COUNTING DIHEDRAL AND QUATERNIONIC EXTENSIONS

ÉTIENNE FOUVRY, FLORIAN LUCA, FRANCESCO PAPPALARDI AND IGOR E. SHPARLINSKI

Abstract. We give asymptotic formulas for the number of biquadratic extensions of $\mathbb{Q}$ that admit a quadratic extension which is a Galois extension of $\mathbb{Q}$ with a prescribed Galois group, for example, with a Galois group isomorphic to the Quaternionic group. Our approach is based on a combination of the theory of quadratic equations with some analytic tools such as the Siegel–Walfisz theorem and double oscillations theorems.

Contents

Date: November 25, 2009.
1991 *Mathematics Subject Classification.* Primary 11R11, 11R16, Secondary 11D09, 11L40.

1. Introduction

1.1. **Background.** The problem of enumerating Galois extensions of a given field has increasingly attracted the attention of several researchers. Very strong and difficult conjectures due to Malle (see [11, 12]) predict the precise distribution of the number of extensions with discriminant in absolute value not exceeding a certain bound and whose Galois closure over a fixed ground field has a given Galois group. Here, we take a different point of view, namely we fix the Galois group but let the ground field vary.

More precisely, we want to enumerate biquadratic extensions of $\mathbb{Q}$ that admit a quadratic extension with given Galois group over $\mathbb{Q}$. These extension have been characterized explicitly by Kiming in [8], where he gives explicit realizations of several extensions of fields of odd characteristics with given Galois structures. We use several parts of the work [8] here. The special classical case of Quaternionic extensions has been studied extensively (see, for example, [7, 13, 17]).

Let $\mathcal{F}$ be the set of pairs (m,n) of distinct squarefree positive integers with $m>1, n>1$. For a fixed group H of order 8, we define $\mathcal{F}_H$ as the subset of $(m,n)\in\mathcal{F}$ such that $\mathbb{Q}(\sqrt{m},\sqrt{n})$ admits a quadratic extension $\mathbb{K}$ with

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q})\cong H.$$

It is well known (see, for example, [1, page 170]) that there are 5 possibilities for H, namely

$$C_2\times C_2\times C_2,\quad C_4\times C_2,\quad C_8,\quad D_4,\quad \mathbb{H},$$

where C_m stands for the cyclic group of order m, D_4 is the group of the symmetries of the square, and $\mathbb{H}$ denotes the Quaternionic group.

It is quite easy to see that $\mathcal{F}_{C_2\times C_2\times C_2}=\mathcal{F}$. In fact, for any $(m,n)\in\mathcal{F}$ and any squarefree integer $a>1$ coprime to mn, the extension $\mathbb{Q}(\sqrt{m},\sqrt{n},\sqrt{a})$ has Galois group over $\mathbb{Q}$ isomorphic to $C_2\times C_2\times C_2$. Hence, $(m,n)\in\mathcal{F}_{C_2\times C_2\times C_2}$.

It is also clear that $\mathcal{F}_{C_8}=\emptyset$, since the cyclic group C_8 cannot admit the non cyclic quotient $C_2\times C_2$.

From now on, we concentrate on the remaining cases of the groups $C_4\times C_2$, D_4 and $\mathbb{H}$.

1.2. **Our results.** For a subset $\mathcal{A}$ of $\mathbb{N}^2$ and a positive real number T, we write $\mathcal{A}(T)$ for the set of $(a,b)\in\mathcal{A}$ with $a\le T$ and $b\le T$. Analogously, if $\mathcal{B}\subseteq\mathbb{N}$, we write $\mathcal{B}(T)$ for the set of $b\in\mathcal{B}$ with $b\le T$.

We recall that

$$\sharp\,\mathcal{F}(T)=\frac{36}{\pi^4}T^2+O(T^{3/2}),\qquad \text{as } T\to\infty$$

(see [6, Theorem 333]).

Let

$$\vartheta=\frac{1}{\sqrt{2}}\prod_{\substack{q \text{ prime}\\ q\equiv 3 \bmod 4}}\left(1-\frac{1}{q^2}\right)^{-1/2}=0.764223\ldots. \tag{1}$$

be the Landau–Ramanujan constant. We also define

$$\rho=\prod_{p\ge 3}\left(1+\frac{1}{2p(p+1)}\right)=1.084095\ldots. \tag{2}$$

In this paper, we prove the following results:

Theorem 1. *We have*

$$\sharp\,\mathcal{F}_{C_2\times C_4}(T) = \left(\frac{72\vartheta}{\pi^4} + o(1)\right)\frac{T^2}{\sqrt{\log T}}, \qquad \text{as } T\to\infty,$$

where ϑ is given by (1).

Theorem 2. *We have*

$$\sharp\,\mathcal{F}_{D_4}(T) = \left(\frac{33\rho}{\pi^3} + o(1)\right)\frac{T^2}{\log^2 T}, \qquad \text{as } T\to\infty,$$

where ρ is given by (2).

Theorem 3. *We have*

$$\sharp\,\mathcal{F}_{\mathbb{H}}(T) = \left(\frac{7\rho}{\pi^3} + o(1)\right)\frac{T^2}{\log^2 T}, \qquad \text{as } T\to\infty,$$

where ρ is given by (2).

Let $\widetilde{\mathcal{F}}$ be the set of pairs (m,n) of coprime natural numbers, $m>1, n>1$, which are odd and squarefree. In analogy with the above, for a fixed group H of order 8 we define $\widetilde{\mathcal{F}}_H$ as the set of $(m,n)\in\widetilde{\mathcal{F}}$ such $\mathbb{Q}(\sqrt{m},\sqrt{n})$ admits a quadratic extension $\mathbb{K}$ with

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong H.$$

Theorem 4. *The following asymptotic formula holds*

$$\sharp\,\widetilde{\mathcal{F}}_{\mathbb{H}}(T) = \left(\frac{2}{\pi^3} + o(1)\right)\frac{T^2}{\log T}, \qquad \text{as } T\to\infty.$$

Theorem 5. *The following asymptotic formula holds*

$$\sharp\,\widetilde{\mathcal{F}}_{D_4}(T) = \left(\frac{18}{\pi^3} + o(1)\right)\frac{T^2}{\log T}, \qquad \text{as } T\to\infty.$$

We also point out that there is another way to count the extensions $\mathbb{K}$ satisfying

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \sim \mathbb{H}.$$

It consists in ordering the fields $\mathbb{K}$ according to the value of $|\mathrm{Disc}\,(\mathbb{K}/\mathbb{Q})|$. Klüners in [9, Satz 7.2] has shown that for some positive constant c_1 one has

$$\sharp\,\{\mathbb{K}\subseteq\mathbb{C}\,;\ |\mathrm{Disc}\,(\mathbb{K}/\mathbb{Q})|\le T,\ \mathrm{Gal}(\mathbb{K}/\mathbb{Q})\sim\mathbb{H}\} \sim c_1\,T^{\frac14}, \qquad \text{as } T\to\infty.$$

This proves Malle's Conjecture [12] for the Quaternionic group $\mathbb{H}$. The analogue conjecture for the group D_4 states that there exists a positive constant c_2 such that

$$\sharp\,\{\mathbb{K}\subseteq\mathbb{C}\,;\ |\mathrm{Disc}\,(\mathbb{K}/\mathbb{Q})|\le T,\ \mathrm{Gal}(\mathbb{K}/\mathbb{Q})\sim D_4\} \sim c_2\,T^{\frac14}\log^2 T, \qquad \text{as } T\to\infty.$$

This conjecture is still unproven, as far as we know.

1.3. **Notation.** We recall that $U=O(V)$, $U\ll V$ and $V\gg U$ are all equivalent to the statement that the inequality $|U|\le c\,V$ holds with some constant $c>0$. Sometimes we write $U=O_\lambda(V)$, $U\ll_\lambda V$ and $V\gg_\lambda U$ to emphasise that the implied constant may depend on a certain parameter λ.

For a positive integer n we write $\mu(n)$, $\omega(n)$, and $\varphi(n)$ with their standard meaning as being the Möbius function of n, the number of distinct prime factors of n, and the Euler function of n, respectively.

Finally, we write $\gcd(a,b)$ for the greatest common divisor of integers a and b.

2. Squarefree numbers with congruence conditions

2.1. **Necessary results.** Let m and n, two integers, coprime or not, such that n is nonzero and squarefree. We say that m is a *square modulo* n if and only if the equation $x^2 \equiv m \bmod n$ is solvable. This is equivalent to the fact that for every odd prime p dividing n, we have $(\frac{m}{p}) = 0$ or 1, where $(\frac{\bullet}{p})$ is the Legendre symbol with respect to p. We write that condition as $m \equiv \square \bmod n$.

