mathbb{N}^3,d=d_1d_2d_3}\gcd(d_1,b_2b_3)\gcd(d_2,b_1b_3)\gcd(d_3,b_1b_2),$$

where the sum is subject to $\gcd(d_i,d_jm_ib_i)=1$ for all $i\neq j$. To analyse it at prime powers p^α we use that d_i are coprime to infer that $\mathfrak{F}(p^\alpha)$ equals

$$\gcd(p^\alpha,b_2b_3)\mathbb{1}(p\nmid b_1m_1)+\gcd(p^\alpha,b_1b_3)\mathbb{1}(p\nmid b_2m_2)+\gcd(p^\alpha,b_1b_2)\mathbb{1}(p\nmid b_3m_3).$$

Since b_i are coprime in pairs and square-free we see that if $p\mid b_1b_2b_3$ then the above becomes $2p$ because $\gcd(b_i,m_j)=1$ for all $i\neq j$. If $p\nmid b_1b_2b_3m_1m_2m_3$ then the sum becomes 3. If $p\nmid b_1b_2b_3$ and $p\mid m_1m_2m_3$ then it becomes 2. Thus, $\mathfrak{F}(d)$ equals

$$2^{\sharp\{p|(b,d)\}}\gcd(b,d)3^{\sharp\{p|d:p\nmid bm\}}2^{\sharp\{p|(d,m):p\nmid b\}}.$$

Using (4.6) we see that the contribution of $\mathbf{b}$ with $b_i > N_i^\delta$ for some i is

$$\ll L(1,\chi_{-N})N^{1/2}(\log\log N)^3\tau(d)6^{\omega(d)}d \sum_{\substack{\mathbf{b}\in\mathbb{N}^3\\ \exists i: b_i > N^{\delta_i}}} \frac{2^{\omega(b_1b_2b_3)}}{(b_1b_2b_3)^2} \ll L(1,\chi_{-N})N^{1/2}d^2N^{-\frac{1}{2\min\delta_i}},$$

which is acceptable since $\min\delta_i > \delta/800$. To conclude the proof we note that the condition $p \mid d, p \mid N, p\nmid bm \Rightarrow p\equiv 1 \pmod 4$ is equivalent to $\mathfrak{C}_d \mid bm$. □

Finally, we simplify the main term in Lemma 4.10. The error term will be obtained by taking $\delta = 80/120003$. Denote for a prime p, $c_p = 1 - \frac{1}{p}\left(\frac{-1}{p}\right)$.

Lemma 4.11. *Fix any $\varpi > 0$. For all $\mathbf{m}\in\mathbb{N}^3$ as in (4.7) with $\max m_i \leqslant (\log N)^\varpi$, all square-free positive integers $N\equiv 3 \pmod 8$ and all $d\in\mathbb{N}$ we have*

$$C_d(N) = M(N)g_N(d) + O(d^{12}N^{1/2-1/1200030}(\log N)^{100\varpi}L(1,\chi_{-N})),$$

where the implied constant depends at most on ϖ. Further,

$$M(N) = \frac{8}{\pi}L(1,\chi_{-N})N^{1/2}\frac{2^{\omega(m_1m_2m_3)}}{(m_1m_2m_3)^2}\prod_{p\mid m_1m_2m_3} c_p\left(1-\frac{1}{p^2}\right)\prod_{\substack{p\nmid m_1m_2m_3\\ (\frac{N}{p})=1}}\left(1-\frac{6c_p}{p^2}\right)$$

and

$$\begin{aligned} g_N(d) =& \mathbb{1}(p \mid (d,N) \Rightarrow p\equiv 1 \pmod 4)\frac{\mathbb{1}(2\nmid d)}{d}2^{\sharp\{p\mid d: p\mid m_1m_2m_3N\}}3^{\sharp\{p\mid d: p\nmid m_1m_2m_3\}} \\ &\times \prod_{\substack{p\mid m_1m_2m_3\\ p\mid d}}\left(1+\frac{1}{p}\right)^{-1}\prod_{\substack{p\nmid m_1m_2m_3\\ p\mid d, (\frac{N}{p})=1}}\frac{1}{\left(1-\frac{6c_p}{p^2}\right)\left(1-\frac{4}{pc_p}\right)}\prod_{\substack{p\mid d\\ p\nmid m_1m_2m_3}} c_p\left(1-\frac{1}{p}\left(\frac{-N}{p}\right)\right). \end{aligned}$$

