ON THE NEGATIVE PELL EQUATION

ÉTIENNE FOUVRY AND JÜRGEN KLÜNERS

Abstract. We give asymptotic upper and lower bounds for the number of squarefree d ($0 < d \leq X$) such that the equation $x^2 - dy^2 = -1$ is solvable. These estimates, as usual, can equivalently be interpreted in terms of real quadratic fields with a fundamental unit with norm -1 and give strong evidence in the direction of a conjecture due to P. Stevenhagen.

1. Statement of the results

Let D be a fundamental discriminant, i.e. the discriminant of a quadratic extension of $\mathbb{Q}$ and let d be the unique squarefree number such that $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$. In other words, d is defined by

$$d = \begin{cases} D & \text{if } D \text{ is odd,} \\ D/4 & \text{if } D \text{ is even.} \end{cases} \tag{1}$$

A well known equation is the so–called *Pell equation*

$$x^2 - dy^2 = 1 \text{ with } x,\, y \in \mathbb{Z}.$$

The problem of finding non trivial solutions of this equation has a long history, see e.g. [41]. Nowadays it is known that there are non trivial solutions for all squarefree $d > 1$. In this work we are interested in the so–called *negative Pell equation*

$$x^2 - dy^2 = -1 \text{ with } x,\, y \in \mathbb{Z}. \tag{2}$$

It is easy to see that this equation has no solution for negative d. For the rest of this work we assume that we are dealing with real quadratic fields, i.e. $d,\, D > 1$.

A solution of (2) gives a fundamental unit with norm -1 of the order $\mathbb{Z}[\sqrt{d}]$ and vice versa. The index of $\mathbb{Z}[\sqrt{d}]$ in its maximal order $\mathcal{O}_D$ (ring of integers of the field $\mathbb{Q}(\sqrt{D})$) is 1 or 2. Therefore the index of the group of units $\mathbb{Z}[\sqrt{d}]^*$ in $\mathcal{O}_D^*$ is 1 or 3. Thus the solvability of the negative Pell equation (2) is equivalent to the fact that the fundamental unit ϵ_D of $\mathbb{Q}(\sqrt{D})$ satisfies $\mathcal{N}(\epsilon_D) = -1$, where $\mathcal{N}$ is the norm of elements of this field. By convention, we have chosen the fundamental unit ϵ_D such that $\epsilon_D > 1$.

Let X be a large positive real number. We are interested in the number of squarefree integers $d < X$ such that the negative Pell equation (2) is solvable. By (1), such a question is equivalent to count the number of fundamental D such that $\mathcal{N}(\epsilon_D) = -1$. We easily get further restrictions on these d (or D). Let p be a prime dividing d. By reducing (2) modulo that p, we get

$$x^2 \equiv -1 \bmod p.$$

Date: February 18, 2009.

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

The latter equation is only solvable for $p = 2$ or $p \equiv 1 \bmod 4$ which means that the negative Pell equation is not solvable for d or D with a prime divisor congruent to 3 mod 4. Therefore it makes sense to introduce the set of *special discriminants*

$$\mathcal{D} = \big\{D > 0 \text{ fundamental discriminant} : p \mid D \Rightarrow p \equiv 1 \text{ or } 2 \bmod 4\big\},$$

which is the disjoint union of the two subsets

$$\mathcal{D}_{\mathrm{odd}} = \big\{D \in \mathcal{D} :\ D \equiv 1 \bmod 4\big\},$$

and

$$\mathcal{D}_{\mathrm{even}} = \big\{D \in \mathcal{D} :\ D \equiv 0 \bmod 8\big\}.$$

For $X > 1$, we denote by $\mathcal{D}(X)$ the counting function of the set $\mathcal{D}$, that means the cardinality of $\mathcal{D} \cap [0, X]$. The same applies to $\mathcal{D}_{\mathrm{odd}}(X)$ and $\mathcal{D}_{\mathrm{even}}(X)$. The asymptotic behavior of these functions is known (for instance see [36, Satz 3] or [40, p. 122]):

$$\mathcal{D}(X) \sim c_1 \cdot \frac{X}{\sqrt{\log X}},$$

$$\mathcal{D}_{\mathrm{odd}}(X) \sim \frac{8}{9} \cdot c_1 \cdot \frac{X}{\sqrt{\log X}},$$

and

$$\mathcal{D}_{\mathrm{even}}(X) \sim \frac{1}{9} \cdot c_1 \cdot \frac{X}{\sqrt{\log X}},$$

where

$$c_1 = \frac{9}{8\pi} \prod_{p \equiv 1 \bmod 4} \big(1 - p^{-2}\big)^{\frac{1}{2}}.$$

These formulas are variations of a classical theorem of Landau on the integers which are sums of two squares (see [2, Satz 1.8.2] for instance) and are consequences of the analytic properties of the function $\zeta^{-\frac{1}{2}}(s) \prod_{p \not\equiv 3 \bmod 4}(1 - p^{-s})$. In an equivalent manner, by applying (1), we get

$$\sharp\big\{d :\ 1 \le d \le X,\ d \text{ squarefree},\ p \mid d \Rightarrow p = 2 \text{ or } p \equiv 1 \bmod 4\big\} \sim \mathcal{X}, \tag{3}$$

where

$$\mathcal{X} = \frac{4}{3} \cdot c_1 \cdot \frac{X}{\sqrt{\log X}}. \tag{4}$$

It is now a canonical question to ask if it is often, for a special D, to satisfy $\mathcal{N}(\epsilon_D) = -1$. In other words we introduce the counting function

$$\mathcal{D}^-(X) = \sharp\big\{D \in \mathcal{D} :\ 0 < D < X,\ \mathcal{N}(\epsilon_D) = -1\big\},$$

in order to compare it with $\mathcal{D}(X)$. An analogous question concerns the functions $\mathcal{D}^-_{\mathrm{odd}}(X)$, $\mathcal{D}^-_{\mathrm{even}}(X)$. In the statement of our results, we shall frequently meet the constant

$$\alpha := \prod_{j \text{ odd}} (1 - 2^{-j}) = \prod_{j=1}^{\infty} (1 + 2^{-j})^{-1} = .4194224417951\cdots \tag{5}$$

After the construction of an interesting and solid probabilistic model, P. Stevenhagen was led to the following conjectures:

Conjecture 1. [40, Conj. 1.4 & 3.4] *As $X \to \infty$, we have*

$$\mathcal{D}^-(X) \sim (1-\alpha)\,\mathcal{D}(X),$$
$$\mathcal{D}^-_{\mathrm{odd}}(X) \sim (1-\alpha)\,\mathcal{D}_{\mathrm{odd}}(X),$$

and

$$\mathcal{D}^-_{\mathrm{even}}(X) \sim (1-\alpha)\,\mathcal{D}_{\mathrm{even}}(X).$$

Note that the extension of this conjecture to the sets $\mathcal{D}_{\mathrm{odd}}$ and $\mathcal{D}_{\mathrm{even}}$ implicitly appears in [40, p. 123, 2nd col.]. Stevenhagen [40, p. 122] comments this conjecture as follows "*As it stands, this is a basic but very hard problem...*" Appealing to (1), (3) and (4) Stevenhagen also proposed:

Conjecture 2. [40, Conj. 1.2] *The number of positive squarefree $d \le X$ for which the negative Pell equation* (2) *is solvable is asymptotic to*

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

We recall a well known criterion to detect whether the fundamental unit of $\mathbb{Q}(\sqrt{d})$ has norm 1 or -1. This norm is -1 if and only if the period of the expansion of $\sqrt{d}$ in continued fractions is odd, e.g. see [31, Theorem 3.11]. However, we have the feeling that this criterion is useless to prove asymptotic results. Our main result is

Theorem 1. *For $X \to \infty$, we have the inequalities*

$$(\alpha - o(1))\,\mathcal{D}(X) \le \mathcal{D}^-(X) \le \left(\frac{2}{3} + o(1)\right)\,\mathcal{D}(X).$$

Similar inequalities hold for $\mathcal{D}^-_{\mathrm{odd}}(X)$ and $\mathcal{D}^-_{\mathrm{even}}(X)$.

We can summarize our result in familiar words as follows: *Stevenhagen conjectures that about 58% of the special D satisfy $\mathcal{N}(\epsilon_D) = -1$. We prove that this percentage is between 41% and 67%.* By (1), (3) and (4) we easily deduce

Corollary 1. *For $X \to \infty$ we have the inequalities*

$$(\alpha - o(1)) \cdot \mathcal{X} \le \sharp\left\{1 \le d \le X : d \text{ squarefree and } (2) \text{ is solvable }\right\} \le (\frac{2}{3} + o(1)) \cdot \mathcal{X}.$$

As in Theorem 1 the inequalities of Corollary 1 remain true, if we restrict the counting functions to odd squarefree d or even squarefree d, respectively. Since the set $\{d : d \text{ squarefree}, p \mid d \Rightarrow p \equiv 1 \bmod 4\}$ has a positive density in the set $\{d : p \mid d \Rightarrow p \equiv 1 \bmod 4\}$, we easily deduce that the equation $x^2 - dy^2 = -1$ is solvable for a positive proportion of d composed entirely of prime factors congruent to 1 modulo 4. This is exactly the content of a conjecture of Hooley (see [23, Conj. 5, p. 118]).

As far as we know, for the lower bound, the best results were of the type $\mathcal{D}^-(X) \gg_k X(\log\log X)^k/\log X$ for any positive integer k, (see [40, Cor. 4.2]) and quite recently $\mathcal{D}^-(X) \gg X/(\log X)^{.62}$, due to V. Blomer [1]. For the upper bound, nothing non trivial was known on $\limsup \mathcal{D}^-(X)/\mathcal{D}(X)$ before our result (see the comment [40, p. 122, 2nd col.]).

Theorem 1 is ineffective in both aspects: lower and upper bounds. This lacuna means that, being given real numbers η_1 and η_2 satisfying $0 < \eta_1 < \alpha$ and $2/3 < \eta_2 < 1$, our proof does not give an explicit value of X_1 and X_2, such that, for $X \ge X_1$, we have $\mathcal{D}^-(X) \ge \eta_1\,\mathcal{D}(X)$ and for $X > X_2$, we have $\mathcal{D}^-(X) \le \eta_2\,\mathcal{D}(X)$. The origin of this inefficiency is the Siegel–Walfisz Theorem (see Lemma 30 and Proposition 7).

1.1. **How to attack Theorem 1.** For its proof, we neglect the approach via the Pell equation itself, we prefer the interpretation of this question via the comparison of the *ordinary class group* Cl_D and the *narrow class group* C_D. Let us collect here some well known results. For more details we refer the reader to §3.1. We have the following exact sequence of groups

$$\{1\} \to F_\infty \to \mathrm{C}_D \to \mathrm{Cl}_D \to \{1\}, \tag{6}$$

where $F_\infty \leq \mathbb{Z}/2\mathbb{Z}$. Furthermore $|F_\infty| = 2$ if and only if $D > 0$ and $\mathcal{N}(\epsilon_D) = 1$ (see e.g. [31, Corollary 2, p. 112]).

Hence the equality $\mathcal{N}(\epsilon_D) = -1$ is equivalent to the isomorphism of the groups

$$\mathrm{C}_D \cong \mathrm{Cl}_D. \tag{7}$$

We recall:

Lemma 1. *Let $D > 0$ be a discriminant with $|F_\infty| = 2$. Then the following two statements are equivalent:*

- $\mathrm{C}_D \cong \mathbb{Z}/2\mathbb{Z} \times \mathrm{Cl}_D$,
- *there exists a prime $p \mid D$ such that $p \equiv 3 \bmod 4$.*

In this case we have: $\mathrm{C}_D^2 \cong \mathrm{Cl}_D^2$.

The statement of Lemma 1 can be found in the literature at several places: [16, p. 518], (with Hasse's notation we have $g^+ = 2^{\mathrm{rk}_2(\mathrm{C}_D)}$ and $g = 2^{\mathrm{rk}_2\mathrm{Cl}_D}$), [4, Table 14.1, p. 142], [29, Thm 8], and [27, Thm 6.9] (with a proof based on K-theory). However, in some other places this statement appears in an uncorrect form or with a non convincing proof. Using this lemma it is clear that $D > 0$ belongs to $\mathcal{D}$ if and only if $\mathrm{rk}_2(\mathrm{C}_D) = \mathrm{rk}_2(\mathrm{Cl}_D)$. Here the p–rank of a finite multiplicative abelian group A is denoted by $\mathrm{rk}_p(A) (= \dim_{\mathbb{F}_p} A/A^p)$. The 4–rank is denoted by $\mathrm{rk}_4(A) = \mathrm{rk}_2(A^2)$, by definition, and more generally, we define the 2^k–rank by $\mathrm{rk}_{2^k}(A) := \mathrm{rk}_2(A^{2^{k-1}})$. Using this terminology and equation (6) we get for all fundamental discriminants:

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

Using Lemma 1 and (7) we get for special discriminants $D \in \mathcal{D}$:

$$\mathcal{N}(\epsilon_D) = -1 \ \Leftrightarrow \ \mathrm{rk}_{2^k}(\mathrm{C}_D) = \mathrm{rk}_{2^k}(\mathrm{Cl}_D) \ \forall k \geq 2. \tag{9}$$

However, this last equality is too difficult for a general approach by analytic methods. Hence we shall only play with the 4–rank ($k = 2$). Actually, the good numerical quality of the constants appearing in Theorem 1 is due to the fact that the main contribution comes from what happens with the 4–rank. Approaching to Stevenhagen's constant $(1-\alpha)$ in Theorem 1 would require to play with the 8–rank, the 16–rank, and so on. To prove the lower bound announced in Theorem 1, we use the fact that the function $k \mapsto \mathrm{rk}_{2^k}(\mathrm{C}_D)$ is positive and decreasing to deduce

Lemma 2. *Let $D \in \mathcal{D}$ such that $\mathrm{rk}_4(\mathrm{C}_D) = 0$. Then we have $\mathcal{N}(\epsilon_D) = -1$.*

For the upper bound, we use the following lemma.

Lemma 3. *Let $D \in \mathcal{D}$ such that $\mathcal{N}(\epsilon_D) = -1$. Then we have the equality*

$$\mathrm{rk}_4(\mathrm{Cl}_D) = \mathrm{rk}_4(\mathrm{C}_D).$$

Hence, our way of attacking Theorem 1 is reduced to the distribution of the functions $\mathrm{rk}_4(\mathrm{C}_D)$ and $\mathrm{rk}_4(\mathrm{Cl}_D)$.

1.2. **Results concerning the** 4**–ranks of class groups.** Let a and b be two non negative integers. We denote by $\delta(a,b)$, if it exists, the real number

$$\delta(a,b) := \lim_{X\to\infty} \frac{\sharp\{D\in\mathcal{D}\,:\, D<X,\, \mathrm{rk}_4(\mathrm{C}_D)=a \text{ and } \mathrm{rk}_4(\mathrm{Cl}_D)=b\}}{\mathcal{D}(X)}.$$

Similarly, we define $\delta_{\mathrm{odd}}(a,b)$ and $\delta_{\mathrm{even}}(a,b)$. As in [40] we introduce the function

$$\alpha_\infty(r) := \frac{\alpha}{\prod_{j=1}^{r}(2^j-1)}, \tag{10}$$

defined for any integer $r\geq 0$. We shall prove

Theorem 2. *The real number $\delta(a,b)$ exists for all non negative integers a and b, and satisfies*

$$\delta(a,b)=\begin{cases} 0 & \text{if } 0\leq a<b,\\ 0 & \text{if } 0\leq b<a-1,\\ 2^{-a}\cdot\alpha_\infty(a) & \text{if } a=b,\\ (1-2^{-a})\cdot\alpha_\infty(a) & \text{if } a=b+1.\end{cases} \tag{11}$$

Similar statements are true for $\delta_{\mathrm{odd}}(a,b)$ and $\delta_{\mathrm{even}}(a,b)$.

The first two cases of (11) are direct consequences of (8). From Theorem 2 we easily deduce

Corollary 2. *For any integer $r\geq 0$ and for $X\to\infty$ we have*

$$\sharp\left\{D\in\mathcal{D}\,:\, D<X,\ \mathrm{rk}_4(\mathrm{C}_D)=r\right\}\sim\alpha_\infty(r)\cdot\mathcal{D}(X),$$

and

$$\sharp\left\{D\in\mathcal{D}\,:\, D<X,\ \mathrm{rk}_4(\mathrm{Cl}_D)=r\right\}\sim 3\cdot 2^{-r-1}\alpha_\infty(r)\cdot\mathcal{D}(X).$$

The same relations are true when we replace $\mathcal{D}$ by $\mathcal{D}_{\mathrm{odd}}$ or $\mathcal{D}_{\mathrm{even}}$.

Proof. Compute $\delta(r,r)+\delta(r,r-1)$ and $\delta(r,r)+\delta(r+1,r)$. □

Now we deduce Theorem 1 from Theorem 2.

Proof of Theorem 1. Combining Lemma 2 with the first part of Corollary 2 corresponding to the case $r=0$, we obtain the minoration of $\mathcal{D}^-(X)$ announced in Theorem 1.

For the upper bound of $\mathcal{D}^-(X)$ we proceed as follows. Lemma 3 and (8) imply that, for every integer $R\geq 1$, we have the lower bound

$$\mathcal{D}(X)-\mathcal{D}^-(X)\geq\sum_{r=1}^{R}\sharp\left\{D\in\mathcal{D}\,:\,0<D<X,\,\mathrm{rk}_4(\mathrm{C}_D)=r \text{ and } \mathrm{rk}_4(\mathrm{Cl}_D)=r-1\right\}.$$

From (11) we deduce for every positive η, and $X\geq X_0(R,\eta)$ the inequality

$$\mathcal{D}(X)-\mathcal{D}^-(X)\geq\Big(-\eta+\sum_{r=1}^{R}\delta(r,r-1)\Big)\mathcal{D}(X).$$

Since $\sum_r(\delta(r,r)+\delta(r,r-1))=1$, the above inequality is equivalent to

$$\begin{aligned}\mathcal{D}^-(X) &\le \Big(1+\eta-\sum_{r=1}^{R}\delta(r,r-1)\Big)\mathcal{D}(X)\\ &\le \Big(\eta+\sum_{r=0}^{R}\delta(r,r)+\sum_{r=R+1}^{\infty}(\delta(r,r)+\delta(r,r-1))\Big)\mathcal{D}(X).\end{aligned}$$

By letting $\eta\to 0$ and $R\to\infty$ we obtain the upper bound announced in Theorem 1 after writing the list of equalities

$$\begin{aligned}\sum_{r=0}^{\infty}\delta(r,r) &= \alpha\sum_{r\ge 0}2^{-r}\prod_{j=1}^{r}(2^j-1)^{-1}\\ &= \alpha\sum_{r=0}^{\infty}\frac{(1/2)^r\ (1/2)^{\frac{r(r+1)}{2}}}{(1-(1/2))(1-(1/2)^2)\cdots(1-(1/2)^r)}\\ &= \alpha\prod_{j=1}^{\infty}\big(1+(1/2)^{j+1}\big)\\ &= \frac{2}{3}\cdot\big(\alpha\cdot(1+\frac{1}{2})(1+\frac{1}{4})(1+\frac{1}{8})\cdots\big)=\frac{2}{3}.\end{aligned}$$

The third equality is a consequence of Lemma 4 (with $t=u=1/2$) and the last one is a consequence of the definition (5) of α. □

Finally, it is time to further push the comment after (9) and to explain the rather good quality of the inequalities contained in Theorem 1 compared with the weakness of the criteria contained in Lemmata 2 and 3. The origin is due to the fact as $r\to\infty$, the density $\alpha_\infty(r)$ goes to 0 very quickly. In other words, we easily get that $(\log\alpha_\infty(r))/\log 2\sim -(r^2/2)$, as $r\to\infty$. Hence most of the cases D with $\mathcal{N}(\epsilon_D)=-1$ correspond to D with a very small value of $\mathrm{rk}_4(\mathrm{C}_D)$.

Our technique is optimal to give the asymptotic cardinalities of the sets of special D such that $\mathrm{rk}_4(\mathrm{C}_D)=0$ or such that $\mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{Cl}_D)$. Using this we are able to exhibit the bounds written in Theorem 1. On the other hand, our method is inoperative to attack the cases, where a study of the 8–rank, (or 16–rank,...) is required. In order to illustrate this matter of further investigations, we think that, to improve the constant α appearing in Theorem 1, the first natural step will certainly be to incorporate the density, if it exists, of the set of the special D satisfying

$$\mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{Cl}_D)=1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D)=0.$$

We expect that this set has density $\alpha/4$, which would improve the coefficient of the lower bound from α to $5\alpha/4=0.524278\ldots$. In the opposite direction, to improve the constant $2/3$ in the upper bound of the same theorem, the first step would be to subtract the density of the subset of the special D such that

$$\mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{Cl}_D) \text{ and } \mathrm{rk}_8(\mathrm{C}_D)=\mathrm{rk}_8(\mathrm{Cl}_D)+1.$$

1.3. **Remarks concerning Corollary 2.** The first part of this corollary proves that the probability for a special discriminant to have its 4–rank equal to r is $\alpha_\infty(r)$. This value exactly fits to the value predicted by Stevenhagen [40, Conj 3.4(ii)], but it is quite different from the probability for a positive fundamental discriminant to

have its 4–rank equal to r, since by [11, Theorem 3] and [10, Corollary 1], we know that this probability is equal to

$$2^{-r(r+1)}\frac{\prod_{j=1}^{\infty}(1-2^{-j})}{\prod_{j=1}^{r}(1-2^{-j})\prod_{j=1}^{r+1}(1-2^{-j})}. \tag{12}$$

This distortion between *special* and *fundamental* discriminants can be easily explained by the fact that if D belongs to $\mathcal{D}$, then every odd and coprime divisors D_0 and D_3 of D are congruent to 1 mod 4, hence, by the quadratic reciprocity law for Jacobi symbols, the product

$$(-1/D_3)(D_0/D_3)(D_3/D_0), \tag{13}$$

in Lemmata 10 & 11, is equal to 1 and provides no oscillation. In other words the function $\mathrm{rk}_4(\mathrm{C}_D)$ has on average a tendency to be larger when D is special than when it is fundamental and positive (see the comment after Theorem 3).

We remark that Theorem 2 is a first step in the direction of proving [40, Conj 3.4(i)].

Corollary 3. *For every integer $e \geq 0$, we have the inequality*

$$\limsup_{X\to\infty}\frac{\sharp\{D\leq X, D\in\mathcal{D}^-, \mathrm{rk}_4(\mathrm{C}_D)=e\}}{\sharp\{D\leq X, D\in\mathcal{D}, \mathrm{rk}_4(\mathrm{C}_D)=e\}}\leq\frac{1}{2^e}.$$

Proof. Using Theorem 2 we get that in $1/2^e$ of the cases, the 4–ranks of the ordinary and the narrow class groups coincide. By Lemma 3 the set of these cases contains the cases, where the negative Pell equation is solvable. □

We remark that the bound is sharp in the case $e = 0$. For $e \geq 1$ we get an upper bound of the conjectured density $\frac{1}{2^{e+1}-1}$.

The result (12) (and more generally [11]) can be seen as the first significative evidence sustaining the truth of the so called *Cohen–Lenstra heuristics* [3] (extended by Gerth [13] to the 4–rank) which predict the average behavior of the group C_D, when D goes all over the set of positive fundamental discriminants and of negative fundamental discriminants. Since C_D^2 and Cl_D^2 may be different only when D belongs to $\mathcal{D}$, and since $\mathcal{D}$ is a negligible subset of the set of fundamental discriminants (in terms of cardinalities), the average behavior of the 2–part of Cl_D^2 is not covered by the heuristics of Cohen–Lenstra–Gerth as written in [3] and [13].

1.4. **Results on moments.** The usual way to attack the distribution law of an arithmetic function is to compute the integral moments of this function and then hope to deduce this law from the values of these moments. For the case of the function $D\in\mathcal{D}\mapsto \mathrm{rk}_4(\mathrm{C}_D)$, we rather work with the function $D\in\mathcal{D}\mapsto 2^{\mathrm{rk}_4(\mathrm{C}_D)}$ which has a more natural algebraic interpretation (see Proposition 2 below). In §7 and 9 (Propositions 11 & 13), we shall prove

Theorem 3. *For every integer $k \geq 0$ and for every positive ϵ we have*

$$\sum_{D\in\mathcal{D},\, D\leq X} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)} = \prod_{j=0}^{k-1}(2^j+1)\cdot\mathcal{D}(X)+O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big)$$

uniformly for $X \geq 3$. The same relations are true when we replace $\mathcal{D}$ by $\mathcal{D}_{\mathrm{odd}}$ or $\mathcal{D}_{\mathrm{even}}$.

There exists a corresponding expansion for the sum $2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}$ over all fundamental discriminants $0 < D < X$ (see [11, Theorems 7, 9 & 11]). In that case, the coefficient of the main term is equal to

$$\frac{1}{2^k}\big(\mathbf{N}(k+1,2) - \mathbf{N}(k,2)\big), \tag{14}$$

where $\mathbf{N}(k,2)$ is the total number of vector subspaces of $\mathbb{F}_2^k$. In order to measure the size of this coefficient we write it in the form 2^{ν_k}. Then we easily see that $\nu_k \sim \frac{k^2}{4}$ as k tends to infinity. However, by Theorem 3 the corresponding ν_k in the case of special discriminants is $\sim \frac{k^2}{2}$. This shows, that on average, $\mathrm{rk}_4(\mathrm{C}_D)$ is significantly larger when D is special than when D is fundamental and positive.

