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 the double oscillations theorem.

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 extensions have been characterized explicitly by Kiming in [8], where he gives explicit realizations of several extensions of fields of odd characteristic 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

\[
\text{Gal}(\mathbb{K}/\mathbb{Q}) \cong H.
\]

It is well known (see, for example, [11, 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 $F_{C_2 \times C_2 \times C_2} = F$. In fact, for any $(m, n) \in F$ 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, $(m, n) \in F_{C_2 \times C_2 \times C_2}$.

It is also clear that $F_{C_8} = \emptyset$, since the cyclic group $C_8$ cannot admit the noncyclic quotient $C_2 \times C_2 \times C_2$.

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

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

We recall that $\#F(T) = \frac{36}{\pi^4} T^2 + O(T^{3/2})$, as $T \to \infty$ (see [6, Theorem 333]).

Let

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

be the Landau–Ramanujan constant. We also define

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

In this paper, we prove the following results:

**Theorem 1.** We have

$$\#F_{C_2 \times C_4}(T) = \left(\frac{72\vartheta}{\pi^4} + o(1)\right) \frac{T^2}{\sqrt{\log T}}, \quad \text{as } T \to \infty,$$

where $\vartheta$ is given by (1).

**Theorem 2.** We have

$$\#F_{D_4}(T) = \left(\frac{33\varrho}{\pi^3} + o(1)\right) \frac{T^2}{\log^2 T}, \quad \text{as } T \to \infty,$$

where $\rho$ is given by (2).

**Theorem 3.** We have

$$\#F_{H}(T) = \left(\frac{7\varrho}{\pi^3} + o(1)\right) \frac{T^2}{\log^2 T}, \quad \text{as } T \to \infty,$$

where $\rho$ is given by (2).

Let $\tilde{F}$ 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 $\tilde{F}_H$ as the set of $(m, n) \in \tilde{F}$ such $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ admits a quadratic extension $K$ with $\text{Gal}(K/\mathbb{Q}) \cong H$.

**Theorem 4.** The following asymptotic formula holds:

$$\#\tilde{F}_H(T) = \left(\frac{2}{\pi^3} + o(1)\right) \frac{T^2}{\log T}, \quad \text{as } T \to \infty.$$
Theorem 5. The following asymptotic formula holds:

\[ \# \mathcal{D}_4(T) = \left( \frac{18}{\pi^3} + o(1) \right) \frac{T^2}{\log T}, \quad \text{as } T \to \infty. \]

We also point out that there is another way to count the extensions \( K \) satisfying \( \text{Gal}(K/Q) \sim \mathbb{H} \). It consists in ordering the fields \( K \) according to the value of \( |\text{Disc}(K/Q)| \). Klüners in [9, Satz 7.2] has shown that for some positive constant \( c_1 \) one has

\[ \# \{ K \subseteq \mathbb{C} ; |\text{Disc}(K/Q)| \leq T, \text{Gal}(K/Q) \sim \mathbb{H} \} \sim c_1 T^{\frac{3}{4}}, \quad \text{as } T \to \infty. \]

This proves Malle’s Conjecture [12] for the quaternionic group \( \mathbb{H} \). The analogous conjecture for the group \( D_4 \) states that there exists a positive constant \( c_2 \) such that

\[ \# \{ K \subseteq \mathbb{C} ; |\text{Disc}(K/Q)| \leq T, \text{Gal}(K/Q) \sim D_4 \} \sim c_2 T^{\frac{1}{4} \log 2}, \quad \text{as } T \to \infty. \]

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 \( |U| \leq cV \) 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 \( \lambda \).

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 the integers \( a \) and \( b \).

2. Squarefree numbers with congruence conditions

2.1. Necessary results. Let \( m \) and \( n \) be 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 \( x^2 \equiv m \mod n \) 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 \( (\frac{m}{p}) \) is the Legendre symbol with respect to \( p \). We write that condition as \( m \equiv \square \mod n \).