Proof. Let $\mathfrak{G}(b)$ be the number of $\mathbf{b}\in\mathbb{N}^3$ with $b=b_1b_2b_3$ and $\gcd(b_i,b_jm_j)=1$ for all $i\neq j$. Using $2^{\sharp\{p\mid d: p\nmid bm\}}2^{\sharp\{p\mid d, p\mid m, p\nmid b\}}2^{\sharp\{p\mid (d,b)\}} = 2^{\omega(d)}$ we can write

$$M_2 = M_3 3^{\sharp\{p\mid d: p\nmid m\}}\frac{2^{\omega(d)}}{2^{\sharp\{p\mid d: p\nmid mN\}}}\prod_{p\mid d, p\nmid m} c_p\left(1-\frac{1}{p}\left(\frac{-N}{p}\right)\right),$$

where M_3 is given by

$$\sum_{\substack{b\in\mathbb{N}, 2\nmid b, \mathfrak{C}_d\mid bm\\ p\mid b, p\nmid m\Rightarrow (\frac{N}{p})=1}} 2^{\sharp\{p\mid b: p\nmid m\}}\frac{\mu(b)\gcd(d,b)}{b^2}\frac{2^{\sharp\{p\mid b: p\nmid mN, p\mid d\}}}{3^{\sharp\{p\mid b: p\nmid m, p\mid d\}}}\mathfrak{G}(b)\prod_{\substack{p\mid b, p\nmid m\\ p\mid d}} c_p^{-2}\prod_{p\mid b, p\nmid m} c_p.$$

For a prime p we have $\mathfrak{G}(p) = \mathbb{1}(p\nmid m_1m_2) + \mathbb{1}(p\nmid m_1m_3) + \mathbb{1}(p\nmid m_2m_3)$. Since the m_i are coprime in pairs, $\mathfrak{G}(p)$ becomes 1 or 3 according to whether p divides m or not. Hence, $\mathfrak{G}(b) = 3^{\sharp\{p\mid b: p\nmid m\}}$ for all square-free b, thus, M_3 can be written as

$$\sum_{\substack{b\in\mathbb{N}, 2\nmid b, \mathfrak{C}_d\mid bm\\ p\mid b, p\nmid m\Rightarrow (\frac{N}{p})=1}} 6^{\sharp\{p\mid b: p\nmid m\}}\frac{\mu(b)\gcd(d,b)}{b^2}\frac{2^{\sharp\{p\mid b: p\nmid mN, p\mid d\}}}{3^{\sharp\{p\mid b: p\nmid m, p\mid d\}}}\prod_{\substack{p\mid b, p\nmid m\\ p\mid d}} c_p^{-2}\prod_{p\mid b, p\nmid m} c_p.$$

Let us show that if the sum over b is non-empty then $\mathfrak{C}_d = 1$. To see that, assume there is a prime $p\mid \mathfrak{C}_d$. Then the condition $p\mid \mathfrak{C}_d \mid bm$ implies that $p\mid m$ or $p\nmid m$ and $p\mid b$. In the first case, the condition present in M_1 shows that $(\frac{N}{p}) = 1$, which violates the condition $p\mid \mathfrak{C}_d \mid N$. In the second case, we have $p\nmid m$ and $p\mid b$, hence, the condition in the sum over b shows that $(\frac{N}{p})=1$, which is a contradiction. Factor $b=b_0b_1$, where $b_0 \mid m$ and b_1 is coprime to m. We can thus write $M_3=M_4M_5$, where