Since Theorem 2 concerns the joint distribution of the functions $D \in \mathcal{D} \mapsto (\mathrm{rk}_4(\mathrm{C}_D), \mathrm{rk}_4(\mathrm{Cl}_D))$, we would be obliged to compute the mixed moments $2^{k\,\mathrm{rk}_4(\mathrm{C}_D)} \cdot 2^{\ell\,\mathrm{rk}_4(\mathrm{Cl}_D)}$ for all k and $\ell \geq 0$. However, the inequalities (8) (for the 4-rank) imply that in addition to the moments computed in Theorem 3, we only require to compute one mixed moment. This remark avoids a huge amount of work (see formula (100)). In §8 and §10 we will prove

Theorem 4. *For every integer $k \geq 0$ and for every positive ϵ we have*

$$\begin{aligned}\sum_{D\in\mathcal{D},\, D<X} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)} \cdot 2^{\mathrm{rk}_4(\mathrm{Cl}_D)} =& (2^{k-1}+1)\cdot \prod_{j=0}^{k-1}(2^j+1)\cdot \mathcal{D}(X)\\ &+ O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big)\end{aligned}$$

uniformly for $X \geq 3$. The same relations are true when we replace $\mathcal{D}$ by $\mathcal{D}_{\mathrm{odd}}$ or $\mathcal{D}_{\mathrm{even}}$.

Comparing this result with the asymptotic expansion written in Theorem 3 (with the parameter $k+1$), once again, we see that $\mathrm{rk}_4(\mathrm{Cl}_D)$ is oftenly strictly smaller than $\mathrm{rk}_4(\mathrm{C}_D)$.

1.5. **Organization of the paper.** In the introduction we presented the results and reduced the proofs of everything to the proof of Theorems 2, 3 & 4. In §2 we will show how to prove Theorem 2, when we assume Theorems 3 & 4. In the rest of the paper we will prove those theorems. The proof of Theorem 3 is much easier than the proof of Theorem 4. In case we are only interested in the proof of Theorem 3, we can skip the study of §3–6. In those sections we recall some results already given in [11] and generalize them in a way that they can be used for proving Theorem 4. For the study of Theorem 3 we only use Lemmata 10 and 11 from §3. From §5 and 6 we use Lemma 30 (Siegel-Walfisz) and Lemma 33 (double oscillation). Using these tools Theorem 3 is then proved in §7 (odd discriminants) and §9 (even discriminants).

The main difference in the proofs of Theorems 3 and 4 comes from the fact that the algebraic criterion for the 4–rank of the ordinary class group is much more complicated than the criterion of the narrow class group. The latter one can be described by a suitable product of Jacobi–symbols (see Lemmata 10 and 11), where the first one additionally needs the square of quartic characters over $\mathbb{Z}[i]$ (see Theorem 6). The goal of §3 is to prove Theorem 5. In §4 we collect properties of quartic residue symbols. Using those we can reformulate Theorem 5 in a way which can be used for counting purposes and the result is Theorem 6.

In the analytic part we make heavy use of oscillation of characters. Here we use two important tools, namely Siegel-Walfisz theorems and double oscillation. In §5 we recall in Lemma 30 the Siegel–Walfisz theorem for primitive Dirichlet characters. The main result of this section is the proof of the corresponding result for squares of quartic characters (see Proposition 7).

The same story applies for the double oscillation of characters in §6. In Lemma 33 we recall the corresponding result for Jacobi symbols. Again, we prove a corresponding version for the square of quartic characters in Proposition 9.

In §7 (odd discriminants) and §9 (even discriminants) we prove Theorem 3. Finally we prove Theorem 4 in §8 and §10.

The structure of those four paragraphs is very similar. Therefore we only give an overview of what happens in §7.

In §7.1 we introduce the functions κ_1 and κ_k which allow us to express the k-th moment $2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}$ in a clever way. The function κ_k appears as an exponent of any possible Jacobi symbol. It takes the values 0 or 1 and so detects which Jacobi symbols appear and which do not. The result is given in Lemma 36. In the following subsections we want to compute the asymptotic behavior of this function.

In §7.2 we start with the first preparations of the summation. In a first step we can restrict to those discriminants which do not have too many prime factors, see the discussion before formula (61) for the precise formulation. By introducing the dissection parameter $\Delta := 1 + (\log X)^{-2^k}$ we are allowed to split our sum in many small pieces, see (62), (63), and (64), which we can analyze separately. These pieces are parametrized by $\mathbf{A} = (A_{\mathbf{r}})$. In formulas (66) and (67) we show that we can get rid of the constraint $\prod D_{\mathbf{r}} \leq X$ and make the variables independent this way. In [11, p.47, (33)] this was the first family. In Lemma 38 we prove that we can ignore the contribution of all $\mathbf{A}$ such that at most $2^k - 1$ of the $A_{\mathbf{r}}$ are bigger than some constant $X^{\ddagger}$ defined in (70). In the proof of this lemma we use a result of Shiu (Lemma 37) in order to get a sufficiently good error bound. In [11, p. 475] this was the second family. We remark that this is the only place for the error term, where we have to use the fact that we deal with special discriminants. Certainly, we have to use properties of special discriminants, when we compute the main term.

In §7.3 we introduce the notion of *linked indices* (this notion was introduced by Heath-Brown in [17] and already exploited in [11]). The goal is that we want to find other families which disappear in the error term. In §5 and §6 we prepared Siegel-Walfisz and double oscillation techniques which we want to apply here. When two indices $\mathbf{r_0}$ and $\mathbf{s_0}$ are linked, we can use the oscillation of the symbol $\left(\frac{D_{\mathbf{r_0}}}{D_{\mathbf{s_0}}}\right)$ in order to prove that some families disappear in the error term. In §7.4 we apply Lemma 33 (double oscillation) to suitable linked indices. This was the third family in [11, p. 476]. In §7.5 we apply Lemma 30 (Siegel-Walfisz) to suitable linked indices. We remark that during the proof of this step we use the fact that we bounded the number of prime factors of our discriminants. In [11, p.476] this was our fourth family. After having done all this work we arrive at Lemma 39. In condition (83) of this lemma the remaining cases are listed which we have to consider in the following paragraphs. This condition has to be compared with [11, (48)].

The goal of the final two subparagraphs is to compute the main term. We have to interpret condition (83) in more geometric terms in order to compute it efficiently. As in [17] we are confronted with with questions of geometry in characteristic 2. In §7.6 we introduce in (84) a quadratic form P_k defined over $\mathbb{F}_2^{2k}$. It turns out to be

that it is of great interest to us to find maximal subspaces of $\mathbb{F}_2^{2k}$ which consist only of vectors which are pairwise unlinked. These spaces correspond (see Lemmata 40 and 41) to subspaces of $\mathbb{F}_2^{2k}$ on which the quadratic form $P_k \equiv 0$ vanishes identically. As a result we get that our main term heavily depends on the number of maximal unlinked vector subspaces of $\mathbb{F}_2^{2k}$ in Lemma 42. Finally, by using the theory of quadratic forms in characteristic 2, we compute this number in §7.7.

1.6. **Differences to the case of fundamental discriminants.** We already mentioned that many of the analytic tools already appear in [11], where we determined the asymptotic behavior of the 4–rank of the narrow class group of quadratic number fields. The proof of Theorem 3 is very similar, because it only deals with the narrow class group. The main difference is that we only look at special discriminants, which has the following two effects:

(i) The number of special discriminants smaller than X behaves like $c_1 \frac{X}{\sqrt{\log X}}$.
(ii) Many Jacobi symbols become trivial for special discriminants.

When we look at all real quadratic number fields, the contribution of special discriminants disappear in the error term. The second difference is that for special discriminants many Jacobi symbols become trivial and the formula for the 4–rank of the narrow class group simplifies (see Lemmata 10 and 11), e.g. the formula for odd $D > 0$

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2 \cdot 2^{\omega(D)}} \sum_{D = D_0 D_1 D_2 D_3} \left(\frac{-1}{D_3}\right)\left(\frac{D_2}{D_0}\right)\left(\frac{D_1}{D_3}\right)\left(\frac{D_0}{D_3}\right)\left(\frac{D_3}{D_0}\right)$$

simplifies for $D \in \mathcal{D}_{\mathrm{odd}}$ to the equality

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2 \cdot 2^{\omega(D)}} \sum_{D = D_0 D_1 D_2 D_3} \left(\frac{D_0}{D_2}\right)\left(\frac{D_1}{D_3}\right).$$

As usual $\omega(D)$ is the number of distinct prime factors of D. In order to deal with the k-th moment of those functions this expression has to be raised to the k-th power. In order to avoid a combinatorial nightmare, we use an idea of Heath–Brown to describe the right possibilities by quadratic forms in characteristic 2. Because of the different nature of the above mentioned formulas for the 4–rank, the description is different. In [11, p. 471] we can describe the exponent function Φ_1 by a polynomial. Here we have to use an abstract function κ_1 defined in (54). When we come to the definition of linked indices, amazingly in both cases we can use the same quadratic form over $\mathbb{F}_2^k$, see (84) and compare it with the quadratic form P defined in [11, p. 473]. Nevertheless, we get different constants due to the fact that the above mentioned formulas for the 4–rank of the narrow class group are different. In both cases we have to count maximal unlinked vector spaces of $\mathbb{F}_2^{2k}$ on which $P_k \equiv 0$, but in the case of [11] these subspaces must satisfy the extra condition that some bilinear form over $\mathbb{F}_2^{2k}$ is identically equal to 0. This explains why the coefficient (14) of the main term of [11, Theorem 7] is smaller than the corresponding one in Theorem 3 and quantitatively shows the effect of the oscillations due to the extra factor (13).

The biggest differences occur when we prove Theorem 4. Since the criterion for the ordinary class group is much more complicated and involves quartic symbols, we have to develop the corresponding theory to deal with those. We remark that in the ordinary class group case both types of symbols occur. However, since the function

$2^{\mathrm{rk}_4(\mathrm{Cl}_D)}$ appears with exponent 1, we can connect the combinatorics associated to the mixed moments treated in Theorem 4 to the combinatorics treated in Theorem 3. This is an important gain of work to deal with the main term. In order to summarize we can say that the case of the function $\mathrm{rk}_4(\mathrm{Cl}_D)$ appears to be more involved than the case of $\mathrm{rk}_4(\mathrm{C}_D)$, not only by the required tools coming from algebraic number theory, but also by the fact that analytic number theory is made over the Gaussian integers instead over $\mathbb{Z}$.

Acknowledgements. The authors are grateful to A. Faisant, E. Kowalski, Ph. Michel, and P. Sarnak for interesting conversations about our results.

2. From Theorems 3 & 4 to Theorem 2

2.1. **A first approach.** This paragraph uses analytic and combinatorial methods. The strategy is similar to [10, §4] (see also [17, §8]). Our first step is to work with Theorem 3 only, to deduce, roughly speaking, the value of $\delta(a,a)+\delta(a,a-1)$, without proving the existence of the terms of this sum (for more precisions, see (21) below). In other words, we directly prove the first part of Corollary 2. For $r\geq 0$ and $X\geq 5$, let

$$d(r,X):=\frac{\sharp\big\{D\in\mathcal{D}\,:\;D<X,\mathrm{rk}_4(\mathrm{C}_D)=r\big\}}{\mathcal{D}(X)}.$$

This is the proportion of special discriminants $\leq X$ with 4–rank of the narrow class group equal to r. Let

$$C_k:=\prod_{j=0}^{k-1}(2^j+1).$$

Then we write Theorem 3 in the form

$$\sum_{r=0}^{\infty}d(r,X)\cdot 2^{kr}=C_k+o_k(1)\ (X\to\infty,\ k=0,\,1,\,2,\dots). \tag{15}$$

Applying (15) with k replaced by $k+1$ and using positivity, we obtain

$$d(r,X)\,2^{(k+1)r}=O_k(1),$$

which leads to

$$0\leq d(r,X)=O_k\big(2^{-(k+1)r}\big), \tag{16}$$

uniformly for $X\geq 5$ and $r\geq 0$. Since for all $r\geq 0$ and $X\geq 5$ we have $d(r,X)\in[0,1]$, by an infinite diagonal process, we construct a sequence $(d_i)_{i\geq 0}\in[0,1]$, and an infinite sequence $\mathcal{M}$ of integers m with the property

$$d(r,m)\to d_r\ (m\in\mathcal{M},\ m\to\infty).$$

The relation (16) allows us to apply Lebesgue's dominated convergence theorem to (15). This gives the equality

$$\sum_{r=0}^{\infty}d_r\ 2^{kr}=C_k\ (k=0,\,1,\,2,\dots).$$

Therefore we consider the infinite system of linear equations

$$\sum_{r=0}^{\infty}x_r\ 2^{kr}=C_k\ (k=0,\,1,\,2,\dots). \tag{17}$$

Before we can give a solution to the system (17), we need the following combinatorial tool coming from the theory of partitions (see e.g. [5, formula [5k] p. 105]).

Lemma 4. *We have the formal equality*

$$\prod_{i\geq 1}(1+ut^i) = 1+\sum_{m\geq 1}\frac{u^m t^{\frac{m(m+1)}{2}}}{(1-t)(1-t^2)\cdots(1-t^m)}.$$

Now we can give a solution, where $\alpha_\infty(r)$ is defined in (10).

Lemma 5. *The sequence $x_r = \alpha_\infty(r)$ $(r\geq 0)$ satisfies the system* (17).

Proof. By replacing x_r by $\alpha_\infty(r)$ in the left of (17) we get

$$\sum_{r=0}^{\infty} x_r 2^{kr} = \alpha\sum_{r=0}^{\infty}\frac{2^{kr}}{\prod_{j=1}^{r}(2^j-1)} = \alpha\sum_{r=0}^{\infty}\frac{2^{kr}\cdot 2^{-\frac{r(r+1)}{2}}}{\prod_{j=1}^{r}(1-2^{-j})}.$$

We apply Lemma 4 with the choice $u=2^k$ and $t=1/2$ and get

$$\sum_{r=0}^{\infty} x_r 2^{kr} = \alpha\prod_{i\geq 1}(1+2^{k-i}) = \prod_{j=0}^{k-1}(2^j+1) = C_k,$$

by the definition of α given in (5). □

In order to ensure the unicity of solutions of (17), we appeal to the following lemma, which is proved by Jensen's inequality. We have

Lemma 6. [10, Lemma 6] *Let $\ell\geq 0$ be an integer and $a\in\mathbb{C}$ such that $|a|>1$. Furthermore let $g(z)$ be an entire function which has a zero of order ℓ at $z=0$ and satisfies $g(a^k)=0$ for any $k\geq 0$. Then for every $k\geq 0$ the function $g(z)$ satisfies the inequality*

$$\sup_{|z|=|a|^k}|g(z)| \geq \frac{|g^{(\ell)}(0)|}{\ell!}\cdot|a|^{\frac{k(k+1)}{2}+k\ell}.$$

Now suppose that we have two non negative solutions (x_r) and (x'_r) of (17). By positivity we have the inequalities

$$0\leq x_r,\, x'_r \leq 2^{-kr}C_k, \tag{18}$$

for any k and $r\geq 0$. By the definition of C_k we easily obtain the inequality $C_k\leq c_0\, 2^{\frac{k(k-1)}{2}}$ for an absolute c_0. By choosing $k=r$ in (18) we obtain

$$0\leq x_r,\ x'_r \leq c_0\, 2^{-\frac{r^2}{2}}. \tag{19}$$

Now consider the function

$$g(z) = \sum_{r=0}^{\infty}(x_r - x'_r)z^r \tag{20}$$

of the complex variable z. The radius of convergence of this series is $+\infty$ by (19). It is an entire function, which by assumption is zero at each 2^k $(k\geq 0)$. It also satisfies the inequality

$$|g(z)| \leq 2c_0\sum_{r=0}^{\infty}2^{-\frac{r^2}{2}}|z|^r.$$

In particular, in the case $|z| = 2^k$ we get for some absolute c_0':

$$|g(z)| \leq 2c_0 \sum_{r=0}^{\infty} 2^{-\frac{r^2}{2}}\, 2^{kr} \leq c_0'\, 2^{\frac{k^2}{2}}.$$

Suppose that g has a zero of finite order ℓ at $z = 0$. By Lemma 6 we would have the inequality

$$c_0'\ 2^{\frac{k^2}{2}} \geq \frac{|g^{(\ell)}(0)|}{\ell!} \cdot 2^{\frac{k(k+1)}{2}+k\ell},$$

which is false for k large. This contradiction means that $g \equiv 0$, in other words, we have $x_r = x_r'$ for every $r \geq 0$. So we proved

Lemma 7. *The system* (17) *has at most one non negative solution* $(x_r)_{r\geq 0}$.

By Lemma 5, we know that the system (17) has a positive solution and now we know that it is unique. This unique positive solution is given by $x_r = \alpha_\infty(r)$, from which we deduce that we have $d_r = \alpha_\infty(r)$. This equality also implies that, as X tends to infinity, $d(r, X)$ has only one limit point which is the density of the set of special discriminants with 4–rank equal to r and its value is equal to $\alpha_\infty(r)$. This is exactly the first part of Corollary 2.

2.2. **Proof of Theorem 2.** We always assume that Theorems 3 and 4 are proved.

For $r \geq 0$ and $X \geq 5$ define

$$\delta(r, r, X) := \frac{\sharp\left\{D \in \mathcal{D} :\ D \leq X,\ \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{Cl}_D) = r\right\}}{\mathcal{D}(X)},$$

and

$$\delta(r, r-1, X) := \frac{\sharp\left\{D \in \mathcal{D} :\ D \leq X,\ \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{Cl}_D) + 1 = r\right\}}{\mathcal{D}(X)}.$$

We trivially have the equality

$$\delta(r, r, X) + \delta(r, r-1, X) = d(r, X),$$

and in §2.1 we proved

$$\delta(r, r, X) + \delta(r, r-1, X) \to \alpha_\infty(r),\ (X \to \infty,\ r = 1, 2, \dots) \tag{21}$$

and

$$\lim_{X\to\infty} \delta(0, 0, X) = \alpha_\infty(0).$$

For $k \geq 0$ we define

$$C_k' := (2^{k-1}+1)C_k = (2^{k-1}+1)\prod_{j=0}^{k-1}(2^j+1),$$

and we write Theorems 3 and 4 in the following equivalent forms:

$$\begin{aligned}
\sum_{r=0}^{\infty} \left(\delta(r, r, X) + \delta(r, r-1, X)\right) 2^{(k+1)r} &= C_{k+1} + o(1),\\
\sum_{r=0}^{\infty} \left(\delta(r, r, X) + \frac{\delta(r, r-1, X)}{2}\right) 2^{(k+1)r} &= C_k' + o(1).
\end{aligned}$$

By linear combination and by the equality $2C'_k - C_{k+1} = C_k$ we deduce the equality

$$\sum_{r=0}^{\infty} (2^r \delta(r,r,X))\, 2^{kr} = C_k + o(1) \text{ for } X \to \infty \text{ and } k = 0,1,2,\dots.$$

Then we recognize the equation (15) with $d(r,X)$ replaced by $2^r\delta(r,r,X)$. Therefore we deduce that

$$\delta(r,r,X) \to 2^{-r}\alpha_\infty(r) \text{ for } X \to \infty \text{ and } r = 0,1,2,\dots.$$

Using equation (21) we get that

$$\delta(r,r-1,X) \to (1-2^{-r})\alpha_\infty(r) \text{ for } X \to \infty \text{ and } r = 0,1,2,\dots.$$

This is exactly the content of (11) in Theorem 2.

3. From 4–ranks to symbols

The goal of this section is to give criterions for the 4–rank of the class group and the narrow class group. For the narrow class group we give in Proposition 2 a criterion which we already used in [11]. Using this criterion we are able to produce formulas given in Lemmata 10 and 11. Dealing with the ordinary class group is more difficult. As a general rule we need to decide how many of the unramified degree 4 extensions of our given quadratic field are real. Later on we only need Theorem 5. More or less all the results in this section can be already found in old papers by Redei, Reichardt, and Scholz. The proofs are distributed over many papers and sometimes they are a little bit sketchy. For this reason we decided to give proofs for those results.

In Section 4 we show how to transform this criterion to the ordinary class group and give a new formula in Theorem 6. This result is analogous with Lemmata 10 and 11.

3.1. **Hilbert class fields and some class field theory.** In this section we collect some necessary tools from class field theory. In the introduction we introduced the notion of ordinary and narrow class groups of a (quadratic) number field. In the following let D be a fundamental discriminant and $K := \mathbb{Q}(\sqrt{D})$ be a quadratic number field. Denote by I_K the (multiplicative) group of fractional ideals of K and by P_K the (multiplicative) group of fractional principal ideals. Furthermore we introduce P_K^+ which is the group of fractional principal ideals which have a generator which is totally positive. For $D < 0$ all elements are totally positive and therefore $P_K = P_K^+$. For $D > 0$ every element of K has two real conjugates and an element is totally positive if both conjugates (as real numbers) are positive. Now the ordinary class group is $\mathrm{Cl}_D := I_K/P_K$ and the narrow class group is defined via $\mathrm{C}_D := I_K/P_K^+$. Since $P_K^+ \subseteq P_K$ and everything is abelian we easily see that Cl_D is a quotient of C_D and we have the following exact sequence (see (6)):

$$\{1\} \to F_\infty \to \mathrm{C}_D \to \mathrm{Cl}_D \to \{1\}, \tag{22}$$

where F_∞ is a group of order at most 2. We can assume that elements in F_∞ are represented by principal ideals generated by units of the ring of integers of $\mathcal{O}_K$. In order to distinguish those elements in F_∞ only the signs of the two conjugates are important. Therefore we have at most 4 possibilities. Since $(\alpha) = (-\alpha)$ the number of possibilities is reduced to 2, i.e. we have to distinguish the case that

both conjugates have the same sign or not. We are able to show the classical result, already mentioned in the introduction:

Lemma 8. *Let $D > 0$ be a fundamental discriminant. Then $\mathrm{C}_D = \mathrm{Cl}_D$ if and only if $\mathcal{O}_K$ has a unit of norm -1. This situation is equivalent to say that the negative Pell equation for d defined in* (1) *has a solution.*

Proof. This is very classical and the proof can be found in various places in the literature, e.g. [31, Cor. 1, p. 112] or [26, p. 243]. □

We will make heavy use of the main theorem of class field theory which states that for every class group there is an abelian extension of our given field which has the class group as Galois group. We only need the Hilbert class field and the extended Hilbert class field. We formulate the following proposition for general number fields.

Proposition 1. *Let K be a number field with class group Cl_K and narrow class group C_K. Denote by H_K the maximal abelian at all places unramified extension and by H_K^+ the maximal abelian at all finite places unramified extension. Clearly, $H_K \subseteq H_K^+$ and we get that $\mathrm{Gal}(H_K/K) = \mathrm{Cl}_K$ and $\mathrm{Gal}(H_K^+/K) = \mathrm{C}_K$.*

A proof for this proposition can be found in every textbook about class field theory, e.g. in [26, p. 228 & 242]. We remark that a field extension of a totally real field is unramified (at all places) in infinity, if and only if it is totally real. Our question concerning the equality $\mathrm{C}_D = \mathrm{Cl}_D$ can be reformulated as the question whether the extended Hilbert class field is totally real or not. It is clear that only the even parts of C_D are interesting for that question. In this section we are interested in the 4–part. We want to consider the maximal abelian extension N of K which is unramified at all finite places and which is of exponent dividing 4. By the main theorem of Galois theory this extension N/K has Galois group $A := \mathrm{C}_K \,/\, \mathrm{C}_K^4 \cong C(4)^r \times C(2)^s$, where $C(m)$ denotes the cyclic group of order m.

We are interested in the following question: *How many extensions of K do exist with Galois group $C(4)$, which are unramified at all finite places ?* This counting will be performed by using the following lemma from abelian group theory and by applying the main theorem in Galois theory.

Lemma 9. *Let $A \cong C(4)^r \times C(2)^s$ with $r \geq 1$ be an abelian group. Denote by $H \leq A$ a subgroup such that $A/H \cong C(4)$ and denote by $H \leq U \leq A$ the unique intermediate subgroup U of index 2 in A. Then:*

(i) *The number of $C(4)$–quotients of A is exactly $(2^r - 1) \cdot 2^{r+s-1}$.*
(ii) *The number of subgroups $\tilde{H} \leq U$ such that $A/\tilde{H} \cong C(4)$ is equal to 2^{r+s-1}.*

Proof. (i) By dualizing it is equivalent to count subgroups of A isomorphic to $C(4)$. Each of those subgroups has 2 generators of order 4, so we need to count half of the elements of order 4:

$$\frac{1}{2}(4^r 2^s - 2^{r+s}) = \frac{1}{2}(2^r - 1)(2^{r+s}).$$

(ii) There are $2^r - 1$ subgroups U of index 2 which contain a subgroup H such that $A/H \cong C(4)$. Therefore for our given U we have 2^{r+s-1} possibilities using the first part of this lemma.

□

3.2. **Case of narrow class group.** In a first step we quote rather old results concerning the 4–rank. There are two similar criterions to determine the 4–rank of the narrow class group of a quadratic number field. The first criterion is the one we used to determine the asymptotics of 4–ranks of narrow class groups of quadratic number fields ([11] & [10]). Here $(a \mid b)$ denotes the norm symbol which was introduced in [11, Definition 2] and which is defined by:

Definition 1. *Let a and b be two non zero rational numbers. Then we have $(a \mid b) = 0$ or 1, and $(a \mid b) = 1$ if and only if the quadratic equation $x^2 - ay^2 - bz^2 = 0$ has a non trivial solution in $\mathbb{Q}^3$.*

Now we recall

Proposition 2. *(First criterion) For every fundamental discriminant D, positive or negative, we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2}\sharp\big\{a \mid D \,:\, a>0,\, a \text{ squarefree },\ (a \mid -D/a) = 1\big\}.$$

This result is given in [11, Theorem 5], but it was already known to Redei ([33] & [34]). We want to make Proposition 2 more practicable. We appeal to Legendre's Theorem on ternary quadratic forms (see Lemma 12 below), which implies that, if a and b are squarefree and coprime with $b > 0$, then $(a \mid b) = 1$ if and only if a is a square modulo b and b is a square modulo $|a|$ (see [11, Lemma 6]), and to the classical detecting identity

$$\frac{1}{2^{\omega(n)}}\prod_{p\mid n}\Big(1+\Big(\frac{m}{p}\Big)\Big) = \begin{cases} 1 \text{ if } m \text{ is a square } \bmod n,\\ 0 \text{ otherwise };\end{cases}$$

(which is true for m and n coprime integers, with n odd and positive), and arrive at two of the key formulas of [11]:

Lemma 10. [11, Lemma 27 & formula (77)] *For any positive odd fundamental discriminant D we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D)}}\sum_{D=D_0D_1D_2D_3}\Big(\frac{-1}{D_3}\Big)\Big(\frac{D_2}{D_0}\Big)\Big(\frac{D_1}{D_3}\Big)\Big(\frac{D_0}{D_3}\Big)\Big(\frac{D_3}{D_0}\Big).$$

In particular, for $D \in \mathcal{D}_{\mathrm{odd}}$ we have the equality

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D)}}\sum_{D=D_0D_1D_2D_3}\Big(\frac{D_0}{D_2}\Big)\Big(\frac{D_1}{D_3}\Big).$$

For even discriminants we have:

Lemma 11. [11, Lemma 38 & formula (111)] *For any positive fundamental discriminant $D \equiv 0 \bmod 8$ we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D/8)}}\sum_{D=8D_0D_1D_2D_3}\Big(\frac{2}{D_3}\Big)\Big(\frac{D_2}{D_0}\Big)\Big(\frac{D_1}{D_3}\Big)\Big(\frac{D_3}{D_0}\Big)\Big(\frac{D_0}{D_3}\Big)\times\Big[\Big(\frac{-1}{D_0}\Big)+\Big(\frac{-1}{D_3}\Big)\Big].$$

In particular, for $D \in \mathcal{D}_{\mathrm{even}}$ we have the equality

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2^{\omega(D/8)}}\sum_{D=8D_0D_1D_2D_3}\Big(\frac{2}{D_3}\Big)\Big(\frac{D_0}{D_2}\Big)\Big(\frac{D_1}{D_3}\Big).$$

Redei also found another characterization of the 4–rank, based on the number of decompositions of second type.