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

\[ \# \{ (a,b) ; 1 \leq a \leq A, 1 \leq b \leq B, \mu^2(2ab) = 1, a \equiv \square \mod b \& b \equiv \square \mod a \} \]

\[ = \frac{AB}{\sqrt{\log A} \sqrt{\log B}} \left( \frac{6}{\pi^3} + O_\delta \left( \frac{1}{\log A} + \frac{1}{\log B} \right) \right). \]

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, [10] 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

\[ aX^2 + bY^2 + cZ^2 = 0 \]
has a nonzero integer solution \((X,Y,Z)\) if and only if the following three conditions are satisfied: 
\[-ab \equiv \square \pmod{c}, -ac \equiv \square \pmod{b} \text{ and } -bc \equiv \square \pmod{a}.
\]

Results such as 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 the 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 \(\tilde{F}(T) = \{(a,b) \in \mathbb{N}^2 : 1 \leq a, b \leq T, \mu^2(2ab) = 1\}\). Then, as \(T \to \infty\), we have the following asymptotic formulas:

\[
\sharp \left\{ (a,b) \in \tilde{F}(T) : a \equiv \square \pmod{b} \& b \equiv \square \pmod{a} \right\} \sim \frac{6}{\pi^3} \cdot \frac{T^2}{\log T},
\]

\[
\sharp \left\{ (a,b) \in \tilde{F}(T) : -a \equiv \square \pmod{b} \& b \equiv \square \pmod{a} \right\} \sim \frac{6}{\pi^3} \cdot \frac{T^2}{\log T},
\]

\[
\sharp \left\{ (a,b) \in \tilde{F}(T) : -a \equiv \square \pmod{b} \& -b \equiv \square \pmod{a} \right\} \sim \frac{2}{\pi^3} \cdot \frac{T^2}{\log T}.
\]

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

\[a \equiv b \equiv 1 \pmod{4}.
\]

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

For the proof of Theorem 2 we decompose

\[\mathcal{F} = \mathcal{F}^{11} \sqcup \mathcal{F}^{22} \sqcup \mathcal{F}^{12} \sqcup \mathcal{F}^{21},\]

where

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

Let \(\epsilon\) and \(\eta\) 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

\[(5) \quad X^2 - \epsilon aY^2 - \eta bZ^2 = 0\]

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

\[
dX^2 - cmY^2 - \eta nZ^2 = 0
\]

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

\[
N_{\epsilon, \eta}^{ij}(T) = \sharp \left\{ (a, b) \in F^{ij}(T) : ca \equiv \square \mod b, \ \eta b \equiv \square \mod a, \ -\epsilon \eta \frac{ab}{d^2} \equiv \square \mod d \right\}.
\]

Furthermore, we use the last expression to define \( N_{\epsilon, \eta}^{ij}(T) \) 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,

\[
N_{\epsilon, \eta}^{ij}(T) \sim \frac{\alpha_{ij}}{ij} \frac{\rho}{\pi^3} \frac{T^2}{\log T},
\]

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 \( F(T) = \{(a, b) \in \mathbb{N}^2 : 1 < a, b \leq T, \ \mu^2(a) = \mu^2(b) = 1\} \). Uniformly in \( T \geq 2 \) we have

\[
\sharp \left\{ (a, b) \in F(T) : a \text{ and } -a \equiv \square \mod b & b \equiv \square \mod a \right\} \ll \frac{T^2}{\log^{5/4} T}.
\]

**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 \( \beta \) 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

\[
c(r) = \pi^{-\frac{1}{2}} \prod_{\nu^2 \geq 2} \left( 1 + \frac{1}{2p} \right) \left( 1 - \frac{1}{p} \right)^{\frac{1}{2}} \prod_{p^r} \left( 1 + \frac{1}{2p} \right)^{-1}.
\]

**Lemma 1.** Let \( \gcd(ad, q) = 1 \), where \( q = q_1q_2 \), with \( (q_1, q_2) = 1 \). For a character \( \chi_2 \) modulo \( q_2 \) and for any constant \( C \), we have the equality

\[
\sum_{\substack{n \leq x \\ \gcd(n, d) = 1 \\ n \equiv a \mod q_1}} \mu^2(n) \frac{\chi_2(n)}{2^{\nu(n)}} = \delta_{\chi_2} \cdot \frac{c(d)}{\varphi(q_1)} \cdot \frac{x}{\sqrt{\log x}} \left( 1 + O \left( \frac{(\log \log 3dq)^2}{\log x} \right) \right)
\]

\[
+ O_C(2^{2(\nu(d))}q_2x(\log x)^{-C}),
\]
where $\delta_{\chi_2}$ is equal to 1 or 0 according to whether $\chi_2$ is principal or not, and $c(r)$ is defined by \footnote{7}.

The second result deals with double sums of Jacobi symbols. This is \footnote{4} Lemma 2].

**Lemma 2.** Let $\alpha_m$ and $\beta_n$ 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 \footnote{2}.

$$M(T, a_0, c_0) = \sum_{ab \leq T \atop c \leq T} \frac{\mu^2(2abcd)}{2=\left(a\right), 2\left(\frac{c}{d}\right)} \left( \frac{b}{a} \right) \left( \frac{c}{d} \right). \tag{8}$$

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

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

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

holds as $T \to \infty$.