$$M_4=\sum_{b_0|m}\frac{\mu(b_0)\gcd(d,b_0)}{b_0^2}=\prod_{\substack{p|m\\p|d}}\left(1-\frac{1}{p}\right)\prod_{\substack{p|m\\p\nmid d}}\left(1-\frac{1}{p^2}\right)$$

and M_5 is given by

$$\sum_{\substack{b_1\in\mathbb{N},\gcd(b_1,2m)=1\\p|b_1\Rightarrow(\frac{N}{p})=1}}6^{\sharp\{p|b_1\}}\frac{\mu(b_1)\gcd(d,b_1)}{b_1^2}\left(\frac{2}{3}\right)^{\sharp\{p|b_1:p|d\}}\prod_{p|b_1}c_p\prod_{\substack{p|b_1\\p|d}}c_p^{-2},$$

where we used the conditions $b_0 \mid m$ and $\gcd(b_1,m)=1$ to infer that b_0,b_1 are coprime and thus split $\mu(b_0b_1)$. The Euler product for M_5 equals

$$\prod_{\substack{p\nmid 2m\\(\frac{N}{p})=1}}\left(1-\frac{6c_p}{p^2}\right)\prod_{\substack{p|d,p\nmid 2m\\(\frac{N}{p})=1}}\frac{1}{\left(1-\frac{6c_p}{p^2}\right)\left(1-\frac{4}{pc_p}\right)}.$$

□

4.5. **The proof of Theorem 4.1.** We focus on the hardest case $\alpha=3$. We use Theorem 2.4 with $\mathcal{A}$ being the set of vectors $\mathbf{y}\in(\mathbb{Z}\setminus\{0\})^3$ satisfying $\gcd(y_i,y_j)=1$ for all $i\neq j$ and $c_a=|y_1y_2y_3|$. Further, we let $T=N$ and $\chi_N(a)=\mathbb{1}_{\{N\}}((m_2m_3y_1)^2+(m_1m_3y_2)^2+(m_1m_2y_3)^2)$. To verify assumption (2.6) we use Lemma 4.11. Note that $2^{\omega(m)}\prod_{p|m}(1-1/p)\geqslant 1$, hence

$$\frac{N^{1/2}L(1,\chi_{-N})}{(\log N)^{6\varpi}}\leqslant\frac{N^{1/2}L(1,\chi_{-N})}{(m_1m_2m_3)^2}\ll M\ll N^{1/2}L(1,\chi_{-N}) \tag{4.8}$$

with absolute implied constants. Fix any strictly positive constants ξ and θ satisfying $12\theta+\xi<1/600015$. For any positive integer $d\leqslant M^\theta$, the error term in Lemma 4.11 is

$$\ll M^{12\theta}N^{1/2}L(1,\chi_{-N})N^{-1/1200030}(\log N)^{100\varpi}\ll M^{1+12\theta}N^{-1/1200030}(\log N)^{106\varpi}$$

by the lower bound (4.8). Using the upper bound of the same inequality we obtain

$$\ll M^{1-1/600015+12\theta}L(1,\chi_{-N})^{1/2400060}(\log N)^{106\varpi}\ll M^{1-1/600015+12\theta}(\log N)^{1+106\varpi}$$

by the bound $L(1,\chi_{-N})\ll\log N$. The error term is $O(M^{1-\xi})$ as we have chosen ξ so that $12\theta+\xi<1/600015$. This verifies assumption (2.6) of Theorem 2.4. The remaining assumptions are easily seen to hold since the function g_N in Lemma 4.11 satisfies $p^eg_N(p^e)=O(1)$ for all $e\geqslant 1$ and primes p with an absolute implied constant. Hence, one has for all $\mathbf{m}$ with $\max m_i\leqslant(\log N)^A$

$$\sum_{\substack{\mathbf{y}\in(\mathbb{Z}\setminus\{0\})^3:\sum_i(m_jm_ky_i)^2=N\\\gcd(y_i,y_j)=1\forall i\neq j}}f(|y_1y_2y_3|)\ll M(N)T(M(N)),$$