Definition 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 always meet the trivial decompositions $\{D, 1\}$ and $\{1, D\}$. As usual we want to express this condition with our symbol defined in Definition 1. For this the following result of Legendre is useful.

Lemma 12. *(see* [8, p.428]*) Let a, b and c be three integers, not all of the same sign, such that abc is squarefree. Then the quadratic form*

$$ax^2 + by^2 + cz^2$$

has a non trivial zero $(x, y, z) \in \mathbb{Z}^3$ if and only if $-bc$, $-ac$ and $-ab$ are squares modulo $|a|$, $|b|$ and $|c|$, respectively.

We want to apply this to our symbol $(D_1 \mid D_2)$ and the above lemma states in the case D odd that this symbol is 1 if and only if the following three conditions hold:

(i) $D_1 > 0$ or $D_2 > 0$,
(ii) D_1 is a square modulo $|D_2|$,
(iii) D_2 is a square modulo $|D_1|$.

When D is even, we necessarily have $D_1 \equiv 8, 12 \bmod 16$. Using the equality $(D_1 \mid D_2) = (D_1/4 \mid D_2)$ we recover the conditions (i), (ii), and (iii) with D_1 replaced by $D_1/4$. Now we are able to prove.

Lemma 13. *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) $(D_1 \mid D_2) = 1$.
(ii) *If $2 \mid D_1$, then we have $D_2 \equiv 1 \bmod 8$.*

Proof. Let $\{D_1, D_2\}$ be a decomposition of second type. If $2 \mid D$ then $2 \mid D_1$ and therefore from the Kronecker symbol we get $\left(\frac{D_2}{2}\right) = 1$ which implies $D_2 \equiv 1 \bmod 8$.

For odd primes the Kronecker symbol behaves like the Jacobi symbol. So by the hypothesis, we have $\left(\frac{D_1}{p}\right) = 1$ for all primes dividing D_2 and $\left(\frac{D_2}{p}\right) = 1$ for all odd primes dividing D_1. This implies that D_1 is a square modulo $|D_2|$ and D_2 is a square modulo $|D_1|$ (if D_1 is odd) or modulo $|D_1|/4$ (if D_1 is even). Recall in the last case that every odd number is a square modulo 2. It remains to check that D_1 and D_2 cannot be both negative. This is trivial for $D < 0$ and for special discriminants. Since we do not need the other cases in this paper, we leave these cases as an exercise to the reader.

Now assume that the conditions (i) and (ii) of Lemma 13 are satisfied. The second one gives the right value for the Kronecker symbol at $p = 2$. When D is odd, the condition $(D_1 \mid D_2) = 1$ implies D_1 is a square modulo $|D_2|$ and vice versa, which gives the right values for the Kronecker (resp. Jacobi) symbols at odd primes p. When D is even, $(D_1 \mid D_2) = 1$ implies that $(D_1/4 \mid D_2) = 1$. Again, we can deduce that $D_1/4$ (and D_1) is a square modulo $|D_2|$ and D_2 is a square modulo $|D_1|/4$. This gives the right values for the symbols at odd primes, too. □

For special discriminants we can improve this result.

Lemma 14. *Let D be a special 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*

$$(D_1 \mid D_2) = 1.$$

Proof. Using the preceding lemma, we only need to check that $(D_1 \mid D_2) = 1$ and $8 \mid D$ imply $D_2 \equiv 1 \bmod 8$.

We define $D_1' := D_1/4$ which is exactly divisible by 2 and look at the non trivial solution of

$$x^2 - D_1' y^2 - D_2 z^2 = 0,$$

where we can assume that xzD_2 is odd. Certainly we have that $x^2 \equiv z^2 \equiv 1 \bmod 8$ and we get:

$$1 - D_1' y^2 - D_2 \equiv 0 \bmod 8$$

and this equation has only a solution if $2 \mid y$ and $D_2 \equiv 1 \bmod 8$ since we know that $D_2 \equiv 1 \bmod 4$. □

For non special discriminants the second condition of Lemma 13 is important since for $D = -20$ we get $-20 = -4 \cdot 5$, which is not a decomposition of second type, but $(-4 \mid 5) = 1$. Certainly $5 \not\equiv 1 \bmod 8$ in this case.

The following proposition is proved in [33]. As a side effect we will reprove it later in this section in the case of special discriminants.

Proposition 3. *(Second criterion) Let D be a fundamental discriminant. Then we have*

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

These two criterions are different since they are counting different objects as the following example shows.

Example 1. *Consider $D = 21$. Then using Proposition 2, we compute the symbols*

$$(1 \mid -21) = 1,\ (3 \mid -7) = 0,\ (7 \mid -3) = 1,\ (21 \mid -1) = 0.$$

This gives $\mathrm{rk}_4(\mathrm{C}_{21}) = 0$.

If we apply Proposition 3, we compute the symbols

$$(1 \mid 21) = 1,\ (-3 \mid -7) = 0,\ (-7 \mid -3) = 0,\ (21 \mid 1) = 1,$$

and of course we recover the equality $\mathrm{rk}_4(\mathrm{C}_{21}) = 0$.

Note also that for $D \in \mathcal{D}$, the two criterions coincide, i.e. we can give a canonical bijection between symbols used in the first and second criterion. Let $\{D_1, D_2\}$ be

a decomposition of second type of a special D. We note that $(D_1 \mid -1) = 1$ and define a to be the squarefree part of D_1, i.e. $a = D_1$ or $a = D_1/4$. Then:

$$(D_1 \mid D_2) = (D_1 \mid -D_2) = (a \mid -D/D_1) = (a \mid -D/a).$$

This means that for special discriminants Propositions 2 and 3 are equivalent.

In [11] we used the first criterion because from an analytic point of view, it was more natural to consider ordinary factorizations of D compared to decompositions in fundamental discriminants. The decompositions of the second type have the big advantage that algebraically speaking they have more structure which we want to use for a criterion for the 4–rank of the ordinary class group. For us it is nice that for special discriminants these two approaches coincide.

Now we are able to give an algebraic interpretation which was already known to Redei and Reichardt [32]. It is a well known fact that unramified cyclic extensions of quadratic number fields are normal over $\mathbb{Q}$ with dihedral Galois group. We have not found a good citation for that, so we provide an elementary proof for our situation.

Lemma 15. *Let D be a fundamental discriminant and $K := \mathbb{Q}(\sqrt{D})$. Furthermore assume that K_4/K is a $C(4)$-extension which is unramified at all finite places. Then $K_4/\mathbb{Q}$ is Galois with dihedral Galois group D_4 of order 8.*

Proof. Let σ be the automorphism of K defined via $\sigma(\sqrt{D}) = -\sqrt{D}$. Furthermore denote by N/K the maximal abelian at finite places unramified extension of K of exponent 4. Then $N/\mathbb{Q}$ is normal since conjugated extensions stay unramified and the normal closure is the union of those. We remark that $\mathrm{Gal}(N/K) = A := \mathrm{C}_D \,/\, \mathrm{C}_D^4$. Since N/K is unramified, we get that a ramified prime ideal in $\mathcal{O}_N$ has ramification index 2. Using Theorem 16.30 (or Corollary 16.31) in [4, p.206], we get that the Galois group G of $N/\mathbb{Q}$ is generated by elements of order 2.

We get the following exact sequence:

$$1 \to A \to G \to \langle \sigma \rangle \to 1.$$

Now σ acts by conjugation on A, i.e. for $a \in A$ we define $a^\sigma := \sigma a \sigma^{-1}$. We would like to prove that $a^\sigma = a^{-1}$ for all $a \in A$. For elements of order 2 this is true by genus theory, since we know that unramified quadratic extensions of K lead to V_4-extensions which implies the trivial action of σ, i.e. $a^\sigma = a^{-1} = a$. Here $V_4 = C(2) \times C(2)$ is the Klein 4-group. Let $a \in A$ be an element of order 4. We have three different possibilities for the action of σ: $a^\sigma = a, a^\sigma = a^{-1}$, or $a^\sigma = b$ with $b \notin \langle a \rangle$. Let us consider the first case, i.e. $a^\sigma = a$ and $a \in A$ is of order 4. This means that a central $C(4)$-extension of $C(2)$ is a quotient of G. Such a group is either $C(4) \times C(2)$ or $C(8)$ and both groups need a generator of order at least 4 which is impossible since G is generated by elements of order 2 and therefore all quotients, too.

Now we consider the last case and define $c := ab$. Then $c^\sigma = a^\sigma b^\sigma = ba = ab = c$ and we get an element c of order 4 with trivial action. We have seen in the first case that this situation is impossible.

Therefore we have proved that $a^\sigma = a^{-1}$ for all $a \in A$ which means that an unramified $C(4)$-extension K_4/K leads to a normal non-abelian degree 8-extension. Now D_4 is the only group of order 8 which satisfies these restrictions, since the quaternion group cannot be generated by elements of order 2. □

Remark. The same type of proof works for other abelian groups of exponent m. We want to stress the fact that it is important that the base field is $\mathbb{Q}$, otherwise we cannot apply Theorem 16.30 in [4, p.206] and we can produce counterexamples. For example there exist unramified degree 8 extensions of quadratic fields which are normal with quaternion group Q_8.

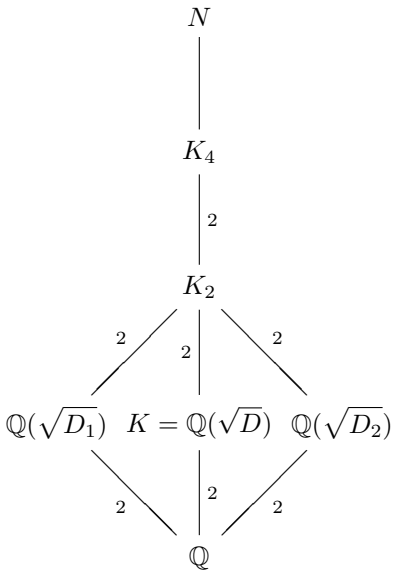
Now we prove

Lemma 16. *Let D be a fundamental discriminant, $K := \mathbb{Q}(\sqrt{D})$ and K_4/K be an at finite places unramified $C(4)$-extension. Then $K_4/\mathbb{Q}$ contains three quadratic extensions of $\mathbb{Q}$ with discriminants D, D_1, D_2 and the relation $D = D_1 D_2$ is true. There are exactly 2^{t-2} fields K_4 which correspond to the same decomposition $\{D_1, D_2\}$, where $t = \omega(|D|)$.*

Proof. The existence of K_4 implies $\mathrm{rk}_4(\mathrm{C}_D) \geq 1$ which certainly is only possible when $t \geq 2$ (see Proposition 2). Using Lemma 15 we know that $K_4/\mathbb{Q}$ is normal with Galois group D_4. In this case the maximal abelian quotient of D_4 is $V_4 = C(2) \times C(2)$ which implies that K_4 contains three quadratic subfields, one of those must be of discriminant D. The discriminant of the V_4-field is D^2 since it is unramified over $\mathbb{Q}(\sqrt{D})$. An easy application of the "Führerdiskriminantenproduktformel", e.g. see [37, p. 104] yields that the discriminant of a V_4-field is just the product of the discriminants of the three subfields. This gives $D^2 = D_1 D_2 D$ and therefore $D = D_1 D_2$, where D_1 and D_2 are the discriminants of the other two quadratic subfields.

Denote by N/K the maximal abelian at finite places unramified extension of exponent 4. The Galois group of this extension is $A := \mathrm{C}_D \,/\, \mathrm{C}_D^4$ and our given field K_4 is a subfield of N. We are interested to count the number of fields $\tilde{K}_4 \leq N$ such that $[\tilde{K}_4 : K] = 4$ and $\tilde{K}_4$ contains $\mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$. The latter field corresponds by the main theorem of Galois theory to a subgroup U of index 2 in A. Our given field K_4 corresponds to a subgroup $H \leq A$ of index 4 such that $A/H \cong C(4)$ and $H \leq U$. We need to count all subgroups $\tilde{H} \leq U$ such that $A/\tilde{H} \cong C(4)$. Since $|A/A^2| = |\,\mathrm{C}_D \,/\, \mathrm{C}_D^2\,| = 2^{t-1}$ we get that we have 2^{t-2} such $\tilde{H}$ by applying Lemma 9. □

Now we can show that unramified $C(4)$–extensions will lead to decompositions of second type.



Lemma 17. *Let K_4/K be an unramified $C(4)$–extension corresponding to the decomposition $\{D_1, D_2\}$ of D (as in Lemma 16). Then $\{D_1, D_2\}$ is a decomposition of second type of D.*

Proof. Let $p \mid D_1$ be a prime and choose a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{K_4}$ lying over (p). Then the ramification index is 2 and therefore the inertia field L of $\mathfrak{p}$ has degree 4. Since all prime ideals above (p) in $K_2 := \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ are ramified we get that $L \neq K_2$ and therefore $L/\mathbb{Q}$ is not normal. Therefore p must be ramified in L and we get that there must be at least two prime ideals in $\mathcal{O}_{K_4}$ lying above p. This means that the decomposition field of $\mathfrak{p}$ must contain $\mathbb{Q}(\sqrt{D_2})$ which implies that p is split in this field. Therefore the Kronecker symbol $\left(\frac{D_2}{p}\right)$ is 1. By switching the roles of D_1 and D_2 we get the other direction. Therefore $\{D_1, D_2\}$ is a decomposition of second type by Definition 2. □

Remark. For a non trivial decomposition $\{D_1, D_2\}$ of second type of a fundamental discriminant D we can construct an unramified $C(4)$–extension K_4/K such that K_4/K contains $\mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$. We say that K_4 *corresponds to* $\{D_1, D_2\}$. However, we only need this result for special discriminants and the corresponding proof is given in Lemma 20.

Field theoretically there is a nice description of all fields K_4 which correspond to a given decomposition $\{D_1, D_2\}$. Define $K := \mathbb{Q}(\sqrt{D})$ and $K_2 := \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ and let K_4 be one field corresponding to $\{D_1, D_2\}$, i.e. $K_2 \subseteq K_4$. Now let $\tilde{D} \mid D$ be a fundamental discriminant not contained in $\{1, D_1, D_2, D\}$. Now $K_4 Q(\sqrt{\tilde{D}})/K_2$ is an unramified (at finite places) V_4-extension and therefore contains three subfields $K_4, K_2(\sqrt{\tilde{D}})$, and $\tilde{K}_4$. $\tilde{K}_4/K$ is an unramified $C(4)$-extension which contains K_2. We remark that we get the same $\tilde{K}_4$ if two different $\tilde{D}$ only differ by a square in K_2. D has $2^{\omega(D)}$ different squarefree divisors which means that modulo squares in

K_2 we have $2^{\omega(D)-2}$ possibilities to twist. This coincides with the number given in Lemma 16.

The following result is only interesting when $D \in \mathcal{D}$, since otherwise we know that the 2-ranks of our class groups differ and therefore the 4-ranks are the same.

Lemma 18. *Let D be a special discriminant and $D = D_1 D_2$. Assume that K_4 and $\tilde{K}_4$ are two different unramified $C(4)$-extensions corresponding to the non trivial decomposition $\{D_1, D_2\}$ of D. Then K_4 is totally real if and only if $\tilde{K}_4$ is totally real.*

Proof. Since $D \in \mathcal{D}$ all fundamental divisors are positive. By the above construction this means that $\tilde{K}_4$ is contained in $K_4(\sqrt{\tilde{D}})$ for some $\tilde{D} \mid D$. Therefore $\tilde{K}_4$ is totally real if K_4 is totally real and vice versa. □

We remark that the corresponding statement is wrong if we want to consider 8-ranks. In this case it may happen that only some of the corresponding unramified $C(4)$-extensions are embeddable into an unramified $C(8)$-extension.

Our goal is to find a criterion to detect when the extensions corresponding to $\{D_1, D_2\}$ are totally real. This will give a criterion to compute $\mathrm{rk}_4(\mathrm{Cl}_D)$. In order to decide reality it is useful to explicitly compute a corresponding extension to a decomposition of second type.

The following results are very classical, e.g. see [32, 35]. However, we think that these references are too sketchy. We prefer to give a proof which is based on a unpublished preprint of Franz Lemmermeyer [28] (see Lemma 21 and Proposition 6). Later on we will use the following proposition of Hecke which we will use to show that some quadratic extension is unramified at all finite places. The only critical places are the ones above 2. The corresponding local result can be found in [31, Thm 5.6, p. 221].

Proposition 4. *Let L be a number field and $\alpha \in L \setminus L^2$ which is chosen relatively prime to 2. Then $L(\sqrt{\alpha})/L$ is unramified at all finite places if and only if the (fractional) principal ideal (α) (in L) is a square and the congruence*

$$X^2 \equiv \alpha \bmod 4$$

is solvable for some number $X \in L$.

Proof. This is the special case $\ell = 2$ of [21, Theorem 120]. □

We will apply this proposition in the following way. An odd prime ideal $\mathfrak{p} \subseteq \mathcal{O}_L$ is unramified in $L(\sqrt{\alpha})/L$ if $\mathfrak{p} \nmid (\alpha)$. For even prime ideals this is only necessary, but not sufficient. We have to check a further congruence.

In order to simplify the following proofs we restrict to special discriminants.

Lemma 19. *Let D be a special discriminant and $\{D_1, D_2\}$ be a decomposition of second type of D, where we assume that D_2 is odd. Then there exists a non trivial solution $(x, y, z) \in \mathbb{Z}^3$ of*

$$x^2 - D_1 y^2 - D_2 z^2 = 0 \tag{23}$$

such that the following holds:

(i) *$x^2, D_1 y^2, D_2 z^2$ are pairwise coprime, $y \geq 0$, $z \geq 0$,*
(ii) *x odd, $D_1 y$ even, and $D_2 z$ odd (by changing the roles of D_1 and D_2, if necessary),*

(iii) $x+y \equiv 1 \bmod 4$ *if* $2 \nmid D$, $x \equiv 1 \bmod 4$ *if* $2 \mid D$ *and* y *even,* $x \equiv 3 \bmod 4$, *if* $2 \mid D$ *and* y *odd.*

Proof. Note that D_1, D_2 are always coprime even if $2 \mid D$ because D_1, D_2 are fundamental discriminants. Using Lemma 14 and Definition 1 we get a non trivial solution in $\mathbb{Q}^3$ which can be assumed to be in $\mathbb{Z}^3$ by clearing denominators. Let p be an odd prime which divides more than one of the terms. Then it must divide all the terms and furthermore $p^2 \nmid D_1 D_2$ which implies that p divides x, y, and z and therefore we can simplify the solution. For $p = 2$ we can apply the same argument when $2 \nmid D_1 D_2$. Now assume that 2 divides all terms which means that $2 \mid x, 2 \mid D_1, 2 \mid z$. We can assume that $2 \nmid y$, otherwise we can easily simplify our solution. Since D is special we have that 8 exactly divides D_1. By considering the equation modulo 16, we get that

$$x^2 \equiv 0, 4 \bmod 16,\ D_1 y^2 \equiv 8 \bmod 16,\ D_2 z^2 \equiv 0, 4 \bmod 16.$$

A solution of this type cannot exist. By choosing $y, z \geq 0$ we have proved the first claim.

For (ii) we first note that exactly one of the summands $x^2, D_1 y^2$, and $D_2 z^2$ is even. Then consider the equation modulo 4 which implies that x^2 must be odd.

By choosing the sign of x we can easily reach the last condition. □

Let D be a special discriminant and $\{D_1, D_2\}$ be a non trivial decomposition of second type of D. Choose the solution (x, y, z) from the previous lemma and note that y, z are positive. Let us define $\alpha := x + y\sqrt{D_1}$ and let us look at the following fields:

$$K := \mathbb{Q}(\sqrt{D}), K_2 := \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2}) = \mathbb{Q}(\sqrt{D})(\sqrt{D_1}), K_4 := K_2(\sqrt{\alpha}).$$

Lemma 20. *K_4/K is a cyclic extension of degree 4 which is unramified at all finite places. Furthermore the extension $K_4/\mathbb{Q}$ is normal with Galois group D_4 of order 8. The quadratic subfields contained in K_4 are $K, \mathbb{Q}(\sqrt{D_1})$, and $\mathbb{Q}(\sqrt{D_2})$.*

Proof. By the above we only need to prove that K_4/K is unramified and normal with Galois group $C(4)$.

Define $\beta := x - y\sqrt{D_1}$ and

$$\sigma : K_4 \to K_4, \sqrt{\alpha} \mapsto \sqrt{\beta}, \sqrt{D_1} \mapsto -\sqrt{D_1}, \sqrt{D_2} \mapsto -\sqrt{D_2}.$$

Using $\sqrt{\alpha}\sqrt{\beta} = \sqrt{x^2 - D_1 y^2} = z\sqrt{D_2}$ we get: $\sigma^2(\sqrt{\alpha}) = \sigma(\sqrt{\beta}) = -\sqrt{\alpha}$ which implies $\sigma^2 \neq 1$ and $\sigma^4 = 1$. Therefore K_4/K is cyclic of order 4. The extension K_2/K is unramified at all finite places which means that we need to prove the same for K_4/K_2. For this we want to apply Proposition 4 with $L = K_2$.

First we want to prove that the ideal (α) is the square of an ideal in the ring of integers of K_2. This is equivalent to prove that no prime ideal $\mathfrak{p}$ divides (α) to an odd power. First consider a prime ideal $\mathfrak{p}$ of odd norm dividing (α) to an odd power. Since $K_2(\sqrt{\alpha}) = K_2(\sqrt{\beta})$ we deduce that $\mathfrak{p} \mid (\beta)$ from which we deduce that $\mathfrak{p} \mid (\alpha + \beta)$ and therefore $\mathfrak{p} \mid (x)$ since $\mathfrak{p}$ is odd. Similarly, we have $\mathfrak{p} \mid (y\sqrt{D_1})$ which leads to a contradiction because we assumed that $\gcd(x, yD_1) = 1$. Secondly, the norm α over $\mathbb{Q}$ is $(\alpha\beta)^2 = (x^2 - y^2 D_1)^2 = (D_2 z^2)^2$ which is odd. Therefore no even prime ideal divides α. In conclusion, we checked the first condition of Proposition 4.

We have to check the second condition: $X^2 \equiv \alpha \bmod 4\mathcal{O}_{K_2}$. Note that $\gamma \equiv \delta \bmod 4\mathcal{O}_{K_2}$ for two elements $\gamma, \delta \in \mathcal{O}_{K_2}$ simply means that $\gamma - \delta$ is divisible by 4

in $\mathcal{O}_{K_2}$. We remark that the sign of x in Lemma 23 (iii) is chosen in a way such that $X^2 \equiv \alpha \bmod 4\mathcal{O}_{K_2}$ is solvable. We consider the different cases corresponding to the value of y.

(i) If $4 \mid y$ then $\alpha \equiv x \bmod 4\mathcal{O}_{K_2}$ and by choosing $X = 1$, we have $X^2 \equiv x \bmod 4\mathcal{O}_{K_2}$ and $x \equiv 1 \bmod 4$ by Lemma 19 (iii).

The same applies when y is even and D_1 is even, since in this case $y\sqrt{D_1}$ is divisible by 4 in $\mathcal{O}_{K_2}$.

(ii) In the case $y \equiv 2 \bmod 4$ and D_1 odd we have $x \equiv 3 \bmod 4$. Then $(x-1) + y\sqrt{D_1}$ is divisible by 4 since $x-1$ and y are congruent to 2 modulo 4 and elements of the form $a + b\sqrt{D_1}$ are divisible by 2 for ab odd. Therefore $\alpha \equiv 1 \bmod 4\mathcal{O}_{K_2}$ and by choosing $X = 1$ our equation is solvable.

(iii) The final case is y odd which implies that $D_1 \equiv 0 \bmod 8$. Here we choose $X = 1 + \frac{\sqrt{D_1}}{2} \in \mathcal{O}_{K_2}$ and get that

$$X^2 = 1 + \sqrt{D_1} + D_1/4 \equiv 1 + \sqrt{D_1} + 2 \equiv 3 + \sqrt{D_1} \bmod 4\mathcal{O}_{K_2}.$$

In this case we have $x \equiv 3 \bmod 4$ by Lemma 19 (iii) and we see that our equation $X^2 \equiv \alpha \bmod 4\mathcal{O}_{K_2}$ is solved.

□

Now we are able to give a proof of Proposition 3 in the case of special discriminants. However, this restriction suffices for the proof of Theorems 1–6.

