THE PARITY OF THE PERIOD OF THE CONTINUED FRACTION OF $\sqrt{d}$

ÉTIENNE FOUVRY AND JÜRGEN KLÜNERS

Abstract. We prove that, asymptotically, in the set of squarefree integers d, not divisible by primes congruent to 3 mod 4, the period of the expansion of $\sqrt{d}$ in continued fractions is more frequently odd than even.

1. Statement of the results

The subject of the expansion of the real numbers in simple continued fractions remains a very opaque domain in the theory of numbers. One of the very few achievements of this theory is the following famous theorem due to Lagrange (see [22, Theorem 3 p. 317], for instance).

Theorem A. *Let d be a non square positive integer. Then the irrational number $\sqrt{d}$ has a periodic expansion in simple continued fractions.*

With the classical notations, we have the equality

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \cdots, a_s}].$$

In that formula, $s = s(d)$ is the period of the expansion, and we have the equality $a_t = a_{s-t}$, for any $1 \leq t \leq s-1$ and also the inequality $s < 2d$. Hence Theorem A defines an application $s : d \mapsto s(d)$, from the set of non square integers to $\mathbb{N}^*$. The image of s is equal to $\mathbb{N}^*$ (see [22, Theorem 6 p.325]) and more precisely for every positive integer s_0, the equation $s(d) = s_0$ has infinitely many solutions in d. Recall that if the real number α has an ultimately periodic expansion in continued fractions, then α is an algebraic number of degree 2 (see [22, p.328] for instance).

The application s is very mysterious at many points of view. Here we shall be concerned by the frequency of the odd values of this function. We recall a very useful link between the parity of $s(d)$ and the associated negative Pell equation.

Theorem B. [22, Theorem 9 p.333] *Let d be a non square positive integer. Then the associated period $s(d)$ is odd if and only if the equation*

$$x^2 - dy^2 = -1 \tag{1}$$

is solvable in integers x and y.

By easy congruence considerations, we see that

$$(1) \text{ solvable } \Rightarrow \ (p \mid d \Rightarrow p \not\equiv 3 \bmod 4).$$

By convention, the letter p is reserved to prime numbers throughout this paper. If a is a positive integer, then $v_p(a)$ and $\omega(a)$ will denote the p–adic valuation of a

Date: October 2, 2008.

2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R11.

and its number of distinct prime divisors. The Möbius function of a is $\mu(a)$ and the Euler function is $\phi(a)$. If a and $k \geq 0$ are integers, we also use the notation $p^k \mid\mid a$ to say that $v_p(a) = k$.

A classical application of the half dimensional sieve (or of Landau's Theorem concerning integers which are sums of two squares [1, Satz 1.8.2]) implies the equality

$$\sharp \left\{ d \leq X\,;\ p \mid d \Rightarrow p = 2 \text{ or } p \equiv 1 \bmod 4 \right\} = O\Big(\frac{X}{\sqrt{\log X}}\Big),$$

as $X \to \infty$. This proves that, for almost d, the period $s(d)$ is even, more precisely, we have

$$\sharp \left\{ d \leq X\,;\ d \text{ not a square and } s(d) \equiv 0 \bmod 2 \right\} = X + O\Big(\frac{X}{\sqrt{\log X}}\Big).$$

Hence the question of the parity of $s(d)$ is highly more interesting if we restrict the set of definition of s to the set

$$\mathcal{A} := \left\{ d;\ d \text{ squarefree, } d \geq 2,\ p \mid d \Rightarrow p = 2 \text{ or } p \equiv 1 \bmod 4 \right\}, \tag{2}$$

and its two natural subsets $\mathcal{A}_{\text{even}}$ and $\mathcal{A}_{\text{odd}}$ corresponding to the extra condition d even and d odd, respectively. We introduce the counting function

$$\mathcal{A}(X) := \sharp\big(\mathcal{A} \cap [2, X]\big), \tag{3}$$

and its analogues $\mathcal{A}_{\text{odd}}(X)$, $\mathcal{A}_{\text{even}}(X)$. The set $\mathcal{A}$ is a rather dense subset of integers, since, for $X \to \infty$, it satisfies

$$\mathcal{A}_{\text{odd}}(X) \sim \frac{8}{9} \cdot C \cdot \frac{X}{\sqrt{\log X}},$$

$$\mathcal{A}_{\text{even}}(X) = \mathcal{A}_{\text{odd}}(X/2) \sim \frac{4}{9} \cdot C \cdot \frac{X}{\sqrt{\log X}},$$

which leads to

$$\mathcal{A}(X) \sim \frac{4}{3} \cdot C \cdot \frac{X}{\sqrt{\log X}}, \tag{4}$$

with

$$C = \frac{9}{8\pi} \prod_{p \equiv 1 \bmod 4} (1 - p^{-2})^{\frac{1}{2}}.$$

These asymptotic formulae are consequences of Landau's Theorem (see [23, p.122], [4, §1]). The intrusion of the condition d *squarefree* in the definition (2), will be explained in §1 below. Also let

$$\mathcal{A}^- := \left\{ d;\ d \in \mathcal{A},\ s(d) \equiv 1 \bmod 2 \right\},$$

and its two subsets $\mathcal{A}^-_{\text{odd}}$ and $\mathcal{A}^-_{\text{even}}$. Also let $\mathcal{A}^-(X)$, $\mathcal{A}^-_{\text{odd}}(X)$ and $\mathcal{A}^-_{\text{even}}(X)$ be their counting functions, up to the bound X.

The present work is motivated by the following questions:

(5) *What are the relative sizes of* $\mathcal{A}^-(X)$*and* $\mathcal{A}(X)$?

and the easier one

(6) *Is it true that asymptotically, 50 % of the elements* $d \in \mathcal{A}$ *satisfy* $s(d)$*odd ?*

Of course, the same type of questions apply to the restricted subsets $\mathcal{A}_{\text{odd}}$ and $\mathcal{A}_{\text{even}}$.

Actually, we shall adopt another point of view of these questions: it is also well known that the question of the solvability of (1) has a rich interpretation in the domain of algebraic number theory. To be more precise, to any $d \in \mathcal{A}$ we associate the integer D defined by

$$D = \begin{cases} d & \text{if } d \text{ is odd,} \\ 4d & \text{if } d \text{ is even.} \end{cases}$$

The discriminant of the field $\mathbb{Q}(\sqrt{d})$ is D precisely. We give the name of *special discriminant* to such a discriminant. The set of the special discriminants is denoted by $\mathcal{D}$. It clearly satisfies the equality

$$\mathcal{D} := \big\{D \geq 2\,;\, v_p(D) = 0 \text{ if } p \equiv 3 \bmod 4, \\ v_p(D) = 0 \text{ or } 1 \text{ if } p \equiv 1 \bmod 4 \text{ and } v_2(D) = 0 \text{ or } 3\big\},$$

and is split into two natural subsets $\mathcal{D}_{\text{odd}}$ and $\mathcal{D}_{\text{even}}$. We also denote a fundamental unit of $\mathbb{Q}(\sqrt{D})$ by ϵ_D and the norm function in this field is denoted by $\mathcal{N}$. Now we recall the following classical result (see [23, p. 122]):

Proposition 1. *With the above notations, let d an element of $\mathcal{A}$. Then we have*

$$(1) \textit{ solvable} \iff \mathcal{N}(\epsilon_D) = -1.$$

Hence, for $d \in \mathcal{A}$, we have seen that the problem of the parity of $s(d)$ is equivalent to the solvability of (1) and to the value of $\mathcal{N}(\epsilon_D)$. However, the last approach certainly is the more attractive one, since we can incorporate many of the tools of algebraic number theory. The results can equivalently enunciated in terms of the counting functions associated to the set $\mathcal{A}$ or to the set $\mathcal{D}$. Let

$$\mathcal{D}^- := \{D \in \mathcal{D}\ ;\ \mathcal{N}(\epsilon_D) = -1\},$$

and its two natural subsets $\mathcal{D}^-_{\text{odd}}$ and $\mathcal{D}^-_{\text{even}}$ be its two natural subsets. For $X \geq 2$, the symbols $\mathcal{D}(X)$, $\mathcal{D}_{\text{odd}}(X)$, $\mathcal{D}_{\text{even}}(X)$, $\mathcal{D}^-(X)$, $\mathcal{D}^-_{\text{odd}}(X)$, $\mathcal{D}^-_{\text{even}}(X)$ are the associated counting functions defined similarly as in (3). We remark that there are the following trivial equalities:

$$\mathcal{D}_{\text{odd}}(X) = \mathcal{A}_{\text{odd}}(X) \text{ and } \mathcal{D}_{\text{even}}(X) = \mathcal{A}_{\text{even}}(X/4) = \mathcal{A}_{\text{odd}}(X/8).$$

We shall make some progress in the study of the first question (5), but our result, though not complete, will be strong enough to answer negatively to the second one (6). The answer to (6) is negative also for the restricted subsets $\mathcal{A}_{\text{even}}$ and $\mathcal{A}_{\text{odd}}$. To present the results, we firstly introduce the constant

$$\alpha := \prod_{j \text{ odd}} (1 - 2^{-j}) = \prod_{j=1}^{\infty} (1 + 2^{-j})^{-1} = .41942\cdots$$

and

$$c_k = \prod_{j=0}^{k-1} (2^j + 1), \ k = 0, 1, 2, \ldots \tag{7}$$

In [4, Theorem 1] we proved

Theorem C. *As X tends to infinity, we have*

$$\big(\alpha - o(1)\big)\ \mathcal{A}(X) \leq\ \mathcal{A}^-(X) \leq \big(\frac{2}{3} + o(1)\big)\ \mathcal{A}(X).$$

Similar inequalities are true for the restricted subsets $\mathcal{A}_{\rm even}$ and $\mathcal{A}_{\rm odd}$. Analogous inequalities also hold for the set $\mathcal{D}$ and its restricted subsets $\mathcal{D}_{\rm even}$ and $\mathcal{D}_{\rm odd}$.

The purpose is to improve the constant α appearing in the lower bound to a constant $> 1/2$. More precisely, we shall prove

Theorem 1. *As X tends to infinity, we have*

$$\mathcal{A}^-(X) \geq \Bigl(\frac{5\alpha}{4} - o(1)\Bigr)\ \mathcal{A}(X).$$

Similar statements are true for the sets $\mathcal{A}^-_{\rm even}$ and $\mathcal{A}^-_{\rm odd}$, and also for $\mathcal{D}^-$, $\mathcal{D}^-_{\rm even}$ and $\mathcal{D}^-_{\rm odd}$

In familiar words, Theorem 1 asserts that in $\mathcal{A}$ (and also in $\mathcal{A}_{\rm odd}$ and in $\mathcal{A}_{\rm even}$), at least 52% of the elements d are such $\sqrt{d}$ has an odd period for its expansion in continued fraction. Hence we may now give a negative answer to the question (6). Similarly, we can state that in $\mathcal{D}$ – and also in $\mathcal{D}_{\rm even}$, and in $\mathcal{D}_{\rm odd}$ – at least 52% of the special discriminants D satisfy $\mathcal{N}(\epsilon_D) = -1$.

The preceding work [4] was motivated by an important paper of Stevenhagen [23], where the author constructed a clever and convincing probabilistic model to guess the answer to the question (5). His investigations led him to enunciate

Conjecture 1. [23, Conj.1.2]. *As X tends to infinity, we have*

$$\mathcal{A}^-(X) \sim (1-\alpha)\ \mathcal{A}(X).$$

Analogous asymptotic behaviors are also true for $\mathcal{A}_{\rm odd}$, $\mathcal{A}_{\rm even}$, $\mathcal{D}$, $\mathcal{D}_{\rm odd}$ and $\mathcal{D}_{\rm even}$.

Stevenhagen has chosen to enunciate his conjecture in the context of the set of the solvability of (1), but his probabilistic model is built on the algebraic structure of the ideal class group associated with $\mathbb{Q}(\sqrt{D})$. The inequalities

$$5\alpha/4 = .52475 < 1-\alpha = .58057\cdots\ < 2/3,$$

show that the results of Theorems C & 1 go in the direction of the truth of Conjecture 1. We also remark that it is out of reach of present computers to exhibit a large X such that $\mathcal{A}^-(X)/\mathcal{A}(X)$ is close to 0.58 (see [23, p. 123, 2nd column]).

We may ask if it is possible to generalize Theorem 1 to subsets of integers larger than $\mathcal{A}$. The main question is to know if one can smoothen the condition d *square-free* contained in the definition (2) of $\mathcal{A}$. One part of the answer is rather simple since we have

Lemma 1. *Let d be an integer and p an odd divisor of d. Then*

$$(1)\ \textit{solvable for } d \iff (1)\ \textit{solvable for } dp^2.$$

Proof. The only non trivial part is to prove that if (1) is solvable for d, it is also solvable for dp^2. It suffices to check that the integers T and U defined by $T+U\sqrt{d} = (t+u\sqrt{d})^p$ (where $t^2-du^2=-1$) are such that $p \mid U$ and satisfy $T^2-dU^2=-1$ (see [18, Satz 1]). □

So we can extend the results to the set

$$\tilde{\mathcal{A}} := \bigl\{d \geq 2\,;\, v_p(d) = 0 \text{ if } p \equiv 3 \bmod 4,$$
$$v_p(d) \in \{0,\,1,\,3,\,5,\,7,\dots\} \text{ if } p \equiv 1 \bmod 4 \text{ and } v_2(d) = 0 \text{ or } 1\bigr\},$$

However, in the literature, we did not find easy criterions which link the solvability of (1) for $d \in \mathcal{A}$ and the solvability of the same equation for dp^2 for $p \not| \, d$ and $p \not\equiv 3 \bmod 4$. For instance, (1) is solvable for $d = 5$, solvable for $d = 5 \cdot 13^2$, but not solvable for $d = 5 \cdot 29^2$ (we trivially have $s(5) = 1$ and, with the help of a computer we find $s(5 \cdot 13^2) = 5$ and $s(5 \cdot 29^2) = 12$). In the opposite direction, if (1) is not solvable for some $d = d_0$ then it is trivially not solvable for any $d = d_0 \cdot p^2$. Following these investigations would have led our present work out of its initial scope.

2. Sketch of the proof of Theorem 1

2.1. **The 2^k–rank of the class groups.** Let D be a fundamental discriminant, *i.e.* the discriminant of a quadratic field, real or complex. On the set of non zero ideals of the ring of integers $\mathcal{O}_D$ of $\mathbb{Q}(\sqrt{D})$, equipped with the multiplication of ideals, we can define two group structures

- *the ordinary class group* denoted by Cl_D,

and

- *the narrow class group* denoted by C_D .

The first one is obtained by saying that two non zero ideals $\mathfrak{I}$ and $\mathfrak{J}$ of $\mathcal{O}_D$ are equivalent, if and only if, there exists $a \in \mathcal{O}_D$, such that $\mathfrak{I} = (a)\,\mathfrak{J}$. For the second one, we impose the extra condition $\mathcal{N}(a) > 0$. These two definitions of course coincide when $D < 0$. Playing with the sign of $\mathcal{N}(\epsilon_D)$, we have the following well known result (e.g. see [4, Lemma 8]):

Lemma 2. *Let $D \in \mathcal{D}$ be a special discriminant. Then*

$$D \in \mathcal{D}^- \iff \mathrm{C}_D \simeq \mathrm{Cl}_D.$$

Since the group Cl_D is factor group of C_D of index at most 2, we have

$$\mathrm{rk}_{2^k}(\mathrm{Cl}_D) \leq \mathrm{rk}_{2^k}(\mathrm{C}_D) \leq \mathrm{rk}_{2^k}(\mathrm{Cl}_D) + 1 \text{ for all } k \geq 1,$$

and

$$\mathrm{rk}_{p^k}(\mathrm{Cl}_D) = \mathrm{rk}_{p^k}(\mathrm{C}_D) \text{ for all } p \geq 3 \text{ and } k \geq 1.$$

As usual $\mathrm{rk}_{p^k}(A)$ is the p^k–rank of the abelian group A and is defined by the equality $\mathrm{rk}_{p^k}(A) = \dim_{\mathbb{F}_p} A^{p^{k-1}}/A^{p^k}$. It is now easy to see that Lemma 2 has the equivalent form

$$D \in \mathcal{D}^- \iff \mathrm{rk}_{2^k}(\mathrm{C}_D) = \mathrm{rk}_{2^k}(\mathrm{Cl}_D) \text{ for all } k \geq 1. \tag{8}$$

However for $D \in \mathcal{D}$, we have the equality

$$\mathrm{rk}_2(\mathrm{Cl}_D) = \mathrm{rk}_2(\mathrm{C}_D) = \omega(D) - 1. \tag{9}$$

The second equality of (9) is a particular case of a famous result of Gauss, the first one is recalled in [4, Lemma 1]. Its proof can be found in [6, p. 518]. Now we transform (8) into

Lemma 3. *Let $D \in \mathcal{D}$. Then*

$$D \in \mathcal{D}^- \iff \mathrm{rk}_{2^k}(\mathrm{C}_D) = \mathrm{rk}_{2^k}(\mathrm{Cl}_D) \textit{ for all } k \geq 2.$$

In [4, Corollary 2], we proved, that, as $X \to \infty$, we have

$$\sharp\big\{D \in \mathcal{D}\,;\, D \leq X,\, \mathrm{rk}_4(\mathrm{C}_D) = r\big\} \sim \alpha_\infty(r) \cdot \mathcal{D}(X) \ (r = 0,\, 1,\, 2, \dots). \tag{10}$$

with

$$\alpha_\infty(r) = \frac{\alpha}{\prod_{j=1}^r (2^j - 1)}.$$

The result (10) is also true for $\mathcal{D}_{\text{odd}}$ and $\mathcal{D}_{\text{even}}$ and perfectly fits to a prediction of Stevenhagen [23, Conj 3.4 (ii)]. Choosing $r = 0$ in (10), we obtain

$$\sharp\big\{D \in \mathcal{D}\,;\, D \leq X,\, \mathrm{rk}_4(\mathrm{C}_D) = 0\big\} \sim \alpha \cdot \mathcal{D}(X) \tag{11}$$

and noticing that Lemma 3 trivially implies

$$D \in \mathcal{D} \text{ and } \mathrm{rk}_4(\mathrm{C}_D) = 0 \Rightarrow D \in \mathcal{D}^-, \tag{12}$$

we recover the proof of the lower bound contained in Theorem C.

To improve the lower bound contained in Theorem 1, we shall consider another easy consequence of Lemma 3, independent from (12)

$$D \in \mathcal{D},\, \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{Cl}_D) = 1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D) = 0 \Rightarrow D \in \mathcal{D}^-. \tag{13}$$

In §3 we shall deduce from Theorem 3

Theorem 2. *The following equalities hold:*

$$\sharp\big\{D \in \mathcal{D}\,;\; D \leq X,\; \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{Cl}_D) = 1 \textit{ and } \mathrm{rk}_8(\mathrm{C}_D) = 0\big\} = \big(\frac{\alpha}{4} + o(1)\big) \cdot \mathcal{D}(X)$$

and

$$\sharp\big\{D \in \mathcal{D}\,;\; D \leq X,\; \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{Cl}_D) = 1 \textit{ and } \mathrm{rk}_8(\mathrm{C}_D) = 1\big\} = \big(\frac{\alpha}{4} + o(1)\big) \cdot \mathcal{D}(X).$$

Similar equalities are also true for the restricted subsets $\mathcal{D}_{\text{odd}}$ and $\mathcal{D}_{\text{even}}$.

The set of which the cardinality is asymptotically evaluated in Theorem 2 has an empty intersection with the set encountered in (11). Adding the cardinalities of these two sets and using (12) and (13) we see that Theorem 1 is a consequence of (11) and Theorem 2.

2.2. **The central result.** We shall be mainly occupied by the proof of

Theorem 3. *There exists a function λ_D defined on the set $\mathcal{D}$ satisfying the following conditions*
(i) the function 2^{λ_D} takes its values in the set $\{1, 2, 3, \dots\}$,
(ii) for every $D \in \mathcal{D}$, we have the inequalities

$$\mathrm{rk}_8(\mathrm{C}_D) \leq \lambda_D \leq \mathrm{rk}_4(\mathrm{Cl}_D) \leq \mathrm{rk}_4(\mathrm{C}_D),$$

(iii) when $\mathrm{rk}_4(\mathrm{C}_D) \leq 1$, we have the equality $\lambda_D = \mathrm{rk}_8(\mathrm{C}_D)$,
(iv) for every $\epsilon > 0$, for every $k \geq 0$, we have the equality

$$\sum_{\substack{D \in \mathcal{D}\\ D \leq X}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)} \cdot 2^{\lambda_D} = c_k \cdot (2^{k-2} + 1) \cdot \mathcal{D}(X) + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2} - \frac{1}{2^{k+2}} + \epsilon}\big), \tag{14}$$

where c_k is defined in (7),
(v) equalities similar to (14) are also true for the restricted subsets $\mathcal{D}_{\text{odd}}$ and $\mathcal{D}_{\text{odd}}$.

The function λ_D will be explicitly defined in Definition 2 below. Since the definition is not so easy, we prefer to postpone it. Remark that in (14), the last term is an error term, this follows from (4). We also remark that (10) and (iii) imply that we have the equality $\mathrm{rk}_8(C_D) = \lambda_D$ at least for 83.8% of the $D \in \mathcal{D}$. This is a consequence of the equality $\alpha_\infty(0) = \alpha_\infty(1) = \alpha$.

3. From Theorem 3 to Theorem 2

We assume that Theorem 3 is proved and we restrict the proof of Theorem 2 to the case of the whole set $\mathcal{D}$, since the cases of $\mathcal{D}_{\rm odd}$ and $\mathcal{D}_{\rm even}$ are absolutely similar. What follows already appears in [3] and [4] and is a slight modification of [4, §2.2]. This illustrates the theory of moments.

For a and b positive integers, and $X \geq 5$, let $\Delta_X(a,b)$ be the density of the set of $D \in \mathcal{D}$ such that $D \leq X$, $2^{{\rm rk}_4({\rm C}_D)} = a$ and $2^{\lambda_D} = b$. In other words

$$\Delta_X(a,b) := \frac{\sharp\ \{D \in \mathcal{D};\, D \leq X,\, 2^{{\rm rk}_4({\rm C}_D)} = a \text{ and } 2^{\lambda_D} = b\}}{\mathcal{D}(X)}. \tag{15}$$

We write (14) in the form

$$\sum_{a=1}^{\infty} a^k \Big(\sum_b b\ \Delta_X(a,b)\Big) = \Gamma_k + o_k(1) \quad (X \to \infty,\ k = 0,\, 1,\, 2,\, \cdots), \tag{16}$$

with

$$\Gamma_k = c_k \cdot (2^{k-2} + 1). \tag{17}$$

By the conditions (i) and (ii) of Theorem 3 we can restrict the summation in (16) to the cases, where a is a power of 2 and b is a positive integer less than a. Write $a = 2^n$ and

$$\xi(n, X) := \sum_{b=1}^{2^n} b\, \Delta_X(2^n, b). \tag{18}$$

With these conventions we see that (16) is equivalent to

$$\sum_{n=0}^{\infty} \xi(n,X) \cdot 2^{kn} = \Gamma_k + o_k(1) \quad (X \longrightarrow \infty,\ k = 0, 1,\, 2, \dots). \tag{19}$$

Applying (19) with k replaced by $k+1$ and using positivity, we obtain

$$\xi(n,X) \cdot 2^{(k+1)n} = O_k(1),$$

which leads to

$$0 \leq \xi(n,X) = O_k(2^{-(k+1)n}), \tag{20}$$

uniformly for $X \geq 5$ and $n \geq 0$. By an infinite diagonal process, we construct an increasing sequence $\mathcal{M}$ of integers m and real numbers $\xi_n \geq 0$ such that for every $n \geq 0$ we have

$$\xi(n,m) \to \xi_n,$$

as $m \in \mathcal{M}$ tends to infinity. We can give a better lower bound of ξ_n by the following considerations. By the definition of (18) we have the inequality

$$\xi(n,X) \geq \sum_{b=1}^{2^n} \Delta_X(2^n, b) = \frac{\#\{D \in \mathcal{D}; D \leq X, {\rm rk}_4(C_D) = n\}}{\mathcal{D}(X)},$$

and by (10) we deduce the inequality

$$\xi_n \geq \alpha_\infty(n) \text{ for } n \geq 1. \tag{21}$$

The same type of argument gives

$$\xi_0 = \alpha_\infty(0). \tag{22}$$

The relation (20) allows us to apply Lebesgue's dominated convergence theorem to (19). This gives the equality

$$\sum_{n=0}^{\infty} \xi_n \cdot 2^{kn} = \Gamma_k \ (k = 0,\, 1,\, 2, \dots). \tag{23}$$

Therefore we are led to consider the infinite system of linear equations

$$\sum_{r=0}^{\infty} x_r \cdot 2^{kr} = \Gamma_k \ (k = 0,\ 1,\ 2,\ \cdots), \tag{24}$$

where the unknowns must satisfy $x_r \geq \alpha_\infty(r)$ for $r \geq 1$ and $x_0 = \alpha_\infty(0)$ (see (21) and (22)). We prove

Proposition 2. *The infinite system of linear equations (24) has only one solution* $(x_r)_{r\geq 0}$ *satisfying* $x_r \geq \alpha_\infty(r)$ *for* $r \geq 1$ *and* $x_0 = \alpha_\infty(0)$*. It is given by*

$$x_r = \frac{3 + 2^r}{4} \cdot \alpha_\infty(r).$$

Proof. The proof is based on the following lemma which is a consequence of formulas of partition theory and of Jensen's formula. We recall that c_k is defined in (7).

Lemma 4. *(*[4, Lemmata 5 and 7]*) The infinite system of linear equations*

$$\sum_{r=0}^{\infty} y_r \cdot 2^{kr} \ (k = 0,\, 1,\, 2, \dots)$$

has only one solution $(y_r)_{r\geq 0}$ *satisfying* $y_r \geq 0$*. It is given by*

$$y_r = \alpha_\infty(r).$$

By writing $x_r = z_r + \alpha_\infty(r)$ we deduce from Lemma 4 that the study of (24) is equivalent to the study of

$$\sum_{r=0}^{\infty} z_r \cdot 2^{kr} = \Gamma_k - c_k \ (k = 0,\, 1,\, 2, \dots), \tag{25}$$

where now we impose $z_r \geq 0$ for $r \geq 1$ and $z_0 = 0$. We remark that $\Gamma_k - c_k = 2^{k-2} c_k$ and use linearity, in order to deduce with $\rho := r - 1$ that the system (25) is equivalent to

$$z_0 = 0, z_r \geq 0 \text{ for } r \geq 1 \text{ and } \sum_{\rho=0}^{\infty} (4 z_{\rho+1}) \cdot 2^{k\rho} = c_k \ (k = 0,\, 1,\, 2, \dots).$$

Applying Lemma 4 once again, we get that

$$4 z_{\rho+1} = \alpha_\infty(\rho) \text{ for all } \rho \geq 0 \text{ and } z_0 = 0.$$

Gathering the above discussions we see that the only solutions to (24) are given by

$$x_0 = \alpha_\infty(0) \text{ and } x_r = \alpha_\infty(r) + \frac{1}{4}\alpha_\infty(r-1) \text{ for } r \geq 1.$$

We finish the proof of Proposition 2 by the equality $\alpha_\infty(r-1) = (2^r - 1)\alpha_\infty(r)$ for $r \geq 1$. □

Since (24) (with the condition (21) and (22)) has only one solution, we deduce that the sequence $(\xi_n)_{n\geq 0}$ is unique. In other words we proved that

$$\sum_{b=1}^{2^n} b\ \Delta_X(2^n, b) \to \xi_n := \frac{3+2^n}{4}\alpha_\infty(n) \text{ for } X\to\infty, \tag{26}$$

without the restriction $X \in \mathcal{M}$.