where $T(y)=\prod_{1\ll p\leqslant y}(1-g_N(p))\sum_{a\leqslant y}f(a)g_N(a)$ and the implied constant depends at most on s and ϖ. We have $T(y)\asymp\exp(S(y))$ by Lemma 2.5, where $S(y)$ is

$$6\sum_{\substack{p|N\\p\equiv1(\mathrm{mod}\ 4)}}\frac{f(p)-1}{p}+3\sum_{\substack{p\leqslant y\\p\nmid N}}\frac{f(p)-1}{p}+O\Big(1+\sum_{p|m_1m_2m_3}\frac{1}{p}+\sum_{\substack{p|N\\p>y}}\frac{1}{p}\Big).$$

The main term is

$$3\sum_{p\mid N}\left(\frac{-1}{p}\right)\frac{f(p)-1}{p}+3\sum_{p\leqslant y}\frac{f(p)-1}{p}+O\Big(\sum_{\substack{p\mid N\\ p>y}}\frac{1}{p}\Big).$$

The sum over $p \mid N, p > y$ is $\ll \omega(N)/y \ll (\log N)/y$. Thus, with $c_f(N)$ as in (4.1), there exists a positive constant $\nu = \nu(s)$ such that for all $y \geqslant \log N$ one has

$$\prod_{p\mid m_1m_2m_3}\left(1+\frac{1}{p}\right)^{-\nu}\ll T(y)c_f(y)^{-3}\exp\left(-3\sum_{p\leqslant y}\frac{f(p)-1}{p}\right)\ll\prod_{p\mid m_1m_2m_3}\left(1+\frac{1}{p}\right)^{\nu}.$$

Injecting the upper bound into Lemma 4.8 and using that $M(N) \leqslant N$ we get

$$\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3\\ x_1^2+x_2^2+x_3^2=N}}\prod_{i=1}^3 f(|x_i|)\ll\frac{L(1,\chi_{-N})N^{1/2}}{(\log N)^{A/2-\rho(s)}}+L(1,\chi_{-N})N^{1/2}c_f(N)^3\exp\left(3\sum_{p\leqslant N}\frac{f(p)-1}{p}\right)\mathcal{S}$$

where

$$\mathcal{S}=\sum_{\substack{\mathbf{m}\in\mathbb{N}^3,(4.7)\\ \max m_i\leqslant(\log N)^A}}\prod_{i=1}^3\frac{\tau(m_i)^{2s}}{m_i^2}\prod_{p\mid m_i}\left(1+\frac{1}{p}\right)^{\nu}.$$

Since $\prod_{p|m}(1+1/p) \leqslant \tau(m)$ we can see that $\mathcal{S}$ is bounded. Enlarging the value of A allows the logarithmic exponent $A/2 - \rho(s)$ to exceed any given number and it thus completes the proof of the upper bound in Theorem 4.1 when each α_i is 1.

To prove the lower bound in Theorem 4.1 we note that

$$\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3\\ x_1^2+x_2^2+x_3^2=N}}\prod_{i=1}^3 f(|x_i|)\geqslant\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\setminus\{0\})^3,\ \sum_i x_i^2=N\\ \gcd(x_i,x_j)=1\forall i\neq j}}\prod_{i=1}^3 f(|x_i|)$$

and apply [6, Theorem 1.13] to estimate the right-hand side sum. This has a level-of-distribution assumption that can be verified using the case $m_1 = m_2 = m_3 = 1$ of Lemma 4.11.

References

[1] P. T. Bateman, *On the Representations of a Number as the Sum of Three Squares*, Trans. Amer. Math. Soc. **71** (1951), 70–101.

[2] K. Belabas, *Crible et* 3*-rang des corps quadratiques*, Ann. Inst. Fourier (Grenoble) **46** (1996), 909–949.

