ON THE NUMBER OF PRODUCTS WHICH FORM PERFECT POWERS AND DISCRIMINANTS OF MULTIQUADRATIC EXTENSIONS

RÉGIS DE LA BRETÈCHE, PÄR KURLBERG, AND IGOR E. SHPARLINSKI

Abstract. We study some counting questions concerning products of positive integers $u_1, \ldots, u_n$ which form a non-zero perfect square, or more generally, a perfect k-th power. We obtain an asymptotic formula for the number of such integers of bounded size and in particular improve and generalize a result of D. I. Tolev (2011). We also use similar ideas to count the discriminants of number fields which are multiquadratic extensions of $\mathbb{Q}$ and improve and generalize a result of N. Rome (2017).

1. Introduction

1.1. **Background and motivation.** Here we use a unified approach to study two intrinsically related problems:

- we count the number of integer vectors which are multiplicatively dependent modulo squares or higher powers, in particular we improve a result of Tolev [22];
- we obtains some statistics for towers of radical extensions and extend and improve results of Baily [1] and Rome [19].

Our treatment of both problems is based on similar ideas, namely, on multiplicative decompositions close to those used in [5], see (6.1) and (6.2) in the proofs of Theorems 2.2 and 3.1, respectively, which are our main results.

More precisely, we study the following two groups of questions.

For a fixed integer $n \geqslant 2$ we are, in particular, interested in the distribution on n-dimensional vectors of positive integers

$$\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$$

Date: January 30, 2019.

2010 *Mathematics Subject Classification.* 11N25, 11N37, 11R20, 11R45.

Key words and phrases. Product of integers, perfect square, multiquadratic extension.

whose non-trivial sub-product $a_{i_1} \ldots a_{i_m}$, $1 \leqslant i_1 < \ldots < i_m \leqslant n$, is a perfect square. This seems to be a natural analogue of the question of counting multiplicatively dependent vectors [16].

Motivated by applications to integer factorization algorithm a question of the existence of such perfect square amongst n randomly selected integers of size at most H, has been extensively studied, see [7, 17, 18]. More precisely, for the above applications it is crucial to determine the smallest value of n (as a function of H) for which at least one such products is a perfect square with a probability close to one; this question has recently been answered in a spectacular work of Croot, Granville, Pemantle and Tetali [7].

Further motivation for this work comes from studying the multi-quadratic extensions of $\mathbb{Q}$, that is, fields of the form

$$\mathbb{Q}\left(\sqrt{\mathbf{a}}\right) = \mathbb{Q}\left(\sqrt{a_1}, \ldots, \sqrt{a_n}\right) \tag{1.1}$$

with vectors $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$, see, for example, [1, 2, 19] and references therein. In particular we count the number of distinct discriminants of such fields up a certain bound X, and we also count the number of vectors $\mathbf{a}$ in a box for which $\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)$ has the largest possible Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{\mathbf{a}})/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$. Finally, we also consider towers of radical extensions of higher degree $k \geqslant 2$ and count the number of vectors $\mathbf{a}$ in a box for which these extensions are of the largest possible degree k^n.

1.2. **Our results.** Our main focus is on products forming squares when n is fixed, and thus it is easy to see that the existence of a square product is a rare event. Furthermore, in this case, one can concentrate on the case when such products include all numbers $u_1, \ldots, u_n$.

In particular, we are interested in counting such vectors and more generally, vectors for which $u_1 \ldots u_n$ is a perfect k-th power, for a fixed integer $k \geqslant 2$ in the hypercube

$$\mathfrak{B}_n(H) = [1, H]^n, \tag{1.2}$$

where $H \in \mathbb{N}$. In particular, we study the cardinality

$$N_n^{(k)}(H) = \#\mathscr{N}_n^{(k)}(H)$$

of the set

$$\mathscr{N}_n^{(k)}(H) = \left\{(u_1, \ldots, u_n) \in \mathbb{N}^n \cap \mathfrak{B}_n(H) : \ u_1 \cdots u_n \in \mathbb{N}^{(k)}\right\},$$

where

$$\mathbb{N}^{(k)} = \{s^k : \ s \in \mathbb{N}\}$$

denotes the set of positive integers which are perfect k-th powers.

We note that if $\tau_{n,H}(s)$ denotes the restricted n-ary divisor function of $s \in \mathbb{N}$, that is the number of representation $u_1 \ldots u_n = s$ with integers $1 \leqslant u_1, \ldots, u_n \leqslant H$ then

$$N_n^{(k)}(H) = \sum_{s \leqslant H^{n/k}} \tau_{n,H}(s^k).$$

Here we obtain an asymptotic formula for $N_n^{(k)}(H)$ and then make it more explicit in the case of squares, that is for $k = 2$. In turn this can be used to study multiquadratic extensions of $\mathbb{Q}$ as in (1.1).

In particular, a combination of our results with a result of Balasubramanian, Luca and Thangadurai [2, Theorem 1.1] allows to get an asymptotic formula for the number of vectors $\mathbf{a} \in \mathbb{N}^n \cap \mathfrak{B}_n(H)$ where $\mathfrak{B}_n(H)$ is given by (1.2) for which

$$[\mathbb{Q}(\sqrt{\mathbf{a}}) : \mathbb{Q}] = 2^n. \tag{1.3}$$

We also consider the more difficult questions of counting the discriminants of multiquadratic number fields

We recall that Rome [19], making the result of Baily [1, Theorem 8] more precise, has recently given the asymptotic formula for the number of distinct discriminants of size at most X coming from biquadratic fields $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, see also [6, Section 6.1]. We also refer to [3, 6, 13, 23, 24] for other counting result for discriminants of quartic fields of different types. Here we obtain a generalization of results of Baily [1] and Rome [19] to multiquadratic extensions $\mathbb{Q}(\sqrt{\mathbf{a}})$ for arbitrary length $n \geqslant 2$.

Furthermore, we also count distinct multiquadratic fields having maximal Galois group, as well as the analogous question regarding maximal degree extensions generated by higher *odd* index radicals (that is, extension of the form $\mathbb{Q}(\sqrt[k]{\mathbf{a}}) = \mathbb{Q}(\sqrt[k]{a_1}, \ldots, \sqrt[k]{a_n})$ for odd $k > 2$; here $\sqrt[k]{a_i}$ can denote any k-th root of a_i but it is convenient to always take a real k-th root.)

Our method can easily be adjusted to count $\mathbf{a} \in \mathbb{Z}^n \cap \mathfrak{B}_n^{\pm}(H)$ where

$$\mathfrak{B}_n^{\pm}(H) = ([-H, -1] \cup [1, H])^n, \tag{1.4}$$

see Section 7 for more details.

1.3. **Notation.** We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that $|U| \leqslant cV$ holds with some constant $c > 0$, which throughout this work may depend on the integer parameters $k, n \geqslant 1$, and occasionally, where obvious, on the real parameter $\varepsilon > 0$.

We also denote,

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} \qquad \text{and} \qquad \mathbb{R}_+ = \mathbb{R} \cap (0, \infty).$$

Throughout the paper, the letter p always denotes a prime number.

2. Products which form powers

2.1. **Products which are k-th powers.** We obtain an asymptotic formula, with a power saving in the error term, for $N_n^{(k)}(H)$ for any integer $k \geqslant 2$ which generalizes and improves a result of Tolev [22] that corresponds to $n = 2$ and gives only a logarithmic saving. We always write $\mathbf{m} = (m_1, \ldots, m_n)$ and introduce the sets

$$\begin{aligned}
\mathscr{M}_{n,k} &= \{\mathbf{m} \in \mathbb{N}_0^n \setminus \{\mathbf{0}\} : \ k \mid m_1 + \ldots + m_n\}, \\
\mathscr{M}_{n,k,i} &= \{\mathbf{m} \in \mathscr{M}_{n,k} : \ m_1 + \ldots + m_n = ik\}, \\
\mathscr{M}_{n,k}^* &= \{\mathbf{m} \in \mathscr{M}_{n,k,1} : \ \#\{i : m_i > 0\} \geqslant 2\} \\
\mathscr{E}_{n,k,i} &= \big\{\varepsilon \in \{0, \ldots, k-1\}^n : \ \varepsilon_1 + \ldots + \varepsilon_n = ki\big\}.
\end{aligned}$$

In particular, the set $\mathscr{M}_{n,k,1} \setminus \mathscr{M}_{n,k}^*$ consists of the n vectors $\mathbf{m}$ with exactly one nonzero coordinate which equals k. We also denote

$$\begin{aligned}
q_{n,k} &= \#\mathscr{M}_{n,k,1} = \binom{n+k-1}{k}, \\
q_{n,k}^* &= \#\mathscr{M}_{n,k}^* = \#\mathscr{E}_{n,k,1} = q_{n,k} - n = \binom{n+k-1}{k} - n.
\end{aligned} \tag{2.1}$$

We consider the vectors $\mathbf{t} \in \mathbb{R}_+^{q_{n,k}^*}$, with components indexed by elements of $\mathscr{M}_{n,k}^*$, and define $I_{n,k}$ as the volume of the following polyhedron:

$$I_{n,k} = \operatorname{vol}\Big\{\mathbf{t} = (t_{\mathbf{m}})_{\mathbf{m} \in \mathscr{M}_{n,k}^*} \in \mathbb{R}_+^{q_{n,k}^*} \ : \ \sum_{\mathbf{m} \in \mathscr{M}_{n,k}^*} m_j t_{\mathbf{m}} \leqslant 1, \ 1 \leqslant j \leqslant n\Big\}. \tag{2.2}$$

Remark 2.1. *Clearly the cube $[0, 1/k]^{q_{n,k}^*}$ is inside of the region whose volume is measured by $I_{n,k}$, Hence, we have*

$$k^{-q_{n,k}^*} \leqslant I_{n,k} \leqslant 1.$$

Using the results of [4], which we summarize in Section 4, we derive the following asymptotic formula for $N_n^{(k)}(H)$.