Proof of Proposition 3. Let $A := \mathrm{C}_D \,/\, \mathrm{C}_D^4 \cong C(4)^r \times C(2)^s$. From Lemmata 16 and 17 we know that an at finite places unramified $C(4)$–extension K_4/K with $K \subseteq K_2 = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2}) \leq K_4$ gives rise to a non trivial decomposition $\{D_1, D_2\}$ of second type. On the other hand we have shown in Lemma 20 that a non trivial decomposition $\{D_1, D_2\}$ leads to an at finite places unramified extension K_4/K. Applying Lemma 9 we see that there are exactly $2^r - 1$ groups U of index 2 which contain subgroups H such that $A/H \cong C(4)$. We have to add the trivial group (corresponding to $\{1, D\}$). Since $\{D_1, D_2\}$ and $\{D_2, D_1\}$ correspond to the same extension, we count everything twice which explains the factor $1/2$. □

3.3. **Case of the ordinary class group.** We are searching for similar formulas contained in Propositions 2 & 3 when we replace C_D by the ordinary class group Cl_D.

For any integer a and any odd prime p we define

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

Let also

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

Finally, for b and c positive, 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.

As before, we restrict our attention to special discriminants D. In this case, D is positive, D is either odd and squarefree or D is divisible by 8 and $D/8$ is odd and squarefree. Now, we refer to the following result in [38, Formula (7), p. 109]:

Proposition 5. *Let $D \in \mathcal{D}$ and $\{D_1, D_2\}$ be a non trivial decomposition of second type of D. Then the corresponding unramified $C(4)$-extensions are totally real if and only if*

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

Let us postpone the proof of this proposition for a moment. In case $\mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{Cl}_D)$ all unramified $C(4)$-extensions are real and therefore we have $[D_1, D_2]_4 = [D_2, D_1]_4$ for all decompositions of second type. When the 4–ranks are different, then they differ by 1 (see inequality (8)), i.e. half of the unramified $C(4)$-extensions are real and half of them are complex (here we count the trivial extension as a real extension). Therefore we proved the following theorem using Proposition 5 and by the remark that all squarefree positive divisors of D are fundamental discriminants (except for 2, but multiplying by 4 does not affect the value of the symbol).

Theorem 5. *For any special discriminant D we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{Cl}_D)} = \frac{1}{2} \cdot \sharp\big\{(a,b) \in \mathbb{N}^2 \,:\, D = ab,\ [a,b]_4 = [b,a]_4 = 1 \text{ or } [a,b]_4 = [b,a]_4 = -1\big\}.$$

We remark that if D is even, no (a, b) with a and b even contribute to the right part of the above equality. This is a consequence of the definition of the symbol $[a, b]_4$. Therefore we are allowed to replace the D_1D_2 by divisors ab.

In order to simplify the proof of Proposition 6 we compute some symbols in the following lemma.

Lemma 21. *Let $D \in \mathcal{D}$ and $\{D_1, D_2\}$ be a decomposition of second type. Let*

$$x^2 - D_1 y^2 - D_2 z^2 = 0 \tag{24}$$

be the corresponding solution computed in Lemma 19. Write $D_1 = wD_1'$ and $y = 2^j u$, where $w \in \{1, 8\}$, D_1' and u are odd. Then:

(i) $\left(\frac{z}{D_1'}\right) = \left(\frac{D_1'}{z}\right) = \left(\frac{w}{z}\right)$.
(ii) $\left(\frac{u}{D_2}\right) = \left(\frac{D_2}{u}\right) = 1$.
(iii) $\left(\frac{|x|}{D_2}\right) = [D_1, D_2]_4 \left(\frac{y}{D_2}\right)$.
(iv) $\left(\frac{|x|}{D_1'}\right) = [D_2, D_1']_4 \left(\frac{z}{D_1'}\right)$.
(v) $\left(\frac{D_1 D_2}{|x|}\right) = \left(\frac{-1}{|x|}\right)$.

Proof. We remark that all numbers except possibly D_1, w and y are odd. In particular, we have

$$D_1' \equiv D_2 \equiv 1 \bmod 4. \tag{25}$$

(i) By reducing (24) modulo z we see: $x^2 \equiv D_1 y^2 \bmod z$ which implies $1 = \left(\frac{D_1}{z}\right) = \left(\frac{D_1'}{z}\right)\left(\frac{w}{z}\right)$ and $\left(\frac{D_1'}{z}\right) = \left(\frac{z}{D_1'}\right)$ by (25).
(ii) By reducing (24) modulo u we get: $x^2 \equiv D_2 z^2 \bmod u$ which implies $\left(\frac{D_2}{u}\right) = 1$.

(iii) We reduce (24) modulo each $p \mid D_2$ and get: $x^2 \equiv D_1 y^2 \bmod p$ and therefore we have $\left(\frac{x}{p}\right) = [D_1, p]_4 \left(\frac{y}{p}\right)$. Then we use the multiplicativity of the symbols and the equality $\left(\frac{-1}{D_2}\right) = 1$ which is a consequence of (25).

(iv) Reduce (24) modulo each $p \mid D_1'$ and proceed as in (iii).

(v) Reducing (24) modulo each p dividing $|x|$ and using multiplicativity we get: $1 = \left(\frac{-D_1 D_2}{|x|}\right) = \left(\frac{-1}{|x|}\right)\left(\frac{D_1 D_2}{|x|}\right)$.

□

Now Proposition 5 is an immediate consequence of the following proposition since all corresponding fields to the decomposition $\{D_1, D_2\}$ are real or not, by Lemma 18.

Proposition 6. *The extension $K_4 = K_2(\sqrt{\alpha})$ defined above is totally real if and only if $[D_1, D_2]_4 = [D_2, D_1]_4$.*

Proof. Since $K_4/\mathbb{Q}$ is Galois we have that K_4 is totally real or totally complex. Furthermore $K_4 = K_2(\sqrt{\alpha}) = K_2(\sqrt{\beta})$ which means that K_4 is totally real if and only if $\alpha > 0$ and $\beta > 0$ which is equivalent to $x > 0$.

We assume the notations of Lemma 21. Using the cases (iii) and (iv) of Lemma 21 we get:

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

We simplify the last two symbols using Lemma 21 and by multiplying with $[D_2, w]_4$ we get the equality:

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

A further simplification with Lemma 21 yields:

$$[D_1, D_2]_4 [D_2, D_1]_4 = \left(\frac{-1}{|x|}\right)\left(\frac{w}{|x|}\right)\left(\frac{w}{z}\right)\left(\frac{2}{D_2}\right)^j [D_2, w]_4. \tag{26}$$

The first case is D_1 odd which implies $w = 1$ and $j \geq 1$. By considering (24) modulo 8 we see that $j = 1$ implies $D_2 \equiv 5 \bmod 8$, and $j \geq 2$ implies $D_2 \equiv 1 \bmod 8$ which trivializes the symbol $\left(\frac{2}{D_2}\right)^j$ to $(-1)^{y/2}$. Therefore the right hand side of (26) simplifies to $\left(\frac{-1}{|x|}\right)(-1)^{y/2} = (-1)^{(|x|+y-1)/2}$. Using $x + y \equiv 1 \bmod 4$ we get that the right hand side equals $+1$ if and only if $x > 0$.

The case D_1 even splits into two cases, namely y odd or even. We remark that $D_2 \equiv 1 \bmod 8$ since $D = D_1 D_2$ is a decomposition of second type. Let us start with y even. We consider (24) modulo 16 and get:

$$x^2 \equiv D_2 z^2 \bmod 16.$$

Since an odd square is congruent to $1, 9 \bmod 16$ we get that an even number of x^2, z^2, D_2 are congruent to $9 \bmod 16$. Furthermore we have that $x^2 \equiv 1 \bmod 16$ if and only if $x \equiv \pm 1 \bmod 8$ which is equivalent to $\left(\frac{2}{|x|}\right) = 1$. Therefore an even number of the symbols $\left(\frac{2}{|x|}\right), \left(\frac{2}{z}\right)$, and $[D_2, 2]_4$ are equal to -1, which means that

the right hand side of (26) simplifies to $\left(\frac{-1}{|x|}\right)\left(\frac{2}{D_2}\right)^j = \left(\frac{-1}{|x|}\right) = (-1)^{(|x|-1)/2}$ since $D_2 \equiv 1 \bmod 8$. Therefore the right hand side is $+1$ if and only if $|x| \equiv 1 \bmod 4$, which is equivalent to $x > 0$ since we assumed that $x \equiv 1 \bmod 4$ (see Lemma 19 (iii)).

The last case is D_1 even and y odd, i.e. $j = 0$. Again we consider (24) modulo 16 and get:

$$x^2 - 8 \equiv D_2 z^2 \bmod 16.$$

With the same argumentation as in the last case we now get that an odd number of the symbols $\left(\frac{2}{|x|}\right)$, $\left(\frac{2}{z}\right)$, and $[D_2, 2]_4$ are equal to -1. Therefore the right hand side of (26) simplifies to $-\left(\frac{-1}{|x|}\right)\left(\frac{2}{D_2}\right)^j = -\left(\frac{-1}{|x|}\right) = (-1)^{(|x|+1)/2}$. Therefore the right hand side is $+1$ if and only if $|x| \equiv 3 \bmod 4$, which is equivalent to $x > 0$ since we assumed that $x \equiv 1 \bmod 4$ (see Lemma 19 (iii)). □

As we already said, the proof of Lemma 21 and Proposition 6 is taken from the unpublished preprint of Franz Lemmermeyer [28].

4. Gaussian integers and the quartic residue symbol

This paragraph is useless for the proof of Theorem 3, but it will be used for the proof of Theorem 4. Theorem 5 is based on conditions for some integer to be or not to be a fourth power modulo another integer. This detection will be done with the help of the quartic (or biquadratic) residue symbol. The paragraphs below gather several classical facts and fix some conventions. All this material can be for instance found in [24, p. 119–127], in [25, p. 53–56] and is the algebraic framework of [12]. The goal of this section is to prove Theorem 6.

Let $\mathbb{Z}[i]$ be the ring of Gaussian integers and denote by $\bar{}$ the complex conjugation. This ring is principal and four units ± 1 and $\pm i$. Up to units, the irreducible elements are $(1+i)$, the rational primes $q \equiv 3 \bmod 4$ and the elements π of $\mathbb{Z}[i]$, such that $\pi\overline{\pi}$ is a rational prime $p \equiv 1 \bmod 4$. An element of $\mathbb{Z}[i]$ or an ideal of $\mathbb{Z}[i]$ are said to be *odd* when its norm is odd. Furthermore we denote by $\mathcal{N}$ the norm function of $\mathbb{Z}[i]$. The associates of the Gaussian integer z are $\pm z, \pm iz$.

To choose one element in the set of its associates, we introduce the notion of *primary*. A non unit element $v = a + ib \in \mathbb{Z}[i]$ is called *primary* if and only if it satisfies $v \equiv 1 \bmod 2(1+i)$, or, in other words

$$\begin{cases} a \equiv 1 \bmod 4 \text{ and } b \equiv 0 \bmod 4 & \text{if } |v|^2 \equiv 1 \bmod 8 \\ \text{or} \\ a \equiv 3 \bmod 4 \text{ and } b \equiv 2 \bmod 4 & \text{if } |v|^2 \equiv 5 \bmod 8. \end{cases}$$

A primary element is odd and every odd element has exactly one primary associate. The product of two primary elements is also primary. Every primary element can be written as the product of primary irreducible elements in a unique way up to the order. If v is primary, then $\overline{v}$ is also primary.

Let π be an odd irreducible element of $\mathbb{Z}[i]$, primary or not, and let $v \in \mathbb{Z}[i]$. We define the *quartic* (or *biquadratic*) symbol $\left(\frac{v}{\pi}\right)_4$ by the formulas

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

where j is the unique integer $0 \leq j \leq 3$ such that

$$v^{(\mathcal{N}(\pi)-1)/4} \equiv i^j \bmod \pi,$$

and

$$\Big(\frac{v}{\pi}\Big)_4 = 0, \quad \text{if } (\pi \mid v).$$

If π and π' are associated, then we have $\big(\frac{\cdot}{\pi}\big)_4 = \big(\frac{\cdot}{\pi'}\big)_4$ and the function $v \mapsto \big(\frac{v}{\pi}\big)_4$ is a multiplicative character of the group $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$. If q is a rational prime $\equiv 3 \bmod 4$, the restriction to $\mathbb{Z}$ of the corresponding quartic character $\Big(\frac{\cdot}{q}\Big)_4$ is simply the principal character modulo q. We extend the definition of the quartic character to any odd element $w \in \mathbb{Z}[i]$, by the formula

$$\Big(\frac{v}{w}\Big)_4 = \prod_j \Big(\frac{v}{w_j}\Big)_4,$$

where w is factorized into irreducible elements $w = \prod_j w_j$. Note the identity

$$\Big(\frac{v^3}{w}\Big)_4 = \Big(\frac{v}{w^3}\Big)_4 = \Big(\frac{\overline{v}}{\overline{w}}\Big)_4 = \overline{\Big(\frac{v}{w}\Big)_4}, \tag{27}$$

for any v and odd $w \in \mathbb{Z}[i]$. Now we recall the reciprocity law for quartic symbols.

Lemma 22. [24, Th.2 p. 123] *Let v and w two primary elements, relatively prime or not. Then we have the equality*

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

and in particular

$$\Big(\frac{v}{w}\Big)_4^2 = \Big(\frac{w}{v}\Big)_4^2.$$

The link between quartic characters and Legendre symbols is given by

Lemma 23. *Let $p \equiv 1 \bmod 4$ be a prime number, decomposed as $p = \pi\overline{\pi}$, where π is primary and irreducible. Then we have for every integer v:*

$$\Big(\frac{v}{\pi}\Big)_4^2 = \Big(\frac{v}{p}\Big).$$

Finally, the quartic residue symbol is useful to detect fourth powers.

Lemma 24. *Let $a \in \mathbb{Z}$ be coprime to a given prime $p \equiv 1 \bmod 4$. Suppose that p is decomposed into $p = \pi\overline{\pi}$, where π is a primary and irreducible element of $\mathbb{Z}[i]$. Then we have*

$$a \text{ is a fourth power } \bmod p \iff \Big(\frac{a}{\pi}\Big)_4 = 1,$$

and

$$a \text{ is a square but not a fourth power } \bmod p \iff \Big(\frac{a}{\pi}\Big)_4 = -1.$$

To treat the case of $\mathcal{D}_{\text{even}}$, we shall require the value of the quartic symbol at 2.

Lemma 25. *Let $v = a + ib$ be a primary element. Then we have*

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

We obtain this formula from [25, Theorem 3.6] (which corresponds to the case v primary irreducible) by using multiplicativity and decomposing v in a product of primary irreducible elements. Now we give a key formula for the symbol $[a,p]_4$, which can be easily deduced from Lemma 24.

Lemma 26. *Let $p \equiv 1 \bmod 4$ be a prime, decomposed as $p = \pi\overline{\pi}$. Then for every integer a (divisible by p or not) we have the equality*

$$[a,p]_4 = \frac{1}{2}\Big(1 + \Big(\frac{a}{p}\Big)\Big) \cdot \Big(\frac{a}{\pi}\Big)_4.$$

Of course, the formula in Lemma 26 is invariant by interchanging π and $\overline{\pi}$. This ambiguity in the notation between π and $\overline{\pi}$ leads us to make the following convention. We explain in the remark at the end of §8.3 why we need this definition.

Definition 3. *An irreducible element $\pi = a + ib \in \mathbb{Z}[i]$ is privileged if it is primary and satisfies the conditions*

$$\mathcal{N}(\pi) \equiv 1 \bmod 4 \text{ and } b > 0.$$

We denote by $\mathfrak{P}$, the set of privileged irreducible elements. An element of $\mathbb{Z}[i]$ is privileged if it is the (eventually empty) product of elements of $\mathfrak{P}$.

The set $\mathfrak{P}$ has the property that it is included in the upper half plane of complex numbers, and the characteristic function of this subset of $\mathbb{C}$ can be approached by Hecke characters (see §5). We shall frequently use the fact that

Lemma 27. *Every special odd discriminant D can be written in a unique way as*

$$D = \mathfrak{d}\overline{\mathfrak{d}},$$

where $\mathfrak{d}$ is a privileged element of $\mathbb{Z}[i]$. Such a factorization of D is called privileged.

We continue our transformation of the symbol $[a,b]_4$ defined in §3.3 and we are obliged to separate the case D odd from the case D even.

Lemma 28. *Let $b \in \mathcal{D}_{odd}$ with its privileged factorization $b = \mathfrak{b}\overline{\mathfrak{b}}$. Then for every integer a, odd or even, coprime or not with b, we have the equality*

$$[a,b]_4 = \frac{1}{2^{\omega(b)}} \prod_{p|b} \Big(1 + \Big(\frac{a}{p}\Big)\Big) \cdot \Big(\frac{a}{\mathfrak{b}}\Big)_4. \tag{28}$$

In particular, if a is coprime with b, we have

$$\eta \frac{1}{2 \cdot 2^{\omega(b)}} \Big(\Big(\frac{a}{\mathfrak{b}}\Big)_4 + \eta\Big) \prod_{p|b} \Big(1 + \Big(\frac{a}{p}\Big)\Big) = \begin{cases} 1 & \text{if } [a,b]_4 = \eta, \\ 0 & \text{otherwise,} \end{cases} \tag{29}$$

for any choice of $\eta \in \{\pm 1\}$.

We also have, for every $b \in \mathcal{D}_{\mathrm{odd}}$, for every integer a, coprime or not with $2b$ the equality

$$[a,8b]_4 = [a,2b]_4 = \frac{[a,2]_4}{2^{\omega(b)}} \prod_{p|b} \Big(1 + \Big(\frac{a}{p}\Big)\Big) \cdot \Big(\frac{a}{\mathfrak{b}}\Big)_4. \tag{30}$$

In particular, if a is coprime with $2b$, we have

$$\eta \frac{1}{2 \cdot 2^{\omega(b)}} \Big(\Big(\frac{a}{\mathfrak{b}}\Big)_4 [a,2]_4 + \eta\Big) \prod_{p|b} \Big(1 + \Big(\frac{a}{p}\Big)\Big) [a,2]_4{}^2 = \begin{cases} 1 & \text{if } [a,2b]_4 = \eta, \\ 0 & \text{otherwise,} \end{cases} \tag{31}$$

for any choice of $\eta \in \{\pm 1\}$.

Proof. We apply multiplicativity to Lemma 26, to prove (28) and (30). For (29) and (31), we first check these formulas when a is not a square modulo b or when $[a,2]_4 = 0$, and then treat the remaining cases. □

We deduce from Lemma 28 a more practical expression of Theorem 5.

Corollary 4. *For any* $D \in \mathcal{D}_{\mathrm{odd}}$ *we have the equalities*

$$2^{\mathrm{rk}_4(\mathrm{Cl}_D)} = \frac{2^{\mathrm{rk}_4(\mathrm{C}_D)}}{2} + \frac{1}{4\cdot 2^{\omega(D)}} \sum_{D=ab} \Big(\frac{\mathfrak{a}}{\mathfrak{b}}\Big)_4^2 \prod_{p\mid a}\Big(1+\Big(\frac{b}{p}\Big)\Big)\prod_{p\mid b}\Big(1+\Big(\frac{a}{p}\Big)\Big). \tag{32}$$

and

$$\begin{aligned} 2^{\mathrm{rk}_4(\mathrm{Cl}_{8D})} =& \frac{1}{2\cdot 2^{\omega(D)}} \sum_{\substack{D=ab\\ b\equiv 1 \bmod 8}} \prod_{p\mid a}\Big(1+\Big(\frac{b}{p}\Big)\Big)\prod_{p\mid b}\Big(1+\Big(\frac{2a}{p}\Big)\Big) \\ &+ \frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=ab} [b,2]_4 \Big(\frac{2}{\mathfrak{b}}\Big)_4 \Big(\frac{\mathfrak{a}}{\mathfrak{b}}\Big)_4^2 \prod_{p\mid a}\Big(1+\Big(\frac{b}{p}\Big)\Big)\prod_{p\mid b}\Big(1+\Big(\frac{2a}{p}\Big)\Big). \end{aligned} \tag{33}$$

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

Proof. From Theorem 5 and from (29) (applied to the symbols $[a,b]_4$ and $[b,a]_4$ with the choices $\eta = \pm 1$), we deduce (for $D \in \mathcal{D}_{\mathrm{odd}}$) the equality

$$\begin{aligned} 2^{\mathrm{rk}_4(\mathrm{Cl}_D)} =& \frac{1}{8\cdot 2^{\omega(D)}} \sum_{D=ab} \prod_{p\mid a}\Big(1+\Big(\frac{b}{p}\Big)\Big)\prod_{p\mid b}\Big(1+\Big(\frac{a}{p}\Big)\Big) \\ &\times \Big[\Big(\Big(\frac{a}{\mathfrak{b}}\Big)_4+1\Big)\Big(\Big(\frac{b}{\mathfrak{a}}\Big)_4+1\Big)+\Big(\Big(\frac{a}{\mathfrak{b}}\Big)_4-1\Big)\Big(\Big(\frac{b}{\mathfrak{a}}\Big)_4-1\Big)\Big]. \end{aligned} \tag{34}$$

In the previous line, the quantity inside $[\cdots]$ is equal to

$$2\Big(\Big(\frac{a}{\mathfrak{b}}\Big)_4\Big(\frac{b}{\mathfrak{a}}\Big)_4+1\Big). \tag{35}$$

By the multiplicativity of the quartic character, by a double application of the reciprocity formula (see Lemma 22) and by (27) we have

$$\Big(\frac{a}{\mathfrak{b}}\Big)_4\Big(\frac{b}{\mathfrak{a}}\Big)_4 = \Big(\frac{\mathfrak{a}}{\mathfrak{b}}\Big)_4\Big(\frac{\overline{\mathfrak{a}}}{\mathfrak{b}}\Big)_4\Big(\frac{\mathfrak{b}}{\mathfrak{a}}\Big)_4\Big(\frac{\overline{\mathfrak{b}}}{\mathfrak{a}}\Big)_4 = \Big(\frac{\mathfrak{a}}{\mathfrak{b}}\Big)_4^2. \tag{36}$$

By (34), (35), and (36) we finally have the equality

$$2^{\mathrm{rk}_4(\mathrm{Cl}_D)} = \frac{1}{4\cdot 2^{\omega(D)}} \sum_{D=ab} \Big(1+\Big(\frac{\mathfrak{a}}{\mathfrak{b}}\Big)_4^2\Big) \prod_{p\mid a}\Big(1+\Big(\frac{b}{p}\Big)\Big)\prod_{p\mid b}\Big(1+\Big(\frac{a}{p}\Big)\Big).$$

It remains to insert the following equality

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=ab} \prod_{p\mid a}\Big(1+\Big(\frac{b}{p}\Big)\Big)\prod_{p\mid b}\Big(1+\Big(\frac{a}{p}\Big)\Big), \tag{37}$$

which is true for any $D \in \mathcal{D}_{\mathrm{odd}}$, to complete the proof of the formula (32). Note that (37) is an easy consequence of Propositions 2 or 3 and of the properties of the symbol $(a \mid b)$. This formula is also an easy consequence of [11, Lemma 27] and implies the second part of Lemma 10.

The proof of (33) has a lot of similarities with the above proof. So we only give two hints. By Theorem 5 and by the definition of the symbol $[a,b]_4$, we must only consider the factorizations of $8D$ in two coprime integers. By symmetry, it is sufficient to consider factorizations of $8D$ of the form $8D = (8a)\cdot b$ and finally multiply the result by 2. Secondly, in the formula (31) of Lemma 28 we can suppress the factor $[a,2]_4{}^2$ if we suppose that $a \equiv 1 \bmod 8$. □

Actually, similarily to (32), the first term on the right part of (33) is equal to $2^{\mathrm{rk}_4(\mathrm{C}_{8D})}/2$. This fact will be flagrant in the next theorem, where we transform Corollary 4 in terms of characters.

Theorem 6. *For any $D \in \mathcal{D}_{\mathrm{odd}}$ we have the equalities*

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

and

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

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.

Proof. It is a game with (32), Lemma 23, the second part of Lemma 22, the reciprocity law for Jacobi symbols and the multiplicativity of the symbols. At first, we have

$$\sum_{D=ab} \left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)_4^2 \prod_{p|a}\Big(1+\left(\frac{b}{p}\right)\Big) \prod_{p|b}\Big(1+\left(\frac{a}{p}\right)\Big) = \sum_{D=ab} \left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)_4^2 \Big(\sum_{t|a}\left(\frac{b}{t}\right)\Big)\Big(\sum_{v|b}\left(\frac{a}{v}\right)\Big).$$

Writing $a = tu$ and $b = vw$ and introducing the privileged factorizations of t, u, v and w, the previous expression is equal to

$$\begin{aligned}
\sum_{D=tuvw} \left(\frac{\mathfrak{t}\,\mathfrak{u}}{\mathfrak{v}\,\mathfrak{w}}\right)_4^2 \left(\frac{vw}{t}\right)\left(\frac{tu}{v}\right) &= \sum_{D=tuvw} \left(\frac{\mathfrak{t}\,\mathfrak{u}}{\mathfrak{v}\,\mathfrak{w}}\right)_4^2 \left(\frac{w}{t}\right)\left(\frac{u}{v}\right) \\
&= \sum_{D=tuvw} \left(\frac{\mathfrak{t}\,\mathfrak{u}}{\mathfrak{v}\,\mathfrak{w}}\right)_4^2 \left(\frac{\mathfrak{w}\overline{\mathfrak{w}}}{\mathfrak{t}}\right)_4^2 \left(\frac{\mathfrak{u}\overline{\mathfrak{u}}}{\mathfrak{v}}\right)_4^2, \\
&= \sum_{D=tuvw} \left(\frac{\mathfrak{t}}{\mathfrak{v}}\right)_4^2 \left(\frac{\mathfrak{u}}{\mathfrak{w}}\right)_4^2 \left(\frac{\overline{\mathfrak{w}}}{\mathfrak{t}}\right)_4^2 \left(\frac{\overline{\mathfrak{u}}}{\mathfrak{v}}\right)_4^2. \qquad (38)
\end{aligned}$$

We continue the transformations by appealing to the following equalities

$$\left(\frac{\mathfrak{t}}{\mathfrak{v}}\right)_4^2 = \left(\frac{\mathfrak{v}}{\mathfrak{t}}\right)_4^2,\ \left(\frac{\mathfrak{u}}{\mathfrak{w}}\right)_4^2 = \left(\frac{\overline{\mathfrak{u}}}{\overline{\mathfrak{w}}}\right)_4^2 \text{ and } \left(\frac{\overline{\mathfrak{u}}}{\mathfrak{v}\overline{\mathfrak{w}}}\right)_4^2 = \left(\frac{\mathfrak{v}\overline{\mathfrak{w}}}{\overline{\mathfrak{u}}}\right)_4^2,$$

which, inserted in (38) gives the first equality of Theorem 6.