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

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

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

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

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

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

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

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

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

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

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

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 that these two cases can be reduced to

$$a \leq V, \quad c \leq V$$

and

$$b \leq V, \quad d \leq V,$$

respectively.

Note that, due to the congruence restrictions $a \equiv a_0 \mod 4$ and $c \equiv c_0 \mod 4$, 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

$$M_{(13)}(a_0, c_0) = \sum_{a \leq V} \sum_{c \leq V} \frac{\mu^2(2ac)}{2\omega(ac)} S(a, c),$$

where

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

We now apply Lemma 11 to evaluate $S(a, c)$ according to the values of $a$ and $c$.

- When $a \neq 1$, we apply Lemma 11 with $\chi_2$ being the quadratic character modulo $a$, and then sum trivially over $b$. Using the fact that $\omega(abc) \leq \omega(ac) + \omega(b)$, we get

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

for any $C > 0$.\n
When \( c \neq 1 \), inside \( S(a,c) \) we interchange the roles of \( b \) and \( d \) and then apply Lemma [1] with \( \chi_2 \) being the quadratic character modulo \( c \). This gives

\[
S(a,c) \ll_{C} \frac{T^2}{ac} 2^{\omega(ac)} (\log T)^{-C}
\]

for any \( C > 0 \).

When \( a = c = 1 \), we then necessarily have \( a_0 \equiv c_0 \equiv 1 \mod 4 \). We then obtain the equality

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

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

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

An application of Lemma [1] with \( d = 2\delta \) and \( q_1 = q_2 = 1 \) leads to the relation

\[
S(1,1) = (1 + o(1)) \sum_{\delta \text{ odd}} \frac{\mu(\delta)}{4^{\omega(\delta)}} \left( c(2\delta) \frac{T/\delta}{\sqrt{\log(T/\delta)}} \right)^2 + O \left( \sum_{\delta > \log^{100} T} \frac{T^2}{\delta^2} \right), \quad \text{as } T \to \infty.
\]

This immediately gives

\[
S(1,1) \sim \frac{T^2}{\log T} \sum_{\delta \text{ odd}} \frac{\mu(\delta)c(2\delta)^2}{4^{\omega(\delta)} \delta^2}, \quad \text{as } T \to \infty.
\]

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

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

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

\[
\sum_{\delta \text{ odd}} \frac{\mu(\delta)c(2\delta)^2}{4^{\omega(\delta)} \delta^2} = \frac{16}{25} c(1)^2 \prod_{p \geq 3} \left( 1 - \frac{1}{4p^2(1 + 1/2p)^2} \right) = \frac{4}{\pi^3}.
\]
Collecting (15), (16), (17), (18) and (19), summing over $a$ and $c$ and choosing $C = 1000$, we finally get the estimate

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

The case (14). We write the contribution of the quadruples $(a, b, c, d)$ satisfying (12) to the sum $M$ in the form

\[ M_{(a_0, c_0)} = \sum_{b \leq V} \sum_{d \leq V} \frac{\mu^2(2bd)}{2^{\omega(b)}} S^*(b, d, a_0, c_0), \]

where

\[ S^*(b, d, a_0, c_0) = \sum_{a \leq T/b} \sum_{d \leq V} \frac{\mu^2(a)}{2^{\omega(a)}} \sum_{c \leq T/d} \frac{\mu^2(c)}{2^{\omega(c)}} \left(\frac{b}{c}\right). \]

Recall that the variables $a$ and $c$ satisfy the congruence conditions $a \equiv a_0 \mod 4$ and $c \equiv c_0 \mod 4$. The sums $S^*(b, d, a_0, c_0)$ can be studied with the techniques of Section 2.2. In particular, we apply Lemma 11 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

\[ M_{(a_0, c_0)} = \frac{1}{\pi^3} \cdot \frac{T^2}{\log T} (1 + o(1)), \quad \text{as } T \to \infty, \]

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

From (12), we get

\[ M(a_0, c_0) = M_{(a_0, c_0)} + O(T \log^{-2} T). \]

Combining the above estimate with (20) and (22), we complete the proof. \hfill \square

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

\[ M_{ij}(T, m_0, n_0, d_0) = \sum_{d_1, d_2, m_1, m_2, n_1, n_2 \in \mathbb{N}} \sum_{\max\{m_1m_2, n_1n_2\} \leq T/d_1d_2} \frac{\mu^2(2m_1n_1n_2d_1d_2)}{2^{\omega(m_1m_2n_1n_2d_1d_2)}} \cdot \left(\frac{d_2m_2}{n_1}\right) \left(\frac{d_2n_2}{m_1}\right) \left(\frac{n_2m_2}{d_1}\right). \]