Theorem 2.2. *Let $n \geqslant 1$ and $k \geqslant 2$ be fixed. There exists $\vartheta_{n,k} > 0$ and $Q_{n,k} \in \mathbb{R}[X]$ of degree $q^*_{n,k}$, given by (2.1), such that for any $H \geqslant 2$ we have*

$$N_n^{(k)}(H) = H^{n/k} Q_{n,k}(\log H) + O(H^{n/k-\vartheta_{n,k}}),$$

where the leading coefficient $C_{n,k}$ of $Q_{n,k}$ satisfies

$$C_{n,k} = I_{n,k} \prod_p \left(1 - \frac{1}{p}\right)^{q^*_{n,k}} \left(1 + \sum_{i=1}^{\infty} \frac{\#\mathscr{E}_{n,k,i}}{p^i}\right),$$

where the product is taken over all prime numbers and $I_{n,k}$ is defined in (2.2).

2.2. **Products which are squares.** We now give more explicit form of Theorem 2.2 when $k = 2$; this is important for applications.

In this case we simplify the notation by setting

$$N_n(H) = N_n^{(2)}(H), \quad I_n = I_{n,k}, \quad C_n = C_{n,2}, \quad q_n = q_{n,2} \quad q^*_n = q^*_{n,2}.$$

We now have from (2.1)

$$q_n = \frac{n(n+1)}{2} \qquad \text{and} \qquad q^*_n = \frac{n(n-1)}{2}.$$

Observing that

$$\#\mathscr{E}_{n,2,i} = \binom{n}{2i},$$

we derive

$$C_n = I_n \prod_p \left(1 - \frac{1}{p}\right)^{n(n-1)/2} \left(\frac{1}{2}\left(1 + \frac{1}{p^{1/2}}\right)^n + \frac{1}{2}\left(1 - \frac{1}{p^{1/2}}\right)^n\right)$$

where the product is taken over all prime numbers.

Let $\mathscr{H}$ be the set of integers $h \in [0, 2^n - 1]$ with exactly two nonzero binary digits. In particular, the first element of $\mathscr{H}$ is $2 + 1 = 3$ and the largest element is $2^{n-1} + 2^{n-2} = 3 \cdot 2^{n-2}$.

Then we see that I_n can now be defined as the volume of the following polyhedron:

$$I_n = \mathrm{vol}\left\{\mathbf{t} \in \mathbb{R}_+^{\mathscr{H}} : \sum_{h \in \mathscr{H}} \varepsilon_j(h) t_h \leqslant 1,\ 1 \leqslant j \leqslant n\right\},$$

where $\varepsilon_j(h)$ denotes the j-th digit in the binary expansion of h.

Remark 2.3. *For numerical calculations we can add another condition $t_3 \leqslant \ldots \leqslant t_{3\cdot 2^{n-2}}$ and then multiply by $(n(n-1)/2)!$ the resulting integral. Thus, we have*

$$I_2 = 1, \qquad I_3 = 6\int_{0\leqslant t_3\leqslant t_5\leqslant t_6\leqslant 1-t_5} \mathrm{d}\mathbf{t} = 6\int_0^{1/2} t_5(1-2t_5)\mathrm{d}t_5 = \tfrac{1}{4}.$$

We now see that for $k=2$, Theorem 2.2 implies the following result.

Corollary 2.4. *Let $n \geqslant 1$ be fixed. There exists $\vartheta_n > 0$ and $Q_n \in \mathbb{R}[X]$ of degree $n(n-1)/2$ such that for any $H \geqslant 2$ we have*

$$N_n(H) = H^{n/2}Q_n(\log H) + O(H^{n/2-\vartheta_n}),$$

where the leading coefficient C_n of Q_n satisfies

$$C_n = I_n \prod_p \left(1-\frac{1}{p}\right)^{n(n-1)/2} \left(\frac{1}{2}\left(1+\frac{1}{p^{1/2}}\right)^n + \frac{1}{2}\left(1-\frac{1}{p^{1/2}}\right)^n\right),$$

where the product is taken over all prime numbers.

In particular, for $n=2$, we have

$$\begin{aligned} C_2 &= I_2 \prod_p \left(1-\frac{1}{p}\right)\left(\frac{1}{2}\left(1+\frac{1}{p^{1/2}}\right)^2 + \frac{1}{2}\left(1-\frac{1}{p^{1/2}}\right)^2\right) \\ &= \prod_p \left(1-\frac{1}{p}\right)\left(1+\frac{1}{p}\right) = \prod_p\left(1-\frac{1}{p^2}\right) = \zeta(2)^{-1} = \frac{6}{\pi^2}, \end{aligned}$$

where ζ is the Riemann zeta-function.

3. Counting multiquadratic fields

3.1. **Discriminants of multiquadratic fields.** Let $F_n(X)$ be the number of distinct fields $\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)$ with $\mathbf{a} \in \mathbb{N}^n$ of largest possible degree as in (1.3) whose discriminant over $\mathbb{Q}$ satisfy

$$\mathrm{Discr}\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right), \mathbb{Q}\right) \leqslant X.$$

Let us define

$$t_n = \prod_{k=0}^{n-1}(2^n - 2^k). \tag{3.1}$$

Theorem 3.1. *Let $n \geqslant 1$ and $\varepsilon > 0$ be fixed. There exists a polynomial P_n of degree $2^n - 2$ with the leading coefficient*

$$A_n = \frac{4^n + 5 \cdot 2^n + 10}{2^{3+(n-1)(2^n-2)}(2^n+1)(2^n-2)!t_n} \prod_p \left(1 - \frac{1}{p}\right)^{2^n-1} \left(1 + \frac{2^n - 1}{p}\right),$$

such that, for $X \geqslant 2$,

$$F_n(X) = X^{1/2^{n-1}} \left(P_n(\log X) + O_\varepsilon\left(X^{-\eta_n+\varepsilon}\right)\right),$$

where

$$\eta_n = \frac{3}{2^{n-1}(5+2^n)}.$$

We remark that Rome [19] has obtained a special case of Theorem 3.1 for $n = 2$, however with a larger error term, see also [1, 24].

Let $f_n(d)$ be the number of distinct fields $\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)$ with $\mathbf{a} \in \mathbb{N}^n$ of largest possible degree as in (1.3) whose discriminants over $\mathbb{Q}$ satisfy $\mathrm{Discr}\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right), \mathbb{Q}\right) = d$.

We now explicitly evaluate the generating series

$$g_n(s) = \sum_{d=1}^{\infty} \frac{f_n(d)}{d^s}, \qquad s \in \mathbb{C}.$$

For this we define

$$h_n(s) = \prod_{p>2} \left(1 + \frac{2^n - 1}{p^s}\right), \qquad s \in \mathbb{C},\ \mathfrak{Re}\, s > 1. \tag{3.2}$$

Theorem 3.2. *Let $n \geqslant 1$ be fixed. For any $s \in \mathbb{C}$ with $\mathfrak{Re}\, s > 1/2^{n-1}$ we have*

$$g_n(s) = \frac{h_n\left(2^{n-1}s\right)}{t_n} \left(1 + \frac{2^n - 1}{2^{2^n s}} + \frac{2^{n+1} - 2}{2^{3 \cdot 2^n s}} + \frac{4^n - 3 \cdot 2^n + 2}{2^{2^{n+1} s}}\right).$$

3.2. **Multiquadratic fields with maximal Galois groups.** We also wish to determine the number of distinct multiquadratic fields of the form $\mathbb{Q}(\sqrt{\mathbf{a}})$ for $\mathbf{a} \in \mathbb{N}^n \cap \mathfrak{B}_n(H)$, that have maximal Galois group

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{\mathbf{a}})/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^n,$$

that is,

$$G_n(H) = \#\left\{\mathbb{Q}\left(\sqrt{\mathbf{a}}\right):\ \mathbf{a} \in \mathbb{N}^n \cap \mathfrak{B}_n(H) \text{ and } \#\,\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)/\mathbb{Q}\right) = 2^n\right\}.$$

Theorem 3.3. *We have, as $H \to \infty$,*

$$G_n(H) = \left(\frac{1}{n!\zeta(2)^n} + O\left(\mathrm{e}^{-(1+o(1))\sqrt{(\log H)(\log\log H)/2}} \right) \right) H^n.$$

3.3. **Higher index radical extensions with maximal degree.** Let $k \geqslant 3$ be an odd integer. We can also determine the number of distinct fields

$$K_{\mathbf{a}} = \mathbb{Q}(\sqrt[k]{\mathbf{a}}) = \mathbb{Q}(\sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k}),$$

where $\sqrt[k]{a_i}$ always denotes the real k-th root of a_i, for $\mathbf{a} \in \mathbb{N}^n \cap \mathfrak{B}_n(H)$, that have maximal degree, that is

$$G_n^k(H) = \# \left\{ \mathbb{Q}\left(\sqrt[k]{\mathbf{a}}\right) : \ \mathbf{a} \in \mathbb{N}^n \cap \mathfrak{B}_n(H) \text{ and } [\mathbb{Q}(\sqrt[k]{\mathbf{a}}) : \mathbb{Q}] = k^n \right\}.$$

Clearly $K_{\mathbf{a}}$ is never Galois since $K_{\mathbf{a}} \subseteq \mathbb{R}$ and the Galois closure of $K_{\mathbf{a}}$ must contain the k-th cyclotomic extension $Z_k = \mathbb{Q}(\zeta_k)$, where ζ_k is some fixed primitive k-th root of unity.

Theorem 3.4. *Let $k \geqslant 3$ be an odd integer. Then, as $H \to \infty$,*

$$G_n^k(H) = \left(\frac{1}{n!\zeta(k)^n} + O\left(\mathrm{e}^{-(1+o(1))\sqrt{(\log H)(\log\log H)/2}} \right) \right) H^n.$$

We remark that the general case of adjoining any choice of k-th roots (possibly complex) to $\mathbb{Q}$ follows easily from the case of real roots. Namely, for extensions of maximal degree, Kummer theory, see, for example, [8, Section 14.7] or [14, Ch. VI, §8–§9], implies that the absolute Galois group acts transitively on the set of n-tuples of the form $\left(\zeta_k^{e_1}\sqrt[k]{a_1}, \ldots, \zeta_k^{e_n}\sqrt[k]{a_n}\right)$, as $e_1, \ldots, e_n$ ranges over integers in $[1, k]$.