[3] M. Bhargava, T. Taniguchi, F. Thorne, *Improved error estimates for the Davenport–Heilbronn theorems*, Math. Ann. **389** (2024), 3471–3512.

[4] V. Blomer, J. Brüdern, *A three squares theorem with almost primes*, Bull. Lond. Math. Soc. **37** (2005), 507–513.

[5] Z. Brady, *Divisor function inequalities, entropy, and the chance of being below average*, Math. Proc. Cambridge Philos. Soc. **163** (2017), 547–560.

[6] S Chan, P. Koymans, C. Pagano, E. Sofos, *Averages of multiplicative functions along equidistributed sequences*, `arXiv:2402.08710`.

[7] H. Cohen, H. W. Lenstra, *Heuristics on class groups of number fields*, In: "Lecture Notes in Math.", **1068**, Springer-Verlag, Berlin, 1984, 33–62.

[8] H. Davenport, H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), 405–420.

[9] W. Duke, *On ternary quadratic forms*, J. Number Theory **110** (2005), 37–43.

[10] J. Ellenberg, L. B. Pierce, M. M. Wood, *On ℓ-torsion in class groups of number fields*, Algebra Number Theory **11** (2017), 1739–1778.

[11] E. Fouvry, J. Klüners, *On the* 4*-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), 455–513.

[12] E. Fouvry, J. Klüners, *Cohen–Lenstra heuristics of quadratic number fields*, In: "Lecture Notes in Comput. Sci.", **4076**, Springer-Verlag, Berlin, 2006, 40–55.
[13] E. Fouvry, J. Klüners, *Weighted distribution of the 4-rank of class groups and applications*, Int. Math. Res. Not. IMRN **16** (2011), 3618–3656.
[14] C. Frei, M. Widmer, *Averages and higher moments for the ℓ-torsion in class groups*, Math. Ann. **379** (2021), 1205–1229.
[15] J. Friedlander, H. Iwaniec, "Opera de cribro", Amer. Math. Soc. Colloq. Publ., **57**, American Mathematical Society, Providence, RI, 2010.
[16] C. F. Gauss, *Disquisitiones Arithmeticae*, Translated into English by Arthur A. Clarke, S. J, Yale University Press, New Haven, Conn.-London, 1966.
[17] D. R. Heath-Brown, L. B. Pierce, *Averages and moments associated to class numbers of imaginary quadratic fields*, Compos. Math. **153** (2017), 2287–2309.
[18] K. Henriot, *Nair-Tenenbaum bounds uniform with respect to the discriminant*, Math. Proc. Cambridge Philos. Soc. **152** (2012), 405–424.
[19] E. Jones, *Local densities of diagonal integral ternary quadratic forms at odd primes*, J. Number Theory **17** (2021), 547–575.
[20] P. Koymans, J. Thorner, *Bounds for moments of ℓ-torsion in class groups*, Math. Ann. **390** (2024), 3221–3237.
[21] R. J. Lemke Oliver, F. Thorne, *The number of ramified primes in number fields of small degree*, Proc. Amer. Math. Soc. **145** (2017), 3201–3210.
[22] A. Smith, 2^∞*-Selmer Groups,* 2^∞*-class groups, and Goldfeld's conjecture*, `arXiv:1702.02325`.
[23] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. (2) **61** (2000), 681–690.
[24] G. Tenenbaum, *Fonctions multiplicatives, sommes d'exponentielles, et loi des grands nombres*, Indag. Math. (N.S.) **2** (2016), 590–600.

ISTA, Am Campus 1, 3400 Klosterneuburg, Austria
Email address: `stephanie.chan@ist.ac.at`

Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 TA Utrecht, Netherlands
Email address: `p.h.koymans@uu.nl`

Department of Mathematics, Concordia University, Montreal, H3G 1M8, Canada
Email address: `carlo.pagano@concordia.ca`

Department of Mathematics, Glasgow University, G12 8QQ, UK
Email address: `efthymios.sofos@glasgow.ac.uk`