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

\[ \rho_{d_0} = \sum_{d \equiv d_0 \mod 8} \mu^2(d) \prod_{p|d} \frac{1}{2p(p+1)}, \]

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
and assume that $i,j \in \{1,2\}$. Then, as $T \to \infty$, we have
\[ M^{ij}(T, d_0, m_0, n_0) \sim \frac{4}{\pi^3} \frac{1}{ij} \frac{T^2}{\log T} \left\{ \begin{array}{ll}
\left( \rho + \frac{1}{16} \rho d_0 \right) & \text{if } (d_0, m_0, n_0) \equiv (1,1,1) \mod 8, \\
\frac{1}{16} \rho d_0 & \text{if } (d_0, m_0, n_0) \not\equiv (1,1,1) \mod 8,
\end{array} \right. \]
where $\rho$ 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 $d_1 d_2 \leq T$. We next introduce a parameter $V_0$ and decompose
\[ M^{ij}(T, m_0, n_0, d_0) = M^{ij}_{\leq V_0}(T, m_0, n_0, d_0) + M^{ij}_{> V_0}(T, m_0, n_0, d_0), \]
where the first and second terms, respectively, correspond to the extra conditions $\max\{d_1, d_2\} \leq V_0$ and $\max\{d_1, d_2\} > V_0$. Writing $m = m_1 m_2$ and $n = n_1 n_2$, we trivially have
\[ |M^{ij}_{> V_0}(T, m_0, n_0, d_0)| \leq \sum_{\max\{d_1, d_2\} > V_0} \sum_{m,n \leq T/(d_1 d_2)} 1 \leq 2T^2 \sum_{d_1 < T} \frac{1}{d_1} \sum_{d_2 > V_0} \frac{1}{d_2}, \]
which finally gives
\[ M^{ij}_{> V_0}(T, m_0, n_0, d_0) \ll T^2 V_0^{-1}. \]
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 proving the same result but for $M^{ij}_{\leq V_0}(T, m_0, n_0, d_0)$.

By a straightforward adaptation of the arguments used at the beginning of Lemma 3 (where $m_1, m_2, n_1, n_2$ and $T/(d_1 d_2)$ 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 $M^{ij}_{\leq V_0}(T, m_0, n_0, d_0)$ is
\[ O((T/d_1 d_2)^2 \log^{-2}(T/d_1 d_2)) = O((T/d_1 d_2)^2 \log^{-2} T) \]
(see (12)), except if either
\[ m_1 \leq V, m_2 \geq V, n_1 \leq V, n_2 \geq V \]
or
\[ m_1 \geq V, m_2 \leq V, n_1 \geq V, n_2 \leq V. \]
Summing over all pairs of positive integers $(d_1, d_2)$ such that $\max\{d_1, d_2\} \leq V_0$ gives the total contribution of the order
\[ \sum_{d_1, d_2 \leq V_0} \frac{T^2}{(d_1 d_2)^2 \log^2 T} \ll \frac{T^2}{\log^2 T} \]
from all the cases, except from (26) and (27). Hence, we see that the total contribution from all the sextuples $(m_1, m_2, n_1, n_2, d_1, d_2)$ to the sum $M^{ij}_{\leq V_0}(T, m_0, n_0, d_0)$ is $O(T^2 \log^{-2} T)$, except if either
\[ m_1 \leq V, n_1 \leq V, m_2 \geq V, n_2 \geq V, d_1 \leq V, d_2 \leq V \]
or

\[(29) \quad m_1 \geq V, \ n_1 \geq V, \ m_2 \leq V, \ n_2 \leq V, \ d_1 \leq V, \ d_2 \leq V.\]

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

\[
M^{ij}_{<V_0}(T, m_0, n_0, d_0) = \sum_{\max\{m_1, n_1, d_1\} \leq V} \frac{\mu^2(2m_1n_1d_1)}{2^{\omega(m_2n_2d_2)}} S(m_1, n_1, d_1),
\]

where

\[
S(m_1, n_1, d_1) = \sum_{d_2 \leq V} \frac{\mu^2(2m_1m_2n_1n_2d_1d_2)}{2^{\omega(m_2n_2d_2)}} \left( \frac{d_2m_2}{n_1} \right) \left( \frac{d_2n_2}{m_1} \right) \left( \frac{n_2m_2}{d_1} \right) = \sum_{d_2 \leq V} \frac{\mu^2(2m_1m_2n_1n_2d_1d_2)}{2^{\omega(m_2n_2d_2)}} \left( \frac{d_2}{n_1m_1} \right) \left( \frac{m_2}{n_1d_1} \right) \cdot \sum_{V < m_2 \leq T/(jn_1d_1d_2)} \frac{\mu^2(n_2)}{2^{\omega(n_2)}} \left( \frac{n_2}{m_1d_1} \right).
\]

We now apply Lemma 11 to evaluate the last sum above according to the values of \(m_1, n_1\) and \(d_1\).