Further, since $K_{\mathbf{a}}(\zeta_k)$ is the normal closure of $K_{\mathbf{a}}$, it follows from Kummer theory (cf. Section 6.5) that $\mathrm{Gal}(K_{\mathbf{a}}(\zeta_k)/\mathbb{Q})$ is maximal if and only if $[K_{\mathbf{a}} : \mathbb{Q}] = k^n$. In particular, Theorem 3.4 also allows us to count fields $K_{\mathbf{a}}$ such that the normal closure has maximal Galois group. In fact, it is not difficult to show that the number of $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n \cap \mathfrak{B}_n(H)$ such that $a_1, \ldots, a_n$ are multiplicatively dependent modulo k-th powers is $o(H^n)$, so Theorem 3.4 easily yields an asymptotic formula for the number of distinct fields $K_{\mathbf{a}}$, as well as an asymptotic formula for the number of distinct normal closures $K_{\mathbf{a}}(\zeta_k)$, as $\mathbf{a}$ ranges over elements in $\mathbb{N}^n \cap \mathfrak{B}_n(H)$.

4. Sums of arithmetical functions of several variables

4.1. **Setup.** We say that f is a positive *multiplicative* function if

$$f(e_1, \ldots, e_m) f(d_1, \ldots, d_m) = f(e_1 d_1, \ldots, e_m d_m) \tag{4.1}$$

for all pairs of tuples of positive integers with

$$\gcd(e_1 \cdots e_m, d_1 \cdots d_m) = 1.$$

We next recall some results of La Bretèche [4, Theorems 1 and 2], which for f a positive multiplicative function, links the sum

$$S_{\boldsymbol{\beta}}(X) = \sum_{1 \leqslant d_1 \leqslant X^{\beta_1}} \cdots \sum_{1 \leqslant d_m \leqslant X^{\beta_n}} f(d_1, \ldots, d_m), \tag{4.2}$$

where $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m) \in \mathbb{R}^m$, to the behavior of the associated multiple Dirichlet series

$$F(s_1, \ldots, s_m) = \sum_{d_1=1}^{\infty} \cdots \sum_{d_m=1}^{\infty} \frac{f(d_1, \ldots, d_m)}{d_1^{s_1} \cdots d_m^{s_m}}.$$

The goal is to understand analytic properties of F in order to obtain a tauberian theorem for multiple Dirichlet series. This is for instance possible when F can be written as an Euler product. As in the one dimensional case, this is equivalent to the multiplicativity of f.

In that case, formally we have

$$F(\mathbf{s}) = \prod_{p \text{ prime}} \left(\sum_{\boldsymbol{\nu} \in \mathbb{N}_0^m} \frac{f(p^{\nu_1}, \ldots, p^{\nu_m})}{p^{\nu_1 s_1 + \cdots + \nu_m s_m}} \right),$$

where $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_m)$.

To state the relevant results from [4] we need further notations. We denote by $\mathscr{L}_m(\mathbb{C})$ the space of linear forms

$$\ell(X_1, \ldots, X_m) \in \mathbb{C}[X_1, \ldots, X_m].$$

Let $\{\mathbf{e}_j\}_{j=1}^m$ be the canonical basis of $\mathbb{C}^m$ and let be $\{\mathbf{e}_j^*\}_{j=1}^m$ the dual basis in $\mathscr{L}_m(\mathbb{C})$. We denote by $\mathscr{L}\mathbb{R}_m(\mathbb{C})$ the set of linear forms of $\mathscr{L}_m(\mathbb{C})$ such that their restriction to $\mathbb{R}^m$ maps to $\mathbb{R}$. We define $\mathscr{L}\mathbb{R}_m^+(\mathbb{C})$ similarly with respect to the set $\mathbb{R}_+$ of positive real numbers.

As usual, we use $\|\cdot\|_1$ to denote the L^1-norm and use $\langle \cdot \rangle$ to denote the inner product of vectors from $\mathbb{R}^m$.

We view $\mathbb{R}^m$ as a partially ordered set using the relation $\mathbf{d} > \mathbf{e}$ if and only if this inequality holds component-wise for $\mathbf{d}, \mathbf{e} \in \mathbb{R}^m$.

We also apply the notations $\mathfrak{Re}$ and $\mathfrak{Im}$, for the real and imaginary part, to vectors in the natural component-wise fashion.

4.2. **Asymptotic formula.** We are now able to state [4, Theorem 1] which gives an asymptotic formula for the sums $S_{\boldsymbol{\beta}}(X)$ given by (4.2).

Lemma 4.1. *Let f be a positive arithmetical function on $\mathbb{N}^m$ and F be the associated Dirichlet series*

$$F(\mathbf{s}) = \sum_{d_1=1}^{+\infty} \cdots \sum_{d_m=1}^{+\infty} \frac{f(d_1, \ldots, d_m)}{d_1^{s_1} \cdots d_m^{s_m}}.$$

We assume that there exists $\boldsymbol{\alpha} \in (\mathbb{R}_+)^m$ *such that* F *satisfies the following properties:*

(P1) $F(\mathbf{s})$ *is absolutely convergent for* $\mathbf{s}$ *such that* $\mathfrak{Re}(\mathbf{s}) > \boldsymbol{\alpha}$.

(P2) *There exists a family of* n *non zero linear forms* $\mathscr{L} = \left\{\ell^{(i)}\right\}_{i=1}^{n}$ *of* $\mathscr{L}\mathbb{R}_m^+(\mathbb{C})$ *and a family of* R *non zero linear forms* $\left\{h^{(r)}\right\}_{r=1}^{R}$ *of* $\mathscr{L}\mathbb{R}_m^+(\mathbb{C})$ *and* $\delta_1, \delta_3 > 0$ *such that the function* H *from* $\mathbb{C}^m$ *to* $\mathbb{C}$ *defined by*

$$H(\mathbf{s}) = F(\mathbf{s}+\boldsymbol{\alpha}) \prod_{i=1}^{N} \ell^{(i)}(\mathbf{s})$$

can be analytically continued in the domain

$$\mathscr{D}(\delta_1, \delta_3) = \Big\{\mathbf{s} \in \mathbb{C}^m : \ \mathfrak{Re}\left(\ell^{(i)}(\mathbf{s})\right) > -\delta_1, \ \forall i, \ \text{and} \\ \mathfrak{Re}\left(h^{(r)}(\mathbf{s})\right) > -\delta_3, \forall r\Big\}$$

(P3) *There exists* $\delta_2 > 0$ *such that, for all* $\varepsilon_1, \varepsilon_2 > 0$ *the following upper bound*

$$H(\mathbf{s}) \ll \prod_{i=1}^{n} \left(\left|\,\mathfrak{Im}\left(\ell^{(i)}(\mathbf{s})\right)\right| + 1\right)^{1-\delta_2 \min\left\{0, \mathfrak{Re}\left(\ell^{(i)}(\mathbf{s})\right)\right\}} \left(1 + \|\,\mathfrak{Im}(\mathbf{s})\|_1^{\varepsilon_1}\right)$$

holds uniformly in the domain $\mathscr{D}(\delta_1 - \varepsilon_2, \delta_3 - \varepsilon_2)$.

Let $J(\boldsymbol{\alpha}) = \{j \in \{1, \cdots, m\} : \ \alpha_j = 0\}$. *We set* $r = \#J(\boldsymbol{\alpha})$ *and let* $\ell^{(N+1)}, \ldots, \ell^{(N+r)}$ *be the* r *linear forms* $\mathbf{e}_j^*$ *where* $j \in J(\boldsymbol{\alpha})$. *Then, under previous hypotheses (P1), (P2) and (P3), there exists a polynomial* $Q \in \mathbb{R}[X]$ *of degree less or equal to* $N + r - \operatorname{rank}(\{\ell^{(i)}\}_{i=1}^{N+r})$ *and a real* $\vartheta > 0$, *that depends on* $\mathscr{L}$, $\left\{h^{(r)}\right\}_{r=1}^{R}$, δ_1, δ_2, δ_3, $\boldsymbol{\alpha}$ *and* $\boldsymbol{\beta}$, *such that, for all* $X \geqslant 1$, *we have*

$$S_{\boldsymbol{\beta}}(X) = X^{\langle \boldsymbol{\alpha}, \boldsymbol{\beta} \rangle} \left(Q(\log X) + O(X^{-\vartheta})\right).$$

We remark that in (P2) of Lemma 4.1 we have shifted the argument of F by $\boldsymbol{\alpha}$ so that the critical point is $\mathbf{s} = \mathbf{0}$.

Furthermore, the exact value of the degree of Q is given by [4, Theorem 2], which we state in a form which is sufficient for our purpose. When $\mathscr{L} = \left\{\ell^{(i)}\right\}_{i=1}^{n}$ is a finite subset of $\mathscr{L}\mathbb{R}_m^+(\mathbb{C})$, we define

$$\operatorname{Conv}^*(\mathscr{L}) = \sum_{\ell \in \mathscr{L}} \mathbb{R}_+^* \ell.$$

Lemma 4.2. *Let f be an arithmetical function satisfying all the hypotheses of Lemma 4.1. Let $J(\boldsymbol{\alpha}) = \{j \in \{1, \cdots, m\} : \alpha_j = 0\}$. We set $r = \#J(\boldsymbol{\alpha})$ and $\ell^{(N+1)}, \ldots, l^{(N+r)}$ the r linear forms $\mathbf{e}_j^*$ where $j \in J(\boldsymbol{\alpha})$ as before. If $\operatorname{rank}(\{\ell^{(i)}\}_{i=1}^{N+r}) = m$, $H(0, \ldots, 0) \neq 0$ and*

$$\sum_{j=1}^{m} \beta_j \mathbf{e}_j^* \in \operatorname{Conv}^*(\{\ell^{(i)}\}_{i=1}^{N+r}),$$

then Q is a polynomial

- *of degree $D = N + r - m$,*
- *with the leading coefficient $H(0, \ldots, 0)I$, where*

$$I = \lim_{X \to +\infty} X^{-\langle \boldsymbol{\alpha}, \boldsymbol{\beta} \rangle} (\log X)^{-D} \int_{\substack{\mathbf{y} \in [1,\infty)^N \\ \prod_{i=1}^N y_i^{\ell_i(\mathbf{e}_j)} \leqslant X^{\beta_j} \\ 1 \leqslant j \leqslant m}} \prod_{i=1}^{N} y_i^{\ell_i(\boldsymbol{\alpha}) - 1} \mathrm{d}\mathbf{y}.$$

with $\mathbf{y} = (y_1, \ldots, y_N)$.