Now we list some applications of the existence and of the value of ξ_n.

For $n = 0$, we recover the particular case $r = 0$ of (11).

The particular case $n = 1$ of (26) and the definition of Δ_X in (15) will give Theorem 2 as follows. Asymptotically we have

$$\begin{aligned}&\frac{1}{2}\sharp\left\{D\in\mathcal{D}\,;D<X,\ \mathrm{rk}_4(\mathrm{C}_D)=1 \text{ and } 2^{\lambda_D}=1\right\}\\&+\sharp\left\{D\in\mathcal{D}\,;D<X,\ \mathrm{rk}_4(\mathrm{C}_D)=1 \text{ and } 2^{\lambda_D}=2\right\}\sim\frac{5\alpha}{8}\cdot\mathcal{D}(X).\end{aligned}$$

Appealing to Theorem 3 (iii), we transform the above asymptotic formula into

$$\begin{aligned}&\sharp\left\{D\in\mathcal{D}\,;D<X,\ \mathrm{rk}_4(\mathrm{C}_D)=1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D)=0\right\}\\&+2\,\sharp\left\{D\in\mathcal{D}\,;D<X,\ \mathrm{rk}_4(\mathrm{C}_D)=1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D)=1\right\}\sim\frac{5\alpha}{4}\cdot\mathcal{D}(X).\end{aligned}\tag{27}$$

Applying (10) for $r = 1$, we have

$$\begin{aligned}&\sharp\left\{D\in\mathcal{D}\,;D<X,\ \mathrm{rk}_4(\mathrm{C}_D)=1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D)=0\right\}\\&+\sharp\left\{D\in\mathcal{D}\,;D<X,\ \mathrm{rk}_4(\mathrm{C}_D)=1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D)=1\right\}\sim\alpha\cdot\mathcal{D}(X).\end{aligned}$$

which combined with (27), gives

$$\sharp\left\{D\in\mathcal{D}\,;D<X,\ \mathrm{rk}_4(\mathrm{C}_D)=1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D)=0\right\}\sim\frac{3\alpha}{4}\cdot\mathcal{D}(X)$$

and

$$\sharp\left\{D\in\mathcal{D}\,;D<X,\ \mathrm{rk}_4(\mathrm{C}_D)=1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D)=1\right\}\sim\frac{\alpha}{4}\cdot\mathcal{D}(X).\tag{28}$$

By [4, Theorem 2], we also have the asymptotic relation

$$\sharp\left\{D\in\mathcal{D}\,;D<X,\ \mathrm{rk}_4(\mathrm{C}_D)=1 \text{ and } \mathrm{rk}_4(\mathrm{Cl}_D)=1\right\}\sim\frac{\alpha}{2}\cdot\mathcal{D}(X).\tag{29}$$

By the inequality (ii) of Theorem 3, we know that the set studied in (28) is a subset of the one studied in (29). Taking the difference of the two corresponding cardinalities, we are counting special $D\leq X$, satisfying $\mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{Cl}_D)=1$ and $\mathrm{rk}_8(\mathrm{C}_D)=0$. This completes the proof of Theorem 2.

3.1. **Another application.**

Our application concerns the density of special D, such that C_D contains no element of order 8. Let Υ be the subset of $\mathcal{D}$ defined by

$$\Upsilon := \{D\,;\ D\in\mathcal{D},\ \mathrm{rk}_8(\mathrm{C}_D)=0\},$$

and let $\Upsilon(X)$ its counting function up to the bound $X\geq 5$. In the above paragraphs, we already studied some subsets of Υ:

$$\{D\in\mathcal{D}\,;\ \mathrm{rk}_4(\mathrm{C}_D)=0\},$$

$$\{D\in\mathcal{D}\,;\ \mathrm{rk}_4(\mathrm{C}_D)=1, \text{ and } \mathrm{rk}_4(\mathrm{Cl}_D)=0\},$$

and

$$\{D\in\mathcal{D}\,;\ \mathrm{rk}_4(\mathrm{C}_D)=1,\ \mathrm{rk}_4(\mathrm{Cl}_D)=1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D)=0\}.$$

These three subsets are disjoint and their counting functions up to the bound X are respectively asymptotic to $\alpha \cdot \mathcal{D}(X)$ (by (11)), $\frac{\alpha}{2} \cdot \mathcal{D}(X)$ (by [4, Theorem 2]) and $\frac{\alpha}{4} \cdot \mathcal{D}(X)$ (by Theorem 2). By summing these cardinalities, we get the lower bound

$$\varUpsilon(X) \geq \big(\frac{7\alpha}{4} - o(1)\big) \cdot \mathcal{D}(X) \ (X \to \infty). \tag{30}$$

We shall improve this lower bound in

Corollary 1. *As $X \to \infty$, we have*

$$\#\{D \in \mathcal{D}; D < X, \mathrm{rk}_8(C_D) = 0\} \geq \left(\frac{11\alpha}{6} - o(1)\right) \cdot \mathcal{D}(X).$$

Note that $7\alpha/4 = .73398\cdots$ and $11\alpha/6 = .76893\cdots$. As far as we know, there is no place in the literature, where the distribution law of the function $D \in \mathcal{D} \mapsto \mathrm{rk}_8(C_D)$ is heuristically investigated. Hence, we are unable to measure the quality of the lower bound in Corollary 1.

Proof. By (26) with $n = 2$ we have the equality

$$\begin{aligned}\Delta_X(4,1) + 2\,\Delta_X(4,2) + 3\,\Delta_X(4,3) + 4\,\Delta_X(4,4) &= \frac{7}{4} \cdot \alpha_\infty(2) + o(1)\\ &= \frac{7}{12} \cdot \alpha + o(1),\end{aligned} \tag{31}$$

as X tends to infinity. From the easy fact that, if $\mathrm{rk}_4(\mathrm{C}_D) = 2$, then $2^{\lambda_D} = 1, 2, 3$ or 4 and from (10) with $r = 2$, we obtain the other asymptotic equality

$$\Delta_X(4,1) + \Delta_X(4,2) + \Delta_X(4,3) + \Delta_X(4,4) = \frac{\alpha}{3} + o(1). \tag{32}$$

Multiplying (32) by two and subtracting (31), we get the equality

$$\Delta_X(4,1) - \Delta_X(4,3) - 2\,\Delta_X(4,4) = \frac{\alpha}{12} + o(1).$$

By positivity, we have the asymptotic lower bound

$$\Delta_X(4,1) \geq \frac{\alpha}{12} - o(1).$$

Now we appeal to the general inequality $\lambda_D \geq \mathrm{rk}_8(\mathrm{C}_D)$ (see Theorem 3 (ii)), to deduce

Theorem 4. *As X tends to ∞, we have*

$$\sharp\,\big\{D \in \mathcal{D}\,; D < X,\, \mathrm{rk}_4(\mathrm{C}_D) = 2 \textit{ and } \mathrm{rk}_8(\mathrm{C}_D) = 0\big\} \geq \big(\frac{\alpha}{12} - o(1)\big) \cdot \mathcal{D}(X).$$

It is now easy to deduce Corollary 1 from (30) and Theorem 4, since the lower bound (30) is obtained by only considering special D with $\mathrm{rk}_4(\mathrm{C}_D) \leq 1$ and $\mathrm{rk}_8(\mathrm{C}_D) = 0$. □

3.2. **Remarks on the method.** One may ask if, by the same method, it is possible to obtain some information on the set of special D such that $\mathrm{rk}_4(\mathrm{C}_D) = 3$ and $\mathrm{rk}_8(\mathrm{C}_D) = 0$. The formulae (31) and (32) would be replaced by

$$\sum_{b=1}^{8} b \cdot \Delta_X(8,b) = \frac{11}{4} \cdot \alpha_\infty(3) + o(1) = \frac{11}{4 \cdot 21} \cdot \alpha + o(1), \tag{33}$$

and

$$\sum_{b=1}^{8} \Delta_X(8,b) = \alpha_\infty(3) + o(1) = \frac{1}{21} \cdot \alpha + o(1). \tag{34}$$

But it is impossible to deduce the inequality $\Delta_X(8,1) \geq \delta_0 - o(1)$, (for some positive δ_0) from the equalities (33) and (34) only. However, by linear combination, we easily obtain

$$2 \cdot \Delta_X(8,1) + \Delta_X(8,2) \geq \frac{1}{4 \cdot 21} \cdot \alpha - o(1),$$

which can be written as

$$\begin{aligned} &2\,\sharp\,\big\{D \in \mathcal{D}\,; D < X,\ \mathrm{rk}_4(\mathrm{C}_D) = 3 \text{ and } \lambda_D = 0\big\} \\ &+\sharp\,\big\{D \in \mathcal{D}\,; D < X,\ \mathrm{rk}_4(\mathrm{C}_D) = 3 \text{ and } \lambda_D = 1\big\} \geq \big(\frac{\alpha}{84} - o(1)\big) \cdot \mathcal{D}(X). \end{aligned} \tag{35}$$

In terms of the 8–rank, the inequality $\lambda_D \geq \mathrm{rk}_8(\mathrm{C}_D)$ transforms (35) into the rather disappointing inequality

$$\sharp\,\big\{D \in \mathcal{D}\,; D < X,\ \mathrm{rk}_4(\mathrm{C}_D) = 3 \text{ and } \mathrm{rk}_8(\mathrm{C}_D) \leq 1\big\} \geq \big(\frac{\alpha}{168} - o(1)\big) \cdot \mathcal{D}(X).$$

There is a way to improve and generalize the results just above, by producing other linear equations different from (33) and (34) and satisfied by the $\Delta_X(2^n, b)$ $(1 \leq b \leq 2^n)$. This can be accomplished by studying the mixed moments

$$\sum_{\substack{D \in \mathcal{D} \\ D \leq X}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)} \cdot 2^{\ell\,\lambda_D}$$

for integral values of $\ell \geq 2$. The analytic methods which will be developed below to deal with the case $\ell = 1$, are strong enough to fulfill this desire, at least for small values of ℓ. The case corresponding to a general ℓ will certainly encounter some interesting combinatorial problems. A deeper question is to better detect the function $\mathrm{rk}_8(\mathrm{C}_D)$ by symbols and characters, in other words, to replace the function λ_D in Theorem 3, by a more suitable function, which can be handled by present analytic techniques.

4. An incursion in algebraic number theory

4.1. **Definition of characters and symbols.** All the following tools are the cornerstone of [4]. They have their origin in several papers of Redei, Scholz, Reichardt, Lemmermeyer ([13], [15], [16], [18], [19], [21],...). We briefly mention all these tools.

Definition 1. [4, Def. 2] *Let D be a fundamental discriminant. We say that $\{D_1, D_2\}$ is a decomposition of D if $D = D_1 D_2$ and the integers D_1 and D_2 are fundamental or* 1. *A decomposition $\{D_1, D_2\}$ of D is called decomposition of second type, if the following conditions hold:*

(i) *For all $p \mid D_1$: $\left(\frac{D_2}{p}\right) = 1$,*

(ii) *For all* $p \mid D_2 : \left(\frac{D_1}{p}\right) = 1$,

where $\left(\frac{\cdot}{\cdot}\right)$ *denotes the Kronecker symbol.*

Since D_1 and D_2 are fundamental discriminants, at most one of them can be divisible by 2. In the following we assume $2 \nmid D_2$ by changing the order of D_1 and D_2 if necessary. We want to interpret some results in terms of non-trivial zeros of ternary quadratic forms over $\mathbb{Z}$. For integers $a, b, c \in \mathbb{Z}$ we introduce the notation $Q_{a,b,c}$ to be the quadratic form

$$Q_{a,b,c} := ax^2 + by^2 + cz^2.$$

Using the classical theorem of Legendre on the non-trivial solvability of the equation $Q_{a,b,c}(x, y, z) = 0$ we proved (e.g. see [4, Lemma 13]):

Lemma 5. *Let* D *be a fundamental discriminant and* $\{D_1, D_2\}$ *be a decomposition of* D*, where we assume that* $2 \nmid D_2$*. Then* $\{D_1, D_2\}$ *is a decomposition of second type, if and only if the following two conditions hold:*

(i) The ternary quadratic form $Q_{1,-D_1,-D_2}$ *has a non trivial zero in* $\mathbb{Z}^3$.

(ii) If $2 \mid D_1$*, we have* $D_2 \equiv 1 \bmod 8$.

We can omit the second condition of Lemma 5 by only allowing special solutions of our ternary equation. For this we need a result already known to Dirichlet.

Theorem 5. *Let* $Q_{a,b,c}$ *be given such that* a*,* b *and* $c \in \mathbb{Z}$*, with* abc *squarefree and w.l.o.g.* $2 \nmid ab$*. Assume that* $Q_{a,b,c}$ *admits a non trivial zero* $(x_0, y_0, z_0) \in \mathbb{Z}^3$.

(i) Let $k \geq 1$ *be an integer. Suppose that* $-ab$ *is a square modulo* 8*. Then* $Q_{a,b,c}$ *admits a non trivial zero* $(x, y, z) \in \mathbb{Z}^3$ *such that* $2^k \mid z$ *and* ax^2*,* by^2*,* cz^2 *are pairwise coprime.*

(ii) Assume that abc *is odd and* $-ab$ *is a square modulo* 4*. Then* $Q_{a,b,c}$ *admits a non trivial zero* $(x, y, z) \in \mathbb{Z}^3$ *such that* $2 \mid z$ *and and* ax^2*,* by^2*,* cz^2 *are pairwise coprime.*

Proof. This is result III in [2, p.425] and the final result of §156 on pages 427–428. For the convenience of the reader we give a proof of this result. If $z_0 = 0$, the result is trivial. W.l.o.g. we can assume that ax_0, by_0 and cz_0 are pairwise coprime and that $z_0 \neq 0$. Similarly, we can suppose that $(a, b) \neq (1, -1)$ and $(-1, 1)$.

In the first step we parametrize all the solutions in $\mathbb{Q}^3$ of $ax^2 + by^2 + cz^2 = 0$ and follow an idea given in [14, p. 47]. Let $(x, y, z) \in \mathbb{Q}^3$. Then we can find rational numbers r, s and t such that

$$x = rx_0 + s, \ y = ry_0 + t, \ z = rz_0.$$

For this we find r such that $z = rz_0$ and then we find s and $t \in \mathbb{Q}$. Now (x, y, z) is a zero of $Q_{a,b,c}$ if and only if we have

$$a(rx_0 + s)^2 + b(ry_0 + t)^2 + c(rz_0)^2 = 0.$$

We simplify by taking into account that (x_0, y_0, z_0) is a zero and get, that (x, y, z) is a zero of $Q_{a,b,c}$ if and only if

$$r(2ax_0s + 2by_0t) = -as^2 - bt^2. \tag{36}$$

We define $m := 2ax_0s + 2by_0t$ and note that $rm = -as^2 - bt^2$. We also define

$$\tilde{x} := xm, \ \tilde{y} := ym \text{ and } \tilde{z} := zm.$$

We eliminate r by using (36) and get

$$\tilde{x} = rmx_0 + sm = -x_0(as^2+bt^2) + 2ax_0s^2 + 2sby_0t = x_0(as^2-bt^2) + 2sby_0t, \tag{37}$$

$$\tilde{y} = rmy_0 + tm = -y_0(as^2+bt^2) + 2ax_0st + 2by_0t^2 = y_0(bt^2-as^2) + 2sax_0t, \tag{38}$$

and

$$\tilde{z} = rmz_0 = -z_0(as^2+bt^2). \tag{39}$$

Hence, for any s and $t \in \mathbb{Q}$, the triple

$$(\tilde{x},\tilde{y},\tilde{z}) = \big(x_0(as^2-bt^2) + 2sby_0t, y_0(bt^2-as^2) + 2sax_0t, -z_0(as^2+bt^2)\big),$$

is a zero of $Q_{a,b,c}$. In particular, if s and t are integers, the corresponding $(\tilde{x},\tilde{y},\tilde{z})$ belongs to $\mathbb{Z}^3$. Note also that $\tilde{z} = 0$ if and only if $s = t = 0$ (a consequence of the above restrictions).

Now we want to construct our special solution, i.e. a solution satisfying $2^k \mid z$.

• Assume that x_0y_0 is odd. This implies that cz_0 is even, and therefore we only need to prove something in the case when $-ab$ is a square modulo 8 (case (i) of Theorem 5), which means that $a \equiv -b \bmod 8$. Our goal is to choose the integers s and t in a way that the corresponding $\tilde{x}$ and $\tilde{y}$ are congruent to $4 \bmod 8$. For simplicity let us assume that $a - b \equiv 2a \equiv 2 \bmod 8$. The other case ($a - b \equiv 6 \bmod 8$) is symmetric. Then, if we impose s and t to be odd integers, we have $as^2 - bt^2 \equiv a - b \equiv 2 \bmod 8$, hence by (37) and (38), we deduce

$$\tilde{x} \equiv 2(x_0 - say_0t) \bmod 8 \text{ and } \tilde{y} \equiv 2(3y_0 + sax_0t) \bmod 8, \tag{40}$$

Since $2 \nmid astx_0y_0$, we have

$$3y_0 + sax_0t \equiv y_0 - sax_0t \bmod 4. \tag{41}$$

W.l.o.g. we can choose the signs of x_0 and y_0 in our special solution (x_0, y_0, z_0) (depending on s, t and a) such that

$$x_0 - say_0t \equiv 2 \bmod 4 \text{ and } y_0 - sax_0t \equiv 2 \bmod 4. \tag{42}$$

For this we choose $x_0 - y_0 \equiv 2 \bmod 4$, if $sat \equiv 1 \bmod 4$ and $x_0 - y_0 \equiv 0 \mod 4$, if $sat \equiv 3 \bmod 4$. Combining (40), (41) and (42), we deduce that $\tilde{x}$ and $\tilde{y}$ are exactly divisible by 2^2 and we only used the fact that s and t are odd. Note that $as^2 + bt^2 \equiv a + b \equiv 0 \bmod 8$. This means that $-(b/a)t^2$ is an odd square modulo 8. It is also an odd square modulo 2^k. Therefore, we can find odd s and t such that $2^k \mid as^2 + bt^2$ for any given k. By (39), this implies that $2^k \mid \tilde{z}$.

In conclusion, for any $k \geq 0$, we have constructed a zero $(\tilde{x},\tilde{y},\tilde{z}) \in \mathbb{Z}^3$ of $Q_{a,b,c}$ such that $2^2 \parallel \tilde{x}$, $2^2 \parallel \tilde{y}$ and $2^k \mid \tilde{z}$ ($\neq 0$). Removing the g.c.d., we obtain a zero (x, y, z) of $Q_{a,b,c}$ which satisfies the condition of coprimality $(ax^2, by^2, cz^2) = 1$ and $2^k \mid z$, by changing the value of k.

• Assume that x_0y_0 is even. This means that abc is odd. Note that in both cases of Theorem 5, we suppose that $-ab$ is a square modulo 4, i.e. $ab \equiv 3 \bmod 4$. This implies

$$a - b \equiv 2 \bmod 4 \text{ and for all odd } s,\, t \in \mathbb{Z} : as^2 - bt^2 \equiv 2 \bmod 4. \tag{43}$$

Therefore $2 \parallel as^2 - bt^2$. Assume that x_0 is even (hence y_0 is odd). Let ℓ be the integer ($1 \leq \ell \leq \infty$) such that $2^\ell \parallel x_0$. Then, by (37) and (43), we see that $2 \parallel \tilde{x}$. Similarly, by (38) we see that $2 \parallel \tilde{y}$.

Similarly as before, we have to look at the maximal power of 2 which can divide $\tilde{z}$. Since $a \equiv -b \bmod 4$ we see that $as^2 + bt^2 \equiv 0 \bmod 4$. By (39), we see that $2^2 \mid \tilde{z}$. Hence we constructed an integral zero $(\tilde{x}, \tilde{y}, \tilde{z})$ of $Q_{a,b,c}$ such that $2 \parallel \tilde{x}$, $2 \parallel \tilde{y}$ and $2^2 \mid \tilde{z}$. After clearing the common factors, we arrive at a zero $(x, y, z) \in \mathbb{Z}^3$ satisfying the conditions $2 \nmid xy$ and $2 \mid z$. The proof of Theorem 5 (ii) is now complete.

If we additionally assume that $-ab$ is a square mod 8, similarly to the first case we get $as^2 + bt^2 \equiv 0 \bmod 8$, for odd s and t. Then we choose s and t such that an arbitrary chosen 2–power divides $as^2 + bt^2$, hence $\tilde{z}$. In other words, for every $k \geq 0$, we constructed a zero $(\tilde{x}, \tilde{y}, \tilde{z}) \in \mathbb{Z}^3$ of $Q_{a,b,c}$, such that $2 \parallel \tilde{x}$, $2 \parallel \tilde{y}$ and $2^{k+1} \mid \tilde{z}$. Removing the common factor, we arrive at a solution as required in the part (i) of Theorem 5. It is now proved in all the cases. □

We shall use Theorem 5 to characterize decompositions of the second type in terms of quadratic forms. We have

Lemma 6. *Let D be a fundamental discriminant and $\{D_1, D_2\}$ be a decomposition of D, where we assume that $2 \nmid D_2$. Then $\{D_1, D_2\}$ is a decomposition of second type, if and only if the quadratic form $Q_{1,-D_1,-D_2}$ has a non trivial zero $(x, y, z) \in \mathbb{Z}^3$, such that x, $D_1 y$ and $D_2 z$ are pairwise coprime and $4 \mid y$ when $D_1 \equiv 12 \bmod 16$ and $2 \mid y$ when $D \equiv 1 \bmod 4$ or $D_1 \equiv 8 \bmod 16$.*

Proof. Assume that we have an integral solution (x, y, z) of the ternary equation $x^2 - D_1 y^2 - D_2 z^2 = 0$, with y even and xz odd. We apply Lemma 5 and there is nothing to show when D_1 is odd. When D_1 is even we get that $D_1 y^2 \equiv 0 \bmod 8$ (since $2 \mid y$), we also have $x^2 \equiv z^2 \equiv 1 \bmod 8$. Therefore looking at our ternary equation modulo 8, we see that $D_2 \equiv 1 \bmod 8$. So $\{D_1, D_2\}$ is a decomposition of second type of D.

Now assume that we have a decomposition of second type of D. So, the quadratic form $Q_{1,-D_1,-D_2}$ has a non trivial integral zero, coming from Lemma 5. Our proof depends on the congruence of D_1 mod 16.

- Case $D_1 \equiv 1 \bmod 4$.

We apply Theorem 5 to $Q_{a,b,c} = Q_{1,-D_2,-D_1}$ and note that $-ab = D_2 \equiv 1 \bmod 4$.

- Case $D_1 \equiv 8 \bmod 16$ or $D_1 \equiv 12 \bmod 16$.

We apply Theorem 5 (i) to $Q_{a,b,c} = Q_{1,-D_2,-D_1/4}$. Note that abc is squarefree. Furthermore $-ab = D_2 \equiv 1 \bmod 8$, and therefore it is a square modulo 8. Therefore we know that there exists a $(u, v, w) \in \mathbb{Z}^3$ such that u, vb and wc are coprime, such that $2^k \mid w$, for a given $k \geq 1$ and such that

$$u^2 - v^2 D_2 - w^2 (D_1/4) = 0.$$

It is easy to see that the triple $(x, y, z) = (u, w/2, v)$ fulfills the required conditions, by choosing $k = 3$. □

The generalizes the result of Lemma 19 in [4] to fundamental discriminants. As in the proof of this lemma we can reach the third condition by choosing the sign of x.

Note also that in the case $D_1 \equiv 12 \bmod 16$ we really need a special zero of $Q_{1,-D_1,-D_2}$. E.g. we get for $D = 156$:

$$5^2 - 12 \cdot 1^2 - 13 \cdot 1^2 = 0 \text{ and } \{12, 13\} \text{ is not of second type.}$$

When D is a special discriminant, this definition of a decomposition of second type is equivalent to the following one:

- If $D \in \mathcal{D}_{\text{odd}}$, then $\{D_1, D_2\}$ is a decomposition of the second type of D if and only if D_1 and D_2 belong to $\mathcal{D}_{\text{odd}} \cup \{1\}$, are such that $D = D_1 D_2$ and such that D_1 is a square modulo D_2 and D_2 is a square modulo D_1,
- If $D \in \mathcal{D}_{\text{even}}$, write $D = 8D'$, with $D' \in \mathcal{D}_{\text{odd}}$. Then $\{D_1, D_2\}$ is a decomposition of the second type of D if and only if $(D_1, D_2) = (8D'_1, D'_2)$ (or $(D_1, D_2) = (D'_1, 8D'_2)$), where D'_1 and $D'_2 \in \mathcal{D}_{\text{odd}} \cup \{1\}$ are such that $D' = D'_1 D'_2$ and are such that $2D'_1$ is a square modulo D'_2 and D'_2 a square modulo D'_1 (or D'_1 is a square modulo D'_2 and $2D'_2$ is a square modulo D'_1).

First note that in a decomposition $\{D_1, D_2\}$ of a special D, both D_1 and D_2 are positive and recall that the Kronecker and Legendre symbols coincide when the denominator is an odd prime. The proof of the above equivalent form of a decomposition of second type for an odd special D is straightforward when starting with Definition 1. When D and D_1 are even, we deduce the two equalities $\left(\frac{2D'_1}{D'_2}\right) = \left(\frac{D'_2}{D'_1}\right) = 1$. But since $D'_1 \equiv D'_2 \equiv 1 \bmod 4$, we have $\left(\frac{D'_1}{D'_2}\right) = \left(\frac{D'_2}{D'_1}\right)$, from which we deduce $\left(\frac{2}{D'_2}\right) = 1$ hence $D_2 = D'_2 \equiv 1 \bmod 8$ and $\left(\frac{D_2}{2}\right) = 1$.

The first application of this decomposition of second type is (see [4, Prop. 3]):

Proposition 3. *Let D be a special discriminant. Then we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2}\,\sharp\big\{\{D_1, D_2\}\,;\ \{D_1, D_2\} \textit{ is a decomposition of second type of } D\big\}.$$

Actually, this proposition, originally due to Redei [15], is true for any fundamental discriminant D and a proof is given in [4, §3.2] in the simpler case when D is special.

The construction of the function λ_D requires more sophisticated tools. It is based on the symbol $[a, b]_4$ which is defined as follows. Let p be an odd prime and a be an integer. Then we define

$$[a, p]_4 := \begin{cases} 1 & \text{if } \left(\frac{a}{p}\right) = 1 \text{ and if } a \text{ is a fourth power } \bmod p, \\ -1 & \text{if } \left(\frac{a}{p}\right) = 1 \text{ and if } a \text{ is not a fourth power } \bmod p, \\ 0 & \text{otherwise.} \end{cases}$$

We also define

$$[a, 2]_4 := \begin{cases} 1 & \text{if } a \equiv 1 \bmod 16, \\ -1 & \text{if } a \equiv 9 \bmod 16, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, for b and c positive integers, we impose multiplicativity with the formula

$$[a, bc]_4 := [a, b]_4\, [a, c]_4.$$

We remark that this symbol is not multiplicative in the first component. However, when both $[a, c]_4$ and $[b, c]_4$ belong to $\{+1, -1\}$, then we have the equality $[ab, c]_4 = [a, c]_4\, [b, c]_4$. This symbol was introduced in [4] to prove

Proposition 4. *(*[4, Theorem 5]*) For any special discriminant D, we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{Cl}_D)} = \frac{1}{2}\sharp\Big\{\{D_1, D_2\}\,;\{D_1,D_2\} \textit{ is a decomposition of second type of } D \\ \textit{such that } [D_1,D_2]_4 = [D_2,D_1]_4 = 1 \textit{ or } [D_1,D_2]_4 = [D_2,D_1]_4 = -1\Big\}.$$

4.2. **Definition of λ_D.** It is time to give the following definition:

Definition 2. *For any special discriminant D, the number λ_D is defined by the equality*

$$2^{\lambda_D} = \frac{1}{2}\sharp\Big\{\{D_1, D_2\}\,;\{D_1,D_2\} \textit{ is a decomposition of second type of } D \\ \textit{such that } [D_1,D_2]_4 = [D_2,D_1]_4 = 1\Big\}.$$

By this definition we easily get the property (i) of Theorem 3 by observing that the decompositions $\{1, D\}$ and $\{D, 1\}$ are always present, and by grouping the decompositions $\{D_1, D_2\}$ and $\{D_2, D_1\}$ together. Proposition 4 directly implies the inequalities $\lambda_D \leq \mathrm{rk}_4(\mathrm{Cl}_D) \leq \mathrm{rk}_4(\mathrm{C}_D)$. This constitutes the easy part of the property (ii) of Theorem 3.