- If \(m_1d_1 \neq 1\), we consider the Jacobi character \(\left( \frac{m_2}{m_1d_1} \right)\). Lemma 11 yields

\[
S(m_1, n_1, d_1) \ll C \sum_{d_2 \leq V} \frac{T}{n_1d_1d_2} 2^{\omega(m_1n_1d_1)}(\log T)^{-C} \sum_{m_2 \leq T/(jn_1d_1d_2)} \frac{T^2}{m_1n_1d_1^2} \cdot \frac{2^{\omega(m_1n_1d_1)}}{\log C/T}.
\]

(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 11 to the Jacobi character \(\left( \frac{n_2}{n_1d_1} \right)\) obtaining

\[
S(m_1, n_1, d_1) \ll C 2^{\omega(m_1n_1d_1)} \frac{T^2}{n_1d_1} \cdot \frac{\log C}{T}.
\]

(31)

- If \(m_1 = n_1 = d_1 = 1\), which can only happen when \(m_0 = n_0 = d_0 = 1\), we are led to the sum

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

$$S(1, 1, 1) = \sum_{d \leq V} \frac{\mu^2(2d)}{2^\omega(d)} \sum_{c \leq V \atop \gcd(c, 2d) = 1} \frac{\mu(e)}{2^\omega(e)} \cdot \sum_{V/e \leq m_2 \leq T/(gcd(m_2, 2ed))} \frac{\mu^2(m_2)}{2^\omega(m_2)} \sum_{V/e \leq n_2 \leq T/(gcd(n_2, 2ed))} \frac{\mu^2(n_2)}{2^\omega(n_2)}.$$ 

Thus, using Lemma [11] we derive

$$S(1, 1, 1) = \sum_{d \leq V} \frac{\mu^2(2d)}{2^\omega(d)} \sum_{c \leq V \atop \gcd(c, 2d) = 1} \frac{\mu(e)}{2^\omega(e)} \cdot \sum_{m_2 \leq T/(gcd(m_2, 2ed)) = 1} \frac{\mu^2(m_2)}{2^\omega(m_2)} \sum_{n_2 \leq T/(gcd(n_2, 2ed)) = 1} \frac{\mu^2(n_2)}{2^\omega(n_2)} + O\left(\frac{T^2}{V}\right).$$

$$= \frac{1}{ij} \cdot \frac{16}{25} c(1)^2 \sum_{d \in \mathbb{N}} \frac{\mu^2(2d)}{d^2 2^{\omega(d)}(\log d)^{3/2}} \cdot \sum_{e \in \mathbb{N} \atop \gcd(e, 2d) = 1} \frac{\mu(e)}{e^{2^{\omega(e)}}} \prod_{p|ed} \left(1 + \frac{1}{2p}\right)^{-2} \cdot \frac{T^2}{\log T} + O\left(\frac{T^2}{\log^{3/2} T}\right).$$

We now evaluate (see [19])

$$= \frac{1}{ij} \cdot \frac{16}{25} c(1)^2 \sum_{d \in \mathbb{N}} \frac{\mu^2(2d)}{d^2 2^{\omega(d)}(\log d)^{3/2}} \cdot \sum_{e \in \mathbb{N} \atop \gcd(e, 2d) = 1} \frac{\mu(e)}{e^{2^{\omega(e)}}} \prod_{p|ed} \left(1 + \frac{1}{2p}\right)^{-2} \prod_{p|d} \left(1 - \frac{1}{4p^2(1 + \frac{1}{p})^2}\right)$$

$$= \frac{1}{ij} \cdot \frac{4}{\pi^3} \sum_{d \in \mathbb{N}} \frac{\mu^2(2d)}{d^{2^{\omega(d)}}} \prod_{p|d} \left(1 + \frac{1}{p}\right)^{-1}$$

$$= \frac{1}{ij} \cdot \frac{4}{\pi^3} \prod_{p \geq 3} \left(1 + \frac{1}{2p(p + 1)}\right) = \frac{1}{ij} \cdot \frac{4}{\pi^3} \theta.$$ 

Therefore,

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

$$M_{ij}^{(28)}(T, m_0, n_0, d_0) = \begin{cases} \left( \frac{4p}{\pi^3 ij} + o(1) \right) \frac{T^2}{\log T} & \text{for } (m_0, n_0, d_0) \equiv (1, 1, 1) \mod 8, \\ O\left( \frac{T^2}{\log^2 T} \right) & \text{otherwise,} \end{cases}$$

as $T \to \infty$.