5. Towers of quadratic extensions

5.1. **Degree.** We now recall a result of Balasubramanian, Luca and Thangadurai [2, Theorem 1.1] which gives an explicit formula for the degrees of the fields (1.1).

It is convenient to define

$$\mathbb{Z}_* = \mathbb{Z} \setminus \{0\}.$$

For $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}_*^n$ we define the products

$$b_{\mathscr{J}} = \prod_{j \in \mathscr{J}} a_j. \tag{5.1}$$

Define $\gamma_{\mathbf{a}}$ as the number of subsets $\mathscr{J} \subseteq \{1, \ldots, n\}$ with

$$b_{\mathscr{J}} \in \mathbb{N}^{(2)}.$$

Note that since the empty set $\mathscr{J}$ is not excluded, we always have $\gamma_{\mathbf{a}} \geqslant 1$.

Furthermore, we say that $\mathbf{a}$ is *multiplicatively independent modulo squares* if none of the products $b_{\mathscr{J}}$ with $\mathscr{J} \neq \varnothing$ is a square (that is, if $\gamma_{\mathbf{a}} = 1$).

Lemma 5.1. *For $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}_*^n$ we have*

$$[\mathbb{Q}(\sqrt{\mathbf{a}}) : \mathbb{Q}] = \frac{2^n}{\gamma_{\mathbf{a}}}.$$

Note that $\gamma_{\mathbf{a}}$ is a power of 2 as examining prime factorization of $a_1, \ldots, a_n$ we see that the this the size of the kernel of some matrix over the field of two elements, see also [2, Lemma 2.1]. Hence the right hand side of the formula of Lemma 5.1 is indeed an integer number.

Corollary 5.2. *For $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}_*^n$ the field $\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)$ satisfies (1.3) if and only if $a_1, a_2, \ldots, a_n \in \mathbb{Z}_*$ are multiplicatively independent modulo squares.*

Alternatively, since $\mathbb{Q}$ contains all roots of unity of order two, the corollary also follows from Kummer theory, cf. [8, Proposition 37, Ch. 14] or [14, Theorem 8.1, Ch. VI, §8].

5.2. **Discriminant.** First we recall that for a square-free $a \in \mathbb{Z}_*$ we have

$$\operatorname{Discr} \mathbb{Q}\left(\sqrt{a}\right) = \begin{cases} a, & \text{if } a \equiv 1 \pmod 4, \\ 4a, & \text{if } a \equiv 2, 3 \pmod 4). \end{cases} \tag{5.2}$$

We now examine the discriminant $\operatorname{Discr}(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right) : \mathbb{Q})$ of the field $\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)$ over $\mathbb{Q}$.

Lemma 5.3. *Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}_*$ be multiplicatively independent modulo squares. Then*

$$\operatorname{Discr}(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right), \mathbb{Q}) = \prod_{\substack{\mathscr{J} \subseteq \{1,\ldots,n\} \\ \mathscr{J} \neq \varnothing}} \operatorname{Discr}\left(\mathbb{Q}\left(\sqrt{b_{\mathscr{J}}}\right), \mathbb{Q}\right),$$

where the integers $b_{\mathscr{J}}$ are defined by (5.1).

Proof. Our method relies on the well-known identity for relative discriminants in the tower of field extensions $F \subseteq K \subseteq L$:

$$\operatorname{Discr}(L, F) = \operatorname{Nm}_{K/F}(\operatorname{Discr}(L, K)) \operatorname{Discr}(K, F)^{[L:K]}, \tag{5.3}$$

where $\operatorname{Nm}_{K/F}$ is the norm map from K to F, see, for example, [15, Chapter 2, Exercise 23].

We prove it by induction on n. The hypothesis of rank n is that

$$\operatorname{Discr}(F\left(\sqrt{a_1}, \ldots, \sqrt{a_n}\right), F) = \prod_{\substack{\mathscr{J} \subseteq \{1,\ldots,n\} \\ \mathscr{J} \neq \varnothing}} \operatorname{Discr}\left(F\left(\sqrt{b_{\mathscr{J}}}\right), F\right) \tag{5.4}$$

for any field $F = \mathbb{Q}(\sqrt{b_1}, \ldots, \sqrt{b_\ell})$ such that $a_1, \ldots, a_n, b_1, \ldots, b_\ell$ are multiplicatively independent modulo a square.

For $n = 2$, this formula is already known (see [9, Chapter 8, § 7.23]). Assume the hypothesis (5.4) for the rank $n \geqslant 2$. We write

$$L = F\left(\sqrt{a_1}, \ldots, \sqrt{a_{n+1}}\right).$$

Let us calculate $\Delta = \mathrm{Discr}(L, F)$. We apply the formula (5.3) for $K = F(\sqrt{a_{n+1}})$, where by Corollary 5.2 we have $[L : K] = 2^n$. Hence,

$$\Delta = N_{K/F}(\mathrm{Discr}(L, K))\, \mathrm{Discr}(F(\sqrt{a_{n+1}}), F)^{2^n}. \tag{5.5}$$

The inductive hypothesis and the multiplicativity of the norm give

$$N_{K/F}\left(\mathrm{Discr}(L, K)\right) = \prod_{\substack{\mathscr{J} \subseteq \{1,\dots,n\} \\ \mathscr{J} \neq \varnothing}} N_{K/F}\left(\mathrm{Discr}\left(K\left(\sqrt{b_{\mathscr{J}}}\right), K\right)\right).$$

The formula (5.3) and the induction hypothesis for $n = 2$ yield

$$\begin{aligned} N_{K/F}\left(\mathrm{Discr}\left(K\left(\sqrt{b_{\mathscr{J}}}\right), K\right)\right) &= \frac{\mathrm{Discr}\left(F\left(\sqrt{a_{n+1}}, \sqrt{b_{\mathscr{J}}}\right), F\right)}{\mathrm{Discr}\left(F\left(\sqrt{a_{n+1}}\right), F\right)^2} \\ &= \frac{\mathrm{Discr}\left(F\left(\sqrt{b_{\mathscr{J}}}\right), F\right) \mathrm{Discr}\left(F\left(\sqrt{a_{n+1} b_{\mathscr{J}}}\right), F\right)}{\mathrm{Discr}\left(F\left(\sqrt{a_{n+1}}\right), F\right)}. \end{aligned}$$

Then, from (5.5), we can deduce the required formula. □

5.3. **Maximal Galois groups.** Let $\mathbb{F}_2$ denote the finite field with two elements. Given $H \in \mathbb{R}_+$ we consider an arbitrary $\mathbb{F}_2$-vector space V_H, of dimension $\pi(H)$, where, as usual, $\pi(H)$ denotes the number of primes $p \leqslant H$.

Let $\mathscr{S} \subseteq \mathbb{N}$ denote the set of square-free positive integers. Define a map $\varphi_H : (\mathscr{S} \cap [1, H]) \to V_H$ by

$$\varphi_H(a) = (e_p)_{p \leqslant H} \tag{5.6}$$

identifying the $\pi(H)$-dimensional $\mathbb{F}_2$-vector space, indexed by primes $p \leqslant H$, and where

$$a = \prod_{p \leqslant H} p^{e_p}.$$

We now show that $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)/\mathbb{Q}\right)$ is maximal if and only if the vectors $\varphi_H(a_1), \dots, \varphi_H(a_n)$ are linearly independent over $\mathbb{F}_2$.

Lemma 5.4. *Given* $\mathbf{a} \in (\mathscr{S} \cap [1, H])^n$ *we have* $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)/\mathbb{Q}\right) \simeq (\mathbb{Z}/2\mathbb{Z})^n$ *if and only if*

$$\dim_{\mathbb{F}_2}\left(\mathrm{Span}\left(\varphi_H(a_1), \dots, \varphi_H(a_n)\right)\right) = n.$$

Proof. It is enough to check the parity of the exponents of the ramified primes in all quadratic field extensions K (of $\mathbb{Q}$) such that $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}\left(\sqrt{\mathbf{a}}\right)$. For odd primes this is clear; for ramification at two we note that the two-exponent has odd parity if and only if $K = \mathbb{Q}(\sqrt{a})$ for a even.

Alternatively the statement follows immediately from Kummer theory (cf. [8, Section 14.7] or [14, Ch. VI, §8–S9]). □

6. Proofs of main results

6.1. **Proof of Theorem 2.2.** As usual, for a prime p and an integer $m \geqslant 0$ and $y \neq 0$, we use $p^m \parallel y$ to denote that

$$p^m \mid y \qquad \text{and} \qquad p^{m+1} \nmid y.$$

For $\mathbf{m} \in \mathscr{M}_{n,k}$ and $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{N}^n$ we set

$$u_{\mathbf{m}} = \prod_{\substack{p^{m_j} \parallel u_j \\ \forall j}} p$$

(that is, a prime p is included in the above product if and only if $p^{m_j} \parallel u_j$ for every $j = 1, \ldots, n$, and thus the product is finite since $\mathbf{m} \in \mathscr{M}_{n,k}$ implies that $m_j > 0$ for at least one j).

Then we parametrize the solutions of $u_1 \cdots u_n = w^k$ as follows:

$$u_j = \prod_{\mathbf{m} \in \mathscr{M}_{n,k}} u_{\mathbf{m}}^{m_j}, \qquad 1 \leqslant j \leqslant n. \tag{6.1}$$

We note that this parametrization resembles the one used in [5], yet it is different in that no coprimality condition is imposed.