However, the number λ_D is not necessarily an integer as the following example shows.

Example 1. *Take $D = 135\,505 = 5\cdot 41\cdot 661$. By using a computer algebra system equipped with PARI/GP or Magma, we easily get that $\mathrm{C}_D = C(4)\times C(8)$ and $\mathrm{Cl}_D = C(4)\times C(4)$, where $C(m)$ is the cyclic group of order m. The special discriminant D has eight decompositions $\{D_1, D_2\}$. It is easy to check that all of these are of the second type. Hence we recover the fact the equality $\mathrm{rk}_4(\mathrm{C}_D) = 2$, via Proposition 3.*

We see that 41 and 661 are fourth powers modulo 5, and by using a computer (or by computing quartic symbols), we see that 5 and 661 are not fourth powers modulo 41, that 5 is not a fourth power modulo 661 and that 41 is a fourth power modulo 661. From the multiplicative properties of the symbol $[a,b]_4$, we deduce the values

$$\begin{array}{rlrl}
[135\,505, 1]_4 & = 1, & [1, 135\,505]_4 & = 1,\\
[27\,101, 5]_4 & = 1, & [5, 27\,101]_4 & = 1,\\
[3\,305, 41]_4 & = 1, & [41, 3\,305]_4 & = 1,\\
[205, 661]_4 & = -1, & [661, 205]_4 & = -1.
\end{array}$$

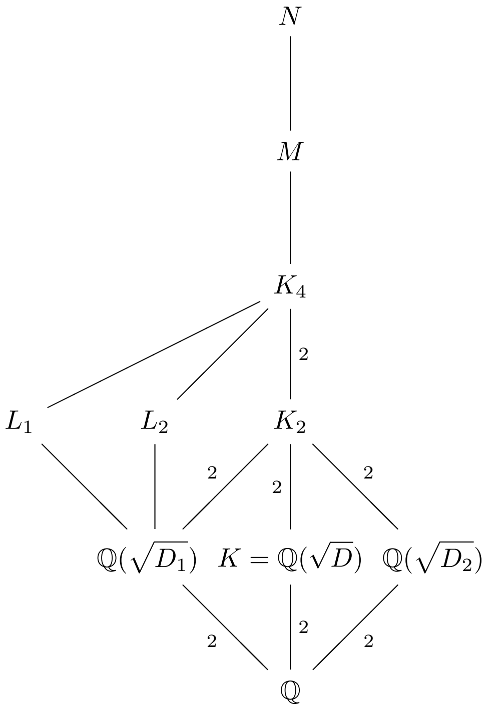
Using Proposition 4, we recover the equality $\mathrm{rk}_4(\mathrm{Cl}_D) = 2$, and Definition 2 gives $\lambda_D = \ln 3/\ln 2$ $(> 1 = \mathrm{rk}_8(\mathrm{C}_D))$.

It remains to prove the inequality $\mathrm{rk}_8(\mathrm{C}_D) \leq \lambda_D$ for any special D and the property (iii) of Theorem 3. Their proofs will be given in §4.3 and 4.4 and require algebraic considerations, which can be considered as variations and extensions of the proof of Proposition 4. The items *(iv)* and *(v)* concerning the sum

$$S^{\mathrm{mix},\lambda}(X,k) := \sum_{\substack{D\in\mathcal{D}\\ D\leq X}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}\cdot 2^{\lambda_D} \tag{44}$$

(and its natural subsums $S^{\mathrm{mix},\lambda}_{\mathrm{odd}}(X,k)$ and $S^{\mathrm{mix},\lambda}_{\mathrm{even}}(X,k)$) are of analytic nature and will be proved in §5 and §6.

4.3. **A criterion for the 8–rank.** The aim of this section is to prove some criteria when unramified $C(8)$–extensions of $\mathbb{Q}(\sqrt{D})$ may occur. We follow closely old works of Reichardt and Redei. Let us give the main field diagram we are going to use. The fields L_1 and L_2 are conjugated with Galois closure K_4. We denote by N the narrow Hilbert class field of K which is the maximal at all finite places unramified extension of K. By class field theory it satisfies $\mathrm{Gal}(N/K) = C_D$.



We already defined decompositions of second type. Let us introduce the decompositions of n-th type which have been introduced by Reichardt [20].

Definition 3. *Let $n \geq 2$ be an integer, D be a fundamental discriminant, and $\{D_1, D_2\}$ be a decomposition. Then this decomposition is called a decomposition of n–th type, if there exists a field $K_{2^{n-1}}$ having the following properties:*

(i) $K_2 := \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2}) \subseteq K_{2^{n-1}}$,
(ii) $\mathrm{Gal}(K_{2^{n-1}}/K) = C(2^{n-1})$,
(iii) *$K_{2^{n-1}}/K$ is unramified at all finite places.*
(iv) *All primes ideals in K dividing D are split in $K_{2^{n-1}}$.*

It is easy to see that for $n = 2$ this definition coincides with the previous definition of a decomposition of second type (see Definition 1). Indeed, we know that for a decomposition of second type every prime ideal in K dividing D is split in K_2. A decomposition of n–th type is also a decomposition of m–type for any $2 \leq m \leq n$. Note that we consider the decompositions $\{D_1, D_2\}$ and $\{D_2, D_1\}$ as distinct. The main theorem of the paper of Reichardt [20, 1. Satz] is:

Theorem D. *Let $n \geq 2$ be an integer, D be a fundamental discriminant, and $K = \mathbb{Q}(\sqrt{D})$. Then*

(i) *If M/K is a cyclic and an at finite places unramified degree 2^n–extension containing $\mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$, then $\{D_1, D_2\}$ is a decomposition of n–th type.*

(ii) *Let $\{D_1, D_2\}$ be a decomposition of n–th type with associated field $K_{2^{n-1}}$ as in Definition 3. Then there corresponds a cyclic and an at finite places unramified degree 2^n–extension M of K containing $K_{2^{n-1}}$.*

Combining this theorem with the fundamental theorem of class field theory we deduce (see also [20, 2. Satz]):

Corollary 2. *Let $n \geq 2$ and D be a fundamental discriminant. Then $2^{\mathrm{rk}_{2^n}(C_D)}$ is equal to half of the number of decompositions of n–type of D.*

We remark that it is well known that the Galois group of such an extension $M/\mathbb{Q}$ is the dihedral group D_{2^n} with 2^{n+1} elements. Let us specialize to the situation that there exists such an extension M over K of degree 8. Such an extension possesses a unique subfield K_4 which corresponds to the same decomposition $\{D_1, D_2\}$. The first part of Theorem D tells us that this decomposition is of third type, which means that every prime ideal of K dividing D is split in K_4. One important trick is to look at the fields L_1 and L_2 in the above diagram. These two fields are conjugated and will be generated by the square roots of the numbers α and β, resp. (see equation (45) below). The normal closure of those extensions over $\mathbb{Q}$ is the field K_4, which means that the splitting behavior of primes in K_4 can already be decided by looking at the splitting behavior of the corresponding primes in L_i. The following lemma of Redei [17, I. Teil] is an application of the criterion of Reichardt given in Theorem D.

Lemma 7. *Let D be a fundamental discriminant and $\{D_1, D_2\}$ be a decomposition of third type. Let M be a corresponding extension with subfields K_4, L_1, L_2. Then the following holds:*

(i) *Let p be a prime dividing D_1. Then there exists a unique prime ideal $\mathfrak{p}$ in $\mathbb{Q}(\sqrt{D_1})$ containing p. This prime ideal splits totally in K_4 and therefore in K_2, L_1, L_2, too.*

(ii) *Let p be a prime dividing D_2. Since $\{D_1, D_2\}$ is a decomposition of second type, p splits into two prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ in $\mathbb{Q}(\sqrt{D_1})$. Since p is ramified in K_2 and therefore in K_4, $\mathfrak{p}_i$ $(i = 1, 2)$ is ramified in exactly one of the extensions L_1 and L_2. In the other extension $\mathfrak{p}_i$ is split.*

Proof. Since $\{D_1, D_2\}$ is a decomposition of third type we know that every prime ideal in K_4 which contains a prime dividing D has inertia degree 1 and ramification index 2. In case (i) $\mathfrak{p}$ has already ramification index 2, which means that in $K_4/\mathbb{Q}(\sqrt{D_1})$ it must be unramified and split. In case (ii) $\mathfrak{p}_i$ is ramified in K_2 and must be ramified in at least one of the fields L_1, L_2 Assuming the opposite would mean that $\mathfrak{p}_i$ is unramified in $L_1L_2 = K_4$ which is a contradiction. If $\mathfrak{p}_i$ is ramified in all of the three extensions K_2, L_1, L_2, then the ramification index in K_4 would be 4, which is a contradiction. The inertia degree of all primes lying above $\mathfrak{p}_i$ in K_4 is one. The same is true for all intermediate fields and the last assertion follows. □

Using symbols defined over $\mathbb{Q}(\sqrt{D_1})$ we want to test, if an unramified prime ideal is split, which means that the generator of L_i is a square modulo the corresponding prime ideal in $\mathbb{Q}(\sqrt{D_2})$. In order to apply this we need the converse of this lemma. The problem with the definition of the decomposition of third type is that it is stated, if there exists a field K_4 corresponding to $\{D_1, D_2\}$ such that some properties hold. Given a decomposition $\{D_1, D_2\}$ of second type, the corresponding field K_4 is not uniquely defined. Given one extension $K_4 = K_2(\sqrt{\alpha})$ corresponding to $\{D_1, D_2\}$ we can get all possible extensions by defining

$$K_{4,E} := K_2(\sqrt{E_1\alpha}) = K_2(\sqrt{E_2\alpha}),$$

where $E := \{E_1, E_2\}$ is a decomposition of D, i.e. $D = E_1E_2$ and the E_i are fundamental discriminants. We remark that these two extensions are the same because $E_1\alpha$ and $E_2\alpha$ differ by a square. In order to get the converse using the criterion of Reichardt it is sufficient that there exists a decomposition E such that $K_{4,E}$ fulfills the criterion that all prime ideals in K_4 above p's dividing D have inertia degree 1 and certainly ramification index 2. So a general criterion has to check all these extensions $K_{4,E}$. Let p be a prime dividing D. Then p divides either E_1 or E_2. Then we define the symbol $\left(\frac{xE}{p}\right)$ to be the symbol $\left(\frac{xE_i}{p}\right)$ such that $p \nmid E_i$ $(i = 1, 2)$.

The following theorem is given in [17, I. Satz].

Theorem 6. *Let D be a fundamental discriminant and $\{D_1, D_2\}$ (with $2 \nmid D_2$) be a decomposition of second type, i.e. we have a solution (x, y, z) of the equation*

$$x^2 - D_1y^2 - D_2z^2 = 0$$

such that x, D_1y, D_2z are coprime with the property that y is even and furthermore $4 \mid y$ if $D_1 \equiv 12 \bmod 16$. Then this decomposition is of third type, if and only if there exists a decomposition $E = \{E_1, E_2\}$ of D such that the following two conditions hold:

(i) $\forall p \mid D_1 : \left(\frac{xE}{p}\right) = 1,$

(ii) $\forall p \mid D_2 : \left(\frac{2xE}{p}\right) = 1.$

Proof. We take a solution from Lemma 6. We can assume $y, z > 0$ and by choosing the sign of x we can get:

$$x + y \equiv 1 \bmod 4, \text{ if } 2 \nmid D, \quad \text{and } x \equiv 1 \bmod 4, \text{ if } 2 \mid D.$$

Let us define

$$\alpha := x + y\sqrt{D_1} \text{ and } \beta := x - y\sqrt{D_1}. \tag{45}$$

A straightforward computation (see the proof of Lemma 20 in [4], in the particular case D is special) shows that $K_4 := K_2(\sqrt{\alpha})$ is an at finite places unramified $C(4)$–extension of K corresponding to $\{D_1, D_2\}$. All these extensions are given by $K_{4,E} := K_2(\sqrt{E_1\alpha}) = K_2(\sqrt{E_2\alpha})$, where $E := \{E_1, E_2\}$ is a decomposition of D. We define

$$L_1 := \mathbb{Q}(\sqrt{D_1})(\sqrt{\alpha}) \text{ and } L_2 := \mathbb{Q}(\sqrt{D_1})(\sqrt{\beta})$$

and also the twists

$$L_{1,E} := \mathbb{Q}(\sqrt{D_1})(\sqrt{E_1\alpha}) = \mathbb{Q}(\sqrt{D_1})(\sqrt{E_2\alpha})$$

and

$$L_{2,E} := \mathbb{Q}(\sqrt{D_1})(\sqrt{E_1\beta}) = \mathbb{Q}(\sqrt{D_1})(\sqrt{E_2\beta}).$$

Now suppose that $\{D_1, D_2\}$ is a decomposition of third type. By Theorem D we get that there exists an at finite places unramified $C(4)$–extension of K corresponding to $\{D_1, D_2\}$ such that all prime ideals in K dividing D are split.

This degree 4 extension is equal to $K_{4,E}$ for some decomposition E of D. Denote by $L_{1,E}$ and $L_{2,E}$ the corresponding subfields. Now we translate the splitting condition into symbols.

Let $2 \neq p \mid D_1$. Then there exists a unique prime ideal $\mathfrak{p}$ in $\mathbb{Q}(\sqrt{D_1})$. By the assumption $\mathfrak{p}$ is split in $K_{4,E}$ and therefore in $L_{1,E}$ and $L_{2,E}$. This mean that for the generalized Kronecker symbol we have

$$\left(\frac{E\alpha}{\mathfrak{p}}\right) = \left(\frac{E(x+y\sqrt{D_1})}{\mathfrak{p}}\right) = \left(\frac{Ex}{\mathfrak{p}}\right) = \left(\frac{Ex}{p}\right),$$

where the latter equality is deduced from the fact that the degree of $\mathfrak{p}$ is 1. So all prime ideals above p are split if and only if this symbol is 1.

Let $p \mid D_2$ be a prime (which is odd). Then p is split in $\mathbb{Q}(\sqrt{D_1})$ and therefore factors into two prime ideals $\mathfrak{p}_1\mathfrak{p}_2$. Both prime ideals are ramified in K_2 and $\mathfrak{p}_1$ is ramified in either L_1 or L_2 (same for $\mathfrak{p}_2$). Suppose that $\mathfrak{p}_1$ is unramified in L_1 and ramified in L_2 and therefore $\mathfrak{p} \mid \beta$. Then we get:

$$\left(\frac{E\alpha}{\mathfrak{p}_1}\right) = \left(\frac{E(\alpha+\beta)}{\mathfrak{p}_1}\right) = \left(\frac{2xE}{\mathfrak{p}_1}\right) = \left(\frac{2xE}{p}\right),$$

since $\mathfrak{p}_1$ is a prime ideal of degree 1. So all prime ideals above p are split if and only if this symbol is 1.

The final case is $2 = p \mid D_1$. In this case there is one prime ideal above 2 in $\mathbb{Q}(\sqrt{D_1})$. In order to guarantee splitting we need to get that α is a square modulo $\mathfrak{p}^5 = 4\mathfrak{p}$. Since $\alpha = x + y\sqrt{D_1}$ we see that $\mathfrak{p}^5 \mid y\sqrt{D_1}$ (we are in the case $D_1 \equiv 8, 12 \bmod 16$). As in the first case we see that

$$\left(\frac{E\alpha}{\mathfrak{p}}\right) = \left(\frac{E(x+y\sqrt{D_1})}{\mathfrak{p}}\right) = \left(\frac{Ex}{\mathfrak{p}}\right) = \left(\frac{Ex}{2}\right),$$

where the symbols are Kronecker symbols. □

This criterion is not very nice for two reasons. Firstly, we have to use the solution x and secondly, we do not know which E has to be chosen. Let us now specialize to special discriminants. It turns out that for a necessary condition these two disadvantages disappear. We need some lemma and the proof follows Redei's arguments in [17].

Lemma 8. *Let D be a special discriminant and $\{D_1, D_2\}$ ($2 \nmid D_2$) be a decomposition of second type. Then we have a solution (x, y, z) of*

$$x^2 - D_1y^2 - D_2z^2 = 0 \tag{46}$$

such that x, D_1y and D_2z are pairwise coprime and y is even. We also have the equalities:

$$\left(\frac{x}{D_1}\right) = [D_2, D_1]_4 \text{ and } \left(\frac{2x}{D_2}\right) = [D_1, D_2]_4. \tag{47}$$

Proof. The first part of this lemma is given by Lemma 6. We remark that by eventually multiplying by -1 we can assume that $x \equiv 1 \bmod 4$, $y > 0$, and $z > 0$. Of course, these new constraints do not affect the values of the symbols $\left(\frac{x}{D_1}\right)$ and $\left(\frac{2x}{D_2}\right)$.

Let p be a prime dividing D_1. Then we have the equalities:

$$\left(\frac{x}{p}\right) = [x^2, p]_4 = [z^2 D_2, p]_4 = \left(\frac{z}{p}\right)[D_2, p]_4 = \left(\frac{p}{z}\right)[D_2, p]_4. \tag{48}$$

For the second equality we used the equation $x^2 - D_1 y^2 - D_2 z^2 = 0$ modulo p. Actually, if D_1 is even, we also have the equality

$$\left(\frac{x}{2}\right) = \left(\frac{2}{z}\right)[D_2, 2]_4. \tag{49}$$

The proof of (49) is done by comparing the values of both sides of this equality. Note that we have $D_1 y^2 \equiv 0 \mod 16$ which implies

$$x^2 \equiv D_2 z^2 \bmod 16, \tag{50}$$

hence $D_2 \equiv 1, 9 \bmod 16$. In order to check (49), it remains to pass in review all the possible congruences $\{1, 5\}$ of x modulo 8, and $\{1, 9\}$ of D_2 modulo 16, and $\{1, 3, 5, 7\}$ of z modulo 8 under the constraint (50).

Multiplying (48) and (49) for every $p \mid D_1$ and using multiplicativity we get:

$$\left(\frac{x}{D_1}\right) = \left(\frac{D_1}{z}\right)[D_2, D_1]_4.$$

Finally, by reducing (46) modulo z, we get $\left(\frac{D_1}{z}\right) = 1$ and we complete the proof of the first equality of (47).

The proof of the second equality of (47) has many similarities. Let p be a prime dividing D_2 and therefore odd. We write $y = 2^j u$, where u is odd and $j \geq 1$. Then we get:

$$\left(\frac{x}{p}\right) = [x^2, p]_4 = [y^2 D_1, p]_4 = \left(\frac{y}{p}\right)[D_1, p]_4 = \left(\frac{2}{p}\right)^j \left(\frac{p}{u}\right)[D_1, p]_4,$$

by appealing to the reciprocity law. By multiplying all $p \mid D_2$ we get:

$$\left(\frac{x}{D_2}\right) = \left(\frac{2}{D_2}\right)^j \left(\frac{D_2}{u}\right)[D_1, D_2]_4.$$

By reducing (46) modulo u we obtain $\left(\frac{D_2}{u}\right) = 1$, which combined with the above formula gives:

$$\left(\frac{2x}{D_2}\right) = \left(\frac{2}{D_2}\right)^{j-1}[D_1, D_2]_4.$$

If $j = 1$, the second formula of (47) is proved. In the case $j \geq 2$ we get that $D_1 y^2 \equiv 0 \bmod 16$ and (50) is satisfied. This implies $\left(\frac{2}{D_2}\right) = 1$ and again the second formula of (47) is proved. □

Theorem 7. *Let D be a special discriminant and $\{D_1, D_2\}$ be a decomposition of third type. Then*

$$[D_1, D_2]_4 = 1 = [D_2, D_1]_4.$$

Proof. Using Theorem 6 we find a decomposition $E = \{E_1, E_2\}$ such that $\forall p \mid D_1 :$ $\left(\frac{xE}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{E}{p}\right) = 1$. We want to multiply this equation for all p dividing D_1.

Unfortunately, the E_i we have to choose is different for each p. By Lemma 8 we have:

$$\prod_{p|D_1}\left(\frac{x}{p}\right)=\left(\frac{x}{D_1}\right)=[D_2,D_1]_4.$$

Therefore we need to prove that:

$$\prod_{p|D_1}\left(\frac{E}{p}\right)=1.$$

Since we choose E_i in a way that $p\notin E_i$ we get:

$$\prod_{p|D_1}\left(\frac{E}{p}\right)=\prod_{p|(E_1,D_1)}\left(\frac{E_2}{p}\right)\prod_{p|(E_2,D_1)}\left(\frac{E_1}{p}\right),$$

where (E_1,D_1) denotes the greatest common divisor. Let us introduce the following notations:

$$e_1:=\prod_{p|(E_1,D_1)}p,\ e_2:=\prod_{p|(E_2,D_1)}p,\ f_1:=\prod_{p|(E_1,D_2)}p,\ f_2:=\prod_{p|(E_2,D_2)}p.$$

Note that $e_1e_2=D_1$ and $f_1f_2=D_2$ up to a possible factor of 4. Then we can continue:

$$\prod_{p|(E_1,D_1)}\left(\frac{E_2}{p}\right)\prod_{p|(E_2,D_1)}\left(\frac{E_1}{p}\right)=\left(\frac{E_2}{e_1}\right)\left(\frac{E_1}{e_2}\right)=\left(\frac{e_2f_2}{e_1}\right)\left(\frac{e_1f_1}{e_2}\right)$$

$$=\left(\frac{e_2}{e_1}\right)\left(\frac{e_1}{e_2}\right)\left(\frac{f_2}{e_1}\right)\left(\frac{f_1}{e_2}\right)=\left(\frac{f_2}{e_1}\right)\left(\frac{f_1}{e_2}\right).$$

Since $\{D_1,D_2\}$ is a decomposition of second type, we have

$$1=\left(\frac{D_2}{e_1}\right)=\left(\frac{f_1}{e_1}\right)\left(\frac{f_2}{e_1}\right)\text{ and }1=\left(\frac{f_1}{D_1}\right)=\left(\frac{f_1}{e_1}\right)\left(\frac{f_1}{e_2}\right)$$

and therefore $\left(\frac{f_2}{e_1}\right)=\left(\frac{f_1}{e_1}\right)$ and $\left(\frac{f_1}{e_2}\right)=\left(\frac{f_1}{e_1}\right)$. So we continue:

$$\left(\frac{f_2}{e_1}\right)\left(\frac{f_1}{e_2}\right)=\left(\frac{f_1}{e_1}\right)\left(\frac{f_1}{e_1}\right)=1.$$

Altogether we get: $\prod_{p|D_1}\left(\frac{E}{p}\right)=1$ and therefore we proved $[D_2,D_1]_4=1$.

Using the same decomposition $E=\{E_1,E_2\}$ we apply Theorem 6 and for all primes p dividing D_2 we get $\left(\frac{2xE}{p}\right)=1$. Then

$$1=\prod_{p|D_2}\left(\frac{2xE}{p}\right)=\left(\frac{2x}{D_2}\right)\prod_{p|D_2}\left(\frac{E}{p}\right)=[D_1,D_2]_4.$$

Here we used Lemma 8 and a similar computation as in the first case to show that the product over the Kronecker symbols is 1. □

4.4. **The special case where the 4-rank is one.** In the last paragraph we have proved the second part of Theorem 3, i.e. we have proved an upper bound for the 8-rank. The goal of this section is to prove the third part, which gives an equality in the case that the 4–rank of C_D is 1. In Theorem 6 we have already proved a criterion for the 8–rank. Unfortunately, the assertion of this theorem is not easily usable for our purpose, because we have the freedom to choose a decomposition $E = \{E_1, E_2\}$. If we have the right decomposition E we need to check $\omega(D)$ symbols which have to take the value 1. In Theorem 7 we group these symbols in two sets and only check, if the product of those symbols in these sets is 1. Obviously, this gives a necessary condition, but there is no reason that this gives a sufficient one.

Now we use the theory of Redei matrices which can be introduced for fundamental discriminants. In order to simplify the presentation we restrict to special discriminants. As usual we denote by d the squarefree part of D, i.e. $d = D$ if D is odd and $d = D/4$ if D is even. We write $d = p_1 \cdots p_t$, hence $t = \omega(D) = \omega(d)$ and all the p_i are distinct and congruent to 2 or 1 modulo 4. Let $M_D := (m_{i,j})_{i,j=1}^t \in \mathbb{F}_2^{t\times t}$ be the matrix, where $m_{i,j} \in \mathbb{F}_2$ are defined by the equations:

$$\begin{cases} (-1)^{m_{i,j}} = \left(\frac{p_i}{p_j}\right) & \text{if } i \neq j \\ (-1)^{m_{i,i}} = \left(\frac{d/p_i}{p_i}\right) & \text{if } i = j. \end{cases}$$

We remark that the multiplicative properties of the Kronecker symbols carry over to additive properties of the rows of M_D.

Let $\{D_1, D_2\}$ be a decomposition of D. Define $v_1 = (v_{i,1})$ and $v_2 = (v_{i,2}) \in \mathbb{F}_2^t$ via

$$d_j = \prod_{i=1}^{t} p_i^{v_{i,j}} \ (j = 1, 2).$$

It is clear that to each decomposition we can associate two vectors v_1 and $v_2 \in \mathbb{F}_2^t$, which have the property that $v_1 + v_2 = (1, \ldots, 1)^{\mathrm{tr}}$. The trivial decomposition corresponds to the zero vector and $(1, \ldots, 1)^{\mathrm{tr}}$ and vice versa.

The following lemma was proved by Redei in [15]. We remark that it can be extended to arbitrary fundamental discriminants.

Lemma 9. *Let D be a special discriminant with $d = p_1 \cdots p_t$. Assume that $E := \{E_1, E_2\}$ is a decomposition corresponding to v_1, v_2. Then we have:*

(i) *$M_D \cdot v_1 = M_D \cdot v_2 = (w_1, \ldots, w_t)^{\mathrm{tr}}$ with $(-1)^{w_i} = \left(\frac{E}{p_i}\right)$ for $1 \le i \le t$.*
(ii) *$\{E_1, E_2\}$ is a decomposition of second type, if and only if v_1 and v_2 are in the kernel of the matrix M_D.*
(iii) $\dim(\ker M_D) = \mathrm{rk}_4(C_D) + 1$.