The case (29). The contribution to the sum $M_{ij}^{(28)}(T, m_0, n_0, d_0)$ of the sextuples in this case is

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

where

$$S^*(m_2, n_2, d_2) = \sum_{d_1 \leq V} \frac{\mu^2(2m_1 m_2 n_2 d_1 d_2)}{2^{\omega(m_1 m_2 n_2 d_1 d_2)}} \left( \frac{d_2 n_2}{m_1} \right) \left( \frac{m_2 n_2}{d_1} \right) \sum_{V < n_1 \leq T/(j n_2 d_1 d_2)} \frac{\mu(n_1)}{2^{\omega(n_1)}} \left( \frac{d_2 m_2 n_1}{n_1} \right).$$

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

$$S^*(1, 1, 1) = \sum_{d_1 \leq V} \frac{\mu^2(m_1 n_1 d_1)}{2^{\omega(m_1 n_1 d_1)}} \sum_{d_1 \mid d_0 \mod 8} \frac{\mu^2(d)}{2^{\omega(d)}} \prod_{p \mid d} \frac{1}{p + 1} \frac{T^2}{\log T},$$

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

$$M_{ij}^{(28)}(m_0, n_0, d_0) = \frac{1 + o(1)}{4ij \pi^3}, \sum_{d \equiv d_0 \mod 8} \mu^2(d) \prod_{p \mid d} \frac{1}{2p(p+1)} \frac{T^2}{\log T},$$

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.

\[\square\]

2.3. \textbf{Proof of Proposition 2.} We follow the proof of [4, Theorem 1]. We restrict ourselves to the case \(A = B = T\) and decide not to estimate the error terms implicitly contained in the formulas of Proposition 2.

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

\[\mu^2(2mn) = 1,\ 1 < m, n \leq T,\ cm \equiv \square \mod n & \eta n \equiv \square \mod m.\]

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

\[\sum_{1 < m, n \leq T} \mu^2(2mn) \prod_{p|m} \left[ 1 + \left( \frac{\eta n}{p} \right) \right] \prod_{p|n} \left[ 1 + \left( \frac{cm}{p} \right) \right].\]

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

\[\kappa_{\epsilon,\eta}(a, c) = \left( \frac{a}{c} \right) \left( \frac{c}{a} \right) \left( \frac{\epsilon}{a} \right) \left( \frac{\eta}{c} \right),\]

to finally reach the equality

\[N_{\epsilon,\eta}(T) = \sum_{ab \leq T, cd \leq T} \mu^2(2abcd) \prod_{p|abcd} \left( \frac{d}{c} \right) \kappa_{\epsilon,\eta}(a, c).\]

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

\[N_{\epsilon,\eta}(T) = \sum_{a_0 = \pm 1} \sum_{c_0 = \pm 1} \kappa_{\epsilon,\eta}(a_0, c_0) M(T, a_0, c_0),\]

where \(M(T, a_0, c_0)\) is given by \((38)\).

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

\[\kappa_{\epsilon,\eta}(a_0, c_0) = \begin{cases} 1 & \text{if } a_0 \equiv c_0 \equiv 1 \mod 4, \\ \epsilon & \text{if } a_0 \equiv -c_0 \equiv 1 \mod 4, \\ \eta & \text{if } a_0 \equiv -c_0 \equiv -1 \mod 4, \\ -\epsilon\eta & \text{if } a_0 \equiv c_0 \equiv -1 \mod 4. \end{cases}\]

Using Lemma \((30)\) together with the relations \((40)\) and \((41)\) with \(\epsilon = \eta = 1\), we obtain

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

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

2.4. \textbf{Proof of Proposition 3.} From the properties of the Jacobi symbols, we have the basic equality

\[N_{\epsilon,\eta}^{ij}(T) = \sum_{d \in \mathbb{N}, m \leq T/(id), n \leq T/(jd)} \mu^2(2mnt) \prod_{p|mnt} \left[ 1 + \left( \frac{njdn}{p} \right) \right] \left( 1 + \left( \frac{cimd}{p} \right) \right) \left( 1 + \left( \frac{-\epsilon\eta jmn}{p} \right) \right).\]
We now expand the three products in each sum, use the multiplicativity property of the Jacobi symbols, factor $m = m_1 m_2$, $n = n_1 n_2$ and $d = d_1 d_2$, and introduce the functions $\kappa_{\epsilon, \eta}(m, n, d)$ and $\varsigma_{i,j}(m, n, d)$ defined as