We observe that

$$N_n^{(k)}(H) = \# \left\{ (u_{\mathbf{m}})_{\mathbf{m} \in \mathscr{M}_{n,k}} : \prod_{\mathbf{m} \in \mathscr{M}_{n,k}} u_{\mathbf{m}}^{m_j} \leqslant H, \ j = 1, \ldots, n \right\},$$

where the vectors $(u_{\mathbf{m}})_{\mathbf{m} \in \mathscr{M}_{n,k}}$ are formed from all possible vectors $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{N}^n$.

We now consider the function $f(d_1, \ldots, d_n)$ which is a product (over $j = 1, \ldots, n$) of the number of representations of each d_j as

$$d_j = \prod_{\mathbf{m} \in \mathscr{M}_{n,k}} u_{\mathbf{m}}^{m_j}.$$

Clearly $f(d_1, \ldots, d_n)$ is multiplicative as in (4.1).

The multiple Dirichlet series associated to this counting problem is

$$\begin{aligned} F(\mathbf{s}) &= \sum_{(u_{\mathbf{m}})_{\mathbf{m} \in \mathscr{M}_{n,k}}} \prod_{j=1}^{n} \left(\prod_{\mathbf{m} \in \mathscr{M}_{n,k}} u_{\mathbf{m}}^{m_j} \right)^{-s_j} \\ &= \prod_p \left(1 + \sum_{\mathbf{m} \in \mathscr{M}_{n,k}} \frac{1}{p^{m_1 s_1 + \ldots + m_n s_n}} \right). \end{aligned}$$

Let $\{\ell_{\mathbf{m}}\}_{\mathbf{m}\in\mathscr{M}_{n,k,1}}$ defined by

$$\ell_{\mathbf{m}}(\mathbf{s}) = \sum_{j=1}^{n} m_j s_j.$$

There exists a holomorphic function $G(\mathbf{s})$, which for any fixed ε is uniformly bounded in

$$\left\{\mathbf{s}\in\mathbb{C}^n : \ \ell_{\mathbf{m}}(s) \geqslant \tfrac{1}{2k}+\varepsilon \quad (\mathbf{m}\in\mathscr{M}_{n,k,1})\right\}$$

such that

$$F(\mathbf{s}) = \prod_{\mathbf{m}\in\mathscr{M}_{n,k,1}} \zeta\left(\ell_{\mathbf{m}}(\mathbf{s})\right) G(\mathbf{s}).$$

We have

$$G\left(\frac{1}{k},\dots,\frac{1}{k}\right) = \prod_p \left(1-\frac{1}{p}\right)^{q_{n,k}} \left(1+\sum_{i=1}^{\infty}\frac{\#\mathscr{M}_{n,k,i}}{p^i}\right).$$

We write $m_j = \varepsilon_j + kh_j$, where $\varepsilon_j \in \{0, k-1\}$ and $h_j\in\mathbb{N}_0$, $j=1,\dots,n$. We have

$$1+\sum_{i=1}^{\infty}\frac{\#\mathscr{M}_{n,k,i}}{p^i} = \left(1-\frac{1}{p}\right)^{-n}\left(1+\sum_{i=1}^{\infty}\frac{\#\mathscr{E}_{n,k,i}}{p^i}\right).$$

We observe that $k \mid m_1+\ldots+m_n$ is equivalent to $k\mid \varepsilon_1+\ldots+\varepsilon_n$. Then we have

$$G\left(\frac{1}{k},\dots,\frac{1}{k}\right) = \prod_p \left(1-\frac{1}{p}\right)^{q_{n,k}-n} \left(1+\sum_{i=1}^{\infty}\frac{\#\mathscr{E}_{n,k,i}}{p^i}\right).$$

The Dirichlet series F satisfies the hypotheses of Lemma 4.1 with

$$\boldsymbol{\alpha} = (\alpha_1,\dots,\alpha_n) = \left(\frac{1}{k},\dots,\frac{1}{k}\right), \quad \text{and } \boldsymbol{\beta} = (\beta_1,\dots,\beta_n) = (1,\dots,1).$$

One can check the hypothesis P3 by using the bound

$$\zeta(1+s)s \ll (1+|\,\mathfrak{Im}\, s|)^{1-\mathfrak{Re}(s)/3+\varepsilon}, \qquad \text{for } \mathfrak{Re}\, s\in\left[-\tfrac{1}{2},0\right].$$

which holds for any fixed $\varepsilon>0$.

Then there exists $\vartheta_{n,k}>0$, $Q_{n,k}\in\mathbb{R}[X]$ such that

$$N_n^{(k)}(H) = H^{n/k}Q_{n,k}(\log H) + O(H^{n/k-\vartheta_{n,k}}).$$

We now apply Lemma 4.2 with $N = \#\mathscr{M}_{n,k,1} = q_{n,k}$,

$$\{\ell^{(i)}\}_{1\leqslant i\leqslant N} = \{\ell_{\mathbf{m}}\}_{\mathbf{m}\in\mathscr{M}_{n,k,1}}$$

and see that $\deg Q_{n,k} = q^*_{n,k}$ since $\ell^{(j)}(\mathbf{s}) = ks_j \in \{\ell_{\mathbf{m}}\}_{\mathbf{m}\in\mathscr{M}_{n,k,1}}$ for all $1 \leqslant j \leqslant n$. Then the set $\mathscr{M}_{n,k}*$ is the subset of $\mathscr{M}_{n,k,1}$ which avoids the forms $\{\ell^{(i)}\}_{1\leqslant i\leqslant N}$. Moreover

$$\begin{aligned} Q_{n,k}(\log H) &\sim \frac{G\left(\frac{1}{k},\dots,\frac{1}{k}\right)}{H^{n/k}} \int_{\substack{(z_{\mathbf{m}})\in[1,\infty)^{\#\mathscr{M}_{n,k,1}}\\ \prod_{\mathbf{m}\in\mathscr{M}_{n,k,1}} z_{\mathbf{m}}^{m_j}\leqslant H}} \mathrm{d}z \\ &\sim G\left(\tfrac{1}{k},\dots,\tfrac{1}{k}\right) \int_{\substack{(z_{\mathbf{m}})\in[1,\infty)^{q_{n,k}}\\ \prod_{\mathbf{m}\in\mathscr{M}^*_{n,k}} z_{\mathbf{m}}^{m_j}\leqslant H}} \frac{\mathrm{d}\mathbf{z}}{\prod_{\mathbf{m}\in\mathscr{M}^*_{n,k}} z_{\mathbf{m}}} \\ &\sim G\left(\tfrac{1}{k},\dots,\tfrac{1}{k}\right) I_{n,k}(\log H)^{q^*_{n,k}}, \end{aligned}$$

as $H\to\infty$, where $I_{n,k}$ is defined in (2.2). This defines the leading coefficient of $Q_{n,k}$ and gives the desired result.

6.2. **Proof of Theorem 3.1.** Let K a field counted by $F_n(X)$. There are 2^n-1 quadratic extensions of $\mathbb{Q}$ in K. We write them as $\mathbb{Q}(\sqrt{c_j})$ with $1\leqslant j\leqslant 2^n-1$ where c_j is square-free.

We now recall that t_n is defined by (3.1). Then, clearly, there are t_n ways to choose $(j_1,\dots,j_n)$ such that $K=\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)$ with the vector $\mathbf{a}=(c_{j_1},\dots,c_{j_n})\in\mathbb{Z}^n$. The other c_j can be calculated from $\mathbf{a}$ by choosing for each of the remaining j some unique set $\mathscr{J}\subseteq\{1,\dots,n\}$ of cardinality $\#\mathscr{J}\geq 2$ and calculating

$$\prod_{k\in\mathscr{J}} c_{j_k} = c_j d_j^2.$$

Then we have

$$\begin{aligned} F_n(X) = \frac{1}{t_n}\#\big\{&(a_1,\dots,a_n)\in\mathbb{Z}^n:\ \mu^2(a_k)=1,\\ &\mathrm{Discr}\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right),\mathbb{Q}\right)\leqslant X,\ [\mathbb{Q}\left(\sqrt{\mathbf{a}}\right):\mathbb{Q}]=2^n\big\}. \end{aligned}$$

Given square-free $a_1,\dots,a_n\in\mathbb{N}$, we write

$$a_j = 2^{\nu_j}\prod_{1\leqslant h\leqslant 2^n-1} z_h^{\varepsilon_j(h)}, \qquad j=1,\dots,n, \tag{6.2}$$

where ν_j, $j=1,\dots,n$ are some nonnegative integers, $h=1,\dots,2^n-1$, and z_h are some odd positive integers. Since $a_1,\dots,a_n$ are square-free, the numbers z_h are coprime. For $\mathscr{J}\subseteq\{1,\dots,n\}$, and $b_{\mathscr{J}}$ as in (5.1) we have

$$b_{\mathscr{J}} = \prod_{j\in\mathscr{J}} a_j = 2^{n_{\mathscr{J}}}\prod_{1\leqslant h\leqslant 2^n-1} z_h^{\sum_{j\in\mathscr{J}}\varepsilon_j(h)} = 2^{n_{\mathscr{J}}} c_{\mathscr{J}} d_{\mathscr{J}}^2, \tag{6.3}$$

where, as before, $\varepsilon_j(h)$ denotes the j-th digit in the binary expansion of h, $n_{\mathscr{J}} = \sum_{j \in \mathscr{J}} \nu_j$, and $c_{\mathscr{J}}$ is odd and square-free. We have

$$c_{\mathscr{J}} = \prod_{\substack{1 \leqslant h \leqslant 2^n - 1 \\ \sum_{j \in \mathscr{J}} \varepsilon_j(h) \equiv 1 \pmod 2}} z_h$$

We write

$$\mathrm{Discr}(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n}), \mathbb{Q}) = 2^W D$$

where D is odd. Using Lemma 5.3 and the formula (5.2), we derive from (6.3) that

$$D = \prod_{\substack{\mathscr{J} \subseteq \{1, \ldots, n\} \\ \mathscr{J} \neq \varnothing}} c_{\mathscr{J}} = \prod_{1 \leqslant h \leqslant 2^n - 1} z_h^{\delta_h}$$

with

$$\delta_h = 2^{n - s(h)} \sum_{\substack{0 \leqslant k \leqslant s(h) \\ k \equiv 1 \pmod 2}} \binom{s(h)}{k} = 2^{n-1}, \qquad 1 \leqslant h \leqslant 2^n - 1,$$

and where

$$s(h) = \sum_{j=1}^{n} \varepsilon_j(h)$$

denotes the sum of digits in the binary expansion of h.