A recent result due to Friedlander and Iwaniec [4, Theorem 1] states that for any fixed $\delta > 0$ and uniformly for A, $B \geq \exp\left((\log AB)^{\delta}\right)$, we have the estimate

(3)
$$\begin{aligned}\sharp\{(a,b)\,;\ &1 \leq a \leq A,\, 1 \leq b \leq B,\\ &\mu^2(2ab) = 1, a \equiv \square \bmod b \,\&\, b \equiv \square \bmod a\}\\ &= \frac{AB}{\sqrt{\log A}\sqrt{\log B}}\left(\frac{6}{\pi^3} + O_\delta\left(\frac{1}{\log A} + \frac{1}{\log B}\right)\right).\end{aligned}$$

The above result can be interpreted in terms of the solvability of a ternary quadratic equation. The following classical theorem due to Legendre, which dates back to 1795, gives necessary and sufficient conditions for the existence of a nontrivial zero of a diagonal quadratic form (see, for example, [16, Chapter 4, Appendix I]).

Proposition 1. *Let a, b and c be pairwise coprime nonzero integers which are squarefree and are not all of the same sign. Then the equation*

$$aX^2 + bY^2 + cZ^2 = 0 \tag{4}$$

has a nonzero integer solution (X, Y, Z) if and only if following three conditions are satisfied: $-ab \equiv \square \bmod c$, $-ac \equiv \square \bmod b$ and $-bc \equiv \square \bmod a$.

Results like the aforementioned asymptotic formula (3) due to Friedlander and Iwaniec are not new in the literature. Let us mention here the work of Guo [5], where the solvability of the ternary equation (4) with free parameters a, b and c having absolute values not exceeding T is studied, as well as the work of the first author with Klüners [2, Theorem 5], where the authors investigate the solvability of equation (4) under the constraints $c = -1$ and $|ab| \leq T$, and interpret their results in terms of the average behavior of the value of the 4–rank of the ideal class group of quadratic fields.

It is natural to notice that the analytic tools appearing in the proofs of the main results in [2], [4] and [5] are all of the same nature: the use of Jacobi symbols as characters, the Siegel–Walfisz theorem for these characters, and double oscillations theorem. We review these tools in Lemmas 1 and 2 below.

The main result of [4, Theorem 1] is too precise for our purposes. Here, we restrict our attention to the case $A = B = T$. However, we require some variations of the statement we mentioned above. More precisely, we prove and use the following proposition.

Proposition 2. *Let $\widetilde{\mathcal{F}}(T) = \{(a,b) \in \mathbb{N}^2\,;\, 1 \leq a,\ b \leq T,\ \mu^2(2ab) = 1\}$. Then, as $T \to \infty$, we have the following asymptotic formulas:*

$$\begin{aligned}
\sharp \left\{(a,b) \in \widetilde{\mathcal{F}}(T);\, a \equiv \square \bmod b \,\&\, b \equiv \square \bmod a\right\} \quad &\sim \quad \frac{6}{\pi^3} \cdot \frac{T^2}{\log T},\\
\sharp \left\{(a,b) \in \widetilde{\mathcal{F}}(T);\, -a \equiv \square \bmod b \,\&\, b \equiv \square \bmod a\right\} \quad &\sim \quad \frac{6}{\pi^3} \cdot \frac{T^2}{\log T},\\
\sharp \left\{(a,b) \in \widetilde{\mathcal{F}}(T);\, -a \equiv \square \bmod b \,\& \ -b \equiv \square \bmod a\right\} \quad &\sim \quad \frac{2}{\pi^3} \cdot \frac{T^2}{\log T}.
\end{aligned}$$

Note 1. *It is worth noticing that if the pair (a,b) is an element of the set appearing in the left hand side of the last asymptotic formula of Proposition 2, we then necessarily have*

$$a \equiv b \equiv 1 \bmod 4.$$

Indeed, this is a straightforward consequence of the Quadratic Reciprocity Law.

For the proof of Theorem 2, we decompose

$$\mathcal{F} = \mathcal{F}^{11} \bigsqcup \mathcal{F}^{22} \bigsqcup \mathcal{F}^{12} \bigsqcup \mathcal{F}^{21},$$

where

$$\mathcal{F}^{ij} = \{(a,b) \in \mathcal{F} :\ a \equiv i \bmod 2, b \equiv j \bmod 2\}.$$

Let ϵ and η be in $\{\pm 1\}$ with

$$(\epsilon, \eta) \neq (-1,-1).$$

We need to study the cardinality $N^{ij}_{\epsilon,\eta}(T)$ of the set of pairs $(a,b) \in \mathcal{F}^{ij}(T)$ satisfying the property that the ternary form

$$X^2 - \epsilon a Y^2 - \eta b Z^2 = 0 \tag{5}$$

has a nontrivial integer solution (X,Y,Z).

We write $d = \gcd(a,b)$, so that $m = a/d$, $n = b/d$, and d are mutually coprime. Note that equation (5) admits a nontrivial solution if and only if the equation

$$dX^2 - \epsilon m Y^2 - \eta n Z^2 = 0 \tag{6}$$

admits a nontrivial solution. To the above form, we can apply Proposition 1, since the integers d, $-\epsilon m$ and $-\eta n$ are squarefree, mutually coprime, and not of the same sign. Hence,

$$\begin{aligned}
&N^{ij}_{\epsilon,\eta}(T)\\
&\quad = \sharp \left\{(a,b) \in \mathcal{F}^{ij}(T) \ :\ \epsilon a \equiv \square \bmod \frac{b}{d},\ \eta b \equiv \square \bmod \frac{a}{d},\ -\epsilon\eta \frac{ab}{d^2} \equiv \square \bmod d\right\}.
\end{aligned}$$

Furthermore, we use the last expression to define $N^{ij}_{\epsilon,\eta}(T)$ also in the case when

$$(\epsilon, \eta) = (-1,-1).$$

Proposition 3. *For each $i, j \in \{1,2\}$ and $\epsilon, \eta \in \{\pm 1\}$, the following asymptotic formula*

$$N^{ij}_{\epsilon,\eta}(T) \sim \frac{\alpha}{ij} \cdot \frac{\rho}{\pi^3} \cdot \frac{T^2}{\log T}$$

holds as $T \to \infty$, where

$$\alpha = \begin{cases} 4, & \text{if } (i,j) \neq (1,1), \\ 6, & \text{if } (i,j) = (1,1) \text{ and } (\epsilon,\eta) \neq (-1,-1), \\ 2, & \text{if } (i,j) = (1,1) \text{ and } (\epsilon,\eta) = (-1,-1). \end{cases}$$

The following upper bound is useful in the proof of Theorem 5.

Proposition 4. *Let $\mathcal{F}(T) = \{(a,b) \in \mathbb{N}^2\,;\, 1 < a,\ b \leq T,\ \mu^2(a) = \mu^2(b) = 1\}$. Uniformly in $T \geq 2$ we have*

$$\sharp\, \{(a,b) \in \mathcal{F}(T);\, a \text{ and } -a \equiv \square \bmod b \,\&\, b \equiv \square \bmod a\} \ll \frac{T^2}{\log^{5/4} T}.$$

Note 2. *With a bit more care, the cardinality of the set studied in Proposition 4 can be shown to be $(\beta + o(1))\, T^2 \log^{-5/4} T$ for some positive constant β as $T \to \infty$.*

2.2. **Preparations.** The proofs of Propositions 2 and 3 are quite similar and are based on estimates of some auxiliary sums.

We extract from [4] two technical results which we use throughout this section. The first one is a variant of Siegel's theorem concerning the distribution of primes in arithmetic progressions. This appears as [4, Corollary 2]. Let us define

$$c(r) = \pi^{-\frac{1}{2}} \prod_{p \geq 2} \left(1 + \frac{1}{2p}\right) \left(1 - \frac{1}{p}\right)^{\frac{1}{2}} \prod_{p \mid r} \left(1 + \frac{1}{2p}\right)^{-1}. \tag{7}$$

Lemma 1. *Let $\gcd(ad, q) = 1$, where $q = q_1 q_2$, with $(q_1, q_2) = 1$. For a character χ_2 modulo q_2 and for any constant C, we have the equality*

$$\sum_{\substack{n \leq x \\ \gcd(n,d)=1 \\ n \equiv a \bmod q_1}} \mu^2(n) \frac{\chi_2(n)}{2^{\omega(n)}} = \delta_{\chi_2} \cdot \frac{c(dq)}{\varphi(q_1)} \cdot \frac{x}{\sqrt{\log x}} \left(1 + O\left(\frac{(\log\log 3dq)^{\frac{3}{2}}}{\log x}\right)\right)$$
$$+ O_C(2^{\omega(d)} q x (\log x)^{-C})$$

where δ_{χ_2} is equal to 1 or 0 according to whether χ_2 is principal or not, and $c(r)$ is defined by (7).

The second result deals with double sums of Jacobi symbols. This is [4, Lemma 2].

Lemma 2. *Let α_m and β_n be any complex numbers supported on odd integers and bounded by 1 in absolute value. We then have*

$$\sum_{m \leq M} \sum_{n \leq N} \alpha_m \beta_n \left(\frac{m}{n}\right) \ll MN(M^{-1/6} + N^{-1/6})(\log 3MN)^{7/6},$$

where the implied constant is absolute.