Proof. We remember that $\left(\frac{E}{p}\right)$ was defined as the symbol $\left(\frac{E_1}{p}\right)$ or $\left(\frac{E_2}{p}\right)$ such that $p \nmid E_i$. Note that $\left(\frac{D/p_i}{p_i}\right) = \prod_{i\neq j=1}^{t} \left(\frac{p_j}{p_i}\right)$ and therefore the vector $(1, \ldots, 1)^{\mathrm{tr}}$ is contained in the kernel and it corresponds to the trivial decomposition (which is of second type). In order to simplify notations w.l.o.g. (by reordering the p_i) we can assume that $v_1 = (1, \ldots, 1, 0, \ldots, 0)$ and it corresponds to $E_1 = \prod_{i=1}^{k} p_i$ for some

$k \leq t$. Now $M_D \cdot v_1 = (w_1, \dots, w_t)^{\mathrm{tr}}$, where $w_i \in \{0,1\}$ is defined via

$$(-1)^{w_i} = \begin{cases} \prod_{i \neq j=1}^{k} \left(\frac{p_j}{p_i}\right)\left(\frac{D/p_i}{p_i}\right) = \prod_{j=k+1}^{t} \left(\frac{p_j}{p_i}\right) = \left(\frac{E_2}{p_i}\right) & \text{if } i \leq k \\ \prod_{j=1}^{k} \left(\frac{p_j}{p_i}\right) = \left(\frac{E_1}{p_i}\right) & \text{if } i > k \end{cases}.$$

We immediately see that the decomposition corresponding to a v in the kernel is a decomposition of second type and vice versa. Since we have to count $\{E_1, E_2\}$ and $\{E_2, E_1\}$ as different elements and we always meet the trivial decompositions we find that we have $2^{\mathrm{rk}_4(C_D)}$ different decompositions. Therefore the rank of the kernel of M_D is $\mathrm{rk}_4(C_D) + 1$. □

In the following we assume that we have a decomposition $\{D_1, D_2\}$ of second type which has the additional property (used in Theorem 7) that $[D_1, D_2]_4 = 1 = [D_2, D_1]_4$ which by Lemma 8 is equivalent to

$$\left(\frac{x}{D_1}\right) = \prod_{p \mid D_1} \left(\frac{x}{p}\right) = 1 \text{ and } \left(\frac{2x}{D_2}\right) = \prod_{p \mid D_2} \left(\frac{2x}{p}\right) = 1. \tag{51}$$

In order to apply Theorem 6 we need to find a decomposition $E = \{E_1, E_2\}$ such that (for a x chosen according to the statement of that theorem):

(i) $\forall p \mid D_1 : \left(\frac{xE}{p}\right) = 1$,

(ii) $\forall p \mid D_2 : \left(\frac{2xE}{p}\right) = 1$.

For every prime dividing D we get a condition:

$$\left(\frac{E}{p}\right) = \begin{cases} \left(\frac{x}{p}\right) & \text{if } p \mid D_1, \\ \left(\frac{2x}{p}\right) & \text{if } p \mid D_2. \end{cases} \tag{52}$$

Using the first part of Lemma 9 we see that the corresponding vectors v_1 and v_2 of the decomposition $E = \{E_1, E_2\}$ have the property that $M_D \cdot v_1 = (w_1, \dots, w_t)^{\mathrm{tr}}$ with $(-1)^{w_i} = \left(\frac{E}{p_i}\right)$.

Therefore we have to answer the question if the vector w corresponding to the condition (52) is in the image of M_D. By Lemma 9 we know that the dimension of the image is $t - 1 - \mathrm{rk}_4(C_D)$. Furthermore by equation (51) we know that the image is contained in (by assuming $D_1 = p_1 \cdots p_k$, $D_2 = p_{k+1} \cdots p_t$ for some $1 \leq k < t$):

$$\{(x_1, \dots, x_t)^{\mathrm{tr}} \mid \sum_{i=1}^{k} x_i = 0, \sum_{i=k+1}^{t} x_i = 0\} \leq \mathbb{F}_2^t.$$

For a non-trivial decomposition $\{D_1, D_2\}$ of second type this space has dimension $t - 2$ and it contains the image of M_D. In case that $\mathrm{rk}_4(C_D) = 1$ this space has the right dimension and it coincides with the image of M_D. This means that in this situation we can always find a decomposition $E = \{E_1, E_2\}$ which satisfies condition (52) and we have proved:

Theorem 8. *Let D be a special discriminant satisfying $\mathrm{rk}_4(C_D) = 1$. Let $\{D_1, D_2\}$ be a decomposition of second type of D with $[D_1, D_2]_4 = 1 = [D_2, D_1]_4$. Then $\{D_1, D_2\}$ is a decomposition of third type and therefore $\mathrm{rk}_8(C_D) = 1$.*

This finishes the proof of the first three parts of Theorem 3. The final parts of this theorem will be proved in the following two sections.

5. Analytic tools

We shall appeal to analytic tools which were already exploited in [4] to study the asymptotic behavior of the following moments:

$$S(X,k)=\sum_{\substack{D\in\mathcal{D}\\ D\leq X}}2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}, \tag{53}$$

$$S^{\mathrm{mix}}(X,k)=\sum_{\substack{D\in\mathcal{D}\\ D\leq X}}2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}\cdot 2^{\mathrm{rk}_4(\mathrm{Cl}_D)} \tag{54}$$

and the corresponding moments $S_{\mathrm{odd}}(X,k)$, $S^{\mathrm{mix}}_{\mathrm{odd}}(X,k)$, $S_{\mathrm{even}}(X,k)$, and $S^{\mathrm{mix}}_{\mathrm{even}}(X,k)$, attached to the subsets $\mathcal{D}_{\mathrm{odd}}$ and $\mathcal{D}_{\mathrm{even}}$. We proved

Proposition 5. *(*[4, Theorems 3 & 4]*) For every integer $k\geq 0$ and for every positive ϵ we have*

$$S(X,k)=c_k\cdot\mathcal{D}(X)+O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big), \tag{55}$$

and

$$S^{\mathrm{mix}}(X,k)=c_k\cdot\big(2^{k-1}+1\big)\cdot\mathcal{D}(X)+O_{\epsilon,k}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big), \tag{56}$$

uniformly for $X\geq 3$. Similar equalities are also true for the sums $S_{\mathrm{odd}}(X,k)$, $S_{\mathrm{even}}(X,k)$, $S^{\mathrm{mix}}_{\mathrm{odd}}(X,k)$ and $S^{\mathrm{mix}}_{\mathrm{even}}(X,k)$.

Notice, that by techniques similar to those employed in §3, Proposition 5 implies the knowledge of the density of the set of special D, such that $\mathrm{rk}_4(\mathrm{C}_D)=a$ and $\mathrm{rk}_4(\mathrm{Cl}_D)=b$ for any pair of integers (a,b). This is the content of [4, Theorem 2], a particular case of which is quoted in (29) above.

5.1. **Heuristic interpretation of formula (14).**

The left part of (56) contains the contribution of two trivial decompositions $\{D,1\}$ and $\{1,D\}$, coming from the decomposition formula of $2^{\mathrm{rk}_4(\mathrm{Cl}_D)}$ given in Proposition 4. Similarly these terms also appear in the left part of (14) (see the definition of 2^{λ_D}). The contribution of these terms to the left hand sides of (14) and (56) is just $\sum_{D\in\mathcal{D},\,D\leq X}2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}$, and by (55), we deduce that this contribution is $\sim c_k\cdot\mathcal{D}(X)$.

Subtracting this easy term from the left hand side of (14) and (56), we exactly obtain the asymptotics $c_k\cdot 2^{k-2}\cdot\mathcal{D}(X)$ and $c_k\cdot 2^{k-1}\cdot\mathcal{D}(X)$, respectively. The main term of the first one is equal to half of the second one. In other words, asymptotically, in the set of non trivial decompositions $\{D_1,D_2\}$ of the second type of D, the number of pairs with $[D_1,D_2]_4=[D_2,D_1]_4=1$ is the same as the number of those satisfying $[D_1,D_2]_4=[D_2,D_1]_4=-1$. The above considerations explain the expansion (14) heuristically. It remains to give a rigorous justification of this interpretation.

5.2. **Gaussian integers.** We gather all the necessary tools from the theory of Gaussian integers, as it is used in [4]. The main idea is to transform the formulas contained in Proposition 3 and in Definition 2 into expressions containing products of Jacobi symbols and of of quartic symbols in order to take advantage of the oscillations of these characters. All what follows is an abstract of [4, §4 & 5]. We classically say that an element of the ring $\mathbb{Z}[i]$ of Gaussian integers is *primary* when it is congruent to 1 mod $2(1+i)$. We also say that $w \in \mathbb{Z}[i]$ is odd if its norm denoted by $\mathcal{N}(w)$ is odd.

Definition 4. *(see* [4, Def. 3]*) An irreducible element π of $\mathbb{Z}[i]$ is said to be privileged if, written as $\pi = a + bi$, it satisfies the three conditions:*
• *$\pi\overline{\pi}$ is a rational prime congruent to* 1 mod 4*,*
• *π is primary,*
• *$b > 0$.*
We denote by $\mathfrak{P}$ the set of privileged irreducible elements.

The third condition is a natural way to choose one element in the set $\{\pi, \overline{\pi}\}$ and $\mathfrak{P}$ appears as a subset of the upper half complex plane. With this convention, note that every integer prime $p \equiv 1 \bmod 4$ has a unique factorization $p = \pi\overline{\pi}$, where π is a privileged prime. We generalize this fact by

Definition 5. *Let D an odd special discriminant. We say that the factorization $D = \mathfrak{D}\overline{\mathfrak{D}}$ is the privileged factorization of D if $\mathfrak{D}$ is the product of elements of $\mathfrak{P}$. Such a factorization exists and is unique for every $D \in \mathcal{D}_{\text{odd}}$.*

Using the Jacobi symbols we can reformulate Proposition 3 as follows.

Proposition 6. *For $D \in \mathcal{D}_{\text{odd}}$ we have the equalities*

$$\begin{aligned} 2^{\mathrm{rk}_4(\mathrm{C}_D)} &= \frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=ab} \prod_{p\mid a}\Big(1+\Big(\frac{b}{p}\Big)\Big) \prod_{p\mid b}\Big(1+\Big(\frac{a}{p}\Big)\Big) \\ &= \frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=D_0D_1D_2D_3} \Big(\frac{D_0}{D_2}\Big)\Big(\frac{D_1}{D_3}\Big), \end{aligned}$$

and

$$\begin{aligned} 2^{\mathrm{rk}_4(\mathrm{C}_{8D})} &= \frac{1}{2^{\omega(D)}} \sum_{D=ab} \prod_{p\mid a}\Big(1+\Big(\frac{2b}{p}\Big)\Big) \prod_{p\mid b}\Big(1+\Big(\frac{a}{p}\Big)\Big) \\ &= \frac{1}{2^{\omega(D)}} \sum_{D=D_0D_1D_2D_3} \Big(\frac{2}{D_3}\Big)\Big(\frac{D_0}{D_2}\Big)\Big(\frac{D_1}{D_3}\Big). \end{aligned}$$

Proof. See [4, Lemmata 12 & 13]. Note that these lemmata are consequences of the first criterion which gives a formula for $2^{\mathrm{rk}_4(C_D)}$ for fundamental D. This first criterion, due to Redei, is based on the study of the norm form on $\mathbb{Q}(\sqrt{D})$, considered as a quadratic form (see [3, Thm. 5] and [4, Prop. 2] for more comments). Proposition 3 of the present paper is a consequence of the second criterion which is based on deeper algebraic number theory. It also simplifies the formulas contained in Proposition 6, by using Jacobi symbols to detect when an integer is a square modulo another integer. □

A similar formula for $2^{\mathrm{rk}_4(\mathrm{Cl}_D)}$ and for 2^{λ_D} is more difficult to produce owing to the symbol $[.,.]_4$ appearing in Proposition 4 and in Definition 2. To transform these formulas, we shall appeal to the quartic (or biquadratic) character on $\mathbb{Z}[i]$: $\left(\frac{\cdot}{\cdot}\right)_4$.

5.3. **Usual properties of the quartic character.** In this subsection, we shall recall the basic properties of the quartic symbol without comments. A good reference is [10, p.119–127].

If $v \in \mathbb{Z}[i]$ and π is an odd irreducible element of $\mathbb{Z}[i]$ not dividing v, we define

$$\left(\frac{v}{\pi}\right)_4 = i^j,$$

where j is the unique integer satisfying $0 \leq j \leq 3$ and $v^{\frac{\mathcal{N}(\pi)-1}{4}} \equiv i^j \bmod \pi$. If $\pi \mid a$, we put $\left(\frac{a}{\pi}\right)_4 = 0$. If w is an odd element of $\mathbb{Z}[i]$ factorized as $w = \pi_1 \cdots \pi_k$, in a product of irreducible elements, we define

$$\left(\frac{v}{w}\right)_4 := \prod_{m=1}^{k} \left(\frac{v}{\pi_m}\right)_4.$$

Both applications $v \mapsto \left(\frac{v}{w}\right)_4$ and $w \mapsto \left(\frac{v}{w}\right)_4$ are multiplicative. If p is a prime $\equiv 1 \bmod 4$, factorized as $p = \pi\overline{\pi}$, then we have $\left(\frac{\cdot}{p}\right) = \left(\frac{\cdot}{\pi}\right)_4^2$. In particular, if a is a rational integer, then $\left(\frac{a}{p}\right) = 1$ if and only if $\left(\frac{a}{\pi}\right)_4 = \pm 1$. The integer a is a fourth power modulo p if and only if $\left(\frac{a}{\pi}\right)_4 = 1$. For every elements v and w of $\mathbb{Z}[i]$, with w odd, we have

$$\overline{\left(\frac{v}{w}\right)_4} = \left(\frac{\overline{v}}{\overline{w}}\right)_4 = \left(\frac{v}{w^3}\right)_4.$$

Finally the so–called *quartic reciprocity law*

$$\left(\frac{v}{w}\right)_4 = \left(\frac{w}{v}\right)_4 (-1)^{\frac{\mathcal{N}(v)-1}{4} \cdot \frac{\mathcal{N}(w)-1}{4}},$$

which is is true for every primary elements v and w in $\mathbb{Z}[i]$. In particular, we have

$$\left(\frac{v}{w}\right)_4^2 = \left(\frac{\overline{v}}{\overline{w}}\right)_4^2 = \left(\frac{w}{v}\right)_4^2.$$

If $v = a + ib$ is a primary element, then we have

$$\left(\frac{2}{v}\right)_4 = i^{-\frac{b}{2}}.$$

5.4. **Basic formulas.** Let us recall

Proposition 7. *(*[4, Thm. 6]*) For every $D \in \mathcal{D}_{\text{odd}}$ we have the equalities*

$$2^{\mathrm{rk}_4(\mathrm{Cl}_D)} = \frac{2^{\mathrm{rk}_4(\mathrm{C}_D)}}{2} + \frac{1}{4 \cdot 2^{\omega(D)}} \sum_{D=abcd} \left(\frac{\mathfrak{a}\overline{\mathfrak{b}}}{\mathfrak{c}\overline{\mathfrak{d}}}\right)_4^2, \tag{57}$$

and

$$2^{\mathrm{rk}_4(\mathrm{Cl}_{8D})} = \frac{2^{\mathrm{rk}_4(\mathrm{C}_{8D})}}{2} + \frac{1}{2 \cdot 2^{\omega(D)}} \sum_{D=abcd} [ab, 2]_4 \left(\frac{2}{\mathfrak{a}\overline{\mathfrak{b}}}\right)_4 \left(\frac{\mathfrak{a}\overline{\mathfrak{b}}}{\mathfrak{c}\overline{\mathfrak{d}}}\right)_4^2, \tag{58}$$

where $a = \mathfrak{a}\overline{\mathfrak{a}}$, $b = \mathfrak{b}\overline{\mathfrak{b}}$, $c = \mathfrak{c}\overline{\mathfrak{c}}$ and $d = \mathfrak{d}\overline{\mathfrak{d}}$ are the privileged factorizations of a, b, c and d.

Now we prove similar formulas for the function 2^{λ_D}:

Proposition 8. *For every $D \in \mathcal{D}_{\mathrm{odd}}$ we have the equalities*

$$2^{\lambda_D} = \frac{2^{\mathrm{rk}_4(\mathrm{C}_D)}}{4} + \frac{1}{4\cdot 2^{\omega(D)}} \sum_{D=abcd} \left(\frac{a}{\bar{\mathfrak{c}}\mathfrak{d}}\right)_4 \left(\frac{b}{\mathfrak{c}\bar{\mathfrak{d}}}\right)_4 + \frac{1}{8\cdot 2^{\omega(D)}} \sum_{D=abcd} \left(\frac{\mathfrak{a}\bar{\mathfrak{b}}}{\mathfrak{c}\bar{\mathfrak{d}}}\right)_4^2, \tag{59}$$

and

$$\begin{aligned} 2^{\lambda_{8D}} = {} & \frac{1}{4\cdot 2^{\omega(D)}} \sum_{D=a_1a_2b_1b_2} \left(\frac{2}{a_1}\right)\left(\frac{b_1}{a_1}\right)\left(\frac{b_2}{a_2}\right) \\ & + \frac{1}{4\cdot 2^{\omega(D)}} \sum_{D=a_1a_2b_1b_2} [a_1a_2,2]_4 \left(\frac{2}{\mathfrak{a}_1\bar{\mathfrak{a}}_2}\right)_4 \left(\frac{\mathfrak{a}_1\bar{\mathfrak{a}}_2}{\mathfrak{b}_1\bar{\mathfrak{b}}_2}\right)_4^2 \\ & + \frac{1}{4\cdot 2^{\omega(D)}} \sum_{D=a_1a_2b_1b_2} [a_1a_2,2]_4 \left(\frac{2}{a_1}\right)\left(\frac{a_1}{\bar{\mathfrak{b}}_1\mathfrak{b}_2}\right)_4 \left(\frac{a_2}{\mathfrak{b}_1\bar{\mathfrak{b}}_2}\right)_4 \\ & + \frac{1}{4\cdot 2^{\omega(D)}} \sum_{D=a_1a_2b_1b_2} \left(\frac{2}{\bar{\mathfrak{a}}_1\mathfrak{a}_2}\right)_4 \left(\frac{b_1}{\bar{\mathfrak{a}}_1\mathfrak{a}_2}\right)_4 \left(\frac{b_2}{\mathfrak{a}_1\bar{\mathfrak{a}}_2}\right)_4. \end{aligned} \tag{60}$$

Note that we ca replace the first line of the right hand side of (60) by $2^{\mathrm{rk}_4(\mathrm{C}_{8D})}/4$. Comparing with Proposition 7, we directly get

Proposition 9. *For every $D \in \mathcal{D}_{\mathrm{odd}}$ we have the equalities*

$$2^{\lambda_D} = \frac{2^{\mathrm{rk}_4(\mathrm{Cl}_D)}}{2} + \frac{1}{4\cdot 2^{\omega(D)}} \sum_{D=abcd} \left(\frac{a}{\bar{\mathfrak{c}}\mathfrak{d}}\right)_4 \left(\frac{b}{\mathfrak{c}\bar{\mathfrak{d}}}\right)_4,$$

and

$$\begin{aligned} 2^{\lambda_{8D}} = {} & \frac{2^{\mathrm{rk}_4(\mathrm{Cl}_{8D})}}{2} + \frac{1}{4\cdot 2^{\omega(D)}} \sum_{D=a_1a_2b_1b_2} [a_1a_2,2]_4 \left(\frac{2}{a_1}\right)\left(\frac{a_1}{\bar{\mathfrak{b}}_1\mathfrak{b}_2}\right)_4 \left(\frac{a_2}{\mathfrak{b}_1\bar{\mathfrak{b}}_2}\right)_4 \\ & + \frac{1}{4\cdot 2^{\omega(D)}} \sum_{D=a_1a_2b_1b_2} \left(\frac{2}{\bar{\mathfrak{a}}_1\mathfrak{a}_2}\right)_4 \left(\frac{b_1}{\bar{\mathfrak{a}}_1\mathfrak{a}_2}\right)_4 \left(\frac{b_2}{\mathfrak{a}_1\bar{\mathfrak{a}}_2}\right)_4. \end{aligned}$$

Proof. Proposition 8 has many similarities with Proposition 7. Hence the proof of Proposition 8 uses many tools already given in [4]. First we detect the value $+1$ of the symbol $[\cdot,\cdot]_4$ as follows:

Lemma 10. *([4, Lemma 28]) Let $b \in \mathcal{D}_{\mathrm{odd}}$ with its privileged factorization $b = \mathfrak{b}\bar{\mathfrak{b}}$. Then we have for every integer a coprime with b*

$$\frac{1}{2\cdot 2^{\omega(b)}} \Big(\Big(\frac{a}{\mathfrak{b}}\Big)_4 + 1\Big) \prod_{p\mid b}\Big(1 + \Big(\frac{a}{p}\Big)\Big) = \begin{cases} 1 & \textit{if } [a,b]_4 = 1, \\ 0 & \textit{otherwise.} \end{cases} \tag{61}$$

If a is coprime with $2b$, we have

$$\frac{1}{2\cdot 2^{\omega(b)}} \Big(\Big(\frac{a}{\mathfrak{b}}\Big)_4 [a,2]_4 + 1\Big) \prod_{p\mid b}\Big(1 + \Big(\frac{a}{p}\Big)\Big) {[a,2]_4}^2 = \begin{cases} 1 & \textit{if } [a,2b]_4 = 1, \\ 0 & \textit{otherwise.} \end{cases} \tag{62}$$

From this we deduce

Lemma 11. *For every $D \in \mathcal{D}_{\text{odd}}$, we have the equalities*

$$2^{\lambda_D} = \frac{2^{\mathrm{rk}_4(\mathrm{C}_D)}}{4} + \frac{1}{4 \cdot 2^{\omega(D)}} \sum_{D=ab} \Big(\frac{a}{\mathfrak{b}}\Big)_4 \prod_{p \mid a}\Big(1 + \Big(\frac{b}{p}\Big)\Big) \prod_{p \mid b}\Big(1 + \Big(\frac{a}{p}\Big)\Big) \tag{63}$$
$$+ \frac{1}{8 \cdot 2^{\omega(D)}} \sum_{D=ab} \Big(\frac{\mathfrak{a}}{\mathfrak{b}}\Big)_4^2 \prod_{p \mid a}\Big(1 + \Big(\frac{b}{p}\Big)\Big) \prod_{p \mid b}\Big(1 + \Big(\frac{a}{p}\Big)\Big),$$

and

(64)
$$2^{\lambda_{8D}} = \frac{1}{4 \cdot 2^{\omega(D)}} \sum_{\substack{D=ab \\ a \equiv 1 \bmod 8}} \Big(1 + [a,2]_4 \Big(\frac{2}{\mathfrak{a}}\Big)_4 \Big(\frac{\mathfrak{a}}{\mathfrak{b}}\Big)_4^2 + [a,2]_4 \Big(\frac{a}{\mathfrak{b}}\Big)_4 + \Big(\frac{2}{\mathfrak{a}}\Big)_4 \Big(\frac{b}{\mathfrak{a}}\Big)_4 \Big)$$
$$\times \prod_{p \mid a}\Big(1 + \Big(\frac{2b}{p}\Big)\Big) \prod_{p \mid b}\Big(1 + \Big(\frac{a}{p}\Big)\Big),$$

where $a = \mathfrak{a}\overline{\mathfrak{a}}$ and $b = \mathfrak{b}\overline{\mathfrak{b}}$ are the privileged factorizations of a and b.

Proof of Lemma 11. By Definition 2 and Lemma 10, we have for $D \in \mathcal{D}_{\text{odd}}$:

$$2^{\lambda_D} = \frac{1}{8 \cdot 2^{\omega(D)}} \sum_{D=ab} \Big(\Big(\frac{a}{\mathfrak{b}}\Big)_4 + 1\Big)\Big(\Big(\frac{b}{\mathfrak{a}}\Big)_4 + 1\Big) \prod_{p \mid a}\Big(1 + \Big(\frac{b}{p}\Big)\Big) \prod_{p \mid b}\Big(1 + \Big(\frac{a}{p}\Big)\Big).$$

We expand the product $\Big(\big(\frac{a}{\mathfrak{b}}\big)_4 + 1\Big)\Big(\big(\frac{b}{\mathfrak{a}}\big)_4 + 1\Big)$ and use the equalities

$$\Big(\frac{a}{\mathfrak{b}}\Big)_4 \Big(\frac{b}{\mathfrak{a}}\Big)_4 = \Big(\frac{a}{\mathfrak{b}}\Big)_4 \Big(\frac{\mathfrak{a}}{b}\Big)_4 = \Big(\frac{\mathfrak{a}}{\mathfrak{b}}\Big)_4 \Big(\frac{\overline{\mathfrak{a}}}{\mathfrak{b}}\Big)_4 \Big(\frac{\mathfrak{a}}{\mathfrak{b}}\Big)_4 \Big(\frac{\mathfrak{a}}{\overline{\mathfrak{b}}}\Big)_4 = \Big(\frac{\mathfrak{a}}{\mathfrak{b}}\Big)_4^2,$$

which are consequences of the multiplicative and conjugacy properties of the quartic character and the quartic reciprocity law. We appeal to Proposition 6 to complete the proof of the first equality of this lemma.

As usual, the prime 2 creates extra difficulty. Using Definition 2, Lemma 10 and symmetry we get for $D \in \mathcal{D}_{\text{odd}}$ the following equality:

$$2^{\lambda_{8D}} = \frac{1}{4 \cdot 2^{\omega(D)}} \sum_{D=ab} {[a,2]_4}^2 \Big(\Big(\frac{a}{\mathfrak{b}}\Big)_4 [a,2]_4 + 1\Big)\Big(\Big(\frac{2b}{\mathfrak{a}}\Big)_4 + 1\Big)$$
$$\prod_{p \mid a}\Big(1 + \Big(\frac{2b}{p}\Big)\Big) \prod_{p \mid b}\Big(1 + \Big(\frac{a}{p}\Big)\Big).$$

By imposing the congruence $a \equiv 1 \bmod 8$, we drop the coefficient ${[a,2]_4}^2$. We expand the product $\Big(\big(\frac{a}{\mathfrak{b}}\big)_4 [a,2]_4 + 1\Big)\Big(\big(\frac{2b}{\mathfrak{a}}\big)_4 + 1\Big)$, as we did before. This completes the proof of Lemma 11. □

Now we pass to the proof of Proposition 8 itself. For the first formula, we sum over the divisors of a and b in order to write the double product as

$$\prod_{p \mid a}\Big(1 + \Big(\frac{b}{p}\Big)\Big) \prod_{p \mid b}\Big(1 + \Big(\frac{a}{p}\Big)\Big) = \sum_{a_1 a_2 = a} \sum_{b_1 b_2 = b} \Big(\frac{a_1}{b_1}\Big)\Big(\frac{a_2}{b_2}\Big), \tag{65}$$

which is consequence of the multiplicative properties of the Jacobi symbol and of the quadratic reciprocity law. We introduce the privileged factorizations of a_1, a_2,

b_1 and b_2 which gives

$$\sum_{D=ab}\left(\frac{a}{\mathfrak{b}}\right)_4\prod_{p\mid a}\Bigl(1+\Bigl(\frac{b}{p}\Bigr)\Bigr)\prod_{p\mid b}\Bigl(1+\Bigl(\frac{a}{p}\Bigr)\Bigr)=\sum_{D=a_1a_2b_1b_2}\left(\frac{a_1a_2}{\mathfrak{b}_1\mathfrak{b}_2}\right)_4\left(\frac{a_1}{b_1}\right)\left(\frac{a_2}{b_2}\right).$$

Now we use some properties of the quartic symbol, listed in §5.3:

$$\begin{aligned}\left(\frac{a_1a_2}{\mathfrak{b}_1\mathfrak{b}_2}\right)_4\left(\frac{a_1}{b_1}\right)\cdot\left(\frac{a_2}{b_2}\right)&=\left(\frac{a_1a_2}{\mathfrak{b}_1\mathfrak{b}_2}\right)_4\left(\frac{a_1}{\mathfrak{b}_1}\right)_4^2\left(\frac{a_2}{\mathfrak{b}_2}\right)_4^2\\ &=\left(\frac{a_1}{\overline{\mathfrak{b}}_1}\right)_4\left(\frac{a_2}{\overline{\mathfrak{b}}_2}\right)_4\left(\frac{a_1}{\mathfrak{b}_2}\right)_4\left(\frac{a_2}{\mathfrak{b}_1}\right)_4=\left(\frac{a_1}{\overline{\mathfrak{b}}_1\mathfrak{b}_2}\right)_4\left(\frac{a_2}{\mathfrak{b}_1\overline{\mathfrak{b}}_2}\right)_4.\end{aligned}\tag{66}$$

This computation proves the second term of the right part of (59), after an obvious change of names of variables. The third term on the right part of (59) comes from the third term in the right part of (63). The proof is the same as above and this computation was already made within the proof of [4, Thm 6]. This completes the proof of (59).