Then D is the largest odd divisor of

$$\mathrm{lcm}\,(\mathbf{a})^{2^{n-1}} = \mathrm{lcm}\,(a_1, \ldots, a_n)^{2^{n-1}}.$$

Let

- $r_{1,4}(\mathscr{J})$ be the number of $j \in \mathscr{J}$ such that $a_j \equiv 1 \pmod 4$,
- $r_{3,4}(\mathscr{J})$ be the number of $j \in \mathscr{J}$ such that $a_j \equiv 3 \pmod 4$,
- $r_{2,8}(\mathscr{J})$ be the number of $j \in \mathscr{J}$ such that $a_j \equiv 2 \pmod 8$,
- $r_{6,8}(\mathscr{J})$ be the number of $j \in \mathscr{J}$ such that $a_j \equiv 6 \pmod 8$.

We have

$$r_{1,4}(\mathscr{J}) + r_{3,4}(\mathscr{J}) + r_{2,8}(\mathscr{J}) + r_{6,8}(\mathscr{J}) = \#\mathscr{J}.$$

We now calculate $v_2\left(\mathrm{Discr}(\mathbb{Q}(\sqrt{b_{\mathscr{J}}}), \mathbb{Q})\right)$, where $b_{\mathscr{J}}$ is as in (5.1) and $v_2(m)$ denotes the largest power of 2 dividing an integer $m \neq 0$.

Then we have

$$v_2\left(\mathrm{Discr}\left(\mathbb{Q}(\sqrt{b_{\mathscr{J}}}),\mathbb{Q}\right)\right)$$
$$=\begin{cases}3, & \text{if } r_{2,8}(\mathscr{J})+r_{6,8}(\mathscr{J})\equiv 1 \pmod 2,\\ 2, & \text{if } r_{3,4}(\mathscr{J})+r_{6,8}(\mathscr{J})\equiv 1 \pmod 2,\\ & \quad \text{and } r_{2,8}(\mathscr{J})+r_{6,8}(\mathscr{J})\equiv 0 \pmod 2,\\ 0, & \text{otherwise.}\end{cases}$$

We now set $\rho_{k_1,k_2}=r_{k_1,k_2}(\{1,\ldots,n\})$. We observe that

$$\rho_{1,4}+\rho_{3,4}+\rho_{2,8}+\rho_{6,8}=n.$$

The U_3 number of $\mathscr{J}$ such that $v_2\left(\mathrm{Discr}(\mathbb{Q}(\sqrt{b_{\mathscr{J}}}),\mathbb{Q})\right)=3$ is

$$U_3=\begin{cases}2^{\rho_{1,4}+\rho_{3,4}+\rho_{2,8}+\rho_{6,8}-1}=2^{n-1} & \text{if } \rho_{2,8}+\rho_{6,8}\geqslant 1,\\ 0 & \text{if } \rho_{2,8}=\rho_{6,8}=0.\end{cases}$$

The number U_2 of $\mathscr{J}$ such that $v_2\left(\mathrm{Discr}(\mathbb{Q}(\sqrt{b_{\mathscr{J}}}),\mathbb{Q})\right)=2$ is

$$U_2=\begin{cases}2^{\rho_{1,4}+\rho_{3,4}+\rho_{2,8}+\rho_{6,8}-2}=2^{n-2} & \text{if } \rho_{3,4}+\rho_{6,8}\geqslant 1,\\ & \quad \rho_{2,8}+\rho_{6,8}\geqslant 1,\ \rho_{2,8}+\rho_{3,4}\geqslant 1,\\ 2^{\rho_{3,4}-1}=2^{n-1} & \text{if } \rho_{3,4}\geqslant 1,\ \ \rho_{2,8}=\rho_{6,8}=0,\\ 0 & \text{if } \rho_{3,4}=\rho_{6,8}=0\\ & \quad \text{or } \rho_{6,8}\geqslant 1,\ \ \rho_{2,8}+\rho_{3,4}=0.\end{cases}$$

Using that

$$W=3U_3+2U_2$$

we now deduce that

$$W=\begin{cases}2^{n+1} & \text{if } \rho_{3,4}+\rho_{6,8}\geqslant 1,\ \ \rho_{2,8}+\rho_{6,8}\geqslant 1,\ \ \rho_{2,8}+\rho_{3,4}\geqslant 1,\\ 3\cdot 2^{n-1} & \text{if } \rho_{3,4},\rho_{6,8}=0,\ \ \rho_{2,8}\geqslant 1,\ \text{or } \rho_{3,4},\rho_{2,8}=0,\ \ \rho_{6,8}\geqslant 1,\\ 2^n & \text{if } \ \rho_{3,4}\geqslant 1,\ \ \rho_{2,8},\rho_{6,8}=0,\\ 0 & \text{if } \rho_{3,4},\rho_{2,8},\rho_{6,8}=0.\end{cases}$$

Let $C_n(W)$ the number of possible configurations of the vectors $\mathbf{a}$ corresponding the for possibilities

$$1(\mathrm{mod}4),\qquad 3(\mathrm{mod}4),\qquad 2(\mathrm{mod}8),\qquad 6(\mathrm{mod}8)$$

which correspond to a given value W.

In particular

$$\sum_{W\in\{2^{n+1},3\cdot 2^{n-1},2^n,0\}} C_n(W)=4^n$$

More precisely, we have

$$C_n(W) = \begin{cases} 4^n - 3\cdot 2^n + 2 & \text{if } W = 2^{n+1}, \\ 2^{n+1} - 2 & \text{if } W = 3\cdot 2^{n-1}, \\ 2^n - 1 & \text{if } W = 2^n, \\ 1 & \text{if } W = 0. \end{cases}$$

For each configuration associated to W, there exists a binary vector $\boldsymbol{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n) = \{-1, 1\}^n$ such that $\mathbf{a}$ has to satisfy

$$(-1)^{m_j} \prod_{h=1}^{2^n-1} z_h^{\varepsilon_j(h)} \equiv \varepsilon_j \mod 4, \qquad j = 1, \dots, n.$$

Summing over all $m_j \in \{0,1\}$, we avoid this congruence condition. Let

$$T_n(x) = \sum_{\mathbf{z}\in\mathscr{Z}} \mu^2 \left(\prod_{1\leqslant h\leqslant 2^n-1} z_h \right),$$

where

$$\mathscr{Z} = \{\mathbf{z} \in \mathbb{N}^{2^n-1} : \; z_1, \dots, z_{2^n-1} \text{ odd and } z_1 \dots z_{2^n-1} \leqslant x\}.$$

Then

$$F_n(X) = \frac{1}{t_n} \sum_{W\in\{2^{n+1}, 3\cdot 2^{n-1}, 2^n, 0\}} C_n(W) T_n\left(\frac{X^{1/2^{n-1}}}{2^{W/2^{n-1}}} \right). \tag{6.4}$$

We have

$$T_n(x) = \sum_{\substack{m\leqslant x\\ m \text{ odd}}} \mu^2(m)(2^n-1)^{\omega(m)}. \tag{6.5}$$

By standard methods, there exists a polynomial Q_n of degree $2^n - 2$ such that for

$$\kappa_n = 3/(5+2^n)$$

we have

$$T_n(x) = \frac{1}{(2^n-2)!} x \left(Q_n(\log x) + O(x^{-\kappa_n+\varepsilon}) \right)$$

for any $\varepsilon > 0$. Moreover the leading coefficient of Q_n is

$$B_n = \frac{2}{2^n+1} \prod_p \left(1 - \frac{1}{p}\right)^{2^n-1} \left(1 + \frac{2^n-1}{p}\right).$$

Indeed, the associated Dirichlet series is $h_n(s)$ which is given by (3.2). It can be written as $h_n(s) = \zeta(s)^{2^n-1}\widetilde{h}_n(s)$ where $\widetilde{h}_n$ can be analytically continued until $\mathfrak{Re}\, s > \frac{1}{2}$. For more details, see [21, Exercise 194].

From (6.4), we deduce that there exists a polynomial P_n of degree 2^n-2 such that

$$F_n(X) = X^{1/2^{n-1}} \left(P_n(\log X) + O\left(X^{-\kappa_n/2^{n-1}+\varepsilon}\right)\right)$$

for any $\varepsilon > 0$. Moreover the leading coefficient of P_n is

$$A_n = \frac{4^n + 5\cdot 2^n + 10}{2^{4+(n-1)(2^n-2)}(2^n-2)!t_n} B_n.$$

6.3. **Proof of Theorem 3.2.** Using $f_n(d) = F_n(d) - F_n(d-1)$ and (6.4), we write

$$\begin{aligned} g_n(s) = \frac{1}{t_n} & \sum_{W\in\{2^{n+1},3\cdot 2^{n-1},2^n,0\}} C_n(W) \\ & \sum_{d=1}^{\infty} \frac{1}{d^s}\left(T_n\left(\frac{d^{1/2^{n-1}}}{2^{W/2^{n-1}}}\right) - T_n\left(\frac{(d-1)^{1/2^{n-1}}}{2^{W/2^{n-1}}}\right)\right). \end{aligned} \tag{6.6}$$

Note that if there is an integer m with

$$\frac{d^{1/2^{n-1}}}{2^{W/2^{n-1}}} \geqslant m > \frac{(d-1)^{1/2^{n-1}}}{2^{W/2^{n-1}}}$$

then $d \geqslant 2^W m^{2^{n-1}} > d-1$. Hence this is possible if and only if $d = 2^W m^{2^{n-1}}$. We now see from (6.5) that

$$\begin{aligned} & T_n\left(\frac{d^{1/2^{n-1}}}{2^{W/2^{n-1}}}\right) - T_n\left(\frac{(d-1)^{1/2^{n-1}}}{2^{W/2^{n-1}}}\right) \\ & \qquad = \begin{cases} \mu^2(m)(2^n-1)^{\omega(m)}, & \text{if } d = 2^W m^{2^{n-1}} \text{ with } m\in\mathbb{N}, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Substituting this in (6.6), we easily obtain

$$g_n(s) = \sum_{W\in\{2^{n+1},3\cdot 2^{n-1},2^n,0\}} C_n(W) \sum_{m=1}^{\infty} \frac{1}{(2^W m^{2^{n-1}})^s}\mu^2(m)(2^n-1)^{\omega(m)}$$

and the result follows.