We now define a sum which plays a key role in the proof of Proposition 2.

$$M(T, a_0, c_0) = \sum\sum_{\substack{ab \leq T \\ a \equiv a_0 \bmod 4,}} \sum\sum_{\substack{cd \leq T \\ c \equiv c_0 \bmod 4}} \frac{\mu^2(2abcd)}{2^{\omega(ab)} \cdot 2^{\omega(cd)}} \left(\frac{d}{a}\right) \left(\frac{b}{c}\right). \tag{8}$$

In the next statement, we use Lemmas 1 and 2 in order to find the asymptotic behavior of the sum $M(T, a_0, c_0)$ appearing in (8) as $T \to \infty$.

Lemma 3. *Let a_0 and c_0 be two odd integers. The asymptotic*

$$M(T, a_0, c_0) \sim \begin{cases} \dfrac{5}{\pi^3} \cdot \dfrac{T^2}{\log T}, & \text{if } (a_0, c_0) \equiv (1,1) \bmod 4, \\ \\ \dfrac{1}{\pi^3} \cdot \dfrac{T^2}{\log T}, & \text{if } (a_0, c_0) \not\equiv (1,1) \bmod 4 \end{cases}$$

holds as $T \to \infty$.

Proof. We let $V \geq 3$ be some parameter depending on T to be specified later. The contribution of the pairs (a, b) such that $\max\{a, b\} \leq V$ to the sum M is trivially

$$M_1 \leq T^{1+o(1)} V^2, \qquad \text{as } T \to \infty. \tag{9}$$

Similarly, the contribution of the pairs (c, d) such that $\max\{c, d\} \leq V$ to the sum M is

$$M_2 \leq T^{1+o(1)} V^2, \qquad \text{as } T \to \infty. \tag{10}$$

To estimate the contribution of the quadruples (a, b, c, d) with $\max\{a, d\} \leq V$ to the sum M, we apply Lemma 2 to the Jacobi symbol $\left(\frac{b}{c}\right)$. Hence, this contribution satisfies

$$M_3 \ll \sum_{a \leq V} \sum_{d \leq V} \frac{T^2}{ad} \left(a^{1/6} T^{-1/6} + d^{1/6} T^{-1/6}\right) \log^{7/6} T \ll T^{11/6} V^{1/6} \log^{13/6} T.$$

Similarly, we see that the contribution of the quadruples (a, b, c, d) with $\max\{b, c\} \leq V$ also satisfies

$$M_4 \ll T^{11/6} V^{1/6} \log^{13/6} T,$$

by applying Lemma 2 to the Jacobi symbol $\left(\frac{d}{a}\right)$.

When $a > V$ and $d > V$, since these two variables are now large, we apply Lemma 2 to the Jacobi symbol $\left(\frac{d}{a}\right)$. That lemma shows that the contribution of such quadruples (a, b, c, d) to the sum M is

$$M_5 \ll \sum_{b < T/V} \sum_{c < T/V} \frac{T^2}{bc} \cdot V^{-1/6} \log^{7/6} T \ll T^2 V^{-1/6} \log^{19/6} T.$$

The same applies to the contribution M_6 to M of the quadruples (a, b, c, d) with $b > V$ and $c > V$, namely

$$M_6 \ll \sum_{a < T/V} \sum_{d < T/V} \frac{T^2}{ad} \cdot V^{-1/6} \log^{7/6} T \ll T^2 V^{-1/6} \log^{19/6} T.$$

We now choose V to be a large power of the logarithm of T. More precisely, we put

$$V = \log^{60} T, \tag{11}$$

and from the estimates for $M_1, \ldots, M_6$ above, we see that the contributions from all these previously counted terms satisfy

$$M_i \ll T^2 \log^{-2} T, \qquad i = 1, \ldots, 6. \tag{12}$$

So, we are left to deal with two more cases, namely when

$$a \leq V, \quad b \geq V, \quad c \leq V, \quad d \geq V,$$

and when

$$a \geq V, \quad b \leq V, \quad c \geq V, \quad d \leq V.$$

Recalling our estimates (9) and (10) on M_1 and on M_2, we see these two cases can be reduced to

$$a \le V,\ c \le V, \tag{13}$$

and

$$b \le V,\ d \le V, \tag{14}$$

respectively.

Note that, due to the congruence restrictions $a \equiv a_0 \bmod 4$ and $c \equiv c_0 \bmod 4$, the cases (13) and (14) are not entirely symmetrical, so we need to analyze each one of them separately.

The case (13). We write the contribution of the quadruples (a, b, c, d) satisfying (13) to the sum M in the form

$$M_{(13)}(a_0, c_0) = \sum_{\substack{a \le V \\ a \equiv a_0 \bmod 4}} \sum_{\substack{c \le V \\ c \equiv c_0 \bmod 4}} \frac{\mu^2(2ac)}{2^{\omega(ac)}} S(a, c), \tag{15}$$

where

$$S(a, c) = \sum_{\substack{b \le T/a \\ \gcd(b, 2ac) = 1}} \frac{\mu^2(b)}{2^{\omega(b)}} \left(\frac{b}{c}\right) \sum_{\substack{d \le T/c \\ \gcd(d, 2abc) = 1}} \frac{\mu^2(d)}{2^{\omega(d)}} \left(\frac{d}{a}\right).$$

We now apply Lemma 1 to evaluate $S(a, c)$ according to the values of a and c.

- When $a \ne 1$, we apply Lemma 1 with χ_2 being the quadratic character modulo a, and then sum trivially over b. Using the fact that $\omega(abc) \le \omega(ac) + \omega(b)$, we get

$$S(a, c) \ll_C \frac{T^2}{ac} 2^{\omega(ac)} (\log T)^{-C} \tag{16}$$

  for any $C > 0$.
- When $c \ne 1$, inside $S(a, c)$ we interchange the roles of b and d and then apply Lemma 1 with χ_2 being the quadratic character modulo c. This gives

$$S(a, c) \ll_C \frac{T^2}{ac} 2^{\omega(ac)} (\log T)^{-C} \tag{17}$$

  for any $C > 0$.
- When $a = c = 1$, we then necessarily have $a_0 \equiv c_0 \equiv 1 \bmod 4$. We then obtain the equality

$$S(1, 1) = \sum_{b \le T} \sum_{d \le T} \frac{\mu^2(2bd)}{2^{\omega(b)} \cdot 2^{\omega(d)}}.$$

  We want to make the variables b and d free from the coprimality condition, so we use Möbius inversion formula and replace b by $b\delta$ and d by $d\delta$ to get the identity

$$S(1, 1) = \sum_{\delta \text{ odd}} \frac{\mu(\delta)}{4^{\omega(\delta)}} \left(\sum_{b \le T/\delta} \frac{\mu^2(2b\delta)}{2^{\omega(b)}} \right)^2.$$

An application of Lemma 1 with $d = 2\delta$ and $q_1 = q_2 = 1$ leads to the relation

$$\begin{aligned} S(1,1) &= (1+o(1)) \sum_{\substack{\delta \text{ odd} \\ \delta \le \log^{100} T}} \frac{\mu(\delta)}{4^{\omega(\delta)}} \left(c(2\delta) \frac{T/\delta}{\sqrt{\log(T/\delta)}} \right)^2 \\ &+ O\left(\sum_{\delta > \log^{100} T} \frac{T^2}{\delta^2} \right), \qquad \text{as } T \to \infty. \end{aligned}$$

This immediately gives

$$S(1,1) \sim \frac{T^2}{\log T} \sum_{\delta \text{ odd}} \frac{\mu(\delta) c(2\delta)^2}{4^{\omega(\delta)} \delta^2}, \qquad \text{as } T \to \infty. \tag{18}$$

To compute the infinite series appearing in (18), we use the following identity

$$c(2\delta) = \frac{4}{5} c(1) \prod_{p \mid \delta} \left(1 + \frac{1}{2p}\right)^{-1} \qquad (2 \nmid \delta).$$

Inserting the above formula into (18) leads to the equality

$$\sum_{\delta \text{ odd}} \frac{\mu(\delta) c(2\delta)^2}{4^{\omega(\delta)} \delta^2} = \frac{16}{25} c(1)^2 \prod_{p \ge 3} \left(1 - \frac{1}{4p^2(1+1/2p)^2}\right) = \frac{4}{\pi^3}. \tag{19}$$

Collecting (15), (16), (17), (18) and (19), summing over a and c and choosing $C = 1000$, we finally get the estimate

$$M_{(13)}(a_0, c_0) = \begin{cases} \dfrac{4}{\pi^3} \cdot \dfrac{T^2}{\log T}(1+o(1)) & \text{for } (a_0, c_0) = (1,1), \qquad \text{as } T \to \infty, \\[2ex] O\left(\dfrac{T^2}{\log^2 T}\right), & \text{otherwise.} \end{cases} \tag{20}$$

The case (14). We write the contribution of the quadruples (a, b, c, d) satisfying (14) to the sum M in the form

$$M_{(14)}(a_0, c_0) = \sum_{b \le V} \sum_{d \le V} \frac{\mu^2(2bd)}{2^{\omega(bd)}} S^*(b, d, a_0, c_0), \tag{21}$$

where

$$S^*(b, d, a_0, c_0) = \sum_{\substack{a \le T/b \\ \gcd(a, 2bd) = 1}} \frac{\mu^2(a)}{2^{\omega(a)}} \left(\frac{d}{a}\right) \sum_{\substack{c \le T/d \\ \gcd(c, 2abd) = 1}} \frac{\mu^2(c)}{2^{\omega(c)}} \left(\frac{b}{c}\right).$$

Recall that the variables a and c satisfy the congruence conditions $a \equiv a_0 \bmod 4$ and $c \equiv c_0 \bmod 4$. The sums $S^*(b, d, a_0, c_0)$ can be studied with the techniques of Section 2.2. In particular, we apply Lemma 1 with $q_1 = 4$ and $a = a_0$, or $a = c_0$. We remark that the main term has its origin in the contribution of the pair $(b, d) = (1, 1)$. After that, by (21), we finally arrive at the estimate

$$M_{(14)}(a_0, c_0) = \frac{1}{\pi^3} \cdot \frac{T^2}{\log T}(1 + o(1)), \qquad \text{as } T \to \infty, \tag{22}$$

which is valid for any a_0 and $c_0 \equiv \pm 1 \bmod 4$.