The proof of (60) concerning $2^{\lambda_{8D}}$ is more intricate than (59), since there are four terms inside $\Bigl(\cdots\Bigr)$ in the right part of (64). Of course, the identity (65) is replaced by

$$\prod_{p\mid a}\Bigl(1+\Bigl(\frac{2b}{p}\Bigr)\Bigr)\prod_{p\mid b}\Bigl(1+\Bigl(\frac{a}{p}\Bigr)\Bigr)=\sum_{a_1a_2=a}\ \sum_{b_1b_2=b}\left(\frac{2b_1}{a_1}\right)\left(\frac{b_2}{a_2}\right).\tag{67}$$

In order to control the congruence

$$a_1a_2\equiv 1 \bmod 8,\tag{68}$$

we appeal to the following equality

$$[a_1a_2,2]_4{}^2=\frac{1}{2}\left(1+\left(\frac{2}{a_1a_2}\right)\right),\tag{69}$$

which is true for any integers a_1 and a_2 congruent to 1 modulo 4. Using the multiplicative properties of the Jacobi symbol and the symmetry between the variables, we get the first term on the right part of (60). Note that a similar trick was already used at the end of the proof of [4, Thm 6].

The contribution of the second term inside $\Bigl(\cdots\Bigr)$ in (64) can be dealt by using (67) and noticing the equalities

$$\begin{aligned}[a,2]_4\left(\frac{2}{\mathfrak{a}}\right)_4\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)_4^2\left(\frac{2b_1}{a_1}\right)\left(\frac{b_2}{a_2}\right)&=[a_1a_2,2]_4\left(\frac{2}{\mathfrak{a}_1\mathfrak{a}_2}\right)_4\left(\frac{\mathfrak{a}_1\mathfrak{a}_2}{\mathfrak{b}_1\mathfrak{b}_2}\right)_4^2\left(\frac{2\mathfrak{b}_1\overline{\mathfrak{b}}_1}{\mathfrak{a}_1}\right)_4^2\left(\frac{\mathfrak{b}_2\overline{\mathfrak{b}}_2}{\mathfrak{a}_2}\right)_4^2\\ &=[a_1a_2,2]_4\left(\frac{2}{\overline{\mathfrak{a}}_1\mathfrak{a}_2}\right)_4\left(\frac{\mathfrak{a}_1\overline{\mathfrak{a}}_2}{\overline{\mathfrak{b}}_1\mathfrak{b}_2}\right)_4^2\\ &=[a_1a_2,2]_4\left(\frac{2}{\overline{\mathfrak{a}}_1\mathfrak{a}_2}\right)_4\left(\frac{\overline{\mathfrak{a}}_1\mathfrak{a}_2}{\mathfrak{b}_1\overline{\mathfrak{b}}_2}\right)_4^2\end{aligned}$$

obtained by writing $a=a_1a_2$, $b=b_1b_2$ and by appealing to the formulas quoted in §5.3. Changing the notations, we recover the second term of the right part of (60).

Similarly, the contribution of the third term on the right part of (64) is transformed as follows

$$[a,2]_4\left(\frac{a}{\mathfrak{b}}\right)_4\left(\frac{2b_1}{a_1}\right)\left(\frac{b_2}{a_2}\right)=[a_1a_2,2]_4\left(\frac{2}{a_1}\right)\left(\frac{a_1}{\overline{\mathfrak{b}}_1\mathfrak{b}_2}\right)_4\left(\frac{a_2}{\mathfrak{b}_1\overline{\mathfrak{b}}_2}\right)_4,$$

by a computation already made in (66). This explains the third term on the right part of (60). Finally, we write for the last term:

$$\left(\frac{2}{\mathfrak{a}}\right)_4\left(\frac{b}{\mathfrak{a}}\right)_4\left(\frac{2b_1}{a_1}\right)\left(\frac{b_2}{a_2}\right)=\left(\frac{2}{\overline{\mathfrak{a}}_1\mathfrak{a}_2}\right)_4\left(\frac{b_1}{\overline{\mathfrak{a}}_1\mathfrak{a}_2}\right)_4\left(\frac{b_2}{\mathfrak{a}_1\overline{\mathfrak{a}}_2}\right)_4.$$

Once again, we appeal to (69) to remove the congruence condition (68). This completes the proof of (60), hence the proof of Proposition 8. □

5.5. **How to explain the main term of (14) ?** We give another explanation of the coefficient Γ_k (see (17)) of the main term appearing in (14). This explanation is different from the one given in §5.1, since it starts from Proposition 9. For simplicity, we restrict to the subsum $S_{\text{odd}}^{\text{mix},\lambda}(X,k)$. Replacing 2^{λ_D} in the definition (44) by its expression given in Proposition 9, we get the equality:

$$S_{\text{odd}}^{\text{mix},\lambda}(X,k)=\frac{1}{2}\sum_{\substack{D\in\mathcal{D}_{\text{odd}}\\ D\leq X}}2^{k\,\text{rk}_4(\text{C}_D)}\cdot 2^{\text{rk}_4(\text{Cl}_D)}$$
$$+\frac{1}{4}\sum_{\substack{D\in\mathcal{D}_{\text{odd}}\\ D\leq X}}\frac{2^{k\,\text{rk}_4(\text{C}_D)}}{2^{\omega(D)}}\sum_{D=abcd}\left(\frac{a}{\overline{\mathfrak{c}}\mathfrak{d}}\right)_4\left(\frac{b}{\mathfrak{c}\overline{\mathfrak{d}}}\right)_4. \tag{70}$$

The first term on the right part of (70) is equal to $\frac{1}{2}S_{\text{odd}}^{\text{mix}}(X,k)$ and is

$$\sim\frac{1}{2}\cdot c_k\cdot(2^{k-1}+1)\cdot\mathcal{D}_{\text{odd}}(X),$$

by (56). For the second term of (70), we follow the intuition that the product $\left(\frac{a}{\overline{\mathfrak{c}}\mathfrak{d}}\right)_4\left(\frac{b}{\mathfrak{c}\overline{\mathfrak{d}}}\right)_4$ creates cancellations as soon as it really oscillates. Hence the main term should come from the cases when this product is identically equal to one, and this happens only when $a=b=1$ or $c=d=1$. These two cases give birth to a main contribution

$$2\cdot\frac{1}{4}\sum_{\substack{D\in\mathcal{D}_{\text{odd}}\\ D\leq X}}\frac{2^{k\,\text{rk}_4(\text{C}_D)}}{2^{\omega(D)}}\cdot 2^{\omega(D)}\sim\frac{1}{2}\cdot c_k\cdot\mathcal{D}_{\text{odd}}(X),$$

by (55). It remains to check the equality $\frac{1}{2}(2^{k-1}+1)c_k+\frac{1}{2}c_k=\Gamma_k$ to finally explain the coefficient of the main term in (14).

The rest of the paper is devoted to give complete justifications to the above way of reasoning.

5.6. **Facts taken from** [4]**.** First we shall deal with odd D's. As already written above, the techniques have many similarities with those used in [4]. We will exploit all these similarities to shorten our proof. Inserting the equality contained in Proposition 7 in the definition (54), we obtained the equality

$$S_{\text{odd}}^{\text{mix}}(X,k)=\frac{1}{2}S_{\text{odd}}(X,k+1)+\frac{1}{4}S_{\text{odd}}^{\diamond}(X,k),$$

(see [4, Lemma 44]), with

$$S^{\diamond}_{\text{odd}}(X,k) = \sum_{\substack{D\in\mathcal{D}_{\text{odd}}\\ D\leq X}} \frac{2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}}{2^{\omega(D)}} \sum_{abcd=D} \left(\frac{\mathfrak{a}\overline{\mathfrak{b}}}{\mathfrak{c}\overline{\mathfrak{d}}}\right)_4^2. \tag{71}$$

In our context, we define the sum

$$S^{\diamond,\lambda}_{\text{odd}}(X,k) = \sum_{\substack{D\in\mathcal{D}_{\text{odd}}\\ D\leq X}} \frac{2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}}{2^{\omega(D)}} \sum_{abcd=D} \left(\frac{a}{\mathfrak{c}\overline{\mathfrak{d}}}\right)_4 \left(\frac{b}{\mathfrak{c}\overline{\mathfrak{d}}}\right)_4. \tag{72}$$

With these conventions, the equality (70) can be stated as

Lemma 12. *For every integer $k \geq 0$ and for every $X \geq 1$ we have the equality*

$$S^{\text{mix},\lambda}_{\text{odd}}(X,k) = \frac{1}{2} S^{\text{mix}}_{\text{odd}}(X,k) + \frac{1}{4} S^{\diamond,\lambda}_{\text{odd}}(X,k).$$

The crucial transformation of $S^{\diamond}_{\text{odd}}(X,k)$ is given in [4, Lemma 45]. To present its contents, we must introduce the following notations and conventions

- k is an integer ≥ 0,
- $\mathcal{Q} := \{0,\,1,\,2,\,3\}$,
- $\Delta := 1 + (\log X)^{-2^{k+1}}$,
- $\Omega' := \mathrm{e}4^{k+1}(\log\log X + B_0)$, where B_0 is a sufficiently large constant, such that the following inequality

$$\sharp\left\{n \leq X \,:\, \omega(n) = \ell,\, \mu^2(n) = 1\right\} \leq B_0 \cdot \frac{X}{\log X} \cdot \frac{(\log\log X + B_0)^{\ell}}{\ell!},$$

for every $X \geq 3$, for every integer $\ell \geq 0$ (the existence of such B_0 is due to Hardy and Ramanujan [5], quoted in [3, Lemma 11]),
- i and j are indices taken in $\mathcal{Q}$,
- $\mathbf{r} = (r_1,\dots,r_k)$ and $\mathbf{s} = (s_1,\dots,s_k)$ are indices taken in $\mathcal{Q}^k$,
- for $(\mathbf{r},i)$ and $(\mathbf{s},j) \in \mathcal{Q}^k \times \mathcal{Q}$, $A_{\mathbf{r},i}$ and $A_{\mathbf{s},j}$ are any numbers in the sequence $1,\ \Delta,\ \Delta^2,\ \Delta^3,\dots$,
- for $(\mathbf{r},\mathbf{s}) \in \mathcal{Q}^k \times \mathcal{Q}^k$, $\kappa_k(\mathbf{r},\mathbf{s}) := \sharp\{1 \leq m \leq k\,;\ s_m - r_m = 2\}$.

For $\mathbf{A} = (A_{\mathbf{r},i})_{(\mathbf{r},i)\in\mathcal{Q}^k\times\mathcal{Q}}$, we introduced the partial sum of $S^{\diamond}_{\text{odd}}(X,k,\mathbf{A})$ defined by (see [4, formula (103)]):

(73)

$$S^{\diamond}_{\text{odd}}(X,k,\mathbf{A}) := \frac{1}{2^k} \sum_{(D_{\mathbf{r},i})} \mu^2\big(\prod_{\mathbf{r},i} D_{\mathbf{r},i}\big) \Big(\prod_{\mathbf{r},i} 2^{-(k+1)\omega(D_{\mathbf{r},i})}\Big) \Big\{\prod_{\mathbf{r},i}\prod_{\mathbf{s},j} \left(\frac{D_{\mathbf{r},i}}{D_{\mathbf{s},j}}\right)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\}$$
$$\times \Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}} \left(\frac{\mathfrak{D}_{\mathbf{r},0}}{\mathfrak{D}_{\mathbf{s},2}}\right)_4^2\Big\} \Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}} \left(\frac{\mathfrak{D}_{\mathbf{r},0}}{\overline{\mathfrak{D}}_{\mathbf{s},3}}\right)_4^2\Big\} \Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}} \left(\frac{\overline{\mathfrak{D}}_{\mathbf{r},1}}{\mathfrak{D}_{\mathbf{s},2}}\right)_4^2\Big\} \Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}} \left(\frac{\overline{\mathfrak{D}}_{\mathbf{r},1}}{\overline{\mathfrak{D}}_{\mathbf{s},3}}\right)_4^2\Big\},$$

with the following conditions of summation

$$\begin{cases} (\mathbf{r},i) \text{ and } (\mathbf{s},j) \in \mathcal{Q}^k \times \mathcal{Q}, \\ A_{\mathbf{r},i} \leq D_{\mathbf{r},i} < \Delta A_{\mathbf{r},i},\ D_{\mathbf{r},i} \in \mathcal{D}_{\text{odd}} \cup \{1\}, \\ A_{\mathbf{s},j} \leq D_{\mathbf{s},j} < \Delta A_{\mathbf{s},j},\ D_{\mathbf{s},j} \in \mathcal{D}_{\text{odd}} \cup \{1\}, \\ \omega(D_{\mathbf{r},i}) \leq \Omega',\ \omega(D_{\mathbf{s},j}) \leq \Omega', \\ D_{\mathbf{r},i} = \mathfrak{D}_{\mathbf{r},i}\overline{\mathfrak{D}}_{\mathbf{r},i} \text{ and } D_{\mathbf{s},j} = \mathfrak{D}_{\mathbf{s},j}\overline{\mathfrak{D}}_{\mathbf{s},j} \\ \text{ are the privileged factorizations of } D_{\mathbf{r},i} \text{ and } D_{\mathbf{s},j}, \end{cases} \tag{74}$$

and the convention $0^0 = 1$.

In [4, Lemma 45] we proved the equality

$$S^{\diamond}_{\text{odd}}(X,k) = \sum_{\mathbf{A}} S^{\diamond}_{\text{odd}}(X,k,\mathbf{A}) + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big), \tag{75}$$

for every $\epsilon > 0$ and every integer $k \geq 0$, where the summation is over all the 4^{k+1}–tuples $(A_{\mathbf{r},i})_{(\mathbf{r},i)\in\mathcal{Q}^{k+1}}$ satisfying the inequality

$$\prod_{\mathbf{r},i} A_{\mathbf{r},i} \leq \Delta^{-4^{k+1}} X. \tag{76}$$

The formulas (71) and (72) show flagrant similarities, hence, by analogy with (73) for our present situation, it is natural to introduce the sum $S^{\diamond,\lambda}_{\text{odd}}(X,k,\mathbf{A})$ defined by

(77)

$$S^{\diamond,\lambda}_{\text{odd}}(X,k,\mathbf{A}) = \frac{1}{2^k}\sum_{(D_{\mathbf{r},i})} \mu^2\big(\prod_{\mathbf{r},i} D_{\mathbf{r},i}\big)\Big(\prod_{\mathbf{r},i} 2^{-(k+1)\omega(D_{\mathbf{r},i})}\Big)\Big\{\prod_{\mathbf{r},i}\prod_{\mathbf{s},j}\Big(\frac{D_{\mathbf{r},i}}{D_{\mathbf{s},j}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\}$$
$$\times\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},0}}{\overline{\mathfrak{D}}_{\mathbf{s},2}}\Big)_4\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},0}}{\overline{\mathfrak{D}}_{\mathbf{s},3}}\Big)_4\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},1}}{\overline{\mathfrak{D}}_{\mathbf{s},2}}\Big)_4\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},1}}{\overline{\mathfrak{D}}_{\mathbf{s},3}}\Big)_4\Big\},$$

where the variables also satisfy the conditions (74). We also have the following lemma, analogous with (75)

Lemma 13. *For every $\epsilon > 0$ and for every integer $k \geq 0$ we have the equality*

$$S^{\diamond,\lambda}_{\text{odd}}(X,k) = \sum_{\mathbf{A}} S^{\diamond,\lambda}_{\text{odd}}(X,k,\mathbf{A}) + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big),$$

where the summation is over all the 4^{k+1}–tuples $(A_{\mathbf{r},i})_{(\mathbf{r},i)\in\mathcal{Q}^{k+1}}$ satisfying the inequality (76).

Proof. We briefly sketch the proof of this lemma. We easily modify the proof of [4, formula (98)] in order to write the equality

$$\frac{2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}}{2^{\omega(D)}}\sum_{abcd=D}\Big(\frac{a}{\overline{\mathfrak{c}}\mathfrak{d}}\Big)_4\Big(\frac{b}{\mathfrak{c}\overline{\mathfrak{d}}}\Big)_4 \tag{78}$$
$$= \frac{1}{2^k\cdot 2^{(k+1)\omega(D)}}\sum_{(D_{\mathbf{r}})}\sum_{\mathbf{d}}\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big(\frac{d_0}{\overline{\mathfrak{d}}_2\mathfrak{d}_3}\Big)_4\Big(\frac{d_1}{\mathfrak{d}_2\overline{\mathfrak{d}}_3}\Big)_4,$$

where the sum is over $(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^k}$ and $\mathbf{d} = (d_0,d_1,d_2,d_3)$ such that

$$D = \prod_{\mathbf{r}} D_{\mathbf{r}} = d_0d_1d_2d_3. \tag{79}$$

We follow the convention that $d_i = \mathfrak{d}_i\overline{\mathfrak{d}}_i$ is the privileged factorization of d_i. To parametrize the solutions to (79), we introduce $D_{\mathbf{r},i} = \text{g.c.d.}(D_{\mathbf{r}}, d_i)$ to write the equalities $D_{\mathbf{r}} = \prod_i D_{\mathbf{r},i}$ and $d_i = \prod_{\mathbf{r}} D_{\mathbf{r},i}$, under the constraint

$$\prod_{\mathbf{r}}\prod_i D_{\mathbf{r},i} = D.$$

Summing (78) over all the odd special $D \leq X$, decomposing the variables $D_{\mathbf{r}}$ and d_i in terms of $D_{\mathbf{r},i}$ and using the multiplicative properties of the characters, we finally arrive at the equality

(80)
$$S_{\mathrm{odd}}^{\diamond,\,\lambda}(X,k) = \frac{1}{2^k} \sum_{(D_{\mathbf{r},i})} \mu^2\big(\prod_{\mathbf{r},i} D_{\mathbf{r},i}\big) \Big(\prod_{\mathbf{r},i} 2^{-(k+1)\omega(D_{\mathbf{r},i})}\Big) \Big\{\prod_{\mathbf{r},i}\prod_{\mathbf{s},j} \Big(\frac{D_{\mathbf{r},i}}{D_{\mathbf{s},j}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\}$$
$$\times \Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},0}}{\overline{\mathfrak{D}}_{\mathbf{s},2}}\Big)_4\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},0}}{\mathfrak{D}_{\mathbf{s},3}}\Big)_4\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},1}}{\mathfrak{D}_{\mathbf{s},2}}\Big)_4\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},1}}{\overline{\mathfrak{D}}_{\mathbf{s},3}}\Big)_4\Big\},$$

where the variables of summation $D_{\mathbf{r},i}$ are taken in the set $\mathcal{D}_{\mathrm{odd}} \cup \{1\}$ and satisfy the inequality

$$\prod_{\mathbf{r}}\prod_{i} D_{\mathbf{r},i} \leq X.$$

To finish the proof of Lemma 13, it remains to introduce the parameters of dissection $A_{\mathbf{r},i}$, to split the sum $S_{\mathrm{odd}}^{\diamond,\,\lambda}(X,k)$ in the corresponding subsums $S_{\mathrm{odd}}^{\diamond,\,\lambda}(X,k,\mathbf{A})$ where the number of prime factors of the variables $D_{\mathbf{r},i}$ is bounded by Ω'. This technical preparation is similar to [4, §7.2, formula (61)], which also mimics [3, §5.4]. It gives birth to an error term in $O\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big)$.

□

5.7. **Oscillations of characters.** Now we recall two of the major analytic ingredients of [4]. The first one is the Siegel–Walfisz Theorem and its variations. As usual, for x a real number, a and q integers, let

$$\pi(x;q,a) := \sharp\,\big\{p \leq x\,;\, p \equiv a \bmod q\big\}.$$

Then we have

Lemma 14. *For every positive A there exists a constant $c_1(A) > 0$ such that for all coprime integers a and q with $q \geq 1$ we have the equality*

$$\pi(x;q,a) = \frac{1}{\phi(q)} \int_2^x \frac{\mathrm{d}t}{\log t} + O\Big(x \exp\big(-c_1(A)\sqrt{\log(2x)}\,\big)\Big),$$

for any real number $x \geq 2$ such that $1 \leq q \leq \log^A(2x)$. The constant implied in the O–symbol is absolute.

An easy consequence of Lemma 14 is (see [11, Corollary 5.29]):

Proposition 10. *For every $A > 0$ there exists a constant $c_2(A)$ such that the following inequality holds:*

(81)
$$\Big|\sum_{\substack{p\leq x\\ p\equiv 1 \bmod 4}} \chi(p)\Big| \leq c_2(A)\, x\, q^{\frac{1}{2}}\, \log^{-A}(2x)$$

for every $x \geq 1$, for every odd integer $q \geq 3$, and for every non principal character χ modulo q.

Similarly, we have the inequalities

$$\left.\begin{array}{r} \Big| \displaystyle\sum_{\substack{p\le x\\ p\equiv 1 \bmod 4}} \left(\frac{2}{p}\right) \chi(p) \Big| \\ \Big| \displaystyle\sum_{\substack{p\le x\\ p\equiv 1 \bmod 4}} \chi(p)\ [cp,2]_4 \Big| \\ \Big| \displaystyle\sum_{\substack{p\le x\\ p\equiv 1 \bmod 4}} \left(\frac{2}{p}\right) \chi(p)\ [cp,2]_4 \Big| \end{array}\right\} \le c_2(A)\, x\, q^{\frac12} \log^{-A}(2x), \tag{82}$$

for every $x \ge 1$, for every odd integer $q \ge 1$, for every character principal or not modulo q, and for every integer c.

This upper bound is valuable only for q less than a fixed power of $\log x$. We shall need an extension of Lemma 14 and Proposition 10 to the set $\mathfrak{P}$ of privileged primes. We introduce the following notation

$$\pi_{\mathrm{priv}}(x; w, a) := \sharp \left\{\pi \in \mathfrak{P} \ : \ \mathcal{N}(\pi) \le x,\ \pi \equiv a \bmod w\right\},$$

with x a real positive number, $\mathcal{N}$ is now the norm in $\mathbb{Z}[i]$, a and w belong to $\mathbb{Z}[i]$, and $\phi(w)$ will be the generalized Euler function, that means the number of invertible elements of $\mathbb{Z}[i]/(w\mathbb{Z}[i])$. By classical methods of analytic number theory we have (see [4, Lemma 32], for instance):

Lemma 15. *Let a and $w \ne 0$ be two elements of $\mathbb{Z}[i]$ with $(a, w) = 1$. If the congruences $z \equiv a \bmod w$ and $z \equiv 1 \bmod 2(1+i)$ are not compatible, then we have*

$$\pi_{\mathrm{priv}}(x; w, a) = 0.$$

Otherwise, these two congruences are equivalent to a unique congruence $z \equiv a' \bmod w'$, where $w' = \mathrm{lcm}(w, 2(1+i))$. Furthermore for every $A > 0$ there exists a positive constant $c_3(A)$ such that the following equality holds

$$\pi_{\mathrm{priv}}(x; w, a) = \frac{2}{\phi(w')} \int_2^x \frac{\mathrm{d}t}{\log t} + O\Big(x \exp\big(-c_3(A)\sqrt{\log(2x)}\,\big)\Big),$$

for every $x \ge 2$, uniformly for a and w as above and satisfying the inequality $1 \le \mathcal{N}(w) \le \log^A(2x)$. The constant implied in the O–symbol is absolute.

A classical application of Lemma 15 concerns the sum of characters.

Proposition 11. *For every $A > 0$ there exists a constant $c_4(A) > 0$ such that the following inequality holds*

$$\Big| \sum_{\substack{\pi\in\mathfrak{P}\\ \mathcal{N}(\pi)\le x}} \chi(\pi) \Big| \le c_4(A)\, x\, \sqrt{\mathcal{N}(w)} \log^{-A}(2x).$$

for every $x \ge 2$, for every odd $w \in \mathbb{Z}[i]$ and for every χ non principal character (over $\mathbb{Z}[i]$) modulo w.

In particular, we have the inequality

$$\Big| \sum_{\substack{\pi\in\mathfrak{P}\\ \mathcal{N}(\pi)\le x}} \left(\frac{\pi}{w}\right)_4 \Big| \le c_4(A)\, x\, \sqrt{\mathcal{N}(w)} \log^{-A}(2x), \tag{83}$$

for every $x \geq 2$ and for every non unit element $w \in \mathbb{Z}[i]$ which is product of elements of $\mathfrak{P} \cup \overline{\mathfrak{P}}$ to a power ≤ 3. We also have

$$\left.\begin{array}{l} \Big| \displaystyle\sum_{\substack{\pi \in \mathfrak{P} \\ \mathcal{N}(\pi) \leq x}} \Big(\frac{2}{\pi\overline{\pi}}\Big)\Big(\frac{\pi}{w}\Big)_4 \Big| \\ \Big| \displaystyle\sum_{\substack{\pi \in \mathfrak{P} \\ \mathcal{N}(\pi) \leq x}} \Big(\frac{2}{\pi}\Big)_4\Big(\frac{\pi}{w}\Big)_4 \Big| \\ \Big| \displaystyle\sum_{\substack{\pi \in \mathfrak{P} \\ \mathcal{N}(\pi) \leq x}} \Big(\frac{2}{\overline{\pi}}\Big)_4\Big(\frac{\pi}{w}\Big)_4 \Big| \end{array}\right\} \leq c_4(A)\, x\, \sqrt{\mathcal{N}(w)}\, \log^{-A}(2x), \tag{84}$$

for every integer a and for every element $w \in \mathbb{Z}[i]$ which is product of elements of $\mathfrak{P} \cup \overline{\mathfrak{P}}$ to a power ≤ 3.

Proof. It is similar to the proof of [4, Prop. 7]. Note that in (83) and (84), w is necessarily odd and that we may have $w = 1$ in (84). □

Now we give results on double oscillation of characters. The archetype problem is the following one: let M and N be large real numbers, $\boldsymbol{\alpha} = (\alpha_m)$ and $\boldsymbol{\beta} = (\beta_n)$ be two sequences of complex numbers of moduli less than one, depending on the integers m and n and let

$$\Xi_1(M, N, \boldsymbol{\alpha}, \boldsymbol{\beta}) := \sum_{m \leq M} \sum_{n \leq N} \alpha_m\, \beta_n\, \mu^2(2m)\, \mu^2(2n) \Big(\frac{m}{n}\Big).$$

This sum of Jacobi symbols contains $\asymp MN$ terms of modulus ≤ 1, but, due to the oscillations of the Jacobi symbols, it is now well known that this sum satisfies $\Xi_1 = o(MN)$ as soon as both M and N go to infinity. Such a statement appears several times in the literature and has many applications (for instance [9], [12], [7], [3], [4, Lemma 32],...) For a deep study of Ξ_1, see [8]. In this paper we only use:

Proposition 12. *For every positive A there exists a constant $K = K(A)$ such that the inequality*

$$|\, \Xi_1(M, N, \boldsymbol{\alpha}, \boldsymbol{\beta})| \leq K \cdot MN \log^{-\frac{A}{2}} MN$$

holds uniformly for M and $N \geq \max\big(2, \log^A MN\big)$ and for sequences $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ such that $\|\boldsymbol{\alpha}\|_\infty$ and $\|\boldsymbol{\beta}\|_\infty \leq 1$.