By similar techniques, we transform the expression of $2^{\mathrm{rk}_4(\mathrm{Cl}_{8D})}$ given in (33) into

$$2^{\mathrm{rk}_4(\mathrm{Cl}_{8D})} = \Sigma_0 + \frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=abcd} [ab,2]_4 \left(\frac{2}{\mathfrak{a}\,\overline{\mathfrak{b}}}\right)_4 \left(\frac{\mathfrak{a}\,\overline{\mathfrak{b}}}{\mathfrak{c}\,\overline{\mathfrak{d}}}\right)_4^2, \qquad (39)$$

where

$$\Sigma_0 := \frac{1}{2\cdot 2^{\omega(D)}} \sum_{\substack{D=abcd\\ ab\equiv 1 \bmod 8}} \Big(\frac{2}{a}\Big)\Big(\frac{a}{c}\Big)\Big(\frac{b}{d}\Big). \tag{40}$$

Using that a and b are congruent to 1 modulo 4, we can replace the condition $ab \equiv 1 \bmod 8$ by inserting the factor

$$\frac{1}{2}\left(1+\left(\frac{2}{ab}\right)\right)$$

in the summation of (40). Using the multiplicate properties of the Jacobi symbols, the equality $\big(\frac{2}{a}\big)^2 = 1$, and the symmetry between the variables a and b, we arrive at the equality

$$\Sigma_0 = \frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=abcd} \Big(\frac{2}{a}\Big)\Big(\frac{a}{c}\Big)\Big(\frac{b}{d}\Big).$$

Finally, Lemma 11 gives the equality $\Sigma_0 = 2^{\mathrm{rk}_4(\mathrm{C}_{8D})}/2$. Combining with (39) we get the desired formula for $2^{\mathrm{rk}_4(\mathrm{Cl}_{8D})}$. □

5. Privileged primes in arithmetic progressions and applications.

First recall the celebrated Siegel–Walfisz theorem which gives the behavior of the quantity $\pi(x;q,a)$. Here $\pi(x;q,a)$ counts the number of positive rational primes $p \le x$ which are congruent to a modulo q, where a and q are given positive and coprime integers. One of the numerous versions of this theorem is

Lemma 29. *For every positive A there exists a constant $c_1(A) > 0$ such that for all coprime integers a and q with $q \ge 1$ 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 $x \ge 2$ such that $1 \le q \le \log^A(2x)$. The constant implied in the O–symbol is absolute.

(See [9, Theorem 55] & [6, p. 133] for instance). Actually, in this work we apply the Siegel–Walfisz theorem in the following form:

Lemma 30. [25, Corollary 5.29] *For every $q \ge 2$, for every primitive Dirichlet character $\chi \bmod q$, for every positive A, and for every $x \ge 1$ we have the inequality*

$$\sum_{p\le x} \chi(p) \ll_A \sqrt{q}\, x\, \log^{-A}(2x).$$

We wish to have generalizations of Lemmas 29 & 30 to the case of the Gaussian integers $\mathbb{Z}[i]$. First, we fix some notations. For any $z \in \mathbb{C}^*$ we define the argument $\arg z$ of z as satisfying $0 \le \arg z < 2\pi$.

For any a and $0 \ne w \in \mathbb{Z}[i]$, any real θ satisfying $0 \le \theta \le 1$, and $x \ge 0$ we define

$$\pi_{\mathbb{Z}[i]}(x; w, a; \theta)$$

as the number of irreducible elements $\pi \in \mathbb{Z}[i]$ satisfying the conditions

$$|\pi| \le x,\ \pi \equiv a \bmod w \text{ and } 0 \le \arg z < 2\pi\cdot\theta.$$

For $0 \ne w \in \mathbb{Z}[i]$ we define $\phi(w)$ as the generalized Euler function, that means the number of invertible elements of $\mathbb{Z}[i]/(w\mathbb{Z}[i])$. With these conventions we have

Lemma 31. *Let a, w, θ and x as above. Then for every $A > 0$ there exists a positive constant $c_2(A)$ such that the equality*

$$\pi_{\mathbb{Z}[i]}(x; w, a; \theta) = \frac{4\,\theta}{\phi(w)} \int_2^{x^2} \frac{\mathrm{d}t}{\log t} + O\Big(x^2 \exp\Big(-c_2(A)\sqrt{\log(2x)}\Big)\Big),$$

holds uniformly for $x \geq 2$, $0 \leq \theta \leq 1$, $(a, w) = 1$, and $1 \leq \mathcal{N}(w) \leq \log^A(2x)$. The constant implied in the O–symbol is absolute.

This lemma is a particular case of [30, Main Theorem p. 35], where the author deals with the similar question in a very wide generality: counting (in a number field K of degree $n = r_1 + 2r_2$) the number of *prime ideal numbers* (for this notion, see [20]), in arithmetic progressions, such that the associated angles and the norms of the conjugates (considered as complex numbers) satisfy prescribed inequalities. In our application, we have $K = \mathbb{Q}[i]$, $r_1 = 0$ and $r_2 = 1$. Note that $|\pi|$ is the absolute value of some conjugate of π and that we have the relation $|\pi|^2 = \mathcal{N}(\pi)$. Since $\mathbb{Z}[i]$ is principal, the notion of prime ideal numbers is equivalent to the notion of irreducible elements, and the factor 4 in the above formula is the number of roots of unity in $\mathbb{Z}[i]$ (or the number of elements associated to an irreducible one).

5.1. **Consequences of Lemma 31.** Now we want to deduce information on the distribution of privileged primes in arithmetic progressions through the function

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

We remark that we now use $\mathcal{N}$ instead of the complex norm in the above definition. We have

Lemma 32. *Let a and $w \neq 0$ 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 $x \geq 2$, uniformly for a and w as above and satisfying the inequality $1 \leq \mathcal{N}(w) \leq \log^A(2x)$. The constant implied in the O–symbol is absolute.

Proof. Since an irreducible element π is primary if and only if it satisfies the congruence $\pi \equiv 1 \bmod 2(1+i)$, we apply Lemma 31 with w replaced by w', x by $x^{\frac{1}{2}}$ and with the choice $\theta = \frac{1}{2}$. Note that if w is odd, we have $w' = 2(1+i)w$, hence $\phi(w') = 4\phi(w)$. □

Actually, in §6 we shall use the following version of the Siegel–Walfisz theorem for $\mathbb{Z}[i]$ for the square of the quartic symbol on the set of privileged primes. This version mimics Lemma 30.

Proposition 7. *For every $A > 0$ there exists a constant $c_4(A)$ such that the following inequality holds*

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

for every $x \geq 1$, for every $w \neq 1$, which is the product of distinct elements of $\mathfrak{P} \cup \overline{\mathfrak{P}}$.

Similarly, we have

$$\Big| \sum_{\substack{\pi \in \mathfrak{P} \\ \mathcal{N}(\pi) \leq x}} \Big(\frac{\pi}{w}\Big)_4^2 \Big(\frac{2}{\pi}\Big)_4 \big[a\pi\overline{\pi}, 2\big]_4 \Big| \leq c_4(A)\, x\, \sqrt{\mathcal{N}(w)}\, \log^{-A}(2x),$$

for every $x \geq 1$, for every integer a, for every w (eventually equal to 1) which is the product of distinct elements of $\mathfrak{P} \cup \overline{\mathfrak{P}}$.

Proof. We may suppose that $\mathcal{N}(w) \leq \log^{2A}(2x)$, otherwise the result is trivial. By the assumptions concerning w, the character $\big(\frac{\cdot}{w}\big)_4^2$ is non principal. In order to apply Lemma 32 we write

(41)
$$\sum_{\substack{\pi \in \mathfrak{P} \\ \mathcal{N}(\pi) \leq x}} \Big(\frac{\pi}{w}\Big)_4^2 = \sum_{\substack{\lambda \bmod w \\ (\lambda, w) = 1}} \Big(\frac{\lambda}{w}\Big)_4^2 \pi_{\mathrm{priv}}(x; w, \lambda) =$$
$$\Big(\frac{1}{2\phi(w)} \int_2^x \frac{\mathrm{d}t}{\log t}\Big) \Big(\sum_{\substack{\lambda \bmod w \\ (\lambda, w) = 1}} \Big(\frac{\lambda}{w}\Big)_4^2 + O\Big(\phi(w) x \exp(-c_3(2A)\sqrt{\log(2x)})\Big).$$

Using that the sum over all λ is 0, we deduce the inequality

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

where we majorize $\exp(-c_3(2A)\sqrt{\log(2x)})$ by $O(\log^{-2A}(2x))$ and use the inequality $\phi(w) \leq \mathcal{N}(w) \leq \sqrt{\mathcal{N}(w)}\log^A(2x)$. This gives the first part of Proposition 7.

For the second one, we note that we can restrict to the case where $a \equiv 1 \bmod 4$, otherwise the sum is zero. We appeal to Lemma 25, which asserts that the value of the symbol $\big(\frac{2}{\pi}\big)_4$ depends only on the class (modulo 8) of the imaginary part of π. Similarly, the value of the symbol $\big[a\pi\overline{\pi}, 2\big]_4$ depends only on the class of π modulo $8\mathbb{Z}[i]$. Let γ be a variable running over the set

$$\Gamma := \{1,\ 5,\ 3+6i,\ 7+6i,\ 1+4i,\ 5+4i,\ 3+2i,\ 7+2i\}.$$

This set Γ represents all the primary classes modulo $8\mathbb{Z}[i]$. Then the symbol $\Big(\frac{2}{\gamma}\Big)_4$ respectively takes the values

$$1,\ 1,\ i,\ i,\ -1,\ -1, -i, -i. \tag{42}$$

Modulo 16, $\gamma\overline{\gamma}$ takes the values

$$1,\ 9,\ 13,\ 5,\ 1,\ 9,\ 13,\ 5. \tag{43}$$

We apply Lemma 32 with w replaced by $8w$ (then we have $w' = 8w$) and make a computation analogous to (41). We also use the fact that

$$\sum_{\gamma \in \Gamma} \Big(\frac{2}{\gamma}\Big)_4 \big[a\gamma\overline{\gamma}, 2\big]_4 \sum_{\substack{\lambda \bmod w \\ (\lambda, w) = 1}} \Big(\frac{\lambda}{w}\Big)_4^2 = 0,$$

which is trivial when $w \neq 1$. When $w = 1$, it can be checked easily, by using the formulas (42) and (43) and by discussing according to the congruence class of a mod 16. □

Remark. Actually, in order to prove Proposition 7 it is not necessary to appeal to the deep result of Mitsui [30] (now generalized by Goldstein [14]). It is possible to prove this proposition, *ab initio* by the theory of Hecke L–functions $L(s,\chi)$, where $\chi(z)=\left(\frac{z}{w}\right)_4^2(z/|z|)^k$ and k is an integer. In the case of $\mathbb{Z}[i]$ these L–functions are simpler and all the necessary analytic tools (zero–free regions, upper bounds, ...) are for instance gathered in [12, §16] and [25, Chap. 5].

6. Double oscillations of characters.

6.1. **The case of Jacobi symbols.** We recall the following

Lemma 33. [11, Lemma 15] *Let α_m and β_n be complex numbers of modulus less than one. Then for every M, $N\geq 1$ and for every positive ϵ, we have*

$$\sum_{m\leq M}\sum_{n\leq N}\alpha_m\beta_n\mu^2(2m)\mu^2(2n)\Big(\frac{n}{m}\Big)\ll_\epsilon MN\big(M^{-\frac{1}{2}+\epsilon}+N^{-\frac{1}{2}+\epsilon}\big).$$

Such an upper bound for Jacobi symbols appears at several places in the literature, maybe for the first time in [22]. The proof followed in [11] mixes an important result of Heath–Brown [18] and the large sieve inequality for multiplicative characters. However, the method which will be developed in §6.2 applies here also, leading to an upper bound of lower quality when M and N are of comparable sizes (see Proposition 9). This is harmless since we only want to improve the trivial bound by a power of logarithm (see (75)).

6.2. **The case of the square of quartic characters.** The purpose of this paragraph is to give non trivial upper bounds for the sum

$$\Xi(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})=\sum_{\mathcal{N}(m)\leq M}^{\dagger}\sum_{\mathcal{N}(n)\leq N}^{\dagger}\alpha_m\beta_n\mu^2(m)\mu^2(n)\Big(\frac{m}{n}\Big)_4^2, \tag{44}$$

where
- the sum is over the Gaussian integers m and n
- $\dagger$ means that we are summing over odd primary elements of $\mathbb{Z}[i]$,
- μ denotes the natural generalization of the Möbius function to $\mathbb{Z}[i]$,
- $\boldsymbol{\alpha}=(\alpha_m)$ and $\boldsymbol{\beta}=(\beta_n)$ are complex numbers of modulus less than 1 (this restriction on these coefficients will be sufficient for our application in §8 and 10).

The trivial bound for Ξ is

$$\Xi(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})\ll MN,$$

and we want to beat this bound as soon as M is not extremely small compared with N. The way that we are following is quite classical and rests on three properties: any type of reciprocity relation leading to the equality $|\Xi(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})|=|\Xi(N,M,\boldsymbol{\beta},\boldsymbol{\alpha})|$, the multiplicative properties for the numerator and the denominator. Before we can give a first non trivial upper bound we need two helping lemmata. The first one is an easy result from euclidean geometry.

Lemma 34. *Let $R>0$ and Ω_0 be a point in the euclidean plane $\mathbb{R}^2$. Let $B(\Omega_0,R)$ be the closed disk of center Ω_0 and radius R. Then the number of $(a,b)\in\mathbb{Z}^2$ such that the square $[a,a+1[\times[b,b+1[$ is included in $B(\Omega_0,R)$ is equal to*

$$\pi R^2+O(R)$$

and the number of those squares which intersect the edge of $B(\Omega_0,R)$ is equal to $O(R+1)$.

We apply a homothety and the definition of residue classes in $\mathbb{Z}[i]$:

Lemma 35. *Let $a \neq 0$ and ζ be elements of $\mathbb{Z}[i]$. Then the number of $m \in \mathbb{Z}[i]$ satisfying $\mathcal{N}(m) \leq M$ and $m \equiv \zeta \bmod a$ is equal to*

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

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

Now we give a non trivial upper bound of (44). We remark that the missing † in the first sum and the missing $\mu^2(m)$ can be reached by changing α_m accordingly.

Proposition 8. *Let α_m and β_n be any complex numbers of modulus less than 1. Then we get uniformly for $M \geq 1$ and $N \geq 1$ the bound:*

$$\sum_{\mathcal{N}(m) \leq M} \sideset{}{^\dagger}\sum_{\mathcal{N}(n) \leq N} \alpha_m \, \beta_n \, \mu^2(n) \Big(\frac{m}{n}\Big)_4^2 \ll MN\big(N^{-\frac{1}{2}} + M^{-\frac{1}{4}} N^{\frac{1}{2}}\big).$$

Proof. Let $E(M, N)$ be the sum studied in Proposition 8. We can suppose

$$N \leq \sqrt{M}, \tag{45}$$

otherwise Proposition 8 is trivial. By applying Cauchy-Schwarz inequality and by expanding the square, we easily get the inequality

$$|E(M,N)|^2 \ll M \cdot \Big\{ \sideset{}{^\dagger}\sum_{n_1} \sideset{}{^\dagger}\sum_{n_2} \mu^2(n_1)\mu^2(n_2) \Big| \sum_{m} \Big(\frac{m}{n_1 n_2}\Big)_4^2 \Big| \Big\}.$$

Now we apply Lemma 35 by summing over m, with $\mathcal{N}(m) \leq M$, according to its congruence class $\zeta \bmod n_1 n_2$, leading to

$$|E(M,N)|^2 \ll M \cdot \Big\{ \sideset{}{^\dagger}\sum_{n_1} \sideset{}{^\dagger}\sum_{n_2} \mu^2(n_1)\mu^2(n_2) \Big| \sum_{\zeta \bmod n_1 n_2} \Big(\frac{\zeta}{n_1 n_2}\Big)_4^2 \Big(\frac{\pi M}{\mathcal{N}(n_1 n_2)} + O\Big(\sqrt{\frac{M}{\mathcal{N}(n_1 n_2)}} + 1\Big)\Big) \Big| \Big\}.$$

Since n_1 and n_2 are odd, squarefree and primary, the character $\Big(\frac{\cdot}{n_1 n_2}\Big)_4^2$ is principal if and only if $n_1 = n_2$. Hence we deduce

$$|E(M,N)|^2 \ll M \cdot \Big\{ MN + M^{\frac{1}{2}} N^3 + N^4 \Big\} \ll M \cdot \Big\{ MN + M^{\frac{1}{2}} N^3 \Big\},$$

by (45). □

Now we want to loosen the restriction (45). In order to enlarge the summation over m, we apply Hölder's inequality in another way. For the sum E studied in Proposition 8, we have the inequality

$$E(M,N) \ll N^{1-\frac{1}{2k}} \Big(\sideset{}{^\dagger}\sum_{\mathcal{N}(n) \leq N} \mu^2(n) \Big| \sum_{\mathcal{N}(m) < M} \alpha_m \Big(\frac{m}{n}\Big)_4^2 \Big|^{2k} \Big)^{\frac{1}{2k}}. \tag{46}$$

for every even integer $2k \geq 2$. Expanding the $2k$–power we write (46) in the form

$$E(M,N) \ll N^{1-\frac{1}{2k}} \tilde{E}(M^{2k}, N)^{\frac{1}{2k}}, \tag{47}$$

where $\tilde{E}(M^{2k},N)$ has a similar definition as $E(M,N)$ but with α_m replaced by the coefficient

$$\tilde{\alpha}_m = \sum_{m=m_1\cdots m_{2k}} \alpha_{m_1}\cdots\alpha_{m_k}\overline{\alpha}_{m_{k+1}}\cdots\overline{\alpha}_{m_{2k}},$$

which satisfies $\tilde{\alpha}_m \ll_\epsilon M^\epsilon$, for every positive ϵ and where β_n is replaced by some $\tilde{\beta}_n$ with modulus less than 1. Inserting in (47) the upper bound contained in Proposition 8, we obtain

$$\begin{aligned} E(M,N) &\ll_\epsilon N^{1-\frac{1}{2k}}\cdot M^\epsilon\big\{M^{2k}N(N^{-\frac12}+M^{-\frac{k}{2}}N^{\frac12})\big\}^{\frac{1}{2k}} \\ &\ll_\epsilon M^\epsilon\big(MN^{1-\frac{1}{4k}}+M^{\frac34}N^{1+\frac{1}{4k}}\big). \end{aligned} \tag{48}$$

Note that (48) is non trivial in regions which were not covered by Proposition 8 (for instance $M=N$, with $k=2$). Hence we have for every $\epsilon>0$ the inequality

$$E(M,N) \ll_\epsilon MN\min\big\{N^{-\frac12}+M^{-\frac14}N^{\frac12}, M^\epsilon(N^{-\frac18}+M^{-\frac14}N^{\frac18})\big\}.$$

By Lemma 22, the variables m and n play a symmetric rôle in the symbol $\left(\frac{m}{n}\right)_4^2$, hence we have the equality $\Xi(M,N,\boldsymbol{\alpha},\boldsymbol{\beta})=\Xi(N,M,\boldsymbol{\beta},\boldsymbol{\alpha})$, which leads to

Proposition 9. *For every $\epsilon>0$, we have*

$$\begin{aligned} \Xi(M,N,\boldsymbol{\alpha},\boldsymbol{\beta}) \ll MN\min\big\{&N^{-\frac12}+M^{-\frac14}N^{\frac12}, M^{-\frac12}+M^{\frac12}N^{-\frac14}, \\ &M^\epsilon(N^{-\frac18}+M^{-\frac14}N^{\frac18}), N^\epsilon(M^{-\frac18}+M^{\frac18}N^{-\frac14})\big\}. \end{aligned} \tag{49}$$

6.3. **Comments.** The proof of Proposition 9 is quite standard and works for a lot of characters: Jacobi symbols (see Lemma 33 above), cubic characters [19], quartic characters. In [12, p. 1025–1027], such a proof was already given to characters that some authors will later call *Jacobi–Dirichlet symbols* to refer to the seminal work of these two pioneers. We recall the definition as it appears in [25, p. 55-56] (see also [12, p. 1018-1021]): Let q a squarefree positive integer, with all prime factors congruent to 1 mod 4. Let t be its number of prime factors. It is well known that q has exactly 2^t decompositions in the form

$$q = u^2+v^2 \text{ with } u+iv \text{ primary.} \tag{50}$$

There is a bijection between the set $\{(u,v)\}$ of representations of q in the form (50) and the set $\{\omega\}$ of solutions to the congruence

$$\omega^2+1\equiv 0 \bmod q. \tag{51}$$

This bijection is given by $(u,v)\mapsto -\overline{u}v \bmod q$, where $\overline{u}$ is the multiplicative inverse of $u \bmod q$. To each root ω of (51) we associate the following Jacobi–Dirichlet character ψ_ω defined in terms of the usual Jacobi symbol

$$\begin{array}{rccc} \psi_\omega: & \mathbb{Z}[i] & \to & \{0,\pm1\} \\ & z=r+is & \mapsto & \left(\frac{r+\omega s}{q}\right). \end{array} \tag{52}$$

It is easy to see that ψ_ω satisfies $\psi_\omega(z)=\psi_\omega(z+q)=\psi_\omega(z+iq)$ for any $z\in\mathbb{Z}[i]$. Hence it is a multiplicative real character over $(\mathbb{Z}[i]/q\mathbb{Z}[i])^*$. Neither in [12] nor in [25] the following equality between Jacobi–Dirichlet characters and squares of quartic symbols was noticed:

Proposition 10. *Let q a positive squarefree integer with all its prime factors $\equiv 1 \bmod 4$. Let ψ_ω as in (52). Then we have the equality*

$$\psi_\omega(\cdot) = \left(\frac{\cdot}{u-iv}\right)_4^2.$$

Proof. By multiplicativity, it is sufficient to prove this proposition for q prime. Since $\mathbb{Z}[i]/(u-iv)\mathbb{Z}[i]$ is a field with q elements, it has only one character of order 2. The character $\left(\frac{\cdot}{u-iv}\right)_4^2$ has this property. The order of ψ_ω is also 2. Hence it is sufficient to prove that ψ_ω is a character modulo $u-iv$. In order to prove this we must check for every z the equalities

$$\psi_\omega(z) = \psi_\omega(z+(u-iv)) = \psi_\omega(z+i(u-iv)).$$

Coming back to the definition (52), the proof of these equalities is equivalent to the divisibility properties $q \mid u-\omega v$ and $q \mid v+\omega u$. This is a trivial consequence of the definition $\omega \equiv -\overline{u}v \bmod q$. □

In conclusion, thanks to Proposition 10 we may say that our Proposition 9 is only a variant of [12, Prop. 21.3 & p. 1027].

7. Proof of Theorem 3. Odd discriminants

Now we have finished the description of the algebraic and analytic scenery of our proof. It is time to enter in this proof itself. Let

$$S_{\mathrm{odd}}(X,k) := \sum_{\substack{D\in\mathcal{D}_{\mathrm{odd}}\\ D<X}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}. \tag{53}$$

This is the k-th moment of the function $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ on the set $\mathcal{D}_{\mathrm{odd}}$. The aim of this paragraph will be to prove

Proposition 11. *For every integer $k \geq 0$ and for every positive ϵ we have uniformly for $X \geq 3$ the equality*

$$S_{\mathrm{odd}}(X,k) = \prod_{j=0}^{k-1}(2^j+1)\cdot\mathcal{D}_{\mathrm{odd}}(X) + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big).$$

The case $k=0$ is trivial. In §9, we shall prove a similar statement for the set $\mathcal{D}_{\mathrm{even}}$ (see Proposition 13). Then, by additivity, we will have completely proved Theorem 3.

7.1. First transformation of the sum.

For r and s elements of the set

$$\mathcal{Q} := \{0,\,1,\,2,\,3\},$$

let $\kappa_1(r,s)$ be the function defined on $\mathcal{Q}^2$ by

$$\kappa_1(r,s) = \begin{cases} 1 & \text{if } s-r=2,\\ 0 & \text{otherwise.}\end{cases} \tag{54}$$

We appeal to the second part of Lemma 10, in order to write the equality

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=D_0D_1D_2D_3} \prod_{r,\,s\in\mathcal{Q}} \left(\frac{D_r}{D_s}\right)^{\kappa_1(r,s)}, \tag{55}$$

for $D \in \mathcal{D}_{\mathrm{odd}}$, with the convention $0^0 = 1$. In order to raise this formula to the kth–power, we use the same technique as in [11, §5.1], which already was applied in [17]. To solve the k–fold equation

$$D_0^{(1)} D_1^{(1)} D_2^{(1)} D_3^{(1)} = \cdots = D_0^{(k)} D_1^{(k)} D_2^{(k)} D_3^{(k)} = D, \tag{56}$$

we introduce, for $\mathbf{r} = (r_1, \ldots, r_k) \in \mathcal{Q}^k$, the 4^k g.c.d. (greatest common divisor)

$$D_{\mathbf{r}} = \text{g.c.d.}(D_{r_1}^{(1)}, \ldots, D_{r_k}^{(k)}).$$

This parametrizes the solutions of (56) as

$$D_r^{(j)} = \prod_{\substack{\mathbf{r} \in \mathcal{Q}^k \\ r_j = r}} D_{\mathbf{r}} \ (r \in \mathcal{Q},\ 1 \le j \le k),$$

with the constraint $\prod_{\mathbf{r}} D_{\mathbf{r}} = D$. With these changes of variables and by the multiplicativity of Jacobi symbols, we arrive at the equality

$$2^{k \,\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2^k \cdot 2^{k\,\omega(D)}} \sum_{(D_{\mathbf{r}})} \prod_{\mathbf{r}} \prod_{\mathbf{s}} \left(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}} \right)^{\kappa_k(\mathbf{r},\mathbf{s})}, \tag{57}$$

where $\mathbf{r} = (r_1, \ldots, r_k)$, $\mathbf{s} = (s_1, \ldots, s_k) \in \mathcal{Q}^k$ and

$$\kappa_k(\mathbf{r}, \mathbf{s}) = \sum_{j=1}^{k} \kappa_1(r_j, s_j).$$

In (57) the sum is made over all the 4^k–tuples $(D_{\mathbf{r}})$ such that $\prod_{\mathbf{r} \in \mathcal{Q}^k} D_{\mathbf{r}} = D$. The equality (57) is the analogue of [11, formula (25)].