From (12), we get

$$M(a_0, c_0) = M_{(13)}(a_0, c_0) + M_{(14)}(a_0, c_0) + O(T \log^{-2} T).$$

Combining the above estimate with (20) and (22), we complete the proof. □

Next, we define a sum which is analogous to the sum $M(T, a_0, c_0)$ appearing in (8) but somewhat more involved. For $i, j \in \{1, 2\}$ we put

$$\begin{aligned}M^{ij}(T, m_0, n_0, d_0) = & \sum\sum\sum\sum\sum\sum_{\substack{d_1,d_2,m_1,m_2,n_1,n_2\in\mathbb{N}\\ \max\{im_1m_2,jn_1n_2\}\le T/(d_1d_2)\\ (d_1,m_1,n_1)\equiv(d_0,m_0,n_0) \bmod 8}} \frac{\mu^2(2m_1m_2n_1n_2d_1d_2)}{2^{\omega(m_1m_2n_1n_2d_1d_2)}}\\ & \cdot \left(\frac{d_2m_2}{n_1}\right)\left(\frac{d_2n_2}{m_1}\right)\left(\frac{n_2m_2}{d_1}\right).\end{aligned} \tag{23}$$

The next statement gives an asymptotic estimate for the sum $M^{ij}(T, m_0, n_0, d_0)$ appearing in (23).

Lemma 4. *Let d_0, m_0, and n_0 be three odd integers, put*

$$\rho_{d_0} = \sum_{\substack{d\in\mathbb{N}\\ d\equiv d_0 \bmod 8}} \mu^2(d) \prod_{p\mid d} \frac{1}{2p(p+1)},$$

and assume that $i, j \in \{1, 2\}$. Then, as $T \to \infty$, we have

$$\begin{aligned}&M^{ij}(T, d_0, m_0, n_0)\\ &\sim \frac{4}{\pi^3}\cdot\frac{1}{ij}\cdot\frac{T^2}{\log T}\cdot\begin{cases}\left(\rho + \dfrac{1}{16}\rho_{d_0}\right), & \text{if } (d_0, m_0, n_0) \equiv (1,1,1) \bmod 8,\\[2mm] \dfrac{1}{16}\rho_{d_0}, & \text{if } (d_0, m_0, n_0) \not\equiv (1,1,1) \bmod 8,\end{cases}\end{aligned}$$

where ρ is given by (2).

Proof. This proof is very similar to the proof of Lemma 3, so we skip some of the details. Observe first from the definition of $M^{ij}(T, m_0, n_0, d_0)$ in (23) that we can assume that $d_1 d_2 \le T$. We next introduce a parameter V_0 and decompose

$$M^{ij}(T, m_0, n_0, d_0) = M^{ij}_{\le V_0}(T, m_0, n_0, d_0) + M^{ij}_{>V_0}(T, m_0, n_0, d_0), \tag{24}$$

where the first and second terms respectively correspond to the extra conditions $\max\{d_1, d_2\} \le V_0$ and $\max\{d_1, d_2\} > V_0$. Writing $m = m_1 m_2$, and $n = n_1 n_2$, we trivially have

$$\left|M^{ij}_{>V_0}(T, m_0, n_0, d_0)\right| \le \sum\sum_{\max\{d_1,d_2\}>V_0} \sum\sum_{m,n\le T/(d_1d_2)} 1 \le 2T^2 \sum_{d_1<T} \frac{1}{d_1^2} \sum_{d_2>V_0} \frac{1}{d_2^2},$$

which finally gives

$$M^{ij}_{>V_0}(T, m_0, n_0, d_0) \ll T^2 V_0^{-1}. \tag{25}$$

We fix

$$V_0 = V = \log^{60} T$$

(see (11)). By (24) and (25), we see that the proof of Lemma 4 is reduced to prove the same result but for $M^{ij}_{\le V_0}(T, m_0, n_0, d_0)$.

By a straightforward adaptation of the arguments used at the beginning of Lemma 3 (where m_1, m_2, n_1, n_2 and $T/(d_1d_2)$ play the roles of a, b, c, d and T, respectively), one shows that for fixed d_1 and d_2 the contribution of the quadruples (m_1, m_2, n_1, n_2) to the sum $M^{ij}_{\le V_0}(T, m_0, n_0, d_0)$ is

$$O((T/d_1d_2)^2 \log^{-2}(T/d_1d_2)) = O((T/d_1d_2)^2 \log^{-2} T)$$

(see (12)), except if either

$$m_1 \le V,\ m_2 \ge V,\ n_1 \le V,\ n_2 \ge V, \tag{26}$$

or

$$m_1 \ge V,\ m_2 \le V,\ n_1 \ge V,\ n_2 \le V. \tag{27}$$

Summing over all pairs of positive integers (d_1, d_2) such that $\max\{d_1, d_2\} \le V_0$ gives the total contribution of the order

$$\sum_{d_1,\, d_2 \le V_0} \frac{T^2}{(d_1d_2)^2 \log^2 T} \ll \frac{T^2}{\log^2 T}$$

from all the cases, except from (26) and (27). Hence, we see that the total contribution from all the sextuples $(m_1, n_1, m_2, n_2, d_1, d_2)$ to the sum $M^{ij}_{\le V_0}(T, m_0, n_0, d_0)$ is $O(T^2 \log^{-2} T)$, except if either

$$m_1 \le V,\ n_1 \le V,\ m_2 \ge V,\ n_2 \ge V,\ d_1 \le V,\ d_2 \le V, \tag{28}$$

or

$$m_1 \ge V,\ n_1 \ge V,\ m_2 \le V,\ n_2 \le V,\ d_1 \le V,\ d_2 \le V. \tag{29}$$

We analyze only the above two cases (28) and (29) in detail.

The case (28). The contribution to the sum $M^{ij}_{<V_0}(T, m_0, n_0, d_0)$ of the sextuples in this case is

$$M^{ij}_{(28)}(T, m_0, n_0, d_0) = \sum_{\substack{\max\{m_1,n_1,d_1\}\le V\\ d_1\equiv d_0 \bmod 8\\ m_1\equiv m_0 \bmod 8\\ n_1\equiv n_0 \bmod 8}} \frac{\mu^2(2m_1n_1d_1)}{2^{\omega(m_1n_1d_1)}} S(m_1, n_1, d_1),$$

where

$$\begin{aligned} S(m_1, n_1, d_1) &= \sum_{\substack{d_2\le V\\ V<m_2\le T/(im_1d_1d_2)\\ V<n_2\le T/(jn_1d_1d_2)}} \frac{\mu^2(2m_1m_2n_1n_2d_1d_2)}{2^{\omega(m_2n_2d_2)}} \left(\frac{d_2m_2}{n_1}\right)\left(\frac{d_2n_2}{m_1}\right)\left(\frac{n_2m_2}{d_1}\right) \\ &= \sum_{\substack{d_2\le V\\ V<m_2\le T/(im_1d_1d_2)}} \frac{\mu^2(2m_1m_2n_1d_1d_2)}{2^{\omega(m_2d_2)}} \left(\frac{d_2}{n_1m_1}\right)\left(\frac{m_2}{n_1d_1}\right) \\ &\qquad \sum_{\substack{V<n_2\le T/(jn_1d_1d_2)\\ \gcd(n_2,2m_1m_2n_1d_1d_2)=1}} \frac{\mu^2(n_2)}{2^{\omega(n_2)}} \left(\frac{n_2}{m_1d_1}\right). \end{aligned}$$

We now apply Lemma 1 to evaluate the last sum above according to the value of m_1, n_1 and d_1.