Proof. We split Ξ_1 into four subsums, where the variables m and n satisfy one of the congruence conditions $\pm 1 \mod 4$. Eventually using the quadratic reciprocity law, each of this sum has the shape

$$\widetilde{\Xi}_1(M, N, \tilde{\boldsymbol{\alpha}}, \tilde{\boldsymbol{\beta}}) := \sum_{m \leq M} \sum_{n \leq N} \tilde{\alpha}_m\, \tilde{\beta}_n\, \mu^2(2m)\, \mu^2(2n) \Big(\frac{m}{n}\Big),$$

where $\|\tilde{\boldsymbol{\alpha}}\|_\infty$ and $\|\tilde{\boldsymbol{\beta}}\|_\infty \leq 1$, and where M and N now satisfy the inequality $\max(2, \log^A MN) \leq N \leq M$. By Cauchy–Schwarz inequality and by [12, Lemma

3], for instance, we have

$$\begin{aligned}\bigl|\,\widetilde{\Xi}_1(M,N,\tilde{\boldsymbol{\alpha}},\tilde{\boldsymbol{\beta}})\,\bigr| &\leq M^{\frac12}\Bigl\{\sum_{m\leq M}\mu^2(2m)\Bigl|\sum_{n\leq N}\mu^2(2n)\tilde{\beta}_n\Bigl(\frac{n}{m}\Bigr)\Bigr|^2\Bigr\}^{\frac12}\\ &\ll M^{\frac12}\bigl\{MN+M^{\frac12}N^2\log^6 N\bigr\}^{\frac12}\\ &\ll MN\bigl(N^{-\frac12}+(MN)^{-\frac18}\log^3 MN\bigr).\end{aligned}$$

□

Such a phenomenon of double oscillations is not special to the Jacobi symbol. For instance in [4, §6.2], we define the sum

$$\Xi_2(M,N,\boldsymbol{\alpha},\boldsymbol{\beta}) := \sum_{\mathcal{N}(m)\leq M}{}^{\dagger}\ \sum_{\mathcal{N}(n)\leq N}{}^{\dagger}\ \alpha_m\,\beta_n\,\mu^2(2m)\,\mu^2(2n)\,\Bigl(\frac{m}{n}\Bigr)_4^2,$$

where now, the summations are over the Gaussian integers m and n, where † means that we are summing over primary elements, and where μ is the natural generalization of the Möbius function to the Gaussian integers. The number of terms in Ξ_2 is also in $\asymp MN$ and we proved in [4, Proposition 9]:

Proposition 13. *Suppose that the sequences $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ satisfy the inequalities $\|\boldsymbol{\alpha}\|_\infty$ and $\|\boldsymbol{\beta}\|_\infty\leq 1$. Then for every positive ϵ we have*

$$\begin{aligned}\Xi_2(M,N,\boldsymbol{\alpha},\boldsymbol{\beta}) \ll_\epsilon MN\min\bigl\{&N^{-\frac12}+M^{-\frac14}N^{\frac12}, M^{-\frac12}+M^{\frac12}N^{-\frac14},\\ &M^{\epsilon}(N^{-\frac18}+M^{-\frac14}N^{\frac18}), N^{\epsilon}(M^{-\frac18}+M^{\frac18}N^{-\frac14})\bigr\}.\end{aligned}$$

In §5.9 and 5.11, we shall meet the following sum

$$\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta}) := \sum_{\substack{m\leq M\\ m \text{ primary}}}\ \sum_{\mathcal{N}(n)\leq N}{}^{\ddagger}\ \alpha_m\,\beta_n\,\mu^2(2m)\,\mu^2(2n)\,\Bigl(\frac{m}{n}\Bigr)_4, \tag{85}$$

where the ‡–symbol means that we are summing over Gaussian integers n, which are product of distinct elements of $\mathfrak{P}\cup\overline{\mathfrak{P}}$. The conditions of summation imply that m is a positive integer $\equiv 1 \bmod 4$ and n is a primary Gaussian integer. The sum Ξ_3 is similar to Ξ_1 and Ξ_2 with the difference that the variables of summation m and n are now of different nature (the former is a rational positive integer, the latter is a Gaussian integer). The sum Ξ_3 also contains $\asymp MN/\sqrt{\log N}$ terms and the assumption that m is supposed to be primary is harmless. However, since m and n are primary and since m is an odd integer (hence $\mathcal{N}(m)\equiv 1 \bmod 8$), the quartic reciprocity law (see §5.3) allows us to write Ξ_3 in the form

$$\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta}) := \sum_{\substack{m\leq M\\ m \text{ primary}}}\ \sum_{\mathcal{N}(n)\leq N}{}^{\ddagger}\ \alpha_m\,\beta_n\,\mu^2(2m)\,\mu^2(2n)\,\Bigl(\frac{n}{m}\Bigr)_4. \tag{86}$$

The sum Ξ_3 also has the property of double oscillation since we shall prove an analog of Proposition 13:

Proposition 14. *Suppose that the sequences $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ satisfy the inequalities $\|\boldsymbol{\alpha}\|_\infty$ and $\|\boldsymbol{\beta}\|_\infty\leq 1$. Then for every positive ϵ we have*

$$\begin{aligned}\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta}) \ll_\epsilon MN\min\bigl\{&N^{-\frac12}+(M/N)^{-\frac12}\log^{\frac12}N\,;\\ &M^{-\frac1{16}}N^{\epsilon}+M^{\frac18}N^{-\frac14+\epsilon}\,; M^{-\frac12}+MN^{-\frac14}\bigr\}\end{aligned} \tag{87}$$

uniformly for M and $N\geq 2$.

Proof. Since we only want a non trivial upper bound for Ξ_3 when M and $N \geq (\log MN)^A$, we shall use very simple tools from analytic number theory in order to adopt two points of view about the character $\left(\frac{m}{n}\right)_4$, as a function of m or as a function of n. These tools can be seen as transpositions of the tools appearing in the proofs of Propositions 12 & 13. Actually, it is possible to appeal to more advanced tools, to obtain better bounds for Ξ_3, for instance Burgess' bound for short sums of Dirichlet characters, or the functional equation of the L–function $L(s, \psi_{m_1,m_2})$, where ψ_{m_1,m_2} is the character over $\mathbb{Z}[i]$ defined in (93) below.

By the Cauchy–Schwarz inequality applied to (85), we have

$$\begin{aligned}\bigl|\,\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\bigr|^2 &\leq M \sum_{m\leq M} \Bigl|\sideset{}{^\ddagger}\sum_{\mathcal{N}(n)\leq N} \beta_n\,\mu^2(2n)\left(\frac{m}{n}\right)_4\Bigr|^2 \\ &\leq M \sideset{}{^\ddagger}\sum_{\mathcal{N}(n_1)\leq N} \mu^2(2n_1) \sideset{}{^\ddagger}\sum_{\mathcal{N}(n_2)\leq N} \mu^2(2n_2)\Bigl|\sum_{m\leq M}\left(\frac{m}{n_1\overline{n}_2}\right)_4\Bigr|. \qquad (88)\end{aligned}$$

Since n_1 and n_2 are products of distinct elements of $\mathfrak{P}\cup\overline{\mathfrak{P}}$, the character over $\mathbb{Z}$, $m\mapsto \left(\frac{m}{n_1\overline{n}_2}\right)_4$ is principal if and only if $n_1 = n_2$. If $n_1 \neq n_2$, this character has modulus $\leq N^2$, and we apply the famous Polya–Vinogradov inequality (see [11, Theorem 12.5]). Hence we deduce from (88) the inequality

$$(89)\qquad \bigl|\,\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\bigr|^2 \ll M\bigl\{MN + N^2\,(\sqrt{N^2}\log N)\bigr\} \ll M^2N + MN^3\log N.$$

This gives the first term inside the min–term in (87). But this term has no interest when M is small compared to N. We shall cope with this drawback by the second term.

We adopt another technique to enlarge the summation over n. We apply Hölder's inequality to (86), with the coefficients $\frac{7}{8}+\frac{1}{8}=1$. This gives

$$(90)\qquad \bigl|\,\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\bigr|^8 \leq M^7\Bigl\{\sum_{m\leq M}\mu^2(2m)\Bigl|\sideset{}{^\ddagger}\sum_{\mathcal{N}(n)\leq N}\beta_n\,\mu^2(2n)\left(\frac{n}{m}\right)_4\Bigr|^8\Bigr\}.$$

Expanding the 8-th power and noticing that the number of solutions in $\mathbb{Z}[i]$ of the equation

$$n = n_1n_2n_3n_4\overline{n}_5\overline{n}_6\overline{n}_7\overline{n}_8$$

is in $O(\mathcal{N}(n)^\epsilon)$, for every $\epsilon > 0$, we deduce from (90) the inequality

$$(91)\qquad \bigl|\,\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\bigr|^8 \ll M^7\,N^\epsilon\Bigl\{\sum_{\mathcal{N}(n)\leq N^8}\Bigl|\sum_{m\leq M}\mu^2(2m)\left(\frac{n}{m}\right)_4\Bigr|\Bigr\}.$$

Now we apply Cauchy–Schwarz inequality to the sum in n and invert summation to write

$$\begin{aligned}&\bigl|\,\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\bigr|^{16} \\ &\ll M^{14}\,N^{8+2\epsilon}\Bigl\{\sum_{m_1\leq M}\sum_{m_2\leq M}\mu^2(2m_1)\mu^2(2m_2)\Bigl|\sum_{\mathcal{N}(n)\leq N^8}\psi_{m_1,m_2}(n)\Bigr|\Bigr\}, \qquad (92)\end{aligned}$$

where ψ_{m_1,m_2} is the character over $\mathbb{Z}[i]$ defined by:

$$(93)\qquad n\mapsto\psi_{m_1,m_2}(n) := \left(\frac{n}{m_1}\right)_4\overline{\left(\frac{n}{m_2}\right)_4} = \left(\frac{n}{m_1m_2^3}\right)_4.$$

Since m_1 and m_2 are squarefree, ψ_{m_1,m_2} is principal if and only if $m_1 = m_2$. In the other cases, we apply the rather simple lemma about lattices in euclidean plane (see [4, Lemma 35] for instance).

Lemma 16. *Let $a \neq 0$ and ζ be elements of $\mathbb{Z}[i]$. Then the number of $n \in \mathbb{Z}[i]$ satisfying $\mathcal{N}(n) \leq N$ and $n \equiv \zeta \mod a$ is equal to*

$$\pi \frac{N}{\mathcal{N}(a)} + O\Big(\sqrt{\frac{N}{\mathcal{N}(a)}} + 1\Big),$$

uniformly for $N > 0$, a and ζ as above.

We apply this lemma with $a = m_1 m_2$, for any $\zeta \bmod m_1 m_2$ to the inner sum over n in the right part of (92). The main term disappear, since the character ψ_{m_1,m_2} is not principal. Summing the error terms, we find that

$$\begin{aligned} \big|\,\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\big|^{16} &\ll M^{14}\, N^{8+2\epsilon}\Big\{MN^8 + M^2 \cdot M^4\big(\sqrt{N^8/M^4}+1\big)\Big\} \\ &\ll M^{14}\, N^{8+2\epsilon}\Big\{MN^8 + M^4N^4 + M^6\Big\} \\ &\ll M^{15}N^{16+2\epsilon} + M^{18}N^{12+2\epsilon}, \end{aligned} \tag{94}$$

since this bound is trivial for $M \geq N^2$. This gives the second part in the min–term in (87), but this term does not cover the case when the term M tends to ∞, but slower than any power of N. In order to solve this case we have to avoid the divisor function. This is the purpose of the third term.

By the Cauchy–Schwarz inequality applied to (86) we deduce

$$\begin{aligned} \big|\,\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\big|^2 &\ll N\Big\{\sum_{\mathcal{N}(n)\leq N}\Big|\sum_{m\leq M}\alpha_m\mu^2(2m)\Big(\frac{n}{m}\Big)_4\Big|^2\Big\} \\ &\ll N\Big\{\sum_{m_1\leq M}\ \sum_{m_2\leq M}\mu^2(2m_1)\mu^2(2m_2)\Big|\sum_{\mathcal{N}(n)\leq N}\psi_{m_1,m_2}(n)\Big|\Big\}. \end{aligned} \tag{95}$$

We appeal to Lemma 16 to treat the second part of (95) as we did for (94). It gives

$$\big|\,\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\big|^2 \ll N\Big\{MN + M^2\cdot M^4\big(\sqrt{N/M^4}+1\big)\Big\} \ll MN^2 + M^4N^{\frac{3}{2}} + M^6N,$$

and finally

$$\big|\,\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\big|^2 \ll MN^2 + M^4N^{\frac{3}{2}},$$

since this bound is trivial for $M \geq N^{\frac{1}{4}}$. This gives the third term in (87). The proof of Proposition 14 is now complete . □

Proposition 14 easily implies this more practicable form

Proposition 15. *For every positive A there exists a constant $K = K(A)$ such that the inequality*

$$\big|\,\Xi_3(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\big| \leq K \cdot MN\, \log^{-\frac{A}{2}}(MN),$$

holds uniformly for M and $N \geq \max\big(2, \log^A(MN)\big)$ and for sequences $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ such that $\|\boldsymbol{\alpha}\|_\infty$ and $\|\boldsymbol{\beta}\|_\infty \leq 1$.

5.8. **Discussion on the order of magnitude of the $A_{\mathbf{r},i}$.** The purpose of the following subsections is to prove the following lemma.

Lemma 17. *Uniformly for $X \geq 2$ we have the equality*
$$\sum_{\mathbf{A}} \bigl| S^{\diamond,\,\lambda}_{\text{odd}}(X,k,\mathbf{A}) \bigr| = O(X(\log X)^{-1}),$$
where the sum is over the $\mathbf{A}$ such that (76) is satisfied and such that
$$\max\{A_{\mathbf{r},0}, A_{\mathbf{r},1}\,;\mathbf{r}\in\mathcal{Q}^k\} > 1 \text{ and } \max\{A_{\mathbf{r},2}, A_{\mathbf{r},3}\,;\mathbf{r}\in\mathcal{Q}^k\} > 1. \tag{96}$$

This proof is rather long and it largely mimics the proof of [4, Lemma 46]. We denote by Σ_1 the sum studied in Lemma 17. First of all, we remark that the number of the 4^{k+1}–tuples $\mathbf{A}$ satisfying (76) is
$$\ll (\log X)^{4^{k+1}(1+2^{k+1})}. \tag{97}$$
We also remark that we can restrict to study the contribution to Σ_1 of the $\mathbf{A}$ such that
$$\prod_{\mathbf{r},i} A_{\mathbf{r},i} \geq X^{\frac{1}{2}}, \tag{98}$$
since the contribution to Σ_1 of the other ones is trivially $O_\epsilon(X^{\frac{1}{2}+\epsilon})$ for every $\epsilon > 0$.

Let $\mathbf{A}$ be given satisfying the inequalities (76), (96) and (98). Our purpose is to prove that we have for such an $\mathbf{A}$:
$$S^{\diamond,\,\lambda}_{\text{odd}}(X,k,\mathbf{A}) \ll X(\log X)^{-1-4^{k+1}(1+2^{k+1})}. \tag{99}$$
This inequality combined with (97) proves Lemma 17.

The restriction (98) implies that, among the $D_{\mathbf{r},i}$, there is at least one large variable, which means that the largest $A_{\mathbf{r},i}$ is greater or equal to $X^{\frac{1}{2\cdot 4^{k+1}}}$. Let us denote by $(\mathbf{u}_0, i_0)$ the corresponding index to this largest $A_{\mathbf{r},i}$. Hence we have
$$A_{\mathbf{u}_0,i_0} \geq X^{\frac{1}{2\cdot 4^{k+1}}}. \tag{100}$$
Obviously, i_0 may take the four values 0, 1, 2 or 3. But due to the unsymmetrical structure of the product of quartic symbols in (77), these four cases cannot be treated in an analogous manner (this was not the case for (73) which was dealt in [4]). However the cases $i_0 = 0$ and $i_1 = 1$ are similar, eventually after taking the conjugate of the corresponding expression. The same remark also applies to the cases $i_0 = 2$ and $i_0 = 3$. Hence we shall restrict to the cases $i_0 = 0$ and $i_0 = 2$.

We recall the following definition of *linked indices*, introduced by Heath–Brown [7] in a slightly different context, and deeply used in [3] and in [4, Definition 4].

Definition 6. *Let $k \geq 0$ be an integer. Two indices $\mathbf{r}$ and $\mathbf{s} \in \mathcal{Q}^k$ are linked if they satisfy the equality*
$$\kappa_k(\mathbf{r},\mathbf{s}) + \kappa_k(\mathbf{s},\mathbf{r}) \equiv 1 \bmod 2.$$
They are unlinked, when
$$\kappa_k(\mathbf{r},\mathbf{s}) + \kappa_k(\mathbf{s},\mathbf{r}) \equiv 0 \bmod 2.$$

Similarly, we extend this definition to the orders of magnitude $A_{\mathbf{r},i}$ and $A_{\mathbf{s},j}$ and to the variables $D_{\mathbf{r},i}$ and $D_{\mathbf{s},j}$, by saying that they are *linked*, if the indices $\mathbf{r}$ and $\mathbf{s}$ are linked. Note that in the case $k = 0$, the two variables $D_{\mathbf{r},i}$ and $D_{\mathbf{s},j}$ are always unlinked. Also note that this definition of being linked is independent of the values of i and j and it simply says that in the right parts of the equalities (73), (77) and (80), after reduction and simplification of the exponents modulo 2, exactly one of the symbols $\left(\frac{D_{\mathbf{r},i}}{D_{\mathbf{s},j}}\right)$ or $\left(\frac{D_{\mathbf{s},j}}{D_{\mathbf{r},i}}\right)$ is really present, for each fixed value of i and j in $\mathcal{Q}$. Recall that, by the quadratic reciprocity law, we have the equality $\left(\frac{D_{\mathbf{r},i}}{D_{\mathbf{s},j}}\right) = \left(\frac{D_{\mathbf{s},j}}{D_{\mathbf{r},i}}\right)$.

Now we enter into the discussion on the value of i_0 and on the values of the index $\mathbf{s}$ linked with $\mathbf{u}_0$.

5.9. **Case** $i_0 = 0$**.** Actually, as said above, this proof will also work if $i_0 = 1$, with obvious tiny modifications. We shall discuss on the way to apply either Proposition 10, 11, 12, or 15 to deduce that, for such an $\mathbf{A}$, the equality (99) is satisfied.

5.9.1. *There is an* $\mathbf{s}_0$*, unlinked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{s}_0,2} \geq (\log X)^{100\cdot 10^k}$. We want to benefit from the oscillations of the symbol $\left(\frac{D_{\mathbf{u}_0,0}}{\overline{\mathfrak{D}}_{\mathbf{s}_0,2}}\right)_4$ in the right part of the definition (77). Since $\{\mathbf{u}_0, \mathbf{s}_0\}$ is unlinked, we know that there is no Jacobi symbol $\left(\frac{D_{\mathbf{u}_0,0}}{D_{\mathbf{s}_0,2}}\right)$ or $\left(\frac{D_{\mathbf{s}_0,2}}{D_{\mathbf{u}_0,0}}\right)$ in (77), after reduction of the exponents modulo 2. Hence, by appealing to the multiplicative properties of the symbol $\left(\frac{\cdot}{\cdot}\right)_4$, we deduce the inequality

$$(101) \qquad S^{\diamond,\lambda}_{\mathrm{odd}}(X,k,\mathbf{A}) \leq \Big(\prod_{\substack{(\mathbf{r},i) \\ \neq(\mathbf{u}_0,0),\,(\mathbf{s}_0,2)}} A_{\mathbf{r},i} \Big) \cdot \big| \, \Xi_3(\Delta A_{\mathbf{u}_0,0}, \Delta A_{\mathbf{s}_0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \, \big|,$$

where Ξ_3 is defined in (85), for some sequences $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, with $\|\cdot\|_\infty \leq 1$. A direct application of Proposition 15 gives the inequality

$$(102) \qquad \big| \, \Xi_3(\Delta A_{\mathbf{u}_0,0}, \Delta A_{\mathbf{s}_0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \, \big| \ll A_{\mathbf{u}_0,0} A_{\mathbf{s}_0,2} (\log X)^{-50\cdot 10^k}.$$

The inequalities (76), (101) and (102) imply (99) for any $\mathbf{A}$ falling in that case.

5.9.2. *There is an* $\mathbf{s}_0$*, linked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{s}_0,2} \geq (\log X)^{100\cdot 10^k}$. In that case, we know that in (77), the Jacobi symbol $\left(\frac{D_{\mathbf{u}_0,0}}{D_{\mathbf{s}_0,2}}\right) = \left(\frac{D_{\mathbf{s}_0,2}}{D_{\mathbf{u}_0,0}}\right)$ appears once and only once after reduction of the exponents modulo 2. From the equality

$$(103) \qquad \left(\frac{a}{p}\right) = \left(\frac{a}{\pi}\right)_4^2 = \left(\frac{a}{\overline{\pi}}\right)_4^2$$

between the Legendre symbol modulo $p = \pi\overline{\pi}$ and the quartic residue symbol (see §5.3), we deduce the equality

$$\left(\frac{D_{\mathbf{u}_0,0}}{D_{\mathbf{s}_0,2}}\right)\left(\frac{D_{\mathbf{u}_0,0}}{\overline{\mathfrak{D}}_{\mathbf{s}_0,2}}\right)_4 = \left(\frac{D_{\mathbf{u}_0,0}}{\overline{\mathfrak{D}}_{\mathbf{s}_0,2}}\right)_4^2 \cdot \left(\frac{D_{\mathbf{u}_0,0}}{\overline{\mathfrak{D}}_{\mathbf{s}_0,2}}\right)_4 = \overline{\left(\frac{D_{\mathbf{u}_0,0}}{\overline{\mathfrak{D}}_{\mathbf{s}_0,2}}\right)_4} = \left(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{D}_{\mathbf{s}_0,2}}\right)_4.$$

Hence, we are led to a study similar to §5.9.1.

5.9.3. *There is an* $\mathbf{s}_0$*, unlinked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{s}_0,3} \geq (\log X)^{100\cdot 10^k}$. The study is similar to the study of §5.9.1 by considering the double oscillations of the character $\left(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{D}_{\mathbf{s}_0,3}}\right)_4$.

5.9.4. *There is an* $\mathbf{s}_0$*, linked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{s}_0,3} \geq (\log X)^{100\cdot 10^k}$. This case is similar to §5.9.2, but here we use the equality

$$\Big(\frac{D_{\mathbf{u}_0,0}}{D_{\mathbf{s}_0,3}}\Big)\Big(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{D}_{\mathbf{s}_0,3}}\Big)_4 = \Big(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{D}_{\mathbf{s}_0,3}}\Big)_4^2 \cdot \Big(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{D}_{\mathbf{s}_0,3}}\Big)_4 = \overline{\Big(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{D}_{\mathbf{s}_0,3}}\Big)_4}.$$

After the discussions made in §5.9.1,...,§5.9.4 and by the assumption (96), we are now led to suppose that, in the cases $i_0 = 0$ or 1, the following inequality holds

$$1 < \max_{\mathbf{s}\in\mathcal{Q}^k}\big(A_{\mathbf{s},2},\, A_{\mathbf{s},3}\big) < (\log X)^{100\cdot 10^k}. \tag{104}$$

Now we discuss on the order of magnitude of the $A_{\mathbf{s},0}$ and $A_{\mathbf{s},1}$ such that $\{\mathbf{s}, \mathbf{u}_0\}$ are linked.

5.9.5. *There is an index* $\mathbf{s}_0$ *linked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{s}_0,0} \geq (\log X)^{100\cdot 10^k}$. This means that (77) really contains the Jacobi symbol $\Big(\frac{D_{\mathbf{u}_0,0}}{D_{\mathbf{s}_0,0}}\Big) = \Big(\frac{D_{\mathbf{s}_0,0}}{D_{\mathbf{u}_0,0}}\Big)$. No quartic symbol contains the pair of variables $\{\mathfrak{D}_{\mathbf{s}_0,0},\, D_{\mathbf{u}_0,0}\}$. Hence we appeal to Proposition 12 (double oscillations of the Jacobi symbol), since we can write, for some $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, with their norm $\|\cdot\|_\infty$ less than 1

$$|S^{\diamond,\,\lambda}_{\rm odd}(X, k, \mathbf{A})| \leq \Big(\prod_{\substack{(\mathbf{r},i)\\ \neq(\mathbf{u}_0,0),\,(\mathbf{s}_0,0)}} A_{\mathbf{r},i}\Big)\cdot \big|\,\Xi_1(\Delta A_{\mathbf{u}_0,0}, \Delta A_{\mathbf{s}_0,0}, \boldsymbol{\alpha}, \boldsymbol{\beta})\,\big|, \tag{105}$$

and deduce the inequality

$$\big|\,\Xi_1(\Delta A_{\mathbf{u}_0,0}, \Delta A_{\mathbf{s}_0,0}, \boldsymbol{\alpha}, \boldsymbol{\beta})\,\big| \ll A_{\mathbf{u}_0,0}\, A_{\mathbf{s}_0,0}\, (\log X)^{-50\cdot 10^k}. \tag{106}$$

Putting (105) and (106) together, we deduce (99) for each $\mathbf{A}$ falling in this case.

5.9.6. *There is an index* $\mathbf{s}_0$ *linked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{s}_0,1} \geq (\log X)^{100\cdot 10^k}$. We operate as in §5.9.5, but we use the character $\Big(\frac{D_{\mathbf{u}_0,0}}{D_{\mathbf{s}_0,1}}\Big)$.