Summing (57) over all $D \in \mathcal{D}_{\mathrm{odd}}$, less than X, we get the following lemma, which can be seen as the analogue of [11, Lemmata 17 & 28]

Lemma 36. *For every $k \ge 1$ and every $X \ge 1$, we have the equality*

$$S_{\mathrm{odd}}(X, k) = \frac{1}{2^k} \sum_{(D_{\mathbf{r}})_{\mathbf{r} \in \mathcal{Q}^k}} \Big(\prod_{\mathbf{r}} 2^{-k\,\omega(D_{\mathbf{r}})} \Big) \prod_{\mathbf{r}} \prod_{\mathbf{s}} \left(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}} \right)^{\kappa_k(\mathbf{r},\mathbf{s})}, \tag{58}$$

where the sum is over all the 4^k–tuples $(D_{\mathbf{r}})_{\mathbf{r} \in \mathcal{Q}^k}$ of coprime integers $D_{\mathbf{r}}$ such that

$$D_{\mathbf{r}} \in \mathcal{D}_{\mathrm{odd}} \cup \{1\} \text{ and } \prod_{\mathbf{r} \in \mathcal{Q}^k} D_{\mathbf{r}} \le X. \tag{59}$$

7.2. **Preparation of the variables.** Let $\ell \ge 1$ be an integer and $\tau_\ell(n)$ be the number of ways of writing n as the product of ℓ positive integers. Note the equality $\tau_\ell(n) = \ell^{\omega(n)}$ for squarefree integers n. From (58) and (59) we directly deduce the inequality

$$|S_{\mathrm{odd}}(X, k)| \le \frac{1}{2^k} \sum_{\substack{D \in \mathcal{D}_{\mathrm{odd}} \\ D \le X}} 2^{-k\,\omega(D)} \tau_{4^k}(D) = \frac{1}{2^k} \sum_{\substack{D \in \mathcal{D}_{\mathrm{odd}} \\ D \le X}} 2^{k\,\omega(D)},$$

which finally gives uniformly for $X \ge 3$:

$$S_{\mathrm{odd}}(X, k) \ll_k X (\log X)^{2^{k-1}-1}. \tag{60}$$

This is a consequence of a now classical result of Shiu [39, Theorem 1], which we will use in the following version:

Lemma 37. *Let γ be a positive real number. Then we have the inequality*

$$\sum_{\substack{n\in\mathcal{D}\\ X-Y<n\le X}} \gamma^{\omega(n)} \ll_\gamma Y(\log X)^{\frac{\gamma}{2}-1},$$

uniformly for $2 \le X\exp\bigl(-\sqrt{\log X}\bigr) \le Y < X$.

If in (60), the summation is over all fundamental discriminants, the crude upper bound would be $\ll_k X(\log X)^{2^k-1}$. The aim of Proposition 11 is to show that the order of magnitude of $S_{\mathrm{odd}}(X,k)$ is $\asymp X/\sqrt{\log X}$, that means much less than the crude estimate (60) by some powers of logarithm. The oscillations of the Jacobi symbols in (58) will be the reason for this gain of powers of $\log X$.

We closely follow the method exposed in [11, §5.3 & 5.4] (see also [17]) which has many similarities with our problem. This allows us to quote the corresponding inequalities in [11] without proving them again in great details. Our first task is to restrict the summation in (58) to the $(D_{\mathbf{r}})$ such that every $D_{\mathbf{r}}$ has not too many prime divisors. By a classical result of Hardy and Ramanujan [15], we know that there exists an absolute B_0, such that for every $X \ge 3$ and for every $\ell \ge 1$ we have the inequality

$$\sharp\bigl\{n \le X \,:\, \omega(n) = \ell,\, \mu^2(n) = 1\bigr\} \le B_0 \cdot \frac{X}{\log X} \cdot \frac{(\log\log X + B_0)^{\ell-1}}{(\ell-1)\,!}.$$

Introducing the parameter

$$\Omega = \mathrm{e}4^k(\log\log X + B_0),$$

and denoting by Σ_1 the contribution to the right part of the equality (58) of the $(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^k}$, which do not satisfy the equality

$$\omega(D_{\mathbf{r}}) \le \Omega, \text{ for all } \mathbf{r} \in \mathcal{Q}^k,$$

we have the inequalities (see [11, formula (30)]):

$$\begin{aligned}\Sigma_1 &\le \sum_{\substack{n\le X\\ \omega(n)\ge\Omega+1}} \mu^2(n)\tau_{4^k}(n)2^{-k\,\omega(n)} = \sum_{\substack{n\le X\\ \omega(n)\ge\Omega+1}} \mu^2(n)2^{k\,\omega(n)}\\ &\le 2^k B_0 \cdot \frac{X}{\log X}\sum_{\ell\ge\Omega} 2^{k\,\ell}\frac{(\log\log X + B_0)^\ell}{\ell\,!},\end{aligned}$$

which finally gives

$$\Sigma_1 \ll \frac{X}{\log X}, \tag{61}$$

by Stirling's formula. This error term is acceptable in view of the error term announced in Proposition 11.

Our next task is to control the order of magnitude of each of the variables $D_{\mathbf{r}}$ appearing in the summation (58) and make these variables independent by transforming the condition $\prod D_{\mathbf{r}} \le X$. We introduce the dissection parameter

$$\Delta := 1 + (\log X)^{-2^k},$$

and for each $\mathbf{r} \in \mathcal{Q}^k$, $A_{\mathbf{r}}$ denotes any number in the set $\{1, \Delta, \Delta^2, \Delta^3, ...\}$. For $\mathbf{A} = (A_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^k}$, we define the restricted sum $S_{\text{odd}}(X, k, \mathbf{A})$ by the formula

$$S_{\text{odd}}(X,k,\mathbf{A}) = \frac{1}{2^k} \sum_{(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^k}} \mu^2\Big(\prod_{\mathbf{r}} D_{\mathbf{r}}\Big)\Big(\prod_{\mathbf{r}} 2^{-k\,\omega(D_{\mathbf{r}})}\Big)\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}, \tag{62}$$

where the sum is over all the 4^k–tuples $(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^k}$ of integers $D_{\mathbf{r}}$ such that

$$A_{\mathbf{r}} \le D_{\mathbf{r}} < \Delta A_{\mathbf{r}},\ D_{\mathbf{r}} \in \mathcal{D}_{\text{odd}} \cup \{1\},\ \omega(D_{\mathbf{r}}) \le \Omega,\ \prod_{\mathbf{r}\in\mathcal{Q}^k} D_{\mathbf{r}} \le X. \tag{63}$$

From Lemma 36, and from formulas (61), (62) and (63), we easily get the equality

$$S_{\text{odd}}(X,k) = \sum_{\mathbf{A}} S_{\text{odd}}(X,k,\mathbf{A}) + O(X(\log X)^{-1}). \tag{64}$$

Actually, in (64), the summation is restricted to the $\mathbf{A}$ such that $\prod_{\mathbf{r}} A_{\mathbf{r}} \le X$ (otherwise the corresponding $S_{\text{odd}}(X, k, \mathbf{A}) = 0$), and by the definition of Δ, the number of terms of $\mathbf{A}$ in consideration in that sum is

$$\ll (\log X)^{4^k(1+2^k)}. \tag{65}$$

We can even restrict to the $\mathbf{A}$ such that

$$\prod_{\mathbf{r}\in\mathcal{Q}^k} A_{\mathbf{r}} < \Delta^{-4^k} X, \tag{66}$$

since the error introduced by this restriction in the right part of (64) is (also see [11, formula (34)]):

$$\le \sum_{\substack{n\in\mathcal{D}_{\text{odd}}\\ \Delta^{-4^k}X\le n\le X}} \mu^2(n)2^{k\,\omega(n)} \ll (1-\Delta^{-4^k})X(\log X)^{2^{k-1}-1} \ll X(\log X)^{-1}, \tag{67}$$

by Lemma 37 and by the definition of Δ. The restriction (66) implies that, in the condition of summations (63), the inequality $\prod_{\mathbf{r}\in\mathcal{Q}^k} D_{\mathbf{r}} \le X$ is now superfluous. In other words, the conditions of summation in the definition (62) of $S_{\text{odd}}(X, k; \mathbf{A})$ are reduced to

$$A_{\mathbf{r}} \le D_{\mathbf{r}} < \Delta A_{\mathbf{r}},\ D_{\mathbf{r}} \in \mathcal{D}_{\text{odd}} \cup \{1\},\ \omega(D_{\mathbf{r}}) \le \Omega. \tag{68}$$

Our next purpose is to prove that in the summation relative to (64), we can also restrict to the case where at least 2^k of the $A_{\mathbf{r}}$ are large. To be more precise we introduce two numbers $X^\dagger$ and $X^\ddagger$ defined by

$$X^\dagger = (\log X)^{3[1+4^k(1+2^k)]} \tag{69}$$

and

$$X^\ddagger \text{ is the least } \Delta^\ell \ge \exp(\log^{\eta(k)} X), \tag{70}$$

where $\eta(k)$ is chosen as a small positive constant $\eta(k) = 2^{-k}\epsilon$. We introduce the condition

$$\text{At most } 2^k - 1 \text{ of the } A_{\mathbf{r}} \text{ are larger than } X^\ddagger. \tag{71}$$

We shall prove

Lemma 38. *For every positive ϵ, for every $k \geq 1$, we have*

$$\sum_{\mathbf{A} \text{ satisfies (71)}} \big|S_{\mathrm{odd}}(X,k,\mathbf{A})\big| \ll_{k,\epsilon} X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon},$$

uniformly for $X \geq 3$.

Proof. We follow the proof of [11, (39)], but we must incorporate the fact that $\mathcal{D}_{\mathrm{odd}}$ is thin. We start from the trivial equality

$$\sum_{\mathbf{A} \text{ satisfies (71)}} \big|S_{\mathrm{odd}}(X,k,\mathbf{A})\big| \leq \sum_{\substack{(D_{\mathbf{r}}) \\ \prod D_{\mathbf{r}} \leq X}} \prod_{\mathbf{r}} 2^{-k\,\omega(D_{\mathbf{r}})}, \tag{72}$$

where the sum is over the 4^k– tuples $(D_{\mathbf{r}})$, where the $D_{\mathbf{r}}$ are coprime elements of $\mathcal{D}_{\mathrm{odd}} \cup \{1\}$, such that at most 2^k-1 of them are larger than $X^{\ddagger}$. Let t $(0 \leq t \leq 2^k-1)$ be the number of these components $D_{\mathbf{r}}$ which are larger than $X^{\ddagger}$. Let n be the product of these $D_{\mathbf{r}}$ and m be the product of the remaining ones. Note that n is also a special odd discriminant. With these conventions and with the help of Lemma 37 and Mertens formula, we transform (72) into

$$\begin{aligned}
&\sum_{\mathbf{A} \text{ satisfies (71)}} \big|S_{\mathrm{odd}}(X,k,\mathbf{A})\big| \\
&\leq \sum_{t=0}^{2^k-1} \sum_{m \leq (X^{\ddagger})^{4^k-t}} \mu^2(m)\tau_{4^k-t}(m)2^{-k\,\omega(m)} \sum_{\substack{n \leq X/m \\ n \in \mathcal{D}_{\mathrm{odd}}}} \tau_t(n)2^{-k\,\omega(n)} \\
&\ll \sum_{t=0}^{2^k-1} \sum_{m \leq (X^{\ddagger})^{4^k-t}} \mu^2(m)\tau_{4^k-t}(m)2^{-k\,\omega(m)}(X/m)(\log X)^{t\,2^{-k-1}-1} \\
&\ll X\Big(\sum_{t=0}^{2^k-1}(\log X)^{t\,2^{-k-1}-1}\Big)\Big(\sum_{m \leq (X^{\ddagger})^{4^k}} \mu^2(m)\frac{2^{k\,\omega(m)}}{m}\Big) \\
&\ll X \cdot (\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}} \cdot (4^k \log X^{\ddagger})^{2^k},
\end{aligned}$$

which gives Lemma 38 with the choice (70). □

7.3. **Linked indices.** In order to push the analysis of the term $S_{\mathrm{odd}}(X,k,\mathbf{A})$ we must enter into the oscillations of the Jacobi symbols. First, we have to determine which symbols $(D_{\mathbf{r}}/D_{\mathbf{s}})$ really appear in the expression (see [11, §5.2], highly inspired by [17]).

Definition 4. *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

$$\kappa_k(\mathbf{r},\mathbf{s}) + \kappa_k(\mathbf{s},\mathbf{r}) \equiv 0 \bmod 2.$$

The same definitions extend to the variables $D_{\mathbf{r}}$ and $D_{\mathbf{s}}$, and similarly to $A_{\mathbf{r}}$ and $A_{\mathbf{s}}$.

The idea behind this notion of linked indices is quite simple: if $\mathbf{r}_0$ and $\mathbf{s}_0$ are linked indices, then, after reduction and simplification of the exponents, in the product $\prod_{\mathbf{r}}\prod_{\mathbf{s}}\left(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\right)^{\kappa_k(\mathbf{r},\mathbf{s})}$ appearing in (62), exactly one of the symbols $\left(\frac{D_{\mathbf{r}_0}}{D_{\mathbf{s}_0}}\right)$

or $\left(\frac{D_{\mathbf{s}_0}}{D_{\mathbf{r}_0}}\right)$ is really present. If the intervals of variations of $D_{\mathbf{r}_0}$ and $D_{\mathbf{s}_0}$ are large enough, there will be cancellations when summing these characters. And the contribution of these terms goes into the error term.

7.4. **First case of oscillation.** We consider the contribution to the right part of (64) of the $\mathbf{A}$ such that

$$\begin{cases}\text{The condition (66) is satisfied}\\ \text{and}\\ \text{there exist two linked indices } \mathbf{r} \text{ and } \mathbf{s} \text{ such that } A_{\mathbf{r}} \text{ and } A_{\mathbf{s}} \geq X^{\dagger}.\end{cases} \tag{73}$$

The following proof mimics [11, (42)]. In that case, we see that $S(X,k,\mathbf{A})$ defined in (62) with the condition of summation (68) satisfies the inequality

$$|S_{\mathrm{odd}}(X,k,\mathbf{A})| \ll (\prod_{\mathbf{u}\neq\mathbf{r},\mathbf{s}} A_{\mathbf{u}})\cdot \sup\Big|\sum_{A_{\mathbf{r}}\leq m<\Delta A_{\mathbf{r}}}\ \sum_{A_{\mathbf{s}}\leq n<\Delta A_{\mathbf{s}}} \alpha_m\beta_n\mu^2(2m)\mu^2(2n)\Big(\frac{n}{m}\Big)\Big|, \tag{74}$$

where the supremum is taken over all the sequences (α_m) and (β_n) with modulus less than 1.

We apply Lemma 33 to the double sum and transform (74) into

$$|S_{\mathrm{odd}}(X,k,\mathbf{A})| \ll \Big(\prod_{\mathbf{u}\neq\mathbf{r},\,\mathbf{s}} A_{\mathbf{u}}\Big)\cdot A_{\mathbf{r}}A_{\mathbf{s}}\big(A_{\mathbf{r}}^{-\frac{1}{3}}+A_{\mathbf{s}}^{-\frac{1}{3}}\big) \ll X(X^{\dagger})^{-\frac{1}{3}}. \tag{75}$$

By (65), (69), and (75) we arrive at

$$\sum_{\mathbf{A}\text{ satisfies (73)}} |S_{\mathrm{odd}}(X,k,\mathbf{A})| \ll X(\log X)^{-1}. \tag{76}$$

7.5. **Second case of oscillation.** Now we consider the contribution of the $\mathbf{A}$ such that

$$\begin{cases}\text{The condition (66) is satisfied,}\\ \text{there exists no pair } \{\mathbf{r},\mathbf{s}\} \text{ of linked indices such that } A_{\mathbf{r}} \text{ and } A_{\mathbf{s}} \geq X^{\dagger}, \text{ and}\\ \text{there exist two linked indices } \mathbf{r} \text{ and } \mathbf{s} \text{ such that } 1 < A_{\mathbf{r}} \leq X^{\dagger} \text{ and } A_{\mathbf{s}} \geq X^{\ddagger}.\end{cases} \tag{77}$$

Now we prove

$$\sum_{\mathbf{A}\text{ satisfies (77)}} |S_{\mathrm{odd}}(X,k,\mathbf{A})| \ll X(\log X)^{-1}. \tag{78}$$

The proof is exactly the same as [11, (43)]. By the assumption (77), we know that there exists an index $\mathbf{s}$ such that $A_{\mathbf{s}} \geq X^{\ddagger}$ and such that the set $\mathcal{R}$ of indices $\mathbf{r}$, which are linked to $\mathbf{s}$, contains no index $\mathbf{r}'$ such that $A_{\mathbf{r}'} \geq X^{\dagger}$ and contains at least one index $\mathbf{r}$ such that $A_{\mathbf{r}} > 1$. Note that the integer d defined by $d = \prod_{\mathbf{r}\in\mathcal{R}} D_{\mathbf{r}}$ is odd, squarefree and satisfies the inequality $1 < d \leq (X^{\dagger})^{4^k}$. With these conventions, we have the inequality

$$|S_{\mathrm{odd}}(X,k,\mathbf{A})| \ll \Big(\prod_{\mathbf{u}\neq\mathbf{s}} A_{\mathbf{u}}\Big)\cdot \max_{a,\,d}\Big|\sum_{\substack{A_{\mathbf{s}}\leq D_{\mathbf{s}}<\Delta A_{\mathbf{s}}\\ (D_{\mathbf{s}},a)=1}} 2^{-k\,\omega(D_{\mathbf{s}})}\Big(\frac{D_{\mathbf{s}}}{d}\Big)\Big|, \tag{79}$$

where

• the maximum is taken over the integers a satisfying $1 \leq a \leq X$ and over the odd squarefree integers d satisfying $1 < d \leq (X^\dagger)^{4^k}$,
• $D_s \in \mathcal{D}_{\mathrm{odd}}$ satisfies $\omega(D_{\mathbf{s}}) \leq \Omega$.

We sum over the value ℓ of $\omega(D_{\mathbf{s}})$ and denote by $P^+(n)$ the greatest prime divisor of the integer $n > 1$. Therefore we write $D_s = np$ in the following formula, where p is the largest prime divisor of D_s and the interior sum of (79) satisfies:

$$\Big|\sum_{D_{\mathbf{s}}} 2^{-k\,\omega(D_{\mathbf{s}})} \Big(\frac{D_{\mathbf{s}}}{d}\Big)\Big| \leq \sum_{1\leq \ell \leq \Omega} 2^{-k\ell} \sum_{n,\, \omega(n)=\ell-1} \Big| \sum_{\substack{\max(P^+(n), A_{\mathbf{s}}/n) < p < \Delta A_{\mathbf{s}}/n \\ p\equiv 1 \bmod 4,\, (p,a)=1}} \Big(\frac{p}{d}\Big)\Big|. \tag{80}$$

We apply Lemma 30 with $q = 4d$, giving the inequality

$$\sum_p \Big(\frac{p}{d}\Big) \ll_A \sqrt{d}\cdot \frac{A_{\mathbf{s}}}{n}\cdot \Big(\log(\frac{A_{\mathbf{s}}}{n})\Big)^{-A} + \log X, \tag{81}$$

for every constant A. We remark that the final log-term is coming from the condition $(a,p)=1$. From the conditions of summation over p, we deduce $p \geq A_{\mathbf{s}}^{\frac{1}{\Omega}}$, then $n < \Delta A_{\mathbf{s}}^{1-\frac{1}{\Omega}}$, and finally

$$\log(\frac{A_{\mathbf{s}}}{n}) \gg \log A_{\mathbf{s}}^{\frac{1}{\Omega}} \gg \log^{\frac{\eta(k)}{2}} X, \tag{82}$$

by (70), (77), and the definition of Ω. Inserting (82) into (81), then into (80), summing over n and ℓ and inserting the result into (79), we finally prove (78), by appealing to (65) and choosing $A = A(k,\epsilon)$ sufficiently large.

Gathering Lemma 38, (64), (76) and (78) we arrive at

Lemma 39. *For every $k \geq 1$ we have*

$$S_{\mathrm{odd}}(X,k) = \sum_{\mathbf{A}\ \textit{satisfies}\ (83)} S_{\mathrm{odd}}(X,k,\mathbf{A}) + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big),$$

where

$$\begin{cases} \textit{The condition } (66) \textit{ is satisfied.} \\ \textit{At least } 2^k \textit{ indices } \mathbf{r} \textit{ satisfy } A_{\mathbf{r}} > X^\ddagger. \\ \textit{Two indices } \mathbf{r} \textit{ and } \mathbf{s} \textit{ such that } A_{\mathbf{r}},\ A_{\mathbf{s}} > X^\dagger \textit{ are always unlinked.} \\ \textit{If } \mathbf{r} \textit{ and } \mathbf{s} \textit{ are linked with } A_{\mathbf{r}} \leq A_{\mathbf{s}}, \textit{ then} \\ \textit{either } A_{\mathbf{r}} = 1 \textit{ or } (2 \leq A_{\mathbf{r}} < X^\dagger \textit{ and } A_{\mathbf{r}} \leq A_{\mathbf{s}} < X^\ddagger). \end{cases} \tag{83}$$

7.6. **Reinterpretation of unlinked indices.** Now we want a deeper knowledge of unlinked indices, to further push the study of the main term in Lemma 39. This will accomplished by appealing to the geometry over the field $\mathbb{F}_2$, as it was done in [11], inspired by [17]. Let ϕ_1 the bijection between $\mathcal{Q}$ and $\mathbb{F}_2^2$ defined by $\phi_1(0) = (0,0)$, $\phi_1(1) = (0,1)$, $\phi_1(2) = (1,0)$, $\phi_1(3) = (1,1)$. This function ϕ_1 can be interpreted as the binary expansion. By concatenation, we obtain a bijection ϕ_k between $\mathcal{Q}^k$ and $\mathbb{F}_2^{2k}$. We shall interpret the property of being unlinked in terms of the quadratic form over $\mathbb{F}_2^{2k}$:

$$P_k(\mathbf{w}) := \sum_{j=1}^{k} w_{2j-1}(w_{2j-1} + w_{2j}), \tag{84}$$

where $\mathbf{w} = (w_1, \dots, w_{2k})$ with $w_i \in \mathbb{F}_2$. We have

Lemma 40. *Two indices* $\mathbf{r}$ *and* $\mathbf{s} \in \mathbb{F}_2^{2k}$ *are unlinked if and only if*

$$P_k\big(\phi_k(\mathbf{r}) + \phi_k(\mathbf{s})\big) = 0.$$

Proof. By Definition 4, two indices $\mathbf{r}$ and $\mathbf{s} \in \mathcal{Q}^k$ are unlinked if and only if the equation $|r_i - s_i| = 2$ has an even number of solutions in $i \in \{1, \dots, k\}$. To finish the proof of Lemma 40, it suffices to incorporate the property for elements r and $s \in \mathcal{Q}$

$$|r - s| = 2 \iff P_1(\phi_1(r) + \phi_1(s)) = 1.$$

This property can be checked case by case. □

For simplicity, we systematically replace the indices $\mathbf{r}$ and $\mathbf{s}$ by their images $\mathbf{u} = \phi_k(\mathbf{r})$ and $\mathbf{v} = \phi_k(\mathbf{s})$ in our computations. Hence $\mathbf{u} = (u_1, \dots, u_{2k})$ and $\mathbf{v} = (v_1, \dots, v_{2k})$ are unlinked if and only if $P_k(\mathbf{u} + \mathbf{v}) = 0$. We remark that this definition coincides with the notion introduced in [11, §5.2]. For $\mathbf{A}$ satisfying (83), let $\mathcal{U} = \mathcal{U}(\mathbf{A})$ be the set of indices $\mathbf{u}$ such that $A_{\mathbf{u}} > X^{\ddagger}$. The set $\mathcal{U}$ satisfies

$$\sharp\mathcal{U}(\mathbf{A}) \geq 2^k, \tag{85}$$

and if $\mathbf{u}$ and $\mathbf{v}$ belong to $\mathcal{U}$, we have $P_k(\mathbf{u} + \mathbf{v}) = 0$, by Lemma 40. The set $\mathcal{U}$ is a set of unlinked indices. We recall some properties of these sets, obtained by the theory of quadratic forms in characteristic 2

Lemma 41. [11, Lemma 18] *Let* $k \geq 1$ *an integer and let* $\mathcal{U} \subset \mathbb{F}_2^{2k}$ *be a set of unlinked indices. Then* $\sharp\mathcal{U} \leq 2^k$ *and for any* $\mathbf{c} \in \mathbb{F}_2^{2k}$, $\mathbf{c}+\mathcal{U}$ *is also a set of unlinked indices. If* $\sharp\mathcal{U} = 2^k$, *then either* $\mathcal{U}$ *is a vector subspace of* $\mathbb{F}_2^{2k}$ *of dimension* k *or a coset of such a subspace of dimension* k.

By (85) and by Lemma 41, we deduce the equality $\sharp\mathcal{U}(\mathbf{A}) = 2^k$ and that $\mathcal{U}(\mathbf{A})$ is a vector subspace or a coset of a vector subspace of dimension k. Furthermore, since there exists no unlinked subset of cardinality $2^k + 1$, we deduce that if $\mathbf{v}$ is such $\mathbf{A}_{\mathbf{v}} < X^{\dagger}$, there exists an index $\mathbf{u}$ linked with $\mathbf{v}$, and such that $A_{\mathbf{u}} > X^{\ddagger}$. The last condition in (83) implies that $A_{\mathbf{v}} = 1$. In conclusion, for every $\mathbf{u} \in \mathcal{U}(\mathbf{A})$, we have $A_{\mathbf{u}} > X^{\ddagger}$, and for every $\mathbf{u} \notin \mathcal{U}(\mathbf{A})$, we have $A_{\mathbf{u}} = 1$. If $\mathcal{U} \subset \mathbb{F}_2^{2k}$ is an unlinked subset of indices $\mathbf{u}$, with cardinality 2^k, we say that $\mathcal{U}$ is *maximal* and if we have $\mathcal{U} = \mathcal{U}(\mathbf{A})$, we say that $\mathbf{A}$ is *associated* to $\mathcal{U}$.