6.4. **Proof of Theorem 3.3.** As, usual we say that an integer a is Q-friable if all prime divisors of a do not exceed Q. Let $\psi(H,Q)$ denote the number of positive Q-friable integers up to H, and let

$$u = \frac{\log H}{\log Q}$$

By [20, Part III, Theorem 5.13] and Hildebrand's theorem [11] for $H \geqslant Q > 2$ we have

$$\psi(H,Q) \ll H u^{-u} \tag{6.7}$$

for $\log Q \geqslant (\log\log H)^{5/3+\varepsilon}$ and any fixed $\varepsilon > 0$.

Furthermore, we recall the classical asymptotic formula

$$\#\left(\mathscr{S} \cap [1,H]\right) = \frac{1}{\zeta(2)} H + O\left(H^{1/2+o(1)}\right). \tag{6.8}$$

where as before $\mathscr{S}$ is the set of square-free integers, see [10, Theorem 334] (note that using the currently best known result of Jia [12] with $17/54$ instead of the exponent $1/2$ does not affect our final result).

Finally, for $Q \leqslant H$, we have the trivial bound

$$\begin{aligned} \#\left\{\mathbf{a} \in \mathfrak{B}_n(H) :\ \text{pw-gcd}(\mathbf{a}) > Q\right\} &\leqslant \frac{n(n-1)}{2} H^{n-2} \sum_{d>Q} \lfloor H/d \rfloor^2 \\ &\ll H^n Q^{-1}, \end{aligned} \tag{6.9}$$

where for $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$ we define the pair-wise greatest common divisor pw-gcd$(\mathbf{a})$ as

$$\text{pw-gcd}(\mathbf{a}) = \max_{1 \leqslant i < j \leqslant n} \gcd(a_i, a_j).$$

For a real $Q \geqslant 2$ we define

$$\begin{aligned} &\mathscr{T}_n(H,Q) \\ &\qquad = \left\{\mathbf{a} \in \mathscr{S}^n \cap \mathfrak{B}_n(H) :\ \text{pw-gcd}(\mathbf{a}) \leqslant Q \text{ and no } a_i \text{ is } Q\text{-friable}\right\}. \end{aligned}$$

Combining (6.7), (6.8) and (6.9), we derive

$$\#\mathscr{T}_n(H,Q) = H^n \left(\frac{1}{\zeta(2)^n} + O\left(H^{-1/2+o(1)} + u^{-u} + Q^{-1}\right)\right). \tag{6.10}$$

We now claim that if $\mathbf{a}, \mathbf{b} \in \mathscr{T}_n(H,Q)$ generate the same multiquadratic field (with full Galois group), then they agree up to a permutation of coordinates.

We see this as follows: applying the map φ_H, given by (5.6), componentwise, we may regard $\mathbf{a}, \mathbf{b}$ as two $\mathbb{F}_2$ matrices, with n rows and $\pi(H)$ columns. Moreover, by the non-friability assumption on $\mathbf{a} \in \mathscr{T}_n(H,Q)$ (together with the assumption of square-freeness), each $\varphi_H(a_i)$ has a one in some p-indexed column for some prime $p > Q$.

Moreover, for $p > Q$, using the condition on pw-gcd$(\mathbf{a})$, we note that there can be at most one nonzero element in each column. That is, each a_i gives rise to some $p_i > Q$ such that the p_i-column has a one in row i, and zeros elsewhere. Recalling Lemma 5.4, this implies that for any $\mathbf{a} \in \mathscr{T}_n(H,Q)$ we have $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)/\mathbb{Q}\right) \simeq (\mathbb{Z}/2\mathbb{Z})^n$.

Now, if the fields are the same, we must have ramification at the same primes. In particular, we see from Lemma 5.3 that for each $i = 1, \ldots, n$ there must exist some j_i, $1 \leqslant j_i \leqslant n$, such that $p_i \mid b_{j_i}$. Thus, after permuting rows in the matrix associated with $\mathbf{b}$, and using that the conditions $\text{pw-gcd}(\mathbf{b}) \leqslant Q$, also holds for $\mathbf{b}$, we find that the matrices associated to $\mathbf{a}$ and $\mathbf{b}$ are identical in the columns indexed by $p_1, \ldots, p_n$; by permuting the rows of the two matrices, both restrictions to these columns are in fact the identity matrix.

Using that the fields $\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)$ and $\mathbb{Q}\big(\sqrt{\mathbf{b}}\big)$ are the same if and only if the associated $\mathbb{F}_2$-vectors generated by the map φ_H have the same span, there must exist some matrix $M \in \mathrm{GL}_n(\mathbb{F}_2)$ that maps the matrix associated with $\mathbf{a}$ into the matrix associated with $\mathbf{b}$; comparing columns indexed by $p_1, \ldots, p_n$ we find that M is in fact the identity matrix, provided that we have permuted the rows as above (note that reordering the rows amounts to reordering the entries in $\mathbf{a}, \mathbf{b}$.)

Thus, after permuting the rows in $\mathbf{b}$ as described above we find that $\mathbf{a}$ and $\mathbf{b}$ are the same.

Hence

$$G_n(H) \geqslant \frac{1}{n!} \# \mathscr{T}_n(H, Q) + O(H^{n-2}Q), \tag{6.11}$$

where the error term comes from vectors $\mathbf{a}$ with two identical components (which cannot exceed Q).

It is also obvious that alternatively we can define $G_n(H)$ using only vectors $\mathbf{a}$ with square-free components, that is, as

$$\begin{aligned} &G_n(H) \\ &\quad = \# \left\{ \mathbb{Q}\left(\sqrt{\mathbf{a}}\right) : \ \mathbf{a} \in \mathscr{S}^n \cap \mathfrak{B}_n(H) \ \text{ and } \# \,\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)/\mathbb{Q}\right) = 2^n \right\}. \end{aligned}$$

Thus, recalling (6.8), we immediately obtain

$$G_n(H) \leqslant H^n \left(\frac{1}{n! \zeta(2)^n} + O\left(H^{-1/2+o(1)}\right) \right). \tag{6.12}$$

Combining (6.10) and (6.11) with (6.12), we obtain

$$G_n(H) = H^n \left(\frac{1}{n! \zeta(2)^n} + O\left(H^{-1/2+o(1)} + u^{-u} + Q^{-1} + H^{-2}Q\right) \right).$$

Choosing

$$Q = \exp\left(\sqrt{(\log H)(\log\log H)/2} \right) \tag{6.13}$$

so that $u = \sqrt{2(\log H)/(\log\log H)}$, we conclude the proof.

6.5. **Proof of Theorem 3.4.** First recall that $Z_k = \mathbb{Q}(\zeta_k)$ denotes the k-th cyclotomic field. We use Kummer theory to analyze the extension $Z_k K_{\mathbf{a}}/Z_k$ and then use the fact that $[Z_k K_{\mathbf{a}} : Z_k] = k^n$ implies that $[K_{\mathbf{a}} : \mathbb{Q}] = k^n$. By Kummer theory, (cf. [8, Section 14.7] or [14, Ch. VI, §8–S9]) we see that $\mathrm{Gal}(Z_k K_{\mathbf{a}}/Z_k)$ is isomorphic to

$$(\langle a_1, \ldots, a_n \rangle (Z_k^\times)^k)/(Z_k^\times)^k$$

where $(Z_k^\times)^k$ denotes the k-th powers in $Z_k^\times$. We begin by showing that any relation, modulo k-th powers in $Z_k^\times$, must already be a relation modulo k-th powers in $\mathbb{Q}^\times$.

Lemma 6.1. *If $k \geqslant 3$ is an odd integer then the map*

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^k \to Z_k^\times/(Z_k^\times)^k$$

is injective. In particular, an element $\alpha \in \mathbb{Q}^\times$ is a k-th power in Z_k if and only if $\alpha \in \mathbb{Q}^{\times k}$

Proof. We first recall that $t^k - \alpha$ is irreducible over $\mathbb{Q}$ (cf. [14, Theorem 9.1, Ch. VI, §9]) provided that α is not a p-th power of some rational number, for all prime divisors $p|k$.

Now, let α denote a element in the kernel of the above map, and assume that α is not a k-th power of any element in $\mathbb{Q}$. If $\alpha = \alpha_1^p$ for some $p|k$ and $\alpha_1 \in \mathbb{Q}$, then $t^{pr} - \alpha_1^p = \prod_{i=1}^p (t^r - \zeta_p \alpha_1)$, so if $t^r - \zeta_p \alpha_1$ has a root in Z_k, we find that $t^r - \alpha_1$ has a root in Z_{pk}. Repeating this procedure a finite number of times, we may thus reduce to the case of showing that the irreducible polynomial $t^{r_l} - \alpha_l$ does not have any roots in Z_{k^2}, for $\alpha_l \in \mathbb{Q} \smallsetminus \{\pm 1\}$, and α_l not a p-th power for any prime $p|r_l|k$. However, by [14, Theorem 9.4, Ch. VI, §9], the Galois group of $t^{r_k} - \alpha_k$ is non-abelian, and hence the roots cannot be contained in Z_{k^2} since the cyclotomic extension $Z_{k^2}/\mathbb{Q}$ is abelian. ☐

Thus, to count fields $K_{\mathbf{a}}$ with maximal degree is the same as counting $\mathbf{a} = (a_1, \ldots, a_n)$ such that the group $< a_1, \ldots, a_n > (\mathbb{Q}^\times)^k/(\mathbb{Q}^\times)^k$ has cardinality k^n — in other words, counting tuples $(a_1, \ldots, a_k)$ such that $a_1, \ldots, a_k$ are independent modulo k-th powers in $\mathbb{Q}^\times$.