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

and

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

to finally reach the equality

$$N^{ij}_{\epsilon, \eta}(T) = \sum_{d_1, d_2, m_1, m_2, n_1, n_2 \in \mathbb{N}} \mu^2(2m_1 m_2 n_1 n_2 d_1 d_2) \frac{1}{2^\nu(m_1 m_2 n_1 n_2 d_1 d_2)} \cdot \left(\frac{d_1 m_2}{n_1}\right) \left(\frac{d_2 n_2}{m_1}\right) \left(\frac{n_2 m_2}{d_1}\right) \varsigma_{i,j}(m, n, d) \kappa_{\epsilon, \eta},$$

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

$$N^{ij}_{\epsilon, \eta}(T) = \sum_{(m_0, n_0, d_0) \in \{\pm 1, \pm 3\}^3} \varsigma_{i,j}(m_0, n_0, d_0) \kappa_{\epsilon, \eta}(m_0, n_0, d_0) M^{ij}(T, m_0, n_0, d_0),$$

where $M^{ij}(T, m_0, n_0, d_0)$ is given by formula (23). At this stage, note thatLemma 3 and identity (42) together imply that

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

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

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

Fixing $d_0$ and summing over all the 16 possible values of $(m_0, n_0) \in \{\pm 1, \pm 3\}^2$, we obtain

$$\sum_{(m_0, n_0) \in \{\pm 1, \pm 3\}^2} \varsigma_{i,j}(m_0, n_0, d_0) = \left[1 + \left(\frac{1}{3}\right)\right] \cdot \left[1 + \left(\frac{1}{3}\right)\right] \cdot \left[2 - (1 - \epsilon)(1 - \eta)\right].$$
Finally, if \( \alpha \) is the quantity defined in the statement of Proposition 3, we then have

\[
\sum_{(d_0,m_0,n_0) \in \{\pm 1, \pm 3\}^3} \rho_{d_0} \zeta_{\xi,\eta} = 4 \cdot (\alpha - 4) \cdot \sum_{d_0 \in \{\pm 1, \pm 3\}} \rho_{d_0} = 4 \cdot (\alpha - 4) \cdot \rho.
\]

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

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

\[
p \mid b, \ p \nmid 2a \Rightarrow p \equiv 1 \mod 4.
\]

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 notation of Section 2.2 and in particular of the proof of Lemma 4, a typical main term is

\[
\sum_{a \leq T} \mu^2(a) \sum_{\substack{b \leq T \mid p \mid d, \ p \nmid 2a \Rightarrow p \equiv 1 \mod 4}} \frac{\mu^2(b)}{2\omega(ab)}
\]

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

\[
\sum_{d \in \mathbb{N}} \left( \sum_{a \leq T/d} \mu^2(a) \right) \sum_{\substack{b \leq 2T/d \mid p \equiv 1 \mod 4}} \frac{\mu^2(b)}{2\omega(b)} \ll \frac{T}{\log^2 T} \cdot \frac{T}{\log^3 T},
\]

by appealing to general bounds for sums of multiplicative functions (see, for instance, [13, 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 a restriction on 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. Hilbert symbols, quadratic forms and the sets \( \mathcal{F}_3 \) and \( \mathcal{F}_{D_4} \)

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 \( \mathcal{F}_3 \) if and only if

\[
-m_1 n_1 \equiv \square \mod d, \quad -m \equiv \square \mod n_1, \quad \text{and} \quad -n \equiv \square \mod m_1.
\]

In particular, \((m, n)\) belongs to \( \tilde{\mathcal{F}}_3 \) if and only if \( \mu^2(2mn) = 1 \) and

\[
-m \equiv \square \mod n \quad \text{and} \quad -n \equiv \square \mod m.
\]

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
holds if and only if

Next, we remark that when

for every

condition (47) holds if and only if the condition (46) holds.