- If $m_1d_1 \neq 1$, we consider the Jacobi character $\left(\frac{n_2}{m_1d_1}\right)$. Lemma 1 yields

$$\begin{aligned} S(m_1,n_1,d_1) &\ll_C \sum_{d_2\le V}\sum_{m_2\le T/(im_1d_1d_2)} \frac{T}{n_1d_1d_2}2^{\omega(m_1n_1d_1)}(\log T)^{-C} \\ &\ll_C \frac{2^{\omega(m_1n_1d_1)}}{m_1n_1d_1^2}\cdot\frac{T^2}{\log^C T}. \end{aligned} \tag{30}$$

- If $n_1d_1 \neq 1$, inside $S(m_1,n_1,d_1)$ we invert the roles of m_2 and n_2 and apply Lemma 1 to the Jacobi character $\left(\frac{m_2}{n_1d_1}\right)$ obtaining

$$S(m_1,n_1,d_1) \ll_C \frac{2^{\omega(m_1n_1d_1)}}{m_1n_1d_1^2}\cdot\frac{T^2}{\log^C T}. \tag{31}$$

- If $m_1 = n_1 = d_1 = 1$, which can only happen when $m_0 = n_0 = d_0 = 1$, we are lead to the sum

$$S(1,1,1) = \sum_{d\le V}\sum_{V\le m_2\le T/(jd)}\sum_{V\le n_2\le T/(jd)} \frac{\mu^2(2m_2n_2d)}{2^{\omega(m_2n_2d)}}.$$

We make the variables m_2 and n_2 free from the coprimality condition by using the Möbius inversion formula. Thus, replacing m_2 and n_2 by em_2 and en_2, respectively, we get

$$\begin{aligned} S(1,1,1) \quad = \quad & \sum_{d\le V}\frac{\mu^2(2d)}{2^{\omega(d)}}\sum_{\substack{e\in\mathbb{N}\\ \gcd(e,2d)=1}}\frac{\mu(e)}{2^{2\omega(e)}} \\ & \sum_{\substack{V/e\le m_2\le T/(ied)\\ \gcd(m_2,2ed)=1}}\frac{\mu^2(m_2)}{2^{\omega(m_2)}}\sum_{\substack{V/e\le n_2\le T/(jed)\\ \gcd(n_2,2ed)=1}}\frac{\mu^2(n_2)}{2^{\omega(n_2)}}. \end{aligned}$$

Thus, using Lemma 1, we derive

$$\begin{aligned} S(1,1,1) &= \sum_{d\le V}\frac{\mu^2(2d)}{2^{\omega(d)}}\sum_{\substack{e\le V\\ \gcd(e,2d)=1}}\frac{\mu(e)}{2^{2\omega(e)}} \\ &\quad \sum_{\substack{m_2\le T/(ied)\\ \gcd(m_2,2ed)=1}}\frac{\mu^2(m_2)}{2^{\omega(m_2)}}\sum_{\substack{n_2\le T/(jed)\\ \gcd(n_2,2ed)=1}}\frac{\mu^2(n_2)}{2^{\omega(n_2)}} \;+\; O\left(\frac{T^2}{V}\right) \\ &= \frac{1}{ij}\sum_{d\le V}\frac{\mu^2(2d)}{d^2 2^{\omega(d)}}\sum_{\substack{e\le V\\ \gcd(e,2d)=1}}\frac{\mu(e)c(2ed)^2}{e^2 2^{2\omega(e)}}\cdot\frac{T^2}{\log T} + O\left(\frac{T^2}{\log^{3/2} T}\right) \\ &= \frac{1}{ij}\cdot\frac{16}{25}c(1)^2\sum_{d\in\mathbb{N}}\frac{\mu^2(2d)}{d^2 2^{\omega(d)}} \\ &\quad \sum_{\substack{e\in\mathbb{N}\\ \gcd(e,2d)=1}}\frac{\mu(e)}{e^2 2^{2\omega(e)}}\prod_{p\mid ed}\left(1+\frac{1}{2p}\right)^{-2}\cdot\frac{T^2}{\log T} \;+\; O\left(\frac{T^2}{\log^{3/2} T}\right). \end{aligned}$$

We now evaluate (see 19)

$$\frac{1}{ij}\cdot\frac{16}{25}c(1)^2\sum_{d\in\mathbb{N}}\frac{\mu^2(2d)}{d^2 2^{\omega(d)}}\sum_{\substack{e\in\mathbb{N}\\ \gcd(e,2d)=1}}\frac{\mu(e)}{e^2 2^{2\omega(e)}}\prod_{p\mid ed}\left(1+\frac{1}{2p}\right)^{-2}$$
$$=\frac{1}{ij}\cdot\frac{16}{25}c(1)^2\sum_{d\in\mathbb{N}}\frac{\mu^2(2d)}{d^2 2^{\omega(d)}}\prod_{p\mid d}\left(1+\frac{1}{2p}\right)^{-2}\prod_{p\nmid 2d}\left(1-\frac{1}{4p^2(1+\frac{1}{2p})^2}\right)$$
$$=\frac{1}{ij}\cdot\frac{4}{\pi^3}\sum_{d\in\mathbb{N}}\frac{\mu^2(2d)}{d^2 2^{\omega(d)}}\prod_{p\mid d}\left(1+\frac{1}{p}\right)^{-1}$$
$$=\frac{1}{ij}\cdot\frac{4}{\pi^3}\prod_{p\geq 3}\left(1+\frac{1}{2p(p+1)}\right)=\frac{1}{ij}\cdot\frac{4}{\pi^3}\rho.$$

Therefore,

$$S(1,1,1)=\frac{4\rho}{ij\pi^3}\cdot\frac{T^2}{\log T}+O\left(\frac{T^2}{\log^{3/2}T}\right). \tag{32}$$

Summing up estimates (30) and (31) over m_1, n_1 and d_1 and choosing as in the proof of Lemma 3 the value $C=1000$, and using also the asymptotic formula (32) when $(m_0,n_0,d_0)=(1,1,1)$, we derive

$$M^{ij}_{(28)}(T,m_0,n_0,d_0)=\begin{cases}\left(\dfrac{4\rho}{\pi^3 ij}+o(1)\right)\dfrac{T^2}{\log T}, & \text{for } (m_0,n_0,d_0)\equiv(1,1,1) \bmod 8,\\[2ex] O\Big(\dfrac{T^2}{\log^2 T}\Big), & \text{otherwise,}\end{cases} \tag{33}$$

as $T\to\infty$.

The case (29). The contribution to the sum $M^{ij}_{<V_0}(T,m_0,n_0,d_0)$ of the sextuples in this case is

$$M^{ij}_{(29)}(T,m_0,n_0,d_0)=\sum_{\max\{m_2,n_2,d_2\}\leq V}\frac{\mu^2(2m_2n_2d_2)}{2^{\omega(m_2n_2d_2)}}S^*(m_2,n_2,d_2), \tag{34}$$

where

$$S^*(m_2,n_2,d_2)=\sum_{\substack{d_1\leq V\\ V<m_1\leq T/(im_2d_1d_2)\\ d_1\equiv d_0 \bmod 8\\ m_1\equiv m_0 \bmod 8}}\frac{\mu^2(2m_1m_2n_2d_1d_2)}{2^{\omega(m_1d_1)}}\left(\frac{d_2n_2}{m_1}\right)\left(\frac{m_2n_2}{d_1}\right)$$
$$\sum_{\substack{V<n_1\leq T/(jn_2d_1d_2)\\ \gcd(n_1,2m_1m_2n_2d_1d_2)=1\\ n_1\equiv n_0 \bmod 8}}\frac{\mu^2(n_1)}{2^{\omega(n_1)}}\left(\frac{d_2m_2}{n_1}\right). \tag{35}$$

The sum $S^*(m_2,n_2,d_2)$ can be dealt with by applying Lemma 1 with $q_1=8$ and either $a=n_0$, or $a=m_0$. We remark that the main term originates from the contribution of the triple $(m_2, n_2, d_2) = (1, 1, 1)$, which is

$$\begin{aligned} S^*(1,1,1) &= \sum_{\substack{d_1 \le V \\ V < m_1 \le T/(id_1) \\ V < n_1 \le T/(jd_1) \\ (m_1,n_1,d_1) \equiv (m_0,n_0,d_0) \bmod 8}} \frac{\mu^2(m_1 n_1 d_1)}{2^{\omega(m_1 n_1 d_1)}} \\ &\sim \frac{1}{ij} \cdot \frac{1}{4\pi^3} \sum_{\substack{d \in \mathbb{N} \\ d \equiv d_0 \bmod 8}} \frac{\mu^2(d)}{d 2^{\omega(d)}} \prod_{p \mid d} \frac{1}{p+1} \frac{T^2}{\log T}, \end{aligned}$$

as $T \to \infty$. By using (34) and (35), we finally arrive the estimate

$$\begin{aligned} M^{ij}_{(29)}(m_0, n_0, d_0) &= \frac{1 + o(1)}{4ij\pi^3} \cdot \sum_{\substack{d \in \mathbb{N} \\ d \equiv d_0 \bmod 8}} \mu^2(d) \prod_{p \mid d} \frac{1}{2p(p+1)} \cdot \frac{T^2}{\log T} \\ &= \frac{\rho_{d_0} + o(1)}{4ij\pi^3} \cdot \frac{T^2}{\log T}, \end{aligned} \tag{36}$$

as $T \to \infty$. Hence,

$$M^{ij}(m_0, n_0, d_0) = M^{ij}_{(28)}(m_0, n_0, d_0) + M^{ij}_{(29)}(m_0, n_0, d_0) + O(T \log^{-2} T),$$

and now using the estimates (33) and (36), the conclusion of the lemma can be easily derived. □

2.3. **Proof of Proposition 2.** We follow the proof of [4, Theorem 1]. We restrict to the case $A = B = T$ and decide not to estimate the error terms implicitely contained in the formulas of Proposition 2.