With $\mathscr{S}_k$ denoting the set of k-free integers, we have

$$\#\left(\mathscr{S}_k \cap [1, H]\right) = \frac{1}{\zeta(k)} H + O\left(H^{1/k}\right).$$

As in the case of squares, we can define $G_n^k(H)$ using only vectors $\mathbf{a}$ with k-free components, that is, as

$$G_n^k(H) = \#\left\{\mathbb{Q}\left(\sqrt{\mathbf{a}}\right) : \ \mathbf{a} \in \mathscr{S}_k^n \cap \mathfrak{B}_n(H) \text{ and } [\mathbb{Q}\left(\sqrt[k]{\mathbf{a}}\right) : \mathbb{Q}] = k^n\right\}.$$

Restricting to the set of "nice" $\mathbf{a}$ as in the argument for multiquadratic fields (that is, to the set of vectors $\mathbf{a}$ having no Q-friable component a_i, as well making sure any pairwise greatest common divisor is at most Q), the argument is essentially the same except for one small caveat: if k is not prime, we cannot use linear algebra over a finite field, but must rather work with the finite ring $\mathbb{Z}/k\mathbb{Z}$. However, as $\mathrm{End}((\mathbb{Z}/k\mathbb{Z})^n) \simeq \mathrm{Mat}_n(\mathrm{End}(\mathbb{Z}/k\mathbb{Z}))$ and the set of invertible endomorphisms can be identified with $\mathrm{GL}_n(\mathbb{Z}/k\mathbb{Z})$ the previous argument applies also for k not prime.

Choosing Q as in (6.13), we conclude the proof.

7. Comments

We note similarly to the quantities $F_n(X)$ and $G_n(H)$ in Sections 3.1 and 3.2, respectively, one can count integer vectors and thus define

$$\begin{aligned} F_n^{\pm}(X) = \frac{1}{t_n}\#\{(a_1,\ldots,a_n) \in \mathbb{Z}^n :\ \mu^2(a_k) = 1,& \\ \mathrm{Discr}\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right),\mathbb{Q}\right) \leqslant X,\ [\mathbb{Q}\left(\sqrt{\mathbf{a}}\right) : \mathbb{Q}] = 2^n\}& \end{aligned}$$

and

$$\begin{aligned} &G_n^{\pm}(H) \\ &\quad = \#\left\{\mathbb{Q}\left(\sqrt{\mathbf{a}}\right) :\ \mathbf{a} \in \mathbb{Z}^n \cap \mathfrak{B}_n^{\pm}(H) \text{ and } \#\,\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)/\mathbb{Q}\right) = 2^n\right\}. \end{aligned}$$

where $\mathfrak{B}_n^{\pm}(H)$ is given by (1.4). We first observe that while the finiteness of $G_n^{\pm}(H)$ is obvious the finiteness of $F_n^{\pm}(X)$ needs some justification (since the discriminants are taken without the absolute value). In fact, we now need to assume $n \geqslant 2$ (as the case of $n = 1$ is special and is not of our interest). It is sufficient to show that for all discriminants counted in $F_n^{\pm}(X)$ are positive. Indeed, similarly to the proof of Theorem 3.1, given square-free $a_1,\ldots,a_n \in \mathbb{Z}$, we write

$$a_j = (-1)^{\mu_j} 2^{\nu_j} \prod_{1 \leqslant h \leqslant 2^n - 1} z_h^{\varepsilon_j(h)}, \qquad j = 1,\ldots,n,$$

where ν_j, $j = 1,\ldots,n$ are some nonnegative integers, $\mu_j \in \{0,1\}$ and z_h, $h = 1,\ldots,2^n - 1$, are some positive integers. Since $a_1,\ldots,a_n$ are square-free, the numbers z_h are coprime. For $\mathscr{J} \subseteq \{1,\ldots,n\}$, and $b_{\mathscr{J}}$ as in (5.1), similarly to (6.3) we have

$$\begin{aligned} b_{\mathscr{J}} = \prod_{j \in \mathscr{J}} a_j &= (-1)^{m_{\mathscr{J}}} 2^{n_{\mathscr{J}}} \prod_{1 \leqslant h \leqslant 2^n - 1} z_h^{\sum_{j \in \mathscr{J}} \varepsilon_j(h)} \\ &= (-1)^{m_{\mathscr{J}}} 2^{n_{\mathscr{J}}} c_{\mathscr{J}} d_{\mathscr{J}}^2. \end{aligned}$$

Since

$$\sum_{\substack{\mathscr{J}\subseteq\{1,\dots,n\}\\ \mathscr{J}\neq\varnothing}} m_{\mathscr{J}} = \sum_{j=1}^{n} 2^{n-1}\mu_j \equiv 0 \pmod 2,$$

the positivity of Discr $\left(\mathbb{Q}\left(\sqrt{\mathbf{a}}\right)\right)$ now follows from Lemma 5.3 and the formula (5.2). Thus for $n \geqslant 2$ we have $F_n^{\pm}(X) = F_n(X)$

Acknowledgment

The authors would like to thank Kevin Destagnol for many useful comments on the initial version of this paper and Jean-François Mestre for explaining the proof of Lemma 5.3.

This work started during a very enjoyable visit by I.S. to the Institute of Mathematics of Jussieu (Paris) and to the Department of Mathematics of KTH (Stockholm), whose support and hospitality are gratefully acknowledged.

During this work, P.K. was partially supported by the Swedish Research Council (2016-03701) and I.S. was supported by the Australian Research Council (DP170100786).

References

[1] A. M. Baily, 'On the density of discriminants of quartic fields?', *J. Reine Angew. Math.* , **315** (1980), 190–210. 1, 2, 3, 7

[2] R. Balasubramanian, F. Luca and R. Thangadurai, 'On the exact degree of $\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_\ell})$ over $\mathbb{Q}$', *Proc. Amer. Math. Soc.*, **138** (2010), 2283–2288. 2, 3, 11, 12

[3] M. Bhargava, 'The density of discriminants of quartic rings and fields', *Ann. of Math.*, **162** (2005), 1031–1063. 3

[4] R. de la Bretèche, 'Estimation de sommes multiples de fonctions arithmétiques', *Compos. Math.*, **128**, (2001), 261–298. 4, 9, 10

[5] R. de la Bretèche, 'Sur le nombre de matrices aléatoires à coefficients rationnels', *Quart. J. Math.*, **68** (2017), 935–955. 1, 14

[6] H. Cohen, F. Diaz y Diaz and M. Olivier, 'Counting discriminants of number fields', *J. Théorie Nombres Bordeaux*, **18** (2006), 573–593. 3

[7] E. Croot, A. Granville, R. Pemantle and P. Tetali, 'On sharp transitions in making squares', *Ann. of Math.*, **175** (2012), 1507–1550. 2

[8] D. S. Dummit and R. F. Foote, *Abstract algebra*, J. Willey Inc., 2004. 8, 12, 13, 23

[9] A. Frölich and M. J. Taylor, *Algebraic number theory*, Cambridge Univ. Press, 1991. 12

[10] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979. 21

[11] A. J. Hildebrand, 'On the number of positive integers $\le x$ and free of prime factors $> y$', *J. Number Theory*, **22** (1986), 289–307. 21

[12] C. H. Jia, 'The distribution of squarefree numbers ', *Sci. China, Ser. A.*, **36** (1993) 154–169. 21

[13] J. Klüners, 'The number of S_4-fields with given discriminant', *Acta Arith.*, **122** (2006), 185?194. 3

[14] S. Lang, *Algebra*, Addison-Wesley Publishing Company, 1993. 8, 12, 13, 23

[15] D. A. Marcus, *Number fields*, Springer-Verlag, 1977. 12

[16] F. Pappalardi, M. Sha, I. E. Shparlinski and C. L. Stewart, 'On multiplicatively dependent vectors of algebraic numbers', *Trans. Amer. Math. Soc.*, **370** (2018), 6221–6244. 2

[17] C. Pomerance, 'The role of smooth numbers in number theoretic algorithms', *Proc. Intern. Cong. of Math. (Zurich, 1994)*, Vol.1, Birkhäuser, 1995, 411–422. 2

[18] C. Pomerance, 'Multiplicative independence for random integers', *Analytic number theory (Allerton Park, IL, 1995)*, Vol.2, Progr. Math. **139** Birkhäuser, 1996, 703–711. 2

[19] N. Rome, 'The Hasse norm principle for biquadratic extensions', *J. Théorie Nombres Bordeaux*, (to appear). 1, 2, 3, 7

[20] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Grad. Studies Math., vol. 163, Amer. Math. Soc., 2015. 21

[21] G. Tenenbaum, J. Wu, *Théorie analytique et probabiliste des nombres, 307 exercices corrigés*, coll. Échelles, Berlin, 2014. 19

[22] D. I. Tolev, 'On the number of pairs of positive integers $x_1, x_2 \leqslant H$ such that x_1x_2 is a k-th power', *Pacific J. Math.*, **249** (2011), 495–507. 1, 4

[23] S. Wong, 'Densities of quartic fields with even Galois group', *Proc. Amer. Math. Soc.*, **133** (2005), n 2873–2881. 3

[24] D. J. Wright, 'Distribution of discriminants of abelian extensions', *Proc. London Math. Soc.* (3) **58** (1989), no. 1, 17–50. 3, 7

Institut de Mathématiques de Jussieu, UMR 7586, Université Paris-Diderot, UFR de Mathématiques, case 7012, Bâtiment Sophie Germain, 75205 Paris Cedex 13, France

E-mail address: regis.de-la-breteche@imj-prg.fr

Department of Mathematics, Royal Institute of Technology, SE-100 44 Stockholm, Sweden

E-mail address: kurlberg@math.kth.se

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au