From the above discussion and from Lemma 39, we deduce the following equality

$$\begin{aligned} S_{\mathrm{odd}}(X,k) =& \frac{1}{2^k} \sum_{\mathcal{U}} \sum_{\mathbf{A}} \sum_{(D_{\mathbf{u}})_{\mathbf{u}\in\mathcal{U}}} \mu^2\Big(\prod_{\mathbf{u}} D_{\mathbf{u}}\Big) \Big(\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big) \\ &+ O\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big), \end{aligned} \tag{86}$$

where the first sum is over all the maximal unlinked subsets $\mathcal{U}$ of $\mathbb{F}_2^{2k}$, the second sum is over all $\mathbf{A}$, associated to $\mathcal{U}$ and satisfying (66), and the last sum is over all $(D_{\mathbf{u}})$ such that

$$A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}},\ D_{\mathbf{u}} \in \mathcal{D}_{\mathrm{odd}},\ \omega(D_{\mathbf{u}}) \leq \Omega.$$

Recall that the index $\mathbf{r} \in \mathcal{Q}^k$ has been replaced by its image $\phi_k(\mathbf{r}) = \mathbf{u} \in \mathbb{F}_2^{2k}$.

In (86), we forget all the indices $\mathbf{u}$ which do not belong to $\mathcal{U}$, since the corresponding $D_{\mathbf{u}}$ is equal to 1. By the same techniques which gave (67) and which led

from (72) to Lemma 38, we glue back all the subsums corresponding to the different $\mathbf{A}$ in (86) to obtain the equality

$$S_{\mathrm{odd}}(X,k) = \frac{1}{2^k}\sum_{\mathcal{U}} \sum_{\substack{(D_{\mathbf{u}})_{\mathbf{u}\in\mathcal{U}} \\ \prod_{\mathbf{u}\in\mathcal{U}} D_{\mathbf{u}} \leq X}} \mu^2\Big(\prod_{\mathbf{u}} D_{\mathbf{u}}\Big)\Big(\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big) + O\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big), \tag{87}$$

where now $(D_{\mathbf{u}})_{\mathbf{u}\in\mathcal{U}}$ satisfy the other conditions $D_{\mathbf{u}} \in \mathcal{D}_{\mathrm{odd}} \cup \{1\}$ and $\omega(D_{\mathbf{u}}) \leq \Omega$. For instance, the error term in (87) contains the contribution of the $(D_{\mathbf{u}})_{\mathbf{u}\in\mathcal{U}}$, such that, at least one of $D_{\mathbf{u}}$ is less than $X^{\ddagger}$. This contribution is

$$\begin{aligned} &\ll \sum_{\substack{d\in\mathcal{D}_{\mathrm{odd}} \\ d\leq X^{\ddagger}}} 2^{-k\,\omega(d)} \sum_{\substack{n\in\mathcal{D}_{\mathrm{odd}} \\ n\leq X/d}} \tau_{2^k-1}(n) 2^{-k\,\omega(n)} \\ &\ll \sum_{\substack{d\in\mathcal{D}_{\mathrm{odd}} \\ d\leq X^{\ddagger}}} 2^{-k\,\omega(d)} \cdot \Big(\frac{X}{d}\Big) \cdot (\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}} \\ &\ll X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon} \end{aligned}$$

by Lemma 37 and Mertens formula. By a computation made to obtain (61), in (87), we can drop the condition of summation: $\omega(D_{\mathbf{u}}) \leq \Omega$ with an acceptable error. By putting $D = \prod_{\mathbf{u}\in\mathcal{U}} D_{\mathbf{u}}$ we write (87) as

$$S_{\mathrm{odd}}(X,k) = \frac{1}{2^k}\sum_{\mathcal{U}} \sum_{\substack{D\in\mathcal{D}_{\mathrm{odd}} \\ D<X}} 1 + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big). \tag{88}$$

By Lemma 41, each $\mathcal{U}$ is a coset of some maximal unlinked vector subspace $\mathcal{U}_0$, and since to each $\mathcal{U}_0$ correspond exactly 2^k cosets $\mathcal{U}$, we finally transform (88) into

Lemma 42. *For every $k \geq 1$, for every positive ϵ we have uniformly for $X \geq 3$:*

$$S_{\mathrm{odd}}(X,k) = \sharp\,\mathcal{MS}(k) \cdot \mathcal{D}_{\mathrm{odd}}(X) + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big), \tag{89}$$

where $\mathcal{MS}(k)$ is the set of maximal unlinked vector subspaces $\mathcal{U}_0$ in $\mathbb{F}_2^{2k}$.

7.7. **Quadratic forms in characteristic 2.** For the purpose of computing the coefficient $\sharp\,\mathcal{MS}(k)$ of the main term in (89), we shall require the following results concerning quadratic forms in geometry in characteristic 2. All these facts can be found in [7].

Let $k \geq 1$ and E be the vector space $E = \mathbb{F}_2^{2k}$. Each element of E is written as $\vec{x} = (x_1, \ldots, x_{2k})$. We consider the quadratic form Q over E defined by

$$Q(\vec{x}) = x_1 x_{k+1} + \cdots + x_k x_{2k}.$$

(Note that by a linear change of variable, we can transform the quadratic form P_k defined in (84) into Q).

The form Q is non degenerate. Since $\mathbb{F}_2$ is perfect and since $\dim E$ is even, Q is non defective (see [7, p. 36]). We say that a vector subspace F is *singular* if $Q_{|F} \equiv 0$. Every singular vector space has dimension $\leq k$. All the maximal (for the inclusion) singular spaces have the same dimension (see [7, p.36 & 4, p. 23]).

Let

$$F := \{(x_1, \ldots, x_k, 0, \ldots, 0) \,:\, x_i \in \mathbb{F}_2, (1 \leq i \leq k)\}.$$

We see that F is trivially singular and it is maximal singular, since it has dimension k. Hence Q has *index* k (see [7, p. 34]). We want to know the cardinality of the set $\mathcal{MS}(E,Q)$ of maximal singular vector subspaces contained in (E,Q).

The orthogonal group $\mathrm{O}(E,Q)$ is the subgroup of $\mathrm{Gl}(E)$ containing all the linear automorphisms u of E, satisfying $Q(u(\vec{x})) = Q(\vec{x})$, for all $\vec{x} \in E$. The orthogonal group naturally operates on $\mathcal{MS}(E,Q)$. It operates in a transitive way, since for every F_1 and F_2 maximal singular spaces, there is at least one $u \in \mathrm{O}(E,Q)$, such that $u(F_1) = F_2$. This is an extension of Witt's theorem due to Arf in characteristic 2 (see [7, p. 36]). From these results we have

$$\sharp\,\mathcal{MS}(E,Q) = \frac{\sharp\,\mathrm{O}(E,Q)}{\sharp\,\mathrm{Stab}(F)}, \tag{90}$$

where $\mathrm{Stab}(F)$ denotes the set of $u \in \mathrm{O}(E,Q)$ such that $u(F) = F$.

The numerator of the right part of (90) is well known: This group $\mathrm{O}(E,Q)$ contains a subgroup of index 2: the group of rotations $\mathrm{O}^+(E,Q)$. Its cardinality is given by [7, p. 69]

$$\sharp\mathrm{O}^+(E,Q) = \sharp\mathrm{O}^+_{2k}(\mathbb{F}_2,Q) = (2^k-1)\prod_{j=1}^{k-1}\big(2^{2j}(2^{2j}-1)\big),$$

from which we deduce

$$\sharp\mathrm{O}(E,Q) = 2(2^k-1)\prod_{j=1}^{k-1}\big(2^{2j}(2^{2j}-1)\big). \tag{91}$$

To characterize an element $u \in \mathrm{O}(E,Q)$, such that $u(F) = F$, we study its matrix U in the canonical basis of E. It has the shape

$$U = \begin{pmatrix} A & B \\ O & C \end{pmatrix}, \tag{92}$$

where $A = (a_{i,j})$, $B = (b_{i,j})$, $C = (c_{i,j})$ (with $1 \le i,\, j \le k$) and O are square matrices with size k, A and C belong to $\mathrm{Gl}(k,\mathbb{F}_2)$ and O is the zero matrix. With these conventions, for $\vec{x} = (x_1,\dots,x_{2k})$ and for $u(\vec{x}) = (y_1,\dots,y_{2k})$ and $1 \le j \le k$, by (92), we have the equalities

$$y_j = a_{j,1}x_1 + \cdots + a_{j,k}x_k + b_{j,1}x_{k+1} + \cdots + b_{j,k}x_{2k},$$

$$y_{k+j} = c_{j,1}x_{k+1} + \cdots + c_{j,k}x_{2k}.$$

The condition $Q(u(\vec{x})) = Q(\vec{x})$ leads to the equality

$$\sum_{j=1}^{k}\big(a_{j,1}x_1 + \cdots + a_{j,k}x_k + b_{j,1}x_{k+1} + \cdots + b_{j,k}x_{2k}\big)\big(c_{j,1}x_{k+1} + \cdots + c_{j,k}x_{2k}\big)$$

$$= \sum_{\ell=1}^{k} x_\ell x_{k+\ell}.$$

By equalizing the coefficient of $x_\ell x_{k+m}$ (for $1 \le \ell,\, m \le k$), we get the equality

$$\sum_{j=1}^{k} a_{j,\ell}c_{j,m} = \begin{cases} 1 & \text{if } \ell = m \\ 0 & \text{if } \ell \ne m, \end{cases} \tag{93}$$

and by equalizing the coefficient of $x_{k+\ell}x_{k+m}$, we have for $1 \leq \ell,\, m \leq k$

$$\sum_{j=1}^{k}\big(b_{j,\ell}c_{j,m}+b_{j,m}c_{j,\ell}\big)=0 \text{ if } \ell \neq m, \tag{94}$$

and

$$\sum_{j=1}^{k} b_{j,\ell}c_{j,\ell}=0. \tag{95}$$

The equation (93) is equivalent to

$$ {}^tCA=\mathrm{Id}_k, \tag{96}$$

and the equations (94) and (95) are equivalent to the property

$$ {}^tCB \text{ is a symmetric matrix with a zero diagonal.} \tag{97}$$

Since the characteristic is 2, the condition (97) is equivalent to say that the bilinear form Ψ associated to ${}^tCB$ is alternate, i.e. $\Psi(\vec{x},\vec{x})=0$ for all $\vec{x}\in\mathbb{F}_2^k$. With these characterizations, it is easy to count the cardinality of those U: there are $\sharp\,\mathrm{Gl}(k,\mathbb{F}_2)$ choices for the matrix A, then C is uniquely determined by (96) and belongs also to $\mathrm{Gl}(k,\mathbb{F}_2)$. Since the set of symmetric matrices with dimension k and with zero diagonal is a $\mathbb{F}_2$–vector space of dimension $k(k-1)/2$, the condition (97) determines $2^{\frac{k(k-1)}{2}}$ matrices B when $C\in\mathrm{Gl}(k,\mathbb{F}_2)$ is given. Hence we arrive at the equality

$$\sharp\,\mathrm{Stab}(F)=2^{\frac{k(k-1)}{2}}\prod_{j=0}^{k-1}\big(2^k-2^j\big)=2^{k(k-1)}\prod_{j=1}^{k}\big(2^j-1\big).$$

It remains to insert this last equation and (91) into (90), in order to prove

Lemma 43. *For every $k\geq 1$ the number of maximal singular vector subspaces of E equipped with Q is equal to*

$$\sharp\,\mathcal{MS}(k)=\sharp\,\mathcal{MS}(E,Q)=\prod_{j=0}^{k-1}\big(2^j+1\big).$$

Together with Lemma 42 we complete the proof of Proposition 11.

8. Proof of Theorem 4. Odd discriminants

Let

$$S_{\mathrm{odd}}^{\mathrm{mix}}(X,k):=\sum_{\substack{D\in\mathcal{D}_{\mathrm{odd}}\\ D<X}}2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}\cdot 2^{\mathrm{rk}_4(\mathrm{Cl}_D)},$$

be the mixed moment of order k. The aim of this paragraph is the following odd part of Theorem 4 in the form of

Proposition 12. *For every integer $k\geq 0$ and for every positive ϵ we have uniformly for $X\geq 3$ the equality*

$$S_{\mathrm{odd}}^{\mathrm{mix}}(X,k)=(2^{k-1}+1)\prod_{j=0}^{k-1}(2^j+1)\cdot\mathcal{D}_{\mathrm{odd}}(X)+O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big).$$

The proof of the even part of Theorem 4 will be given in Proposition 15.

8.1. **First reduction.** Replacing $2^{\mathrm{rk}_4(\mathrm{Cl}_D)}$ by its expression given in Theorem 6, we directly have

Lemma 44. *Let*

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

Then we have for every $k\geq 0$:

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

□

By Proposition 11 and Lemma 44, the proof of Proposition 12 is reduced to the study of the sum $S^{\diamond}_{\mathrm{odd}}$. The equality (57) implies the equality

(98)
$$\frac{2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}}{2^{\omega(D)}}\sum_{abcd=D}\left(\frac{\mathfrak{a}\,\overline{\mathfrak{b}}}{\mathfrak{c}\,\overline{\mathfrak{d}}}\right)_4^2=\frac{1}{2^k\cdot 2^{(k+1)\omega(D)}}\sum_{(D_{\mathbf{r}})}\sum_{\mathbf{d}}\prod_{\mathbf{r}}\prod_{\mathbf{s}}\left(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\right)^{\kappa_k(\mathbf{r},\mathbf{s})}\left(\frac{\mathfrak{d}_0\,\overline{\mathfrak{d}}_1}{\mathfrak{d}_2\,\overline{\mathfrak{d}}_3}\right)_4^2,$$

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

$$D=\prod_{\mathbf{r}}D_{\mathbf{r}}=d_0d_1d_2d_3. \tag{99}$$

When $k=0$, the set $\mathcal{Q}^k$ contains only one element and we fix $\kappa_0\equiv 0$. We also follow the convention that $d_i=\mathfrak{d}_i\overline{\mathfrak{d}}_i$ is the privileged factorization of d_i. For $i\in\mathcal{Q}=\{0,1,2,3\}$ and $\mathbf{r}\in\mathcal{Q}^k$, let $D_{\mathbf{r},i}=\mathrm{g.c.d.}(D_{\mathbf{r}},d_i)$. These numbers parametrize the solutions of the equation (99) by writing $D_{\mathbf{r}}=\prod_i D_{\mathbf{r},i}$ and $d_i=\prod_{\mathbf{r}}D_{\mathbf{r},i}$, if we impose the conditions

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

This classical trick was already used to study (56). Summing (98) over the set of odd special $D\leq X$, we have the equality

(100)
$$S^{\diamond}_{\mathrm{odd}}(X,k)=\frac{1}{2^k}\sum_{(D_{\mathbf{r},i})}\mu^2\Big(\prod_{\mathbf{r},i}D_{\mathbf{r},i}\Big)\Big(\prod_{\mathbf{r},i}2^{-(k+1)\omega(D_{\mathbf{r},i})}\Big)\Big\{\prod_{\mathbf{r},i}\prod_{\mathbf{s},j}\left(\frac{D_{\mathbf{r},i}}{D_{\mathbf{s},j}}\right)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\}$$
$$\times\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\left(\frac{\mathfrak{D}_{\mathbf{r},0}}{\mathfrak{D}_{\mathbf{s},2}}\right)_4^2\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\left(\frac{\mathfrak{D}_{\mathbf{r},0}}{\overline{\mathfrak{D}}_{\mathbf{s},3}}\right)_4^2\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\left(\frac{\overline{\mathfrak{D}}_{\mathbf{r},1}}{\mathfrak{D}_{\mathbf{s},2}}\right)_4^2\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\left(\frac{\overline{\mathfrak{D}}_{\mathbf{r},1}}{\overline{\mathfrak{D}}_{\mathbf{s},3}}\right)_4^2\Big\},$$

- where the indices $\mathbf{r}$ and $\mathbf{s}$ belong to $\mathcal{Q}^k$,
- where the indices i and j belong to $\mathcal{Q}$,
- where the 4^{k+1}–tuples $(D_{\mathbf{r},i})$ satisfy

$$D_{\mathbf{r},i}\in\mathcal{D}_{\mathrm{odd}}\cup\{1\}\text{ and }\prod_{\mathbf{r}\in\mathcal{Q}^k}\prod_{i\in\mathcal{Q}}D_{\mathbf{r},i}\leq X, \tag{101}$$

- and where $D_{\mathbf{r},i}=\mathfrak{D}_{\mathbf{r},i}\overline{\mathfrak{D}}_{\mathbf{r},i}$ is the privileged factorization of $D_{\mathbf{r},i}$.

At that point, we see that (100) is already highly intricate. It is really a chance that the remark (8) avoids to have to treat the more general mixed moment sum $\sum_D 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}2^{\ell\,\mathrm{rk}_4(\mathrm{Cl}_D)}$ for any $k\geq 0$ and any $\ell\geq 0$.

8.2. **Analytic preparation of the variables.** By many points of view, the mixed sum $S^{\diamond}_{\mathrm{odd}}(X,k)$ has similarities with the sum $S_{\mathrm{odd}}(X,k+1)$, in particular by the number 4^{k+1} of independent variables $D_{\mathbf{r},i}$. The technical preparation is the same as in §7.2. For $(\mathbf{r},i)\in\mathcal{Q}^{k+1}$, we introduce 4^{k+1}–tuples $\mathbf{A}=(A_{\mathbf{r},i})_{(\mathbf{r},i)\in\mathcal{Q}^{k+1}}$, where $A_{\mathbf{r},i}$ are any numbers of the form 1, Δ, Δ^2,... and the dissection parameter Δ has the value

$$\Delta=1+(\log X)^{-2^{k+1}}.$$

Now, for bounding the number of prime divisors of the variables of summation, Ω is replaced by

$$\Omega'=\mathrm{e}4^{k+1}(\log\log X+B_0). \tag{102}$$

We also introduce the partial sum of $S^{\diamond}_{\mathrm{odd}}(X,k)$:

(103)

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

where the conditions of summation are the same as in (100), with the difference that (101) is replaced by

$$A_{\mathbf{r},i}\le D_{\mathbf{r},i}<\Delta A_{\mathbf{r},i},\ D_{\mathbf{r},i}\in\mathcal{D}_{\mathrm{odd}}\cup\{1\},\ \omega(D_{\mathbf{r},i})\le\Omega'. \tag{104}$$

With these new conventions we have

Lemma 45. *For every integer $k\ge 0$ and for every positive ϵ we have the equality*

$$S^{\diamond}_{\mathrm{odd}}(X,k)=\sum_{\mathbf{A}}S^{\diamond}_{\mathrm{odd}}(X,k,\mathbf{A})+O_{k,\epsilon}\big(X(\log X)^{-\frac12-\frac{1}{2^{k+2}}+\epsilon}\big), \tag{105}$$

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

$$\prod_{\mathbf{r},i}A_{\mathbf{r},i}\le\Delta^{-4^{k+1}}X. \tag{106}$$

Proof. See the proofs of (61) and (67). □

Note that the number of $\mathbf{A}$ participating to the summation in (105) is

$$\ll(\log X)^{4^{k+1}(1+2^{k+1})}. \tag{107}$$

We can even suppose

$$\prod_{\mathbf{r},i}A_{\mathbf{r},i}\ge X^{\frac12}, \tag{108}$$

since the contribution to the right part of (105) of the terms $\mathbf{A}=(A_{\mathbf{r},i})$ which do not satisfy (108) is trivially negligible by Lemma 37.

8.3. **Oscillations of the symbol $\left(\frac{\cdot}{\cdot}\right)_4^2$.** In that section, we shall concentrate on the cancellations having their origins in the oscillations of the square of some quartic symbol in (100). We shall prove

Lemma 46. *We have the equality*

$$\sum_{\mathbf{A}} |S^{\diamond}_{\mathrm{odd}}(X,k,\mathbf{A})| = O(X(\log X)^{-1}), \tag{109}$$

when the sum is made over the $\mathbf{A}$ *such that* (106) *is satisfied and the following inequalities hold:*

$$\big(\prod_{\mathbf{r}} A_{\mathbf{r},0}\big)\cdot\big(\prod_{\mathbf{r}} A_{\mathbf{r},1}\big) > 1 \text{ and } \big(\prod_{\mathbf{r}} A_{\mathbf{r},2}\big)\cdot\big(\prod_{\mathbf{r}} A_{\mathbf{r},3}\big) > 1.$$

Proof. In (100), we clearly see which symbols $\left(\frac{\cdot}{\cdot}\right)_4^2$ do participate to the expression. The idea of the proof of Lemma 46 is rather simple: find two (rather large) variables which collaborate to one $\left(\frac{\cdot}{\cdot}\right)_4^2$ symbol, then benefit of its oscillation by Proposition 7 or Proposition 9, having in mind this oscillation cannot be destroyed by some associated Jacobi symbol, if any.

By (108) the biggest $A_{\mathbf{r},i}$ is rather large, that means $\geq X^{\frac{1}{2\cdot 4^k+1}}$. For simplicity, we suppose that this happens for the index $(\mathbf{r_0},0)$ for some $\mathbf{r_0}\in\mathcal{Q}^k$. The cases $(\mathbf{r_0},i)$ for $i=1$, 2 or 3 are handled in the same way. We separate the discussion in several cases.

• There exists an index $\mathbf{s_0}$ which satisfies

$$A_{\mathbf{r_0},0} \geq A_{\mathbf{s_0},2} > (\log X)^{100\cdot 10^k} \text{ and } \{\mathbf{r_0},\mathbf{s_0}\} \text{ unlinked.}$$

By Definition 4 there is no Jacobi symbol $\left(\frac{D_{\mathbf{r_0},0}}{D_{\mathbf{s_0},2}}\right)$ in (103). Hence, in order to benefit from oscillations of the character $\left(\frac{\mathfrak{D}_{\mathbf{r_0},0}}{\mathfrak{D}_{\mathbf{s_0},2}}\right)_4^2$, we write $S^{\diamond}_{\mathrm{odd}}(X,k,\mathbf{A})$ in the form

$$|S^{\diamond}_{\mathrm{odd}}(X,k,\mathbf{A})| \leq \Big(\prod_{(\mathbf{r},i)\neq(\mathbf{r_0},0),\,(\mathbf{s_0},2)} A_{\mathbf{r},i}\Big)\cdot\Big|\Xi\big(\Delta A_{\mathbf{r_0},0},\Delta A_{\mathbf{s_0},2},\boldsymbol{\alpha},\boldsymbol{\beta}\big)\Big|, \tag{110}$$

where Ξ is defined in (44) for some coefficients α_m and β_n of modulus less than 1. A direct application of Proposition 9 leads to the inequality

$$\Xi\big(\Delta A_{\mathbf{r_0},0},\Delta A_{\mathbf{s_0},2},\boldsymbol{\alpha},\boldsymbol{\beta}\big) \ll A_{\mathbf{r_0},0}\,A_{\mathbf{s_0},2}\,(\log X)^{-50\cdot 10^k}. \tag{111}$$

To be more precise, if $A_{\mathbf{s_0},2} < X^{\frac{1}{5\cdot 4^k+1}}$, we use the first term inside the min–symbol. If we have $X^{\frac{1}{5\cdot 4^k+1}} \leq A_{\mathbf{s_0},2} \leq A_{\mathbf{r_0},0}$, we use the third term with the choice $\epsilon = (200\cdot 10^k)^{-1}$.

Inserting the bound (111) in (110) and summing over the corresponding $\mathbf{A}$ and using (107), we see that the contribution of these $\mathbf{A}$ to the sum of (109) is in $O(X(\log X)^{-1})$.

• There exists an index $\mathbf{s_0}$ which satisfies

$$A_{\mathbf{r_0},0} \geq A_{\mathbf{s_0},2} > (\log X)^{100\cdot 10^k} \text{ and } \{\mathbf{r_0},\mathbf{s_0}\} \text{ linked.}$$

Since the indices $\mathbf{r_0}$ and $\mathbf{s_0}$ are linked, the Jacobi symbol $\left(\frac{D_{\mathbf{r_0},0}}{D_{\mathbf{s_0},2}}\right)$ is really present in (103). But Lemma 23 allows us to write

$$\left(\frac{D_{\mathbf{r_0},0}}{D_{\mathbf{s_0},2}}\right)\left(\frac{\mathfrak{D}_{\mathbf{r_0},0}}{\mathfrak{D}_{\mathbf{s_0},2}}\right)_4^2 = \left(\frac{\overline{\mathfrak{D}}_{\mathbf{r_0},0}}{\mathfrak{D}_{\mathbf{s_0},2}}\right)_4^2,$$

and we are led to the former case by now considering oscillations of the symbol $\left(\frac{\overline{\mathfrak{D}}_{\mathbf{r_0},0}}{\mathfrak{D}_{\mathbf{s_0},2}}\right)_4^2$.

• By working with conjugates, the same type of reasoning applies if there exists an index $\mathbf{s_0}$ such that

$$A_{\mathbf{r_0},0} \geq A_{\mathbf{s_0},3} > (\log X)^{100\cdot 10^k},$$

(see formula (103)).

• From the previous cases and from the hypothesis of Lemma 46, we are reduced to suppose that

$$1 < \max_{\mathbf{s}\in\mathcal{Q}^k}(A_{\mathbf{s},2},\, A_{\mathbf{s},3}) \leq (\log X)^{100\cdot 10^k}. \tag{112}$$

We are now discussing the sizes of the $A_{\mathbf{r},i}$, when the second index is 0 or 1.