Let ϵ and η be in $\{\pm 1\}$. We want to study the cardinality $N_{\epsilon,\eta}(T)$ of the set of pairs (m, n) of integers satisfying

$$\mu^2(2mn) = 1,\ 1 \ < m,\ n \le T,\ \epsilon m \equiv \square \bmod n \ \&\ \eta n \equiv \square \bmod m.$$

From the properties of Legendre symbols, we have the basic equality

$$N_{\epsilon,\eta}(T) = \sum_{1 < m,} \sum_{n \le T} \frac{\mu^2(2mn)}{2^{\omega(m)} \cdot 2^{\omega(n)}} \prod_{p \mid m} \left[1 + \left(\frac{\eta n}{p}\right)\right] \prod_{p \mid n} \left[1 + \left(\frac{\epsilon m}{p}\right)\right]. \tag{37}$$

To transform (37), it remains to expand both products, use the multiplicativity property of Jacobi symbols, factor $m = ab$ and $n = cd$, and introduce the function

$$\kappa_{\epsilon,\eta}(a, c) = \left(\frac{a}{c}\right)\left(\frac{c}{a}\right)\left(\frac{\epsilon}{c}\right)\left(\frac{\eta}{a}\right), \tag{38}$$

to finally reach the equality

$$N_{\epsilon,\eta}(T) = \sum\sum_{ab \le T} \sum\sum_{cd \le T} \frac{\mu^2(2abcd)}{2^{\omega(ab)} \cdot 2^{\omega(cd)}} \left(\frac{d}{a}\right) \left(\frac{b}{c}\right) \kappa_{\epsilon,\eta}(a, c). \tag{39}$$

Since the value of the function $(a, c) \mapsto \kappa_{\epsilon,\eta}(a, c)$ is constant when we fix the congruence classes of a and c mod 4, we split $N_{\epsilon,\eta}(T)$ into

$$N_{\epsilon,\eta}(T) = \sum_{a_0 = \pm 1} \sum_{c_0 = \pm 1} \kappa_{\epsilon,\eta}(a_0, c_0)\, M(T, a_0, c_0), \tag{40}$$

where $M(T, a_0, c_0)$ is given by (8).

By the Quadratic Reciprocity Law, we see that if a_0 and c_0 are two odd positive integers, then

$$\kappa_{\epsilon,\eta}(a_0,c_0)=\begin{cases}1, & \text{if } a_0\equiv c_0\equiv 1 \bmod 4,\\ \epsilon, & \text{if } a_0\equiv -c_0\equiv 1 \bmod 4,\\ \eta, & \text{if } a_0\equiv -c_0\equiv -1 \bmod 4,\\ -\epsilon\eta, & \text{if } a_0\equiv c_0\equiv -1 \bmod 4.\end{cases}\tag{41}$$

Using Lemma 3 together with the relations (40) and (41) with $\epsilon=\eta=1$, we obtain

$$N_{1,1}(T)\sim\left(\frac{5}{\pi^3}+\frac{1}{\pi^3}+\frac{1}{\pi^3}-\frac{1}{\pi^3}\right)\frac{T^2}{\log T}=\frac{6}{\pi^3}\cdot\frac{T^2}{\log T},$$

as $T\to\infty$. The other relations claimed by Proposition 2 can be derived analogously.

2.4. **Proof of Proposition 3.** From the properties of the Jacobi symbols, we have the basic equality

$$\begin{aligned}N^{ij}_{\epsilon,\eta}(T) &= \sum_{\substack{d\in\mathbb{N}\\ m\le T/(id)\\ n\le T/(jd)}}\frac{\mu^2(2mnd)}{2^{\omega(mnd)}}\\ &\qquad\prod_{p\mid dmn}\left(1+\left(\frac{\eta jdn}{p}\right)\right)\left(1+\left(\frac{\epsilon idm}{p}\right)\right)\left(1+\left(\frac{-\epsilon\eta ijmn}{p}\right)\right).\end{aligned}$$

We now expand the three products in each sum, use the multiplicativity property of the Jacobi symbols, factor $m=m_1m_2$, $n=n_1n_2$ and $d=d_1d_2$, and introduce the functions $\kappa_{\epsilon,\eta}(m,n,d)$ and $\varsigma_{i,j}(m,n,d)$ defined as

$$\kappa_{\epsilon,\eta}(m,n,d)=\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)\left(\frac{\epsilon}{n}\right)\left(\frac{\eta}{m}\right)\left(\frac{m}{d}\right)\left(\frac{d}{m}\right)\left(\frac{d}{n}\right)\left(\frac{n}{d}\right)\left(\frac{-\epsilon\eta}{d}\right),$$

and

$$\varsigma_{i,j}(m,n,d)=\left(\frac{ij}{d}\right)\left(\frac{j}{m}\right)\left(\frac{i}{n}\right),$$

to finally reach the equality

$$\begin{aligned}N^{ij}_{\epsilon,\eta}(T) = \sum_{\substack{d_1,d_2,m_1,m_2,n_1,n_2\in\mathbb{N}\\ m_1m_2\le T/(id_1d_2)\\ n_1n_2\le T/(jd_1d_2)}}&\frac{\mu^2(2m_1m_2n_1n_2d_1d_2)}{2^{\omega(m_1m_2n_1n_2d_1d_2)}}\\ &\left(\frac{d_2m_2}{n_1}\right)\left(\frac{d_2n_2}{m_1}\right)\left(\frac{n_2m_2}{d_1}\right)\varsigma_{i,j}\kappa_{\epsilon,\eta},\end{aligned}$$

where $\kappa_{\epsilon,\eta}=\kappa_{\epsilon,\eta}(m_1,n_1,d_1)$, and $\varsigma_{i,j}=\varsigma_{i,j}(m_1,n_1,d_1)$. Since the value of the function $(m_1,n_1,d_1)\mapsto\varsigma_{i,j}(m_1,n_1,d_1)\kappa_{\epsilon,\eta}(m_1,n_1,d_1)$ is constant when we fix the congruence classes of m_1, n_1 and d_1 mod 8, it follows that we can split $N^{ij}_{\epsilon,\eta}(T)$ into

$$N^{ij}_{\epsilon,\eta}(T)=\sum_{(m_0,n_0,d_0)\in\{\pm1,\pm3\}^3}\varsigma_{i,j}(m_0,n_0,d_0)\kappa_{\epsilon,\eta}(m_0,n_0,d_0)\,M^{ij}(T,m_0,n_0,d_0),\tag{42}$$

where $M^{ij}(T, m_0, n_0, d_0)$ is given by formula (23). At this stage, note that Lemma 4 and identity (42) together imply that

$$N^{ij}_{\epsilon,\eta}(T) \sim \left(\rho + \frac{1}{16}\sum_{(m_0,n_0,d_0)\in\{\pm1,\pm3\}^3} \varsigma_{i,j}\kappa_{\epsilon,\eta}\rho_{d_0}\right)\cdot\frac{4}{\pi^3}\frac{1}{ij}\cdot\frac{T^2}{\log T}, \tag{43}$$

as $T \to \infty$. We also have the following identity which is a direct consequence of the Quadratic Reciprocity Law:

$$\kappa_{\epsilon,\eta}(m_0,n_0,d_0) = \begin{cases} 1, & \text{if } m_0 \equiv n_0 \equiv d_0 \equiv 1 \bmod 4,\\ \epsilon, & \text{if } m_0 \equiv -n_0 \equiv d_0 \equiv 1 \bmod 4,\\ \eta, & \text{if } m_0 \equiv -n_0 \equiv -d_0 \equiv -1 \bmod 4,\\ -\epsilon\eta, & \text{if } m_0 \equiv n_0 \equiv -d_0 \equiv -1 \bmod 4\\ -\epsilon\eta, & \text{if } m_0 \equiv n_0 \equiv -d_0 \equiv 1 \bmod 4,\\ \eta, & \text{if } m_0 \equiv -n_0 \equiv -d_0 \equiv 1 \bmod 4,\\ \epsilon, & \text{if } m_0 \equiv -n_0 \equiv d_0 \equiv -1 \bmod 4,\\ 1, & \text{if } m_0 \equiv n_0 \equiv d_0 \equiv -1 \bmod 4. \end{cases}$$

Fixing d_0 and summing up over all the 16 possible values of $(m_0, n_0) \in \{\pm1, \pm3\}^2$, we obtain

$$\sum_{(m_0,n_0)\in\{\pm1,\pm3\}^2} \varsigma_{ij}\kappa_{\epsilon,\eta} = \left[1+\left(\frac{i}{3}\right)\right]\cdot\left[1+\left(\frac{j}{3}\right)\right]\cdot\left[2-(1-\epsilon)(1-\eta)\right].$$

Finally, if α is the quantity defined in the statement of Proposition 3, we then have

$$\sum_{(d_0,m_0,n_0)\in\{\pm1,\pm3\}^3} \rho_{d_0}\varsigma_{ij}\kappa_{\epsilon,\eta} = 4\cdot(\alpha-4)\cdot\sum_{d_0\in\{\pm1,\pm3\}}\rho_{d_0} = 4\cdot(\alpha-4)\cdot\rho.$$

Inserting the result of the above calculation into in (43), we conclude the proof.