due to the negativity of

the Hilbert product formula

\[
\prod_{p \mid \Delta} \left| p \right| = 839,
\]

we have (45) and (47) are equivalent. Note that we can avoid the tedious case

\[
\text{Lemma 6.} \quad \text{Let } (m,n) \text{ be a pair of squarefree integers } > 1. \text{ Then } (m,n) \text{ belongs to } F_{D_4} \text{ if and only if at least one of three quadratic forms}
\]

\[
\begin{align*}
X^2 + mY^2 - nZ^2 &= 0, \\
X^2 + nY^2 - mZ^2 &= 0, \\
X^2 - mY^2 - nZ^2 &= 0
\end{align*}
\]

(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 \((m,n) \in F\), we have that \((m,n) \in F_{C_4 \times C_4}\) 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, \(F_{C_2 \times C_4}\)
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 \cite{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

\[ \# \mathcal{K}(T) = \left( \frac{6}{\pi^2} \vartheta + o(1) \right) \frac{T}{\sqrt{\log T}}, \quad \text{as } T \to \infty, \]

where \(\vartheta\) is the Landau–Ramanujan constant in \cite{11}. Indeed, this follows from the standard inclusion-exclusion principle applied to the set of sums of two squares and the observation that if \(n = d^2m\) for some integers \(d, m, n,\) then \(n\) is a sum of two squares if and only 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 \(O\left(\frac{T^2}{\log T}\right)\) 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 \(O\left(\frac{T^2}{\log T}\right)\).

From the above discussion, we deduce that

\[ \mathcal{C}_2 \times \mathcal{C}_4(T) = 2 \# \{(m, n) \in \mathcal{F} \mid m, d \mid n, m/d \in \mathcal{K}, n/d \in \mathcal{K}\} + O\left(\frac{T^2}{\log T}\right), \]

which is equivalent to the statement of Theorem \ref{thm:main}.

4.2. Proof of Theorem \ref{thm:main}. We appeal to Proposition \ref{prop:ternaryforms} on the solvability of ternary quadratic forms \(aX^2 + bY^2 + cZ^2 = 0\) and to Lemma \ref{lem:inclusion-exclusion}. The conditions concerning the signs of \(a, b,\) and \(c\) are trivially verified here. Using symmetry and the inclusion–exclusion principle, we get the equality

\[ \# \mathcal{F}_{D_4}(T) = \sum_{(i,j) \in \{1,2\}} \left( N_{i,1}^{ij}(T) + N_{i,-1}^{ij}(T) + N_{-1,1}^{ij}(T) \right) + O\left( \# \{(a, b) \in \mathcal{F}(T), a \text{ and } -a \equiv \square \text{ mod } b \& b \equiv \square \text{ mod } a \} \right). \]

A direct application of Propositions \ref{prop:inclusion-exclusion} and \ref{prop:ternaryforms} easily leads to

\[ \# \mathcal{F}_{D_4}(T) = \left( \frac{33}{\pi^3} \cdot \vartheta + o(1) \right) \frac{T^2}{\log T}, \quad \text{as } T \to \infty, \]

which is what we wanted to prove.
Note 3. Suppose that $m$ and $n$ are odd, squarefree, coprime, and in the residue class $1 \mod 4$. 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 $m \equiv □ \mod n$ and $n \equiv □ \mod m$). 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 $K$ which is a $C_4$–extension of $\mathbb{Q}(\sqrt{D})$, and which is unramified at any place. Furthermore, we have $\text{Gal}(K_4, \mathbb{Q}) = D_4$. In conclusion, in that particular case, we can say more about the extension $K$ we want to build over $\mathbb{Q}(\sqrt{m}, \sqrt{n})$.

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

$$\sharp \mathcal{F}_{D_4}(T) = \sum_{(i, j) \in \{1, 2\}} N^{ij}_{1,-1}(T).$$

Finally, we apply Proposition 3 and deduce that

$$\sharp \mathcal{F}_{D_4}(T) = \left( \frac{2}{1 \cdot 1} + \frac{4}{1 \cdot 2} + \frac{4}{2 \cdot 1} + \frac{4}{2 \cdot 2} \right) \frac{1}{\pi^3} \cdot \rho + o(1) \right) \frac{T^2}{\log T}, \quad \text{as } T \to \infty,$$

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

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

which is what we wanted to prove.

5. Conclusion

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

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

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

and $\gamma$ 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, the second author was supported in part by grant SEP-CONACyT 79685, the third author was supported in part by grant P.R.I.N. 2006 “Problemi diofantei e analitici in Teoria dei Numeri”, and the fourth author 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


Laboratoire de Mathématiques d’Orsay, CNRS, Université Paris-Sud, F-91405 Orsay Cedex, France

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

Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México

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

Dipartimento di Matematica, Università Roma Tre, Largo S. L. Murialdo, 1, Roma, 00146, Italy

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

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

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