In conclusion, after the discussions made in §5.9.5 & 5.9.6, we can now suppose

$$\mathbf{s} \text{ linked with } \mathbf{u}_0 \Rightarrow \max\big(A_{\mathbf{s},0},\, A_{\mathbf{s},1}\big) < (\log X)^{100\cdot 10^k}. \tag{107}$$

5.10. **Use of the classical Siegel–Walfisz Theorem.** With the restrictions (104) and (107), we are left with the case where $D_{\mathbf{u}_0,0}$ (large variable) appears in Jacobi symbols and quartic symbols where the other variables are small, which means $\leq (\log X)^{100\cdot 10^k}$. And, by the assumption (104), at least one of the variables appearing in the denominators of the quartic symbols in the right part of (77) is larger than 1. To summarize this, after using the multiplicative properties, we see that $D_{\mathbf{u}_0,0}$ appears in five types of oscillating characters

$$\Big(\frac{D_{\mathbf{u}_0,0}}{\ell}\Big),\ \Big(\frac{D_{\mathbf{u}_0,0}}{a}\Big)\Big(\frac{D_{\mathbf{u}_0,0}}{\overline{\mathfrak{a}}}\Big)_4,\ \Big(\frac{D_{\mathbf{u}_0,0}}{\overline{\mathfrak{c}}}\Big)_4,\ \Big(\frac{D_{\mathbf{u}_0,0}}{b}\Big)\Big(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{b}}\Big)_4 \text{ and } \Big(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{d}}\Big)_4, \tag{108}$$

where

$$\ell = \prod_{\substack{\mathbf{s}\text{ linked}\\ \text{with } \mathbf{u}_0}} \big(D_{\mathbf{s},0} D_{\mathbf{s},1}\big),\ a = \prod_{\substack{\mathbf{s}\text{ linked}\\ \text{with } \mathbf{u}_0}} D_{\mathbf{s},2},$$

$$b = \prod_{\substack{\mathbf{s}\text{ linked}\\ \text{with } \mathbf{u}_0}} D_{\mathbf{s},3},\ c = \prod_{\substack{\mathbf{s}\text{ unlinked}\\ \text{with } \mathbf{u}_0}} D_{\mathbf{s},2},\ \text{and } d = \prod_{\substack{\mathbf{s}\text{ unlinked}\\ \text{with } \mathbf{u}_0}} D_{\mathbf{s},3}.$$

As usual, $a=\mathfrak{a}\bar{\mathfrak{a}}$, $b=\mathfrak{b}\bar{\mathfrak{b}}$, $c=\mathfrak{c}\bar{\mathfrak{c}}$ and $d=\mathfrak{d}\bar{\mathfrak{d}}$ are the privileged factorizations of the integers a, b, c and d. Finally, the five integers a, b, c, d and ℓ are all coprime and belong to $\mathcal{D}_{\text{odd}}\cup\{1\}$. As a consequence of the above discussion, concerning the orders of magnitude, we have

$$abcd>1 \text{ and } abcd\ell\leq(\log X)^{400\cdot 40^k}. \tag{109}$$

Using (103) and the multiplicative properties of the Jacobi symbol and of the quartic symbol, the product of the five symbols in (108) is gathered in one quartic symbol

$$\Bigl(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{a}\,\bar{\mathfrak{b}}\,\bar{\mathfrak{c}}\,\mathfrak{d}\,\mathfrak{l}^2}\Bigr)_4,$$

with $\ell=\mathfrak{l}\bar{\mathfrak{l}}$ is the privileged factorization. Hence we have the inequality

$$|S_{\text{odd}}^{\diamond,\lambda}(X,k,\mathbf{A})|\leq\sum_{\substack{(D_{\mathbf{r},i})\\(\mathbf{r},i)\neq(\mathbf{u}_0,0)}}\Bigl|\sum_{D_{\mathbf{u}_0,0}}\mu^2\bigl(\prod_{\mathbf{r},i}D_{\mathbf{r},i}\bigr)\,2^{-k\,\omega(D_{\mathbf{u}_0,0})}\Bigl(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{a}\,\bar{\mathfrak{b}}\,\bar{\mathfrak{c}}\,\mathfrak{d}\,\mathfrak{l}^2}\Bigr)_4\Bigr|, \tag{110}$$

where the variables of summation satisfy

$$A_{\mathbf{r},i}\leq D_{\mathbf{r},i}<\Delta A_{\mathbf{r},i},\, D_{\mathbf{r},i}\in\mathcal{D}_{\text{odd}},\,\omega(D_{\mathbf{r},i})\leq\Omega', \tag{111}$$

and where the variables a, b, c, d and ℓ are defined as above. Note that the Dirichlet character $n\mapsto\Bigl(\frac{n}{\mathfrak{a}\,\bar{\mathfrak{b}}\,\bar{\mathfrak{c}}\,\mathfrak{d}\,\mathfrak{l}^2}\Bigr)_4$ is not principal since the integers a, b, c, d and ℓ are squarefree, coprime and satisfy $abcd>1$. The modulus of this character is odd and is less than $(\log X)^{B_k}$ by (109), where B_k is a constant depending only on k. We shall apply Proposition 10 (Siegel–Walfisz Theorem) to the largest prime factor of $D_{\mathbf{u}_0,0}$, as it has been done in [4, §7.5]. We write

(112)
$$|S_{\text{odd}}^{\diamond,\lambda}(X,k,\mathbf{A})|\ll\Bigl(\prod_{(\mathbf{r},i)\neq(\mathbf{u}_0,0)}A_{\mathbf{r},i}\Bigr)\cdot\max_{m,\,\chi}\Bigl|\sum_{\substack{A_{\mathbf{u}_0,0}\leq D_{\mathbf{u}_0,0}<\Delta A_{\mathbf{u}_0,0}\\(D_{\mathbf{u}_0,0},m)=1}}2^{-k\,\omega(D_{\mathbf{u}_0,0})}\chi(D_{\mathbf{u}_0,0})\Bigr|,$$

where

- the maximum is taken over the integers m satisfying $1\leq m\leq X$ and over the non principal characters χ with an odd modulus $\leq(\log X)^{B_k}$,
- $D_{\mathbf{u}_0,0}\in\mathcal{D}_{\text{odd}}$ satisfies $\omega(D_{\mathbf{u}_0,0})\leq\Omega'$.

We sum over the value ω_0 of $\omega(D_{\mathbf{u}_0,0})$ and denote by $P^+(n)$ the greatest prime divisor of the integer $n>1$. In (112), we decompose $D_{\mathbf{u}_0,0}$ into $D_{\mathbf{u}_0,0}=np$, where $p=P^+(D_{\mathbf{u}_0,0})$ in order to write

$$\Bigl|\sum_{D_{\mathbf{u}_0,0}}2^{-k\,\omega(D_{\mathbf{u}_0,0})}\chi(D_{\mathbf{u}_0,0})\Bigr|$$
$$\leq\sum_{1\leq\omega_0\leq\Omega'}\ \sum_{n,\,\omega(n)=\omega_0-1}\Bigl|\sum_{\substack{\max\{P^+(n),A_{\mathbf{u}_0,0}/n\}<p<\Delta A_{\mathbf{u}_0,0}/n\\p\equiv1\bmod 4,\,(p,m)=1}}\chi(p)\Bigr|. \tag{113}$$

By Proposition 10, with q odd $\leq(\log X)^{B_k}$, we have, for every positive A the inequality

$$\sum_p\chi(p)\ll_A(\log X)^{\frac{B_k}{2}}\cdot\frac{A_{\mathbf{u}_0,0}}{n}\cdot\Bigl(\log\bigl(\frac{A_{\mathbf{u}_0,0}}{n}\bigr)\Bigr)^{-A}+\log X, \tag{114}$$

where the final log–term comes from the condition $(p, m) = 1$. When the summation over p in (113) is not empty, we have the inequality $p \geq A_{\mathbf{u}_0,0}^{\frac{1}{\Omega'}}$, from which we deduce $n < \Delta A_{\mathbf{u}_0,0}^{1-\frac{1}{\Omega'}}$ and finally

$$\log\bigl(\frac{A_{\mathbf{u}_0,0}}{n}\bigr) \gg \log A_{\mathbf{u}_0,0}^{\frac{1}{\Omega'}} \gg \log^{\frac{1}{2}} X, \tag{115}$$

by the definition of Ω', given in §5.6 and the inequality (100). Inserting (115) into (114) then into (113), summing over n, then over ω_0, and finally inserting into (112), we see that $S_{\text{odd}}^{\diamond,\lambda}(X, k, \mathbf{A})$ satisfies (99), by choosing A as a large function of k.

5.11. **Case** $i_0 = 2$. Actually, the proof will also work for $i_0 = 3$ as said above by considering conjugate expressions. The assumption $i_0 = 2$ means that we have the inequality

$$A_{\mathbf{u}_0,2} \geq X^{\frac{1}{2\cdot 4^{k+1}}}, \tag{116}$$

and that the associated variable $D_{u_0,2}$, is large and appears twice in the denominator of the quartic symbols in (77).

5.11.1. *There is an* $\mathbf{r}_0$*, unlinked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{r}_0,0} \geq (\log X)^{100\cdot 10^k}$. Consider the double oscillations of the character

$$\left(\frac{D_{\mathbf{r}_0,0}}{\overline{\mathfrak{D}}_{\mathbf{u}_0,2}}\right)_4,$$

and operate as in §5.9.1.

5.11.2. *There is an* $\mathbf{r}_0$*, linked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{r}_0,0} \geq (\log X)^{100\cdot 10^k}$. Use (103) to write

$$\left(\frac{D_{\mathbf{r}_0,0}}{D_{\mathbf{uo},2}}\right)\left(\frac{D_{\mathbf{r}_0,0}}{\overline{\mathfrak{D}}_{\mathbf{u}_0,2}}\right)_4 = \left(\frac{D_{\mathbf{r}_0,0}}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4,$$

and operate as in §5.9.2.

5.11.3. *There is an* $\mathbf{r}_0$*, unlinked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{r}_0,1} \geq (\log X)^{100\cdot 10^k}$. Consider the double oscillations of the character $\left(\frac{D_{\mathbf{r}_0,1}}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4$ and operate as in §5.9.3.

5.11.4. *There is an* $\mathbf{r}_0$*, linked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{r}_0,1} \geq (\log X)^{100\cdot 10^k}$. Write the equality

$$\left(\frac{D_{\mathbf{r}_0,1}}{D_{\mathbf{uo},2}}\right)\left(\frac{D_{\mathbf{r}_0,1}}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4 = \overline{\left(\frac{D_{\mathbf{r}_0,1}}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4},$$

and operate as in §5.9.4.

The conclusion of the discussions made in §5.11.1,..., 5.11.4 and of the condition (96), is that, in the case where $i_0 = 2$, we are now reduced to study the case

$$1 < \max_{\mathbf{r}\in\mathcal{Q}^k}\bigl(A_{\mathbf{r},0},\, A_{\mathbf{r},1}\bigr) < (\log X)^{100\cdot 10^k}. \tag{117}$$

Now we want to control the sizes of the variables $D_{\mathbf{r}_0,2}$ and $D_{\mathbf{r}_0,3}$, when $\mathbf{r}_0$ is linked with $\mathbf{u}_0$.

5.11.5. *There is an index* $\mathbf{r}_0$ *linked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{r}_0,2} > (\log X)^{100\cdot 10^k}$. This means that (77) really contains the symbol $\left(\frac{D_{\mathbf{r}_0,2}}{D_{\mathbf{u}_0,2}}\right) = \left(\frac{D_{\mathbf{u}_0,2}}{D_{\mathbf{r}_0,2}}\right)$. Then operate as in §5.9.5 to benefit from the double oscillations of this Jacobi symbol.

5.11.6. *There is an index* $\mathbf{r}_0$ *linked with* $\mathbf{u}_0$*, such that* $A_{\mathbf{r}_0,3} > (\log X)^{100\cdot 10^k}$. This means that (77) really contains the symbol $\left(\frac{D_{\mathbf{r}_0,3}}{D_{\mathbf{u}_0,2}}\right) = \left(\frac{D_{\mathbf{u}_0,2}}{D_{\mathbf{r}_0,3}}\right)$. Then operate as in §5.9.6.

After the discussion made in §5.11.5 & 5.11.6, we can now suppose that

$$\mathbf{r} \text{ linked with } \mathbf{u}_0 \Rightarrow A_{\mathbf{r},2} \text{ and } A_{\mathbf{r},3} < (\log X)^{100\cdot 10^k}. \tag{118}$$

5.12. **Use of the extended Siegel–Walfisz Theorem.** Now we are working with the restrictions (117) and (118). We are led to a conclusion almost similar to (108): the variable $D_{\mathbf{u}_0,2}$ appears in the five following symbols or products of symbols

$$\left(\frac{D_{\mathbf{u}_0,2}}{\ell}\right);\ \left(\frac{a}{D_{\mathbf{u}_0,2}}\right)\left(\frac{a}{\overline{\mathfrak{D}}_{\mathbf{u}_0,2}}\right)_4;\ \left(\frac{b}{D_{\mathbf{u}_0,2}}\right)\left(\frac{b}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4;\ \left(\frac{c}{\overline{\mathfrak{D}}_{\mathbf{u}_0,2}}\right)_4 \text{ and } \left(\frac{d}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4, \tag{119}$$

with

$$\ell = \prod_{\substack{\mathbf{r}\text{ linked}\\ \text{with } \mathbf{u}_0}} \Big(D_{\mathbf{r},2}\, D_{\mathbf{r},3}\Big),\ a = \prod_{\substack{\mathbf{r}\text{ linked}\\ \text{with } \mathbf{u}_0}} D_{\mathbf{r},0},$$

$$b = \prod_{\substack{\mathbf{r}\text{ linked}\\ \text{with } \mathbf{u}_0}} D_{\mathbf{r},1},\ c = \prod_{\substack{\mathbf{r}\text{ unlinked}\\ \text{with } \mathbf{u}_0}} D_{\mathbf{r},0},\ \text{and } d = \prod_{\substack{\mathbf{r}\text{ unlinked}\\ \text{with } \mathbf{u}_0}} D_{\mathbf{r},1},$$

with a, b, c, d and ℓ are coprime integers belonging to $\mathcal{D}_{\text{odd}} \cup \{1\}$, also satisfying (109). We use (103) to multiply the five expressions written in (119) and obtain the character over $\mathbb{Z}[i]$:

$$\mathfrak{D}_{\mathbf{u}_0,2} \mapsto \left(\frac{\mathfrak{D}_{\mathbf{u}_0,2}}{ad\ell^2}\right)_4 \overline{\left(\frac{\mathfrak{D}_{\mathbf{u}_0,2}}{bc}\right)_4} = \left(\frac{\mathfrak{D}_{\mathbf{u}_0,2}}{ab^3c^3d\ell^2}\right)_4.$$

By (117) and (118), this character is non trivial, with modulus w satisfying $\mathcal{N}(w) \leq (\log X)^{B_k}$, where B_k is a constant depending on k only. Now we operate as in (110)–(115), with the difference that we apply (83) of Proposition 11 (extension of the Siegel–Walfisz Theorem to the set of privileged primes) to the largest (privileged) prime divisor (say π) of $\mathfrak{D}_{\mathbf{u}_0,2}$. Hence the $\mathbf{A}$ falling in the cases studied in §5.11 & 5.12 are such that the associated sums also satisfy (99).

We have covered all the cases of $\mathbf{A}$ satisfying (96). The proof of Lemma 17 is now complete.

5.13. **The final step.** By Lemmas 13 and 17, we now have the equality

$$S_{\text{odd}}^{\diamond,\lambda}(X,k) = \sum_{\mathbf{A}} S_{\text{odd}}^{\diamond,\lambda}(X,k,\mathbf{A}) + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big), \tag{120}$$

where k is any integer ≥ 0 and ϵ any positive number and where the summation is over all the 4^{k+1}–tuples $\mathbf{A} = (A_{\mathbf{r},i})_{(\mathbf{r},i)\in\mathcal{Q}^{k+1}}$ satisfying the inequality (76), and the equalities

$$A_{\mathbf{r},0} = A_{\mathbf{r},1} = 1, \text{ for all } \mathbf{r} \in \mathcal{Q}^k, \tag{121}$$

or

$$A_{\mathbf{r},2} = A_{\mathbf{r},3} = 1, \text{ for all } \mathbf{r} \in \mathcal{Q}^k. \tag{122}$$

Let $\Sigma_{0,1}$ be the contribution of the $\mathbf{A}$ satisfying (121) to the right part of (120) and $\Sigma_{2,3}$ corresponding to the $\mathbf{A}$ satisfying (122). The condition (121) means that the variables of summation $D_{\mathbf{r},0}$ and $D_{\mathbf{r},1}$ can only take the value 1. In the case of (122), the variables $D_{\mathbf{r},2}$ and $D_{\mathbf{r},3}$ are forced to be equal to 1. In both cases, the quartic symbols in the definition (77) of $S^{\diamond,\lambda}_{\text{odd}}(X,k,\mathbf{A})$ have the value 1. Hence, using symmetry, we clearly have $\Sigma_{0,1} = \Sigma_{2,3}$. So we may write (120) in the form

$$S^{\diamond,\lambda}_{\text{odd}}(X,k) = 2\Sigma_{0,1} + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big). \tag{123}$$

For $\mathbf{A}$ satisfying (121), we have the equality

$$S^{\diamond,\lambda}_{\text{odd}}(X,k,\mathbf{A}) = \frac{1}{2^k}\sum_{(D_{\mathbf{r},2})}\sum_{(D_{\mathbf{r},3})}\mu^2\Big(\prod_{\mathbf{r}}(D_{\mathbf{r},2}D_{\mathbf{r},3})\Big) \times\Big(\prod_{\mathbf{r}}2^{-(k+1)\omega(D_{\mathbf{r},2}D_{\mathbf{r},3})}\Big)\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},2}D_{\mathbf{r},3}}{D_{\mathbf{s},2}D_{\mathbf{s},3}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\}, \tag{124}$$

where

$A_{\mathbf{r},i} \leq D_{\mathbf{r},i} < \Delta A_{\mathbf{r},i},\ D_{\mathbf{r},i} \in \mathcal{D}_{\text{odd}}\cup\{1\}$ and $\omega(D_{\mathbf{r},i}) \leq \Omega'$ for all $(\mathbf{r},i) \in \mathcal{Q}^k\times\{2,3\}$.

Summing back all the sums $S^{\diamond,\lambda}_{\text{odd}}(X,k,\mathbf{A})$, where $\mathbf{A}$ satisfies (121), (as written in (124)) and bounding the error terms (as it was done for Lemma 13), we see that the contribution $\Sigma_{0,1}$ of these sums satisfy the equality

$$\begin{aligned}\Sigma_{0,1} = \frac{1}{2^k}\sum_{(D_{\mathbf{r},2})}\sum_{(D_{\mathbf{r},3})}\mu^2\Big(\prod_{\mathbf{r}}(D_{\mathbf{r},2}D_{\mathbf{r},3})\Big)&\\ \times\Big(\prod_{\mathbf{r}}2^{-(k+1)\omega(D_{\mathbf{r},2}D_{\mathbf{r},3})}\Big)\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},2}D_{\mathbf{r},3}}{D_{\mathbf{s},2}D_{\mathbf{s},3}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\}&\\ + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big),&\end{aligned} \tag{125}$$

where the variables $D_{\mathbf{r},2}$ and $D_{\mathbf{r},3}$ belong to $\mathcal{D}_{\text{odd}}\cup\{1\}$ and satisfy the inequality

$$\prod_{\mathbf{r}}(D_{\mathbf{r},2}D_{\mathbf{r},3}) \leq X.$$

Setting $D_{\mathbf{r}} = D_{\mathbf{r},2}D_{\mathbf{r},3}$, (when $D_{\mathbf{r}} \in \mathcal{D}_{\text{odd}}$ is fixed, this equation has $2^{\omega(D_{\mathbf{r}})}$ solutions), we write (125) in the form

$$\Sigma_{0,1} = \frac{1}{2^k}\sum_{(D_{\mathbf{r}})}\mu^2\Big(\prod_{\mathbf{r}}D_{\mathbf{r}}\Big)\Big(\prod_{\mathbf{r}}2^{-k\omega(D_{\mathbf{r}})}\Big)\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\} + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big), \tag{126}$$

where the $D_{\mathbf{r}}$ belong to $\mathcal{D}_{\text{odd}}\cup\{1\}$ and satisfy the inequality

$$\prod_{\mathbf{r}\in\mathcal{Q}^k} D_{\mathbf{r}} \leq X.$$

We recognize an expression already met in [4], in the course of the proof of (55). In fact, by [4, Lemma 36], we have the equality

$$S_{\mathrm{odd}}(X,k)=\frac{1}{2^k}\sum_{(D_{\mathbf{r}})}\mu^2\Bigl(\prod_{\mathbf{r}}D_{\mathbf{r}}\Bigr)\Bigl(\prod_{\mathbf{r}}2^{-k\omega(D_{\mathbf{r}})}\Bigr)\Bigl\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Bigl(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Bigr)^{\kappa_k(\mathbf{r},\mathbf{s})}\Bigr\},$$

where the conditions of summation are the same as in (126). By (55) and by (126), we deduce the equality

$$\Sigma_{0,1}=c_k\cdot\mathcal{D}(X)+O_{k,\epsilon}\bigl(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\bigr). \tag{127}$$

Putting together Lemma 12, (56) from Proposition 5, (123) and (127), we write

$$S_{\mathrm{odd}}^{\mathrm{mix},\lambda}(X,k)=\bigl(\frac{1}{2}(2^{k-1}+1)+\frac{2}{4}\bigr)\cdot c_k\cdot\mathcal{D}_{\mathrm{odd}}(X)++O_{k,\epsilon}\bigl(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\bigr).$$

This completes the proof of Theorem 3*(v)* in the case $\mathcal{D}_{\mathrm{odd}}$.

6. The case of even discriminants

In that section we are concerned with the subsum of $S^{\mathrm{mix},\lambda}(X,k)$ (see (44)) defined by

$$S_{\mathrm{even}}^{\mathrm{mix},\lambda}(X,k):=\sum_{\substack{D\in\mathcal{D}_{\mathrm{even}}\\ D\leq X}}2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}\cdot 2^{\lambda_D},$$

in order to prove the equality (14), with $\mathcal{D}$ replaced by $\mathcal{D}_{\mathrm{even}}$ (see Theorem 3 *(v)*). Note the trivial equality

$$S_{\mathrm{even}}^{\mathrm{mix},\lambda}(X,k)=\sum_{\substack{D\in\mathcal{D}_{\mathrm{odd}}\\ D\leq X/8}}2^{k\,\mathrm{rk}_4(\mathrm{C}_{8D})}\cdot 2^{\lambda_{8D}}.$$

The study of $S_{\mathrm{even}}^{\mathrm{mix},\lambda}(X,k)$ has a lot of similarities with $S_{\mathrm{odd}}^{\mathrm{mix},\lambda}(X,k)$, particularly in the analytic point of view. Using Proposition 9 to decompose $2^{\lambda_{8D}}$, we can easily prove the following lemma:

Lemma 18. *For every $k\geq 0$ and every $X\geq 1$, we have*

$$S_{\mathrm{even}}^{\mathrm{mix},\lambda}(X,k)=\frac{1}{2}S_{\mathrm{even}}^{\mathrm{mix}}(X,k)+\frac{1}{4}\Lambda_1(X,k)+\frac{1}{4}\Lambda_2(X,k) \tag{128}$$

with

$$\Lambda_1(X,k)=\sum_{\substack{D\in\mathcal{D}_{\mathrm{odd}}\\ D\leq X/8}}\frac{2^{k\,\mathrm{rk}_4(\mathrm{C}_{8D})}}{2^{\omega(D)}}\sum_{D=a_1a_2b_1b_2}[a_1a_2,2]_4\Bigl(\frac{2}{a_1}\Bigr)\Bigl(\frac{a_1}{\overline{\mathfrak{b}_1}\mathfrak{b}_2}\Bigr)_4\Bigl(\frac{a_2}{\mathfrak{b}_1\overline{\mathfrak{b}_2}}\Bigr)_4,$$

and

$$\Lambda_2(X,k)=\sum_{\substack{D\in\mathcal{D}_{\mathrm{odd}}\\ D\leq X/8}}\frac{2^{k\,\mathrm{rk}_4(\mathrm{C}_{8D})}}{2^{\omega(D)}}\sum_{D=a_1a_2b_1b_2}\Bigl(\frac{2}{\overline{\mathfrak{a}_1}\mathfrak{a}_2}\Bigr)_4\Bigl(\frac{b_1}{\overline{\mathfrak{a}_1}\mathfrak{a}_2}\Bigr)_4\Bigl(\frac{b_2}{\mathfrak{a}_1\overline{\mathfrak{a}_2}}\Bigr)_4,$$

where $a_i=\mathfrak{a}_i\overline{\mathfrak{a}_i}$ and $b_i=\mathfrak{b}_i\overline{\mathfrak{b}_i}$ are the privileged factorizations of a_i and b_i ($i=1,\,2$).

By (56) we know that the first term on the right side of (128) is equal to

$$\frac{1}{2}S_{\mathrm{even}}^{\mathrm{mix}}(X,k)=\frac{c_k}{2}\cdot(2^{k-1}+1)\cdot\mathcal{D}_{\mathrm{even}}(X)+O_{\epsilon,k}\Bigl(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\Bigr). \tag{129}$$

We want to prove

Proposition 16. *For every integer $k \geq 0$, for every $\epsilon > 0$ and for every $X \geq 2$, we have*

$$\Lambda_2(X,k) = c_k \cdot \mathcal{D}_{\text{even}}(X) + O_{\epsilon,k}\Big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\Big).$$

Since the study of Λ_1 is very similar, we shall only give short indications on the proof of

Proposition 17. *For every integer $k \geq 0$, for every $\epsilon > 0$ and for every $X \geq 2$, we have*

$$\Lambda_1(X,k) = c_k \cdot \mathcal{D}_{\text{even}}(X) + O_{\epsilon,k}\Big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\Big).$$

Gathering (128), (129), Propositions 16 & 17 and summing the coefficients of the main terms, we easily obtain (14) for $\mathcal{D}$ replaced by $\mathcal{D}_{\text{even}}$. This will complete the proof of Theorem 3. It remains to prove Propositions 16 & 17.

6.1. **First transformation of $\Lambda_2(X,k)$.** As we did in §5.6, we shall benefit from the combinatorial and analytic transformations made in [4]. In that paper, we met the sum $G(X,k)$ defined by

$$G(X,k) := \sum_{\substack{D\in\mathcal{D}_{\text{odd}}\\ D\leq X/8}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_{8D})} \cdot \Big(\frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=abcd} [ab,2]_4 \Big(\frac{2}{\mathfrak{a}\overline{\mathfrak{b}}}\Big)_4 \Big(\frac{\mathfrak{a}\overline{\mathfrak{b}}}{\mathfrak{c}\overline{\mathfrak{d}}}\Big)_4^2\Big), \tag{130}$$

(see [4, (130) & (131)]), and in [4, (132)] we proved the equality

(131)

$$G(X,k) = \frac{1}{2} \sum_{\substack{D\in\mathcal{D}_{\text{odd}}\\ D\leq X/8}} \frac{1}{2^{(k+1)\omega(D)}} \sum_{(D_{\mathbf{r}})\ (E_i)} \Big(\prod_{\mathbf{r}\in\mathcal{Q}^k} \Big(\frac{2}{D_{\mathbf{r}}}\Big)^{L_k(\mathbf{r})}\Big)$$
$$\times \Big(\prod_{\mathbf{r},\,\mathbf{s}\in\mathcal{Q}^k} \Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big) \Big(\frac{2}{\mathfrak{E}_2\overline{\mathfrak{E}}_3}\Big)_4 \Big(\frac{\mathfrak{E}_0\overline{\mathfrak{E}}_1}{\mathfrak{E}_2\overline{\mathfrak{E}}_3}\Big)_4^2 [E_2E_3,2]_4,$$

where

- $\mathcal{Q}$ and $\kappa_k(\mathbf{r},\mathbf{s})$ have the same meanings as in (73),
- the sums are over $D \in \mathcal{D}_{\text{odd}}$, $D < X/8$ and over $(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^k}$ and $(E_i)_{i\in\mathcal{Q}}$ such that

$$D = \prod_{\mathbf{r}\in\mathcal{Q}^k} D_{\mathbf{r}} = \prod_{i\in\mathcal{Q}} E_i, \tag{132}$$

with $D_{\mathbf{r}}$ and $E_i \in \mathcal{D}_{\text{odd}} \cup \{1\}$,
- the privileged factorization of E_i is $E_i = \mathfrak{E}_i\overline{\mathfrak{E}}_i$ $(0 \leq i \leq 3)$,
- for $r = (r_1,\dots,r_k) \in \mathcal{Q}^k$, $L_k(\mathbf{r})$ is the number of j $(1 \leq j \leq k)$ such that $r_j = 3$.