2.5. **Proof of Proposition 4.** From the definition of the set that we study here, we deduce that $-a^2 \equiv \square \bmod b$. This is equivalent to

$$p \mid b,\ p \nmid 2a \Rightarrow p \equiv 1 \bmod 4. \tag{44}$$

The strategy of the proof is the same as in the proof of Proposition 3, with the important difference that we must take into account the impact of (44). This explains why the main term is of a different nature. With the notations of Section 2.2 and in particular of the proof of Lemma 4, a typical main term is

$$\sum_{a\le T}\mu^2(a)\sum_{\substack{b\le T\\ p\mid d,\ p\nmid 2a\Rightarrow p\equiv 1 \bmod 4}}\frac{\mu^2(b)}{2^{\omega(ab)}}$$

(compare with $S(1,1,1)$ in the proof of Lemma 4), which we bound as

$$\sum_{d\in\mathbb{N}}\left(\sum_{a\le T/d}\frac{\mu^2(a)}{2^{\omega(a)}}\right)\times\left(\sum_{\substack{b\le 2T/d\\ p\mid b\Rightarrow p\equiv 1 \bmod 4}}\frac{\mu^2(b)}{2^{\omega(b)}}\right) \ll \frac{T}{\log^{\frac12} T}\cdot\frac{T}{\log^{\frac34} T},$$

by appealing to general bounds for sums of multiplicative functions (see, for instance, [15, Theorem 1]).

The error terms are managed in the same way, but with a modification of Lemma 1 (a variant of the Siegel–Walfisz theorem), where we impose to one of the variables to have all its prime factors congruent to 1 modulo 4. If we follow the proof given in [4, Section 8], we have to introduce the function $L^{\frac{1}{4}}(s,\chi)$ instead of $L^{\frac{1}{2}}(s,\chi)$ and the desired conclusion follows by using standard methods in the theory of Dirichlet series.

3. Systems of quadratic equations and the set $\mathcal{F}_{\mathbb{H}}$

In order to prove Theorem 4, we need the following criterion which follows instantly from a result of Kiming [8, Theorem 4].

Lemma 5. *Let $(m,n)\in\mathcal{F}$, and set $d=\gcd(m,n)$, $m=dm_1$, and $n=dn_1$. Then (m,n) belongs to $\mathcal{F}_{\mathbb{H}}$ if and only if*

$$-m_1n_1\equiv\square \bmod d,\qquad -m\equiv\square \bmod n_1,\quad \textit{and}\quad -n\equiv\square \bmod m_1. \tag{45}$$

In particular, (m,n) belongs to $\widetilde{\mathcal{F}}_{\mathbb{H}}$ if and only if $\mu^2(2mn)=1$ and

$$-m\equiv\square \bmod n\quad \textit{and}\quad -n\equiv\square \bmod m. \tag{46}$$

Proof. For the purpose of this proof only, for two integers a and b we write $(a,b)^{(H)}$ for the Hilbert symbol (see [14, Chapter III]). By [8, Theorem 4], we see that $(m,n)\in\mathcal{F}_{\mathbb{H}}$ if and only if $(m,n)^{(H)}(mn,-1)^{(H)}=1$. As noted in [8, Remark, p. 839], we have $(m,n)^{(H)}(mn,-1)^{(H)}=(-m,-n)^{(H)}(-1,-1)^{(H)}$. We now compute $(-m,-n)^{(H)}(-1,-1)^{(H)}$ for all valuations v of $\mathbb{Q}$. At infinity, that is, for $v=\infty$, due to the negativity of $-m$ and $-n$, we obviously have

$$(-m,-n)^{(H)}_{\infty}\cdot(-1,-1)^{(H)}_{\infty}=(-1)\cdot(-1)=1.$$

For every finite valuation $v=p$, we have $(-1,-1)^{(H)}_p=-1$ if $p=2$, and $(-1,-1)^{(H)}_p=1$ if $p\neq 2$. From the above discussion, we see that the equality $(m,n)^{(H)}(mn,-1)^{(H)}=1$ holds if and only if we have

$$(-m,-n)^{(H)}_p=\begin{cases}1, & \text{for every } \ p\neq 2,\\ -1, & \text{for } p=2.\end{cases} \tag{47}$$

Next, we remark that when m and n are both odd the second condition of (47) holds if and only if $m\equiv n\equiv 1 \bmod 4$. Furthermore, the first condition of (47) holds for every $p\nmid 2mn$. Finally, we conclude that for odd coprime integers m and n the condition (47) holds if and only if the condition (46) holds.

The general case where the squarefree m and n are not necessarily odd and coprime, requires more care: here we have to separate the cases $p=2$ or not, $p\mid d$, $p\mid m_1$, $p\mid n_1$, and $p\nmid dm_1n_1$, and apply general formulas giving the values of Hilbert symbols $(a,b)^{(H)}_p$ in terms of Legendre symbols (see [14, Theorem 1 p. 20] for instance). These computations allow to check that the conditions (45) and (47) are equivalent. Note that we can avoid the tedious case $p=2$ by exploiting the Hilbert product formula

$$\prod_v (a,b)^{(H)}_v=1$$

(see [14, Theorem 3, p. 23], for instance). The details are left to the reader. □

The proof of Theorem 2 is based on the following criterion due to Kiming [8, Theorem 5].

Lemma 6. *Let (m,n) be a pair of squarefree integers >1. Then (m,n) belongs to $\mathcal{F}_{D_4}$ if and only if at least one of three quadratic forms*

$$\begin{cases} X^2+mY^2-nZ^2=0, \\ X^2+nY^2-mZ^2=0, \\ X^2-mY^2-nZ^2=0 \end{cases} \tag{48}$$

has a nontrivial integral solution (X,Y,Z).

4. Proofs of main results

4.1. **Proof of Theorem 1.** It is known (see [8, page 832]) that the quadratic extension $\mathbb{Q}(\sqrt{d})$ for a positive integer d can be embedded in a C_4-extension of $\mathbb{Q}$ if and only if d can be written as a sum of two squares of integers. A $C_4\times C_2$-extension of $\mathbb{Q}$ is necessarily a C_4-extension of one of its quadratic subfields. Therefore, given $(m,n)\in\mathcal{F}$, we have that $(m,n)\in\mathcal{F}_{C_2\times C_4}$ if and only if at least one of $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$, or $\mathbb{Q}(\sqrt{mn})$ can be embedded in a C_4–extension of $\mathbb{Q}$. Hence, $\mathcal{F}_{C_2\times C_4}$ consists of those $(m,n)\in\mathcal{F}$ such that either m,n, or mn can be written as a sum of two squares.

We need the following standard statement which follows immediately from a classical result due to Landau [10] applied to all integers instead of only squarefree integers together with the inclusion-exclusion principle. Namely, if $\mathcal{K}$ is the set of the squarefree positive integers that can be written as a sum of two squares, then

$$\sharp\,\mathcal{K}(T)=\left(\frac{6}{\pi^2}\vartheta+o(1)\right)\frac{T}{\sqrt{\log T}}, \qquad \text{as } T\to\infty,$$

where ϑ is the Landau–Ramanujan constant in (1). Indeed, this follows from the standard inclusion-exclusion principle applied to the set of sums of two squares and the observation that is $n=d^2m$ for some integers d,m,n then n is a sum of two squares if and of if m is too.

From the above, it follows immediately that the set of $(m,n)\in\mathcal{F}(T)$ such that both m and n are sums of two squares has $O\left(T^2/\log T\right)$ elements. We also claim that the number S of $(m,n)\in\mathcal{F}(T)$ such that mn is a sum of two squares is $O\left(T^2/\log T\right)$. Indeed,

$$\begin{aligned} S &\le \sum_{d\le T}\sharp\left\{(m,n)\in\mathcal{F}(T), d\mid m, d\mid n, m/d\in\mathcal{K}, n/d\in\mathcal{K}\right\} \\ &\le \sum_{d\le T}\left(\sharp\,\mathcal{K}(T/d)\right)^2=\sum_{d\le\log T}\left(\sharp\,\mathcal{K}(T/d)\right)^2+\sum_{\log T<d\le T}\left(\sharp\,\mathcal{K}(T/d)\right)^2 \\ &\ll T^2\sum_{\log T<d}\frac{1}{d^2}+\sum_{d\le\log T}\frac{1}{d^2}\left(\frac{T}{\sqrt{\log T/d}}\right)^2=O\left(\frac{T^2}{\log T}\right). \end{aligned}$$

From the above discussion, we deduce that

$$\begin{aligned} \mathcal{F}_{C_2\times C_4}(T) &= 2\sharp\left\{(m,n)\in\mathcal{F} \text{ such that } n\in\mathcal{K}\right\}+O\left(\frac{T^2}{\log T}\right) \\ &= 2\left(\frac{6}{\pi^2}+o(1)\right)T\times\sharp\,\mathcal{K}(T)+O\left(\frac{T^2}{\log T}\right) \\ &= 2\left(\frac{36}{\pi^4}\vartheta+o(1)\right)\frac{T^2}{\sqrt{\log T}}, \qquad \text{as } T\to\infty, \end{aligned}$$

which is equivalent to the statement of Theorem 1.

4.2. **Proof of Theorem 2.** We appeal to Proposition 1 on the solvability of ternary quadratic forms $aX^2+bY^2+cZ^2=0$ and to Lemma 6. The conditions concerning the signs of a, b and c are trivially verified here. Using symmetry and inclusion–exclusion principle, we get the equality

$$\begin{aligned}\sharp\,\mathcal{F}_{D_4}(T) = &\sum_{(i,j)\in\{1,2\}}\Big(N^{ij}_{1,1}(T)+N^{ij}_{1,-1}(T)+N^{ij}_{-1,1}(T)\Big)\\ &+O\left(\sharp\,\{(a,b)\in\mathcal{F}(T),\ a \text{ and } -a\equiv\Box \bmod b\,\&\ b\equiv\Box \bmod a\}\right).\end{aligned}$$

A direct application of Propositions 3 and 4 easily leads to

$$\sharp\,\mathcal{F}_{D_4}(T)=\left(\frac{33}{\pi^3}\cdot\rho+o(1)\right)\frac{T^2}{\log T},\qquad \text{as } T\to\infty,$$

which is what we wanted to prove.

Note 3. *Suppose that m and n are odd, squarefee, coprime, and in the residue class* $1 \bmod 4$*. Then they are both positive fundamental discriminants. The same property holds for $D=mn$. Furthermore, suppose that the pair (m,n) satisfies the third condition of (48) (or equivalently $m\equiv\Box \bmod n$ and $n\equiv\Box \bmod m$). Then, following the definition of Redei, we can say that $\{m,n\}$ is a decomposition of second type of D. Redei's theory ensures that $\mathbb{Q}(\sqrt{m},\sqrt{n})$ admits a quadratic extension K_4 which is a C_4–extension of $\mathbb{Q}(\sqrt{D})$, and which is unramified at any place. Furthermore, we have* $\mathrm{Gal}(K_4,\mathbb{Q})=D_4$*. In conclusion, in that particular case, we can say more about the extension $\mathbb{K}$ we want to build over $\mathbb{Q}(\sqrt{m},\sqrt{n})$. For a general presentation of that theory, see* [3, Section 3.2]*, which also includes an application to the behavior of the 4–rank of the ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{D})$.*

4.3. **Proof of Theorem 3.** We appeal to Lemma 5 and deduce that

$$\sharp\,\mathcal{F}_{\mathbb{H}}(T)=\sum_{(i,j)\in\{1,2\}}N^{ij}_{-1,-1}(T).$$

Finally, we apply Proposition 3 and deduce

$$\sharp\,\mathcal{F}_{\mathbb{H}}(T)=\left(\left(\frac{2}{1\cdot1}+\frac{4}{1\cdot2}+\frac{4}{2\cdot1}+\frac{4}{2\cdot2}\right)\times\frac{1}{\pi^3}\cdot\rho+o(1)\right)\frac{T^2}{\log T},\qquad \text{as } T\to\infty,$$

which concludes the proof.

4.4. **Proof of Theorem 4.** The proof follows immediately from Lemma 5 and the last relation of Proposition 2

4.5. **Proof of Theorem 5.** As in the case of the proof of Theorem 2, this proof is also immediate as by Lemma 6, we have

$$\begin{aligned}\sharp\,\widetilde{\mathcal{F}}_{D_4}(T) =&2\,\sharp\,\Big\{(m,n)\in\widetilde{\mathcal{F}}(T),\ -m\equiv\Box \bmod n\,\&\ n\equiv\Box \bmod m\Big\}\\ &+\sharp\,\Big\{(m,n)\in\widetilde{\mathcal{F}}(T),\ m\equiv\Box \bmod n\,\&\ n\equiv\Box \bmod m\Big\}\\ &+O\left(\sharp\,\Big\{(m,n)\in\widetilde{\mathcal{F}}(T),\ m \text{ and } -m\equiv\Box \bmod n\,\&\ n\equiv\Box \bmod m\Big\}\right).\end{aligned}$$

A direct application of Propositions 2 and 4 easily leads to

$$\sharp\,\widetilde{\mathcal{F}}_{D_4}(T) = \left(\frac{6}{\pi^3} + o(1)\right)\frac{T^2}{\log T}, \qquad \text{as } T \to \infty,$$

which is what we wanted to prove.

5. Conclusion

It is likely that one can also derive an asymptotic formula for $\sharp\,\widetilde{\mathcal{F}}_{C_2\times C_4}(T)$ along the lines of those for $\sharp\,\mathcal{F}_{C_2\times C_4}(T)$. More precisely, we believe that

$$\sharp\,\widetilde{\mathcal{F}}_{C_2\times C_4}(T) = \left(\frac{4\vartheta}{\pi^2} \times \kappa + o(1)\right)\frac{T^2}{\sqrt{\log T}} \qquad \text{as } T \to \infty,$$

where ϑ is defined by (1),

$$\kappa = \frac{3e^{\gamma/2}}{4\sqrt{\pi}} \prod_{p\equiv 1 \bmod 4}\left(1 - \frac{1}{p^3}\right)\cdot \prod_{p\equiv 3 \bmod 4}\left(1 - \frac{1}{p^2}\right),$$

and γ is the Euler constant.

Acknowledgements

This work started in May of 2008, while the last three authors were attending the program “New Challenges in Digital Communications” at the NATO Advanced Study Institute in Vlora, Albania. The authors thank Tony Sashka and other organizers for the opportunity of participating in this program. During the preparation of this paper, F. L. was supported in part by grant SEP-CONACyT 79685, F. P. was supported in part by grant P.R.I.N. 2006 “Problemi diofantei e analitici in Teoria dei Numeri”, and I. S. was supported in part by ARC grant DP0881473.

The authors are very grateful to R. Schulze-Pillot for his comments and suggestions, which have led to a significant shortening and simplification of the proof of Theorem 4.

The authors would also like to thank V. Blomer for his interesting comments on the theory of ternary quadratic forms.

References

[1] D. S. Dummit and R. M. Foote, Abstract Algebra. 2nd Ed. *Prentice Hall*, 1999.
[2] E. Fouvry and J. Klüners, *On the 4–rank of quadratic number fields*, Inv. Math., **167** (2007), 455–516.
[3] E. Fouvry and J. Klüners, *On the negative Pell equation*, Ann. of Math., (to appear), (2009).
[4] J.B. Friedlander & H. Iwaniec, *Ternary quadratic forms with rational zeros*, J. Th. Nomb. Bordeaux, (to appear), (2009).
[5] C.R. Guo, *On solvability of ternary quadratic forms*, Proc. London Math. Soc., **70** (1995), 241–263.
[6] G. H. Hardy and E. M. Wright, Introduction to the Theory of Numbers. *Oxford University Press*, Oxford, 1980.
[7] C. U. Jensen and N. Yui, *Quaternion extensions.* Algebraic Geometry and Commutative Algebra, Vol. 1, Kinokuniya, 1988, 155–182.
[8] I. Kiming, *Explicit classifications of some 2-extensions of a field of characteristic different from 2.* Can. J. Math., **42** (1990), 825–855.
[9] J. Klüners, *Über die Asymptotik von Zahlkörpern mit vorgegebener Galoisgruppe*, *Habilitationschrift,* Universität Kassel, D34, 2005.

[10] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen.* Chelsea, New York, 1974.

[11] G. Malle *On the distribution of Galois groups* J. Number Theory, **92** (2002), 315–329.

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

[13] H. Reichardt, *Über Normalkörper mit Quaternionengruppe.* Math. Z., **41** (1936), 218–221.

[14] J.-P. Serre, *A course in arithmetic*, Graduate texts in Mathematics, No. 7, Springer-Verlag, Berlin, 1973.

[15] P. Shiu, *A Brun-Titchmarsh theorem for multiplicative functions*, J. Reine Angew. Math., **313** (1980), 161–170.

[16] A. Weil, *Number theory: An approach through history.* Birkhäuser, Basel, 1984.

[17] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f.* J. Reine Angew. Math. **174** (1936), 237–245.

(É. Fouvry) Univ. Paris–Sud, Laboratoire de Mathématiques d'Orsay, CNRS, F-91405 Orsay Cedex, France

E-mail address: `Etienne.Fouvry@math.u-psud.fr`

(F. Luca) Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México

E-mail address: `fluca@matmor.unam.mx`

(F. Pappalardi) Dipartimento di Matematica, Università Roma Tre, Largo S. L. Murialdo, 1, Roma, 00146, Italy

E-mail address: `pappa@mat.uniroma3.it`

(I. E. Shparlinski) Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

E-mail address: `igor@ics.mq.edu.au`