Using the similarities between the definitions of $\Lambda_2(X,k)$ and the definition (130) of $G(X,k)$ and arguing as in the proof of (131), we can prove

Lemma 19. *With the conventions of (131), we have the equality*

$$\Lambda_2(X,k) = \sum_{\substack{D\in\mathcal{D}_{\text{odd}}\\ D\leq X/8}} \frac{1}{2^{(k+1)\omega(D)}} \sum_{(D_{\mathbf{r}})\ (E_i)} \Big(\prod_{\mathbf{r}\in\mathcal{Q}^k} \Big(\frac{2}{D_{\mathbf{r}}}\Big)^{L_k(\mathbf{r})}\Big) \tag{133}$$
$$\times \Big(\prod_{\mathbf{r},\,\mathbf{s}\in\mathcal{Q}^k} \Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big) \Big(\frac{2}{\mathfrak{E}_2\overline{\mathfrak{E}}_3}\Big)_4 \Big(\frac{E_0}{\mathfrak{E}_2\overline{\mathfrak{E}}_3}\Big)_4 \Big(\frac{E_1}{\overline{\mathfrak{E}}_2\mathfrak{E}_3}\Big)_4,$$

for any integer $k \geq 0$ and any $X \geq 2$.

To solve (132) we operate as for (79): we introduce for $(\mathbf{r},i)\in\mathcal{Q}^k\times\mathcal{Q}$ the g.c.d.

$$D_{\mathbf{r},i}=\text{g.c.d. }(D_{\mathbf{r}},E_i),\tag{134}$$

which gives the relations

$$D_{\mathbf{r}}=\prod_i D_{\mathbf{r},i},\ E_i=\prod_{\mathbf{r}} D_{\mathbf{r},i}.$$

Then we insert this into (133) in order to write

$$\begin{aligned}\Lambda_2(X,k)=\sum_{(D_{\mathbf{r},i})}\mu^2\big(\prod_{\mathbf{r},i}D_{\mathbf{r},i}\big)\Big(\prod_{\mathbf{r},i}2^{-(k+1)\omega(D_{\mathbf{r},i})}\Big)\Big(\prod_{\mathbf{r},i}\Big(\frac{2}{D_{\mathbf{r},i}}\Big)^{L_k(\mathbf{r})}\Big)\\ \times\Big(\prod_{\mathbf{r},i}\prod_{\mathbf{s},j}\Big(\frac{D_{\mathbf{r},i}}{D_{\mathbf{s},j}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big)\Big(\prod_{\mathbf{r}}\Big(\frac{2}{\mathfrak{D}_{\mathbf{r},2}\overline{\mathfrak{D}}_{\mathbf{r},3}}\Big)_4\Big)\\ \times\Big(\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},0}}{\mathfrak{D}_{\mathbf{s},2}\overline{\mathfrak{D}}_{\mathbf{s},3}}\Big)_4\Big)\Big(\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},1}}{\overline{\mathfrak{D}}_{\mathbf{s},2}\mathfrak{D}_{\mathbf{s},3}}\Big)_4\Big),\end{aligned}\tag{135}$$

where the sum is over the 4^{k+1}–tuples $(D_{\mathbf{r},i})$ (with $(\mathbf{r},i)\in\mathcal{Q}^k\times\mathcal{Q}$) satisfying

$$D_{\mathbf{r},i}\in\mathcal{D}_{\text{odd}}\cup\{1\}\text{ and }\prod_{\mathbf{r}}\prod_i D_{\mathbf{r},i}\le X/8.$$

As usual the privileged factorization of $D_{\mathbf{r},i}$ is $D_{\mathbf{r},i}=\mathfrak{D}_{\mathbf{r},i}\overline{\mathfrak{D}}_{\mathbf{r},i}$. We shall use the same splitting process as in §5.6. Let $\Lambda_2(X,k,\mathbf{A})$ be the subsum of $\Lambda_2(X,k)$ defined by the same formula as in (135), but with the extra condition that the variables of summation satisfy the restrictions (74). Similarly, as in Lemma 13 we have

Lemma 20. *For every $\epsilon>0$ and for every integer $k\ge 0$ we have the equality*

$$\Lambda_2(X,k)=\sum_{\mathbf{A}}\Lambda_2(X,k,\mathbf{A})+O_{k,\epsilon}\big(X(\log X)^{-\frac12-\frac{1}{2^{k+2}}+\epsilon}\big),\tag{136}$$

where the summation is over all the 4^{k+1}–tuples $(A_{\mathbf{r},i})_{(\mathbf{r},i)\in\mathcal{Q}^{k+1}}$ satisfying the inequality

$$\prod_{\mathbf{r},\,i}A_{\mathbf{r},i}\le X/(8\Delta^{4^{k+1}}).\tag{137}$$

Our next task is to prove

Lemma 21. *For every integer $k\ge 0$ and uniformly for $X\ge 2$, we have the equality*

$$\sum_{\mathbf{A}}\big|\Lambda_2(X,k,\mathbf{A})\big|=O_k(X(\log X)^{-1}),$$

where the sum is over the $\mathbf{A}$ such that (137) is satisfied and such that

$$\max\{A_{\mathbf{r},2},A_{\mathbf{r},3}\,;\mathbf{r}\in\mathcal{Q}^k\}>1.\tag{138}$$

We remark that, due to the oscillations of characters containing 2 in the numerator, the condition (138) is less demanding than (96).

6.2. **Reduction of the proof of Lemma 21.** The proof follows the path of the proof of Lemma 17. Let Σ_3 be the sum studied in Lemma 21. As in the proof of Lemma 17, we can restrict to show the inequality

$$\Lambda_2(X, k, \mathbf{A}) \ll (\log X)^{-1-4^{k+1}(1+2^{k+1})}, \tag{139}$$

for the $\mathbf{A}$ satisfying (98), (137) & (138). Let $(\mathbf{u}_0, i_0)$ be an index in $\mathcal{Q}^k \times \mathcal{Q}$, such that $A_{\mathbf{u}_0,i_0}$ satisfies (100). Our proof will depend on the value of i_0. However the cases $i_0 = 0$ and $i_0 = 1$ are similar. The cases $i_0 = 2$ and $i_0 = 3$ are the same after conjugating the expressions in question.

6.3. **Proof of (139). The case $i_0 = 0$.** This proof also works when $i_0 = 1$. As in §5.9, we discuss on the size of the other variables, which accompany $D_{\mathbf{u}_0,0}$ in some symbols.

6.3.1. *There is an $\mathbf{s}_0$ unlinked with $\mathbf{u}_0$, such that $A_{\mathbf{s}_0,2} \geq (\log X)^{100\cdot 10^k}$.* We apply Proposition 15 to the symbol $\left(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{D}_{\mathbf{s}_0,2}}\right)_4$ as it was made in §5.9.1 and we obtain (139).

6.3.2. *There is an $\mathbf{s}_0$ linked with $\mathbf{u}_0$, such that $A_{\mathbf{s}_0,2} \geq (\log X)^{100\cdot 10^k}$.* We write the equality $\left(\frac{D_{\mathbf{u}_0,0}}{D_{\mathbf{s}_0,2}}\right)\left(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{D}_{\mathbf{s}_0,2}}\right)_4 = \overline{\left(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{D}_{\mathbf{s}_0,2}}\right)_4}$ and we apply Proposition 15 to the symbol $\left(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{D}_{\mathbf{s}_0,2}}\right)_4$ as it was made in §5.9.2 and we obtain (139).

6.3.3. *There is an $\mathbf{s}_0$ unlinked with $\mathbf{u}_0$, such that $A_{\mathbf{s}_0,3} \geq (\log X)^{100\cdot 10^k}$.* This case is analogous to §6.3.1 by considering the double oscillations of the character $\left(\frac{D_{\mathbf{u}_0,0}}{\overline{\mathfrak{D}}_{\mathbf{s}_0,3}}\right)_4$.

6.3.4. *There is an $\mathbf{s}_0$ linked with $\mathbf{u}_0$, such that $A_{\mathbf{s}_0,3} \geq (\log X)^{100\cdot 10^k}$.* This case is analogous to §6.3.2 by considering the double oscillations of the character $\left(\frac{D_{\mathbf{u}_0,0}}{\overline{\mathfrak{D}}_{\mathbf{s}_0,3}}\right)_4$.

Hence, after the discussions made in §6.3.1–6.3.4, we can now suppose that

$$A_{\mathbf{s},2},\ A_{\mathbf{s},3} < (\log X)^{100\cdot 10^k} \text{ for all } \mathbf{s} \in \mathcal{Q}^k. \tag{140}$$

6.3.5. *There is an $\mathbf{s}_0$ linked with $\mathbf{u}_0$, such that $A_{\mathbf{s}_0,0} \geq (\log X)^{100\cdot 10^k}$.* We apply Proposition 12 to the character $\left(\frac{D_{\mathbf{u}_0,0}}{D_{\mathbf{s}_0,0}}\right)$, and (139) is proved in that case. Similar arguments apply if $A_{\mathbf{s}_0,1} \geq (\log X)^{100\cdot 10^k}$.

After the discussion made in 6.3.5 we can suppose that

$$A_{\mathbf{s},0},\ A_{\mathbf{s},1} < (\log X)^{100\cdot 10^k} \text{ for all } \mathbf{s} \in \mathcal{Q}^k \text{ linked with } \mathbf{u}_0. \tag{141}$$

6.3.6. *The final argument.* By studying the right part of (135), we see that the variable $D_{\mathbf{u}_0,0}$ appears in the following multiplicative symbols

$$\left(\frac{D_{\mathbf{u}_0,0}}{\ell}\right),\ \left(\frac{D_{\mathbf{u}_0,0}}{\mathfrak{a}}\right)_4 \text{ and } \left(\frac{D_{\mathbf{u}_0,0}}{\overline{\mathfrak{b}}}\right)_4, \tag{142}$$

where

$$\ell = \prod_{\substack{\mathbf{r} \text{ linked} \\ \text{with } \mathbf{u}_0}} \prod_i D_{\mathbf{r},i},\ a = \prod_{\mathbf{r}} D_{\mathbf{r},2},\ b = \prod_{\mathbf{s}} D_{\mathbf{s},3},$$

and eventually in the symbol $\left(\frac{2}{D_{\mathbf{u}_0,0}}\right)$, if $L_k(\mathbf{u}_0)$ is odd.

The product of the three symbols in (142) gives a non principal Dirichlet character, $D_{\mathbf{u}_0,0} \mapsto \chi(D_{\mathbf{u}_0,0})$ with an odd modulus $q \leq (\log X)^{B_k}$, where B_k is an explicit function of the integer k. This is a consequence of the assumption (138) and the restrictions (140) and (141).

When $L_k(\mathbf{u}_0)$ is even, we apply formula (81) in Proposition 10 to the largest prime factor p of $D_{\mathbf{u}_0,0}$, as it was done in (112)–(115). And (139) is proved in that case.

When $L_k(\mathbf{u}_0)$ is odd, we proceed in the same manner, by appealing to the formula (82) of Proposition 10. This also gives the proof of (139) in that case.

In conclusion, the proof of (139) is now complete, when $i_0 = 0$ or $i_0 = 1$.

6.4. **Proof of (139). The case $i_0 = 2$.** By assumption, we have (116) and this proof also works when $i_0 = 3$ with tiny modifications. As above, it depends on the sizes of the variables, which accompany $D_{\mathbf{u}_0,2}$ in some characters.

6.4.1. *There is an $\mathbf{r}_0$ unlinked with $\mathbf{u}_0$, such that $A_{\mathbf{r}_0,0} \geq (\log X)^{100\cdot 10^k}$.* We apply Proposition 15 to the symbol $\left(\frac{D_{\mathbf{r}_0,0}}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4$ as it was made in §5.9.1 and we obtain (139).

6.4.2. *There is an $\mathbf{r}_0$ linked with $\mathbf{u}_0$, such that $A_{\mathbf{r}_0,0} \geq (\log X)^{100\cdot 10^k}$.* We write the equality $\left(\frac{D_{\mathbf{r}_0,0}}{D_{\mathbf{u}_0,2}}\right)\left(\frac{D_{\mathbf{r}_0,0}}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4 = \overline{\left(\frac{D_{\mathbf{r}_0,0}}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4}$ and we apply Proposition 15 to this symbol as it was made in §5.9.2 and we obtain (139).

6.4.3. *There is a $\mathbf{r}_0$ linked or not with $\mathbf{u}_0$ such that $A_{\mathbf{r}_0,1} \geq (\log X)^{100\cdot 10^k}$.* The proof is similar to the proofs contained in §6.4.1 & 6.4.2.

After the discussions made in §6.4.1–6.4.3, we can suppose

$$A_{\mathbf{s},0},\ A_{\mathbf{s},1} < (\log X)^{100\cdot 10^k} \text{ for all } \mathbf{s} \in \mathcal{Q}^k. \tag{143}$$

6.4.4. *There is an $\mathbf{r}_0$, linked with $\mathbf{u}_0$, such that $A_{\mathbf{r}_0,2} \geq (\log X)^{100\cdot 10^k}$.* Then we consider the double oscillations of the character $\left(\frac{D_{\mathbf{r}_0,2}}{D_{\mathbf{u}_0,2}}\right)$, and the proof is similar to §6.3.5. Therefore formula (139) is proved again.

6.4.5. *There is an $\mathbf{r}_0$, linked with $\mathbf{u}_0$, such that $A_{\mathbf{r}_0,3} \geq (\log X)^{100\cdot 10^k}$.* Now we consider the character $\left(\frac{D_{\mathbf{r}_0,3}}{D_{\mathbf{u}_0,2}}\right)$. The proof is similar to §6.4.4 and formula (139) is proved again.

After the discussions made in §6.4.4 §6.4.5, we can now suppose that

$$A_{\mathbf{r},2},\ A_{\mathbf{r},3} < (\log X)^{100\cdot 10^k} \text{ for all } \mathbf{r} \in \mathcal{Q}^k \text{ linked with } \mathbf{u}_0. \tag{144}$$

6.4.6. *The final argument.* In this subsection, we shall see the difference with the case $i_0 = 0$ or 1, treated in §6.3 and the true influence of the symbols containing 2. In (135), the variable $D_{\mathbf{u}_0,2}$ appears in the five symbols

$$\left(\frac{2}{D_{\mathbf{u}_0,2}}\right)^{L_k(\mathbf{u}_0)};\ \left(\frac{D_{\mathbf{u}_0,2}}{\ell}\right);\ \left(\frac{2}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4;\ \left(\frac{a}{\mathfrak{D}_{\mathbf{u}_0,2}}\right)_4 \text{ and } \left(\frac{b}{\overline{\mathfrak{D}}_{\mathbf{u}_0,2}}\right)_4 \tag{145}$$

with

$$\ell = \prod_{\substack{\mathbf{r} \text{ linked} \\ \text{with } \mathbf{u}_0}} \prod_i D_{\mathbf{r},i},\ a = \prod_{\mathbf{r}} D_{\mathbf{r},0} \text{ and } b = \prod_{\mathbf{r}} D_{\mathbf{r},1}.$$

Note, that in the present case, we may have $a = b = \ell = 1$. The product of the five symbols appearing in (145) is equal to

$$\Big(\frac{2}{\mathfrak{D}_{\mathbf{u}_0,2}}\Big)_4 \Big(\frac{\mathfrak{D}_{\mathbf{u}_0,0}}{ab^3\ell^2}\Big)_4 \text{ if } L_k(\mathbf{u}_0) \text{ is even,}$$

or

$$\overline{\Big(\frac{2}{\mathfrak{D}_{\mathbf{u}_0,2}}\Big)_4} \Big(\frac{\mathfrak{D}_{\mathbf{u}_0,0}}{ab^3\ell^2}\Big)_4 \text{ if } L_k(\mathbf{u}_0) \text{ is odd.}$$

We appeal to (84) of Proposition 11, which we apply to the largest prime privileged divisor π of $\mathfrak{D}_{\mathbf{u}_0,0}$, by the same technique employed in (112)–(115). In this case we also get (139).

This completes the proof of (139) in the case $i_0 = 2$ or 3. Incorporating the results of §6.3 (case $i_0 = 0$ or 1), the proof of Lemma 21 is now complete.

6.5. **Dealing with the main term.** From Lemmata 20 & 21, we see that the main term (on the right part of (136)) comes from the contribution of the $\Lambda_2(X, k, \mathbf{A})$ with $A_{\mathbf{r},2} = A_{\mathbf{r},3} = 1$, for all $\mathbf{r} \in \mathcal{Q}$. This means that, in these sums, we have $D_{\mathbf{r},2} = D_{\mathbf{r},3} = 1$. Gluing back these sums $\Lambda_2(X, k, \mathbf{A})$ as it was done in (125), with an admissible error in $O_{k,\epsilon}\big(X(\log X)^{-\frac12-\frac{1}{2^{k+2}}+\epsilon}\big)$, we have to consider the contribution $\Lambda_2^{\mathrm{MT}}(X, k)$ of these terms. In other words, let

$$\begin{aligned}(146)\qquad \Lambda_2^{\mathrm{MT}}(X,k) = \sum_{(D_{\mathbf{r},0}),\,(D_{\mathbf{r},1})} \mu^2\big(\prod_{\mathbf{r}} D_{\mathbf{r},0}D_{\mathbf{r},1}\big) \Big(\prod_{\mathbf{r}} 2^{-(k+1)\omega(D_{\mathbf{r},0}D_{\mathbf{r},1})}\Big)\\ \times \Big(\prod_{\mathbf{r}} \Big(\frac{2}{D_{\mathbf{r},0}D_{\mathbf{r},1}}\Big)^{L_k(\mathbf{r})}\Big)\Big(\prod_{\mathbf{r}}\prod_{\mathbf{s}} \Big(\frac{D_{\mathbf{r},0}D_{\mathbf{r},1}}{D_{\mathbf{s},0}D_{\mathbf{s},1}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big),\end{aligned}$$

where the variables $D_{\mathbf{r},0}$ and $D_{\mathbf{r},1}$ belong to $\mathcal{D}_{\mathrm{odd}}$ and satisfy $\prod_{\mathbf{r}}(D_{\mathbf{r},0}D_{\mathbf{r},1}) \le X/8$. Then, from (135) & (146), Lemmas 20 & 21 and the above discussion, we can write the equality

$$(147)\qquad \Lambda_2(X,k) = \Lambda_2^{\mathrm{MT}}(X,k) + O_{k,\epsilon}\big(X(\log X)^{-\frac12-\frac{1}{2^{k+2}}+\epsilon}\big).$$

In (146), we make the change of variables $D_{\mathbf{r},0}D_{\mathbf{r},1} = D_{\mathbf{r}}$, in order to write the equality

(148)

$$\Lambda_2^{\mathrm{MT}}(X,k) = \sum_{(D_{\mathbf{r}})} \mu^2\big(\prod_{\mathbf{r}} D_{\mathbf{r}}\big) \Big(\prod_{\mathbf{r}} 2^{-k\,\omega(D_{\mathbf{r}})}\Big)\Big(\prod_{\mathbf{r}} \Big(\frac{2}{D_{\mathbf{r}}}\Big)^{L_k(\mathbf{r})}\Big)\Big(\prod_{\mathbf{r}}\prod_{\mathbf{s}} \Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big),$$

where the summation is over the 4^k–tuples $(D_{\mathbf{r}})$ of elements of $\mathcal{D}_{\mathrm{odd}} \cup \{1\}$, satisfying $\prod_{\mathbf{r}} D_{\mathbf{r}} \le X/8$. Here also, we recognize a formula already met in [4]. By [4, Lemma 47] we have

$$S_{\mathrm{even}}(X,k) = \sum_{(D_{\mathbf{r}})} \mu^2\big(\prod_{\mathbf{r}} D_{\mathbf{r}}\big) \Big(\prod_{\mathbf{r}} 2^{-k\,\omega(D_{\mathbf{r}})}\Big)\Big(\prod_{\mathbf{r}} \Big(\frac{2}{D_{\mathbf{r}}}\Big)^{L_k(\mathbf{r})}\Big)\Big(\prod_{\mathbf{r}}\prod_{\mathbf{s}} \Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big),$$

with the same conditions of summation. This directly gives the equality

$$(149)\qquad \Lambda_2^{\mathrm{MT}}(X,k) = S_{\mathrm{even}}(X,k).$$

Now Proposition 16 is an easy consequence of (147), (149) and Proposition 5.

6.6. **Proof of Proposition 17.** As announced above, we shall only sketch the proof of Proposition 17 concerning the asymptotic expansion of $\Lambda_1(X,k)$. By the same techniques as those used in the study of $\Lambda_2(X,k)$ (see §6.1–§6.5) we obtain the analogue of Lemma 19:

Lemma 22. *With the conventions of (131), we have the equality*

$$(150)\quad \Lambda_1(X,k) = \sum_{\substack{D\in\mathcal{D}_{\text{odd}}\\ D\le X/8}} \frac{1}{2^{(k+1)\omega(D)}} \sum_{(D_{\mathbf{r}})\ (E_i)} \Bigl(\prod_{\mathbf{r}\in\mathcal{Q}^k}\Bigl(\frac{2}{D_{\mathbf{r}}}\Bigr)^{L_k(\mathbf{r})}\Bigr)$$
$$\times\Bigl(\prod_{\mathbf{r},\,\mathbf{s}\in\mathcal{Q}^k}\Bigl(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Bigr)^{\kappa_k(\mathbf{r},\mathbf{s})}\Bigr)\Bigl(\frac{2}{E_2}\Bigr)\Bigl(\frac{E_2}{\overline{\mathfrak{E}_0}\mathfrak{E}_1}\Bigr)_4\Bigl(\frac{E_3}{\mathfrak{E}_0\overline{\mathfrak{E}_1}}\Bigr)_4[E_2E_3,2]_4,$$

for any integer $k\ge 0$ and any $X\ge 2$.

Now we introduce the $D_{\mathbf{r},i}$ (see (134)) giving the equality

$$(151)\quad \Lambda_1(X,k) = \sum_{(D_{\mathbf{r},i})}\mu^2\Bigl(\prod_{\mathbf{r},i}D_{\mathbf{r},i}\Bigr)\Bigl(\prod_{\mathbf{r},i}2^{-(k+1)\omega(D_{\mathbf{r},i})}\Bigr)\Bigl(\prod_{\mathbf{r},i}\Bigl(\frac{2}{D_{\mathbf{r},i}}\Bigr)^{L_k(\mathbf{r})}\Bigr)$$
$$\times\Bigl(\prod_{\mathbf{r},i}\prod_{\mathbf{s},j}\Bigl(\frac{D_{\mathbf{r},i}}{D_{\mathbf{s},j}}\Bigr)^{\kappa_k(\mathbf{r},\mathbf{s})}\Bigr)\Bigl(\prod_{\mathbf{r}}\Bigl(\frac{2}{D_{\mathbf{r},2}}\Bigr)\Bigr)\Bigl(\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Bigl(\frac{D_{\mathbf{r},2}}{\overline{\mathfrak{D}_{\mathbf{s},0}}\mathfrak{D}_{\mathbf{s},1}}\Bigr)_4\Bigr)$$
$$\times\Bigl(\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Bigl(\frac{D_{\mathbf{r},3}}{\overline{\mathfrak{D}_{\mathbf{s},0}}\mathfrak{D}_{\mathbf{s},1}}\Bigr)_4\Bigr)\Bigl[\prod_{\mathbf{r}}(D_{\mathbf{r},2}D_{\mathbf{r},3}),2\Bigr]_4.$$

We continue with the same strategy as in §6.1, which consists in splitting $\Lambda_1(X,k)$ into subsums $\Lambda_1(X,k,\mathbf{A})$, where the size of each variable $D_{\mathbf{r},i}$ is controlled. Then we arrive at an analogue of Lemma 20, which is

$$(152)\qquad \Lambda_1(X,k) = \sum_{\mathbf{A}}\Lambda_1(X,k,\mathbf{A}) + O_{k,\epsilon}\bigl(X(\log X)^{-\frac12-\frac{1}{2^{k+2}}+\epsilon}\bigr),$$

where the summations are the same as for (136). Now we prove cancellations in some $\Lambda_1(X,k,\mathbf{A})$, by producing either double oscillations of some characters (then use Proposition 12 or 15) or simple oscillations of a character (then use one of the variants of the Siegel–Walfisz Theorem, see Proposition 10 or 11). The conclusion of that study, is that, in the summation of (152), only the $\mathbf{A}$ with $A_{\mathbf{r},2}=A_{\mathbf{r},3}=1$ matter (this means that $D_{\mathbf{r},2}=D_{\mathbf{r},3}=1$). Then, as in §6.5, we glue back these sums, with an admissible error term. In doing so, we exhibit a main term $\Lambda_1^{\text{MT}}(X,k)$, which can directly be seen by imposing $D_{\mathbf{r},2}=D_{\mathbf{r},3}=1$ in (151)). This main term $\Lambda_1^{\text{MT}}(X,k)$ is equal to $\Lambda_2^{\text{MT}}(X,k)$ (see (146)). This finishes the proof of Proposition 17.

References

[1] J. Brüdern, Einführung in die analytische Zahlentheorie. *Springer–Lehrbuch*, 1995.

[2] P.G.L. Dirichlet, Vorlesungen über Zahlentheorie, Chelsea Publishing Co., New York, 1968.

[3] E. Fouvry and J. Klüners, On the 4–rank of class groups of quadratic number fields. *Inv. math.*, 167 : 455–513, 2007.

[4] E. Fouvry and J. Klüners, On the negative Pell equation. to appear in Annals of Math., 2008.

[5] G.H. Hardy and S. Ramanujan, The normal number of prime factors of a number *n. Quart. J. of Math.*, 48 : 76–92, 1920. see also *Collected works of G. H. Hardy* (Oxford University Press) vol II : 100–113, 1967.

[6] H. Hasse, Number Theory, *Grundlehren der mathematischen Wissenschaften*, 229, Springer, 1978.

[7] D.R. Heath–Brown, The size of Selmer groups for the congruent number problem, II *Inv. math.*, 118 : 331–370, 1994.

[8] D.R. Heath–Brown, A mean value estimate for real character sums. *Acta Arith.*, 72 : 235–275, 1995.

[9] H. Heilbronn, On the averages of some arithmetic functions of two variables. *Mathematika*, 5 : 1–7, 1958.

[10] K. Ireland and M. Rosen, A classical introduction to modern number theory (Second edition). *Graduate texts in Mathematics*, 84, Springer, 1990.

[11] H. Iwaniec and E. Kowalski, Analytic Number Theory. *Colloquium Publications*, 53, AMS, 2004.

[12] M. Jutila, On mean values of Dirichlet polynomials with real characters. *Acta Arith.* 27 : 191–198, 1975.

[13] F. Lemmermeyer, The 4–class group of real quadratic number fields. Preprint. http://www.ruszer.uni-heidelberger.de/∼hb3/rank4.ps

[14] L.J. Mordell, Diophantine Equations. Academic Press, London and New York, 1969.

[15] L. Redei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren invariantender absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.* 171 : 55–60, 1934.

[16] L. Redei, Eine obere Schranke der Anzahl der durch vier teilbaren invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.* 171 : 61–64, 1934.

[17] L. Redei, Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.* 171 : 131–148, 1934.

[18] L. Redei, Über die Pellsche Gleichung $t^2 - du^2 = -1$. *J. Reine Angew. Math.* 173 : 193–221, 1935.

[19] L. Redei and H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. *J. Reine Angew. Math.* 170 : 69–74, 1933.

[20] H. Reichardt, Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.* 170 : 75–82, 1933.

[21] A. Scholz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, Math. Z. **39**, 95–111 (1935).

[22] W. Sierpinski, Elementary Theory of numbers. *PWN–Polish Scientific Publishers, Warszawa*, 1987.

[23] P. Stevenhagen, The number of real quadratic fields with units of negative norms. *Experiment. Math.*, 2: 121–136, 1993.

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

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

Mathematisches Institut, Heinrich–Heine–Universität, Universitätstr. 1, 40225 Düsseldorf, Germany.

E-mail address: klueners@math.uni-duesseldorf.de