• There exists an index $\mathbf{s_0}$ such that

$$A_{\mathbf{r_0},0} \geq A_{\mathbf{s_0},0} > (\log X)^{100\cdot 10^k} \text{ and } \{\mathbf{r_0}, \mathbf{s_0}\} \text{ linked.}$$

This means that in (103), there is the Jacobi symbol $\left(\frac{D_{\mathbf{r_0},0}}{D_{\mathbf{s_0},0}}\right)$, but no square of the quartic symbols with arguments the primary variables associated to the privileged factorization of $D_{\mathbf{r_0},0}$ and $D_{\mathbf{s_0},0}$. We benefit from oscillations of the character $\left(\frac{D_{\mathbf{r_0},0}}{D_{\mathbf{s_0},0}}\right)$, exactly as we did in §7.4, by appealing to Lemma 33. The contribution of these $\mathbf{A}$ to the sum in (109) is also is $O(X(\log X)^{-1})$.

• By symmetry the same study applies if there exists an index $\mathbf{s_0}$, such that

$$A_{\mathbf{r_0},0} \geq A_{\mathbf{s_0},1} > (\log X)^{100\cdot 10^k} \text{ and } \{\mathbf{r_0}, \mathbf{s_0}\} \text{ linked.}$$

• By the condition (112) and by the two previous items, we see that we are reduced to the case, where the variable $D_{\mathbf{r_0},0}$ appears as a numerator of Jacobi symbols or of squares of quartic symbols, where all the corresponding denominators are less than $(\log X)^{100\cdot 10^k}$. Note that this event happens 4^{k+1} times at most. To be more precise, by multiplicativity, we have to consider six types of symbols where $D_{\mathbf{r_0},0}$ appears:

$$\left(\frac{\mathfrak{D}_{\mathbf{r_0},0}}{\mathfrak{a}}\right)_4^2,\ \left(\frac{\mathfrak{D}_{\mathbf{r_0},0}}{\overline{\mathfrak{b}}}\right)_4^2,\ \left(\frac{D_{\mathbf{r_0},0}}{c}\right),\ \left(\frac{D_{\mathbf{r_0},0}}{d}\right),\ \left(\frac{D_{\mathbf{r_0},0}}{e}\right),\ \left(\frac{D_{\mathbf{r_0},0}}{f}\right), \tag{113}$$

where $\mathfrak{a}\overline{\mathfrak{a}} = \prod_{\mathbf{s}} D_{\mathbf{s},2} := a$, where $\mathfrak{b}\overline{\mathfrak{b}} = \prod_{\mathbf{s}} D_{\mathbf{s},3} := b$, where $c = \prod D_{\mathbf{s},0}$, $d = \prod D_{\mathbf{s},1}$, $e = \prod D_{\mathbf{s},2}$, $f = \prod D_{\mathbf{s},3}$, where these last four products are made over the indices $\mathbf{s} \in \mathcal{Q}^k$ linked with $\mathbf{r_0}$. Note that the integers a, b, c, and d are pairwise coprime, that e is a divisor of a and f a divisor of b, hence we write $a = ee'$ and $b = ff'$. Note that the condition (112) and the above discussion imply the inequalities

$$ab > 1 \text{ and } abcdef \leq (\log X)^{400\cdot 40^k}. \tag{114}$$

Lemma 23 and multiplicativity properties of the symbols reduce the product of the six symbols appearing in (113) to

$$\Big(\frac{\mathfrak{D}_{\mathbf{r_0},0}}{\mathfrak{c}\overline{\mathfrak{c}}\,\mathfrak{d}\,\overline{\mathfrak{d}}\,\overline{\mathfrak{e}}\,\mathfrak{e}'\,\mathfrak{f}\,\overline{\mathfrak{f}'}}\Big)_4^2.$$

In the denominators of this symbol we recognize factors of the privileged factorizations of the variables c, d, e, e', f, and f'. Hence we have the inequality

$$|S^{\diamond}_{\mathrm{odd}}(X,k,\mathbf{A})| \le \sum_{\substack{(D_{\mathbf{r},i})\\(\mathbf{r},i)\neq(\mathbf{r_0},0)}} \Big|\sum_{D_{\mathbf{r_0},0}} \mu^2\big(\prod_{\mathbf{r},i} D_{\mathbf{r},i}\big) 2^{-k\,\omega(D_{\mathbf{r_0},0})} \Big(\frac{\mathfrak{D}_{\mathbf{r_0},0}}{\mathfrak{c}\overline{\mathfrak{c}}\,\mathfrak{d}\,\overline{\mathfrak{d}}\,\overline{\mathfrak{e}}\,\mathfrak{e}'\,\mathfrak{f}\,\overline{\mathfrak{f}'}}\Big)_4^2\Big|, \tag{115}$$

where the variables of summation satisfy the conditions (104). The denominator of this symbol appearing in (115) is squarefree. The condition $ab > 1$ implies $\overline{\mathfrak{e}}\,\mathfrak{e}'\,\mathfrak{f}\,\overline{\mathfrak{f}'} \neq 1$. This symbol is not trivial and its conductor has its norm less than a fixed power of $\log X$ by (114). We can apply Proposition 7 (Siegel–Walfisz Theorem for privileged primes) in an efficient manner to the (privileged) largest prime divisor of $\mathfrak{D}_{\mathbf{r_0},0}$, as we did in §7.5, see formulas (79) –(82). We choose the parameter A of this Proposition very large, in terms of k, in order to give the bound

$$S^{\diamond}_{\mathrm{odd}}(X,k,\mathbf{A}) \ll X(\log X)^{-1-4^{k+1}(1+2^{k+1})}. \tag{116}$$

It remains to sum over all $\mathbf{A}$ and to use (107) to complete the proof of Lemma 46. □

Remark. It is time to explain our choice of the set $\mathfrak{P}$ of privileged primes. The formulas given in Lemmata 23 and 26 remain true if we replace π by $\overline{\pi}$. Now suppose that, to each $p \equiv 1 \bmod 4$ we associate $\psi(p) := \pi$, where π is primary and irreducible, and $\pi\overline{\pi} = p$. For every p we have two possibilities and any choice of the function ψ will equally produce the notion of privileged primes and privileged factorization (relative to ψ). All the algebraic transformations on the symbols $\big(\frac{\cdot}{\cdot}\big)$ and $\big(\frac{\cdot}{\cdot}\big)_4^2$ will lead to a formula analogous to (115), but relative to ψ. However, the set $\{\psi(p) : p \equiv 1 \bmod 4\}$ must have some geometric regularity in order to apply Hecke's theory used in the proof of Proposition 7. The choice of defining ψ by imposing $\Im(\psi(p)) > 0$ satisfies this regularity condition and certainly is the more natural one. This choice of ψ is crucial only in the proof of (116).

8.4. **The final step.** By Lemmata 22, 45 and 46 and by symmetry we have for every $k \ge 0$ and for every positive ϵ uniformly for $X \ge 3$ the equality

$$S^{\diamond}_{\mathrm{odd}}(X,k) = 2\sum_{\mathbf{A}} S^{\diamond}_{\mathrm{odd}}(X,k,\mathbf{A}) + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big), \tag{117}$$

where the sum is over all the 4^{k+1}–tuples $(A_{\mathbf{r},i})_{(\mathbf{r},i)\in\mathcal{Q}^{k+1}}$, satisfying (106) and

$$\prod_{\mathbf{r}\in\mathcal{Q}^k} A_{\mathbf{r},2} \prod_{\mathbf{r}\in\mathcal{Q}^k} A_{\mathbf{r},3} = 1. \tag{118}$$

Actually, the condition (118) simply means that we have

$$D_{\mathbf{r},2} = D_{\mathbf{r},3} = 1 \ \text{ for all } \mathbf{r} \in \mathcal{Q}^k$$

in the corresponding summations (104). By (100), for the $\mathbf{A}$ satisfying (118), the sum $S^{\diamond}_{\mathrm{odd}}(X,k,\mathbf{A})$ can be written as

(119)
$$S^{\diamond}_{\mathrm{odd}}(X,k,\mathbf{A}) = \frac{1}{2^k}\sum_{D_{\mathbf{r},0}}\sum_{D_{\mathbf{r},1}}\mu^2\Big(\prod_{\mathbf{r}}D_{\mathbf{r},0}\prod_{\mathbf{r}}D_{\mathbf{r},1}\Big) \times\Big(\prod_{\mathbf{r}}2^{-(k+1)\,\omega(D_{\mathbf{r},0}D_{\mathbf{r},1})}\Big)\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},0}D_{\mathbf{r},1}}{D_{\mathbf{s},0}D_{\mathbf{s},1}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\},$$

where

$$A_{\mathbf{r},i}\le D_{\mathbf{r},i}<\Delta A_{\mathbf{r},i},\ D_{\mathbf{r},i}\in\mathcal{D}_{\mathrm{odd}}\cup\{1\}\text{ and }\omega(D_{\mathbf{r},i})\le\Omega'\text{ for all }(\mathbf{r},i)\in\mathcal{Q}^k\times\{0,1\}.$$

Putting back together all the sums $S^{\diamond}_{\mathrm{odd}}(X,k,\mathbf{A})$ appearing in (117) and bounding the error terms as it was done in §8.2, we arrive at the equality

(120)
$$\begin{aligned}S^{\diamond}_{\mathrm{odd}}(X,k) = 2^{-(k-1)}\sum_{D_{\mathbf{r},0}}\sum_{D_{\mathbf{r},1}}\mu^2\Big(\prod_{\mathbf{r}}D_{\mathbf{r},0}\prod_{\mathbf{r}}D_{\mathbf{r},1}\Big)&\\ \times\Big(\prod_{\mathbf{r}}2^{-(k+1)\,\omega(D_{\mathbf{r},0}D_{\mathbf{r},1})}\Big)\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},0}D_{\mathbf{r},1}}{D_{\mathbf{s},0}D_{\mathbf{s},1}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\}&\\ +O_{k,\epsilon}\big(X(\log X)^{-\frac12-\frac{1}{2^{k+2}}+\epsilon}\big),&\end{aligned}$$

where the variables $D_{\mathbf{r},0}$ and $D_{\mathbf{r},1}$ belong to $\mathcal{D}_{\mathrm{odd}}\cup\{1\}$ and satisfy the inequality

$$\prod_{\mathbf{r}}D_{\mathbf{r},0}\prod_{\mathbf{r}}D_{\mathbf{r},1}\le X.$$

Setting $D_{\mathbf{r}}=D_{\mathbf{r},0}D_{\mathbf{r},1}$ (we have $2^{\omega(D_{\mathbf{r}})}$ possibilities) we modify (120) into

$$\begin{aligned}S^{\diamond}_{\mathrm{odd}}(X,k) = 2^{-(k-1)}\sum_{D_{\mathbf{r}}}\mu^2\Big(\prod_{\mathbf{r}}D_{\mathbf{r}}\Big)\Big(\prod_{\mathbf{r}}2^{-k\,\omega(D_{\mathbf{r}})}\Big)\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\}&\\ +O_{k,\epsilon}\big(X(\log X)^{-\frac12-\frac{1}{2^{k+2}}+\epsilon}\big),&\end{aligned}$$

with the constraints $D_{\mathbf{r}}\in\mathcal{D}_{\mathrm{odd}}\cup\{1\}$ and $\prod_{\mathbf{r}}D_{\mathbf{r}}\le X$. Lemma 36 implies the equality

$$S^{\diamond}_{\mathrm{odd}}(X,k) = 2S_{\mathrm{odd}}(X,k)+O_{k,\epsilon}\big(X(\log X)^{-\frac12-\frac{1}{2^{k+2}}+\epsilon}\big).$$

Now we apply Lemma 44 and the previous equality in order to write

$$S^{\mathrm{mix}}_{\mathrm{odd}}(X,k) = \frac12 S_{\mathrm{odd}}(X,k+1)+\frac12 S_{\mathrm{odd}}(X,k)+O_{k,\epsilon}\big(X(\log X)^{-\frac12-\frac{1}{2^{k+2}}+\epsilon}\big).$$

Now we incorporate Proposition 11 twice and easily check the equality

$$\frac12\prod_{j=0}^{k}(2^j+1)+\frac12\prod_{j=0}^{k-1}(2^j+1) = (2^{k-1}+1)\prod_{j=0}^{k-1}(2^j+1),$$

and finish the proof of Proposition 12.

9. Proof of Theorem 3. Even discriminants

In that section we prove the last part of Theorem 3 which concerns properties of $\mathcal{D}_{\rm even}$. Of course there are a lot of resemblance with the study of $\mathcal{D}_{\rm odd}$ made in §7. Similar to (53) we introduce

$$S_{\rm even}(X,k) := \sum_{\substack{D\in\mathcal{D}_{\rm even}\\ D<X}} 2^{k\,{\rm rk}_4(\mathrm{C}_D)}. \tag{121}$$

Our purpose is to prove

Proposition 13. *For every integer $k\geq 0$ and for every positive ϵ we have uniformly for $X\geq 3$:*

$$S_{\rm even}(X,k)=\prod_{j=0}^{k-1}\big(2^j+1\big)\cdot\mathcal{D}_{\rm even}(X)+O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big).$$

This proposition is the last part of Theorem 3. Hence, by combination with Proposition 11, the proof of Theorem 3 will be complete.

9.1. **Transformation of $S_{\rm even}(X,k)$.** Let $L_1:\mathcal{Q}\to\{0,1\}$ defined via $L_1(3)=1$ and $L_1(0)=L_1(1)=L_1(2)=0$. Now we appeal to Lemma 11 in order to write for every $D\in\mathcal{D}_{\rm even}$ the following equality which has to be compared with (55):

$$2^{{\rm rk}_4(\mathrm{C}_D)}=\frac{1}{2^{\omega(D/8)}}\sum_{D=8D_0D_1D_2D_3}\Big(\prod_{r\in\mathcal{Q}}\Big(\frac{2}{D_r}\Big)^{L_1(r)}\Big)\Big(\prod_{r,\,s\in\mathcal{Q}}\Big(\frac{D_r}{D_s}\Big)^{\kappa_1(r,s)}\Big). \tag{122}$$

Now we raise (122) to the k-th power giving

$$2^{k\,{\rm rk}_4(\mathrm{C}_D)}=\frac{1}{2^{k\,\omega(D/8)}}\sum_{(D_{\mathbf{r}})}\Big(\prod_{\mathbf{r}\in\mathcal{Q}^k}\Big(\frac{2}{D_{\mathbf{r}}}\Big)^{L_k(\mathbf{r})}\Big)\Big(\prod_{\mathbf{r},\,\mathbf{s}\in\mathcal{Q}^k}\Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big), \tag{123}$$

with $\mathbf{r}=(r_1,\dots,r_k)$ and $\mathbf{s}=(s_1,\dots,s_k)\in\mathcal{Q}^k$ and

$$L_k(\mathbf{r})=\sum_{j=1}^{k}L_1(r_j),$$

and the sum being made over all the 4^k–tuples $(D_{\mathbf{r}})$ such that $\prod_{\mathbf{r}\in\mathcal{Q}^k}D_{\mathbf{r}}=D/8$. This equality is the even analogue of (57). We easily see that the even analogue of Lemma 36 is

Lemma 47. *For every $k\geq 1$ and every $X\geq 1$ we have the equality*

$$S_{\rm even}(X,k)=\sum_{(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^k}}\Big(\prod_{\mathbf{r}\in\mathcal{Q}^k}\Big(\frac{2}{D_{\mathbf{r}}}\Big)^{L_k(\mathbf{r})}\Big)\Big(\prod_{\mathbf{r}}2^{-k\,\omega(D_{\mathbf{r}})}\Big)\Big(\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big),$$

where the sum is over all the 4^k–tuples $(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^k}$ of coprime integers $D_{\mathbf{r}}$ such that

$$D_{\mathbf{r}}\in\mathcal{D}_{\rm odd}\cup\{1\}\ \text{and}\ \prod_{\mathbf{r}\in\mathcal{Q}^k}D_{\mathbf{r}}\leq X/8. \tag{124}$$

We follow the technique employed in §7.2–7.6 to prepare the variables and to benefit of the oscillations of the characters with however tiny differences to take

care of the character $D_{\mathbf{r}} \mapsto \left(\frac{2}{D_{\mathbf{r}}}\right)$. When we appeal to Lemma 30, we notice that the character $D_{\mathbf{r}} \mapsto \left(\frac{2}{D_{\mathbf{r}}}\right)\left(\frac{D_{\mathbf{s}}}{D_{\mathbf{r}}}\right)$ has conductor $8D_{\mathbf{s}}$.

Recall that, by the bijection ϕ_k (see §7.6), we can work with indices taken in $\mathbb{F}_2^{2k}$, hence, for $\mathbf{u} = (u_1, \dots, u_{2k}) \in \mathbb{F}_2^{2k}$ we define the function λ_k by

$$\lambda_k(\mathbf{u}) = L_k(\phi_k^{-1}(\mathbf{u})) = \sum_{j=1}^{k} u_{2j-1}u_{2j},$$

Then we arrive at the analogue of (86):

(125)

$$\begin{aligned} S_{\mathrm{even}}(X,k) = &\sum_{\mathcal{U}} \sum_{\mathbf{A}} \sum_{(D_{\mathbf{u}})_{\mathbf{u}\in\mathcal{U}}} \mu^2\Big(\prod_{\mathbf{u}} D_{\mathbf{u}}\Big)\Big(\prod_{\mathbf{u}}\Big(\frac{2}{D_{\mathbf{u}}}\Big)^{\lambda_k(\mathbf{u})}\Big)\Big(\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big) \\ &+ O\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big), \end{aligned}$$

where the first sum is over all the maximal unlinked subsets $\mathcal{U}$ of $\mathbb{F}_2^{2k}$, the second sum is over all $\mathbf{A}$, associated to $\mathcal{U}$ and satisfying

$$\prod_{\mathbf{u}} A_{\mathbf{u}} \le \Delta^{-4^k} X/8,$$

and the last sum is over all $(D_{\mathbf{u}})$ with

$$A_{\mathbf{u}} \le D_{\mathbf{u}} < \Delta A_{\mathbf{u}},\ D_{\mathbf{u}} \in \mathcal{D}_{\mathrm{odd}},\ \omega(D_{\mathbf{u}}) \le \Omega,$$

for all $\mathbf{u} \in \mathcal{U}$. By definition, if $\mathbf{A}$ is associated to $\mathcal{U}$, we have $A_{\mathbf{u}} > X^{\ddagger}$ if and only if $\mathbf{u} \in \mathcal{U}$. Otherwise we have $A_{\mathbf{u}} = 1$.

9.2. **Oscillations of the symbol $\left(\frac{2}{\cdot}\right)$.** We can restrict the set of summation on $\mathcal{U}$ in (125) by considering the oscillations of the symbol $\left(\frac{2}{D_{\mathbf{u}}}\right)$, as follows. Let $\mathcal{U}$ be a maximal unlinked subset of $\mathbb{F}_2^{2k}$ such that there exists an $\mathbf{u_0} \in \mathcal{U}$ satisfying $\lambda_k(\mathbf{u_0}) = 1$ and let $\mathbf{A}$ associated to $\mathcal{U}$. By definition we have $A_{\mathbf{u_0}} \ge X^{\ddagger}$. Then for every $B > 0$ we have

$$\sum_{\substack{A_{\mathbf{u_0}} \le D_{\mathbf{u_0}} < \Delta A_{\mathbf{u_0}} \\ D_{\mathbf{u_0}} \in \mathcal{D}_{\mathrm{odd}},\, \omega(D_{\mathbf{u_0}}) \le \Omega}} \mu^2\Big(\prod_{\mathbf{u}} D_{\mathbf{u}}\Big) 2^{-k\,\omega(D_{\mathbf{u_0}})} \left(\frac{2}{D_{\mathbf{u_0}}}\right)^{\lambda_k(\mathbf{u_0})} \ll_B A_{\mathbf{u_0}} \log^{-B} X, \tag{126}$$

by applying Lemma 30 to the character $\left(\frac{2}{p}\right)$, where p is the largest prime divisor of $D_{\mathbf{u_0}}$ to express that p is uniformly distributed between the classes 1 and 5 mod 8. The technique is the same as in §7.5. Then for such an $\mathbf{A}$ we trivially sum over the corresponding $D_{\mathbf{u}}$ ($\mathbf{u} \ne \mathbf{u_0}$) and see that the corresponding sum is $\ll X(\log X)^{-B}$. Choosing B very large, we see that (125) remains true if we restrict the sum over the $\mathcal{U}$ (maximal unlinked subset of $\mathbb{F}_2^{2k}$), such that $\lambda_k(\mathbf{u}) = 0$ for each $\mathbf{u} \in \mathcal{U}$.

By the same technique which led from (87) to Lemma 42 and which glues back the intervals of summation of the $D_{\mathbf{u}}$, we finally prove:

Proposition 14. *For every integer $k \ge 1$ and for every positive ϵ we have uniformly for $X \ge 3$*

$$S_{\mathrm{even}}(X,k) = \sharp\,\mathcal{MS}^*(k) \cdot \mathcal{D}_{\mathrm{even}}(X) + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+1}}+\epsilon}\big), \tag{127}$$

where $\mathcal{MS}^*(k)$ is the set of maximal unlinked subsets $\mathcal{U}$ in $\mathbb{F}_2^{2k}$ with $\lambda_k(\mathcal{U}) = \{0\}$.

9.3. **Computation of $\sharp\mathcal{MS}^*(k)$.** By Lemma 41 we know that every maximal unlinked subset of $\mathbb{F}_2^{2k}$ is of the form $\mathcal{U}=\mathcal{U}_0+\mathbf{c}$ where $\mathbf{c}$ is any element of $\mathbb{F}_2^{2k}$, and $\mathcal{U}_0$ is a maximal unlinked vector subspace of $\mathbb{F}_2^{2k}$.

Lemma 48. *Let $\mathcal{U}_0$ be a given maximal vector subspace of $\mathbb{F}_2^{2k}$, and let*

$$\mathcal{C}(\mathcal{U}_0) := \{\mathbf{c}\in\mathbb{F}_2^{2k} \ : \ \lambda_k(\mathbf{c}+\mathbf{u})=0 \text{ for all } \mathbf{u}\in\mathcal{U}_0\}.$$

Then we have the equality

$$\mathcal{C}(\mathcal{U}_0) = \rho_k + \mathcal{U}_0, \tag{128}$$

where $\rho_k=(0,1,\dots,0,1)$.

Proof. This is an exercise in linear algebra (see [11, Lemma 36]). First of all, we trivially see that $\mathcal{C}(\mathcal{U}_0)$ is stable by translation by any vector of $\mathcal{U}_0$, in other words

$$\mathcal{C}(\mathcal{U}_0)+\mathcal{U}_0=\mathcal{C}(\mathcal{U}_0). \tag{129}$$

Remember that $P_k(\mathbf{u})=u_1+u_1u_2+\cdots+u_{2k-1}+u_{2k-1}u_{2k}=0$ for every $\mathbf{u}\in\mathcal{U}_0$. This allows us to write

$$\begin{aligned}\mathcal{C}(\mathcal{U}_0) =&\{\mathbf{c}\in\mathbb{F}_2^{2k} \ : \ \lambda_k(\mathbf{c})=0 \text{ and}\\ &(c_2+1)u_1+c_1u_2+\cdots+(c_{2k}+1)u_{2k-1}+c_{2k-1}u_{2k}=0 \text{ for all } \mathbf{u}\in\mathcal{U}_0\}.\end{aligned}$$

We see that ρ_k belongs to $\mathcal{C}(\mathcal{U}_0)$. Since the bilinear form

$$\langle\mathbf{u},\mathbf{v}\rangle = u_1v_2+u_2v_1+\cdots+u_{2k-1}v_{2k}+u_{2k}v_{2k-1}$$

is non degenerate and since $\mathcal{U}_0$ has dimension k, the equation

$$(c_2+1)u_1+c_1u_2+\cdots+(c_{2k}+1)u_{2k-1}+c_{2k-1}u_{2k}=0$$

implies that $\mathcal{C}(\mathcal{U}_0)$ is included in an affine subspace of dimension k containing ρ_k. Combining this last property with (129), we obtain (128). □

From Lemma 48 we deduce the equality

$$\sharp\mathcal{MS}(k)=\sharp\mathcal{MS}^*(k).$$

By Lemma 43 we know the cardinality $\sharp\mathcal{MS}(k)$ of the set of $\mathcal{U}_0$ and by Proposition 14, we finish the proof of Proposition 13.

10. Proof of Theorem 4. Even discriminants

In order to prove the even part of Theorem 4, we introduce

$$S^{\mathrm{mix}}_{\mathrm{even}}(X,k) := \sum_{\substack{D\in\mathcal{D}_{\mathrm{even}}\\ D<X}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}\,2^{\mathrm{rk}_4(\mathrm{Cl}_D)},$$

and we shall prove

Proposition 15. *For every integer $k\geq 0$ and for every positive ϵ we have uniformly for $X\geq 3$:*

$$S^{\mathrm{mix}}_{\mathrm{even}}(X,k)=(2^{k-1}+1)\prod_{j=0}^{k-1}(2^j+1)\cdot\mathcal{D}_{\mathrm{even}}(X)+O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big).$$

Of course, the proof has much to do with what was done in §8, but the symbols containing 2 create extra difficulty. To express $2^{k\,\mathrm{rk}_4(\mathrm{C}_{8D})}$ we shall use (123) and for $2^{\mathrm{rk}_4(\mathrm{Cl}_D)}$ we appeal to the second part of Theorem 6, which we write

$$2^{\mathrm{rk}_4(\mathrm{Cl}_{8D})} = \frac{2^{\mathrm{rk}_4(\mathrm{C}_{8D})}}{2} + g(D), \tag{130}$$

with obvious notations. The expression (130) splits $S^{\mathrm{mix}}_{\mathrm{even}}(X,k)$ into

$$S^{\mathrm{mix}}_{\mathrm{even}}(X,k) = \frac{1}{2}\cdot S_{\mathrm{even}}(X,k+1) + G(X,k), \tag{131}$$

where $S_{\mathrm{even}}(X,k)$ is defined in (121) and studied in Proposition 13, and

(132)

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

where the sums are over $D\in\mathcal{D}_{\mathrm{odd}}$, $D\le X/8$, and over $(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^k}$ and $(E_i)_{i\in\mathcal{Q}}$ such that

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

and $E_i = \mathfrak{E}_i\overline{\mathfrak{E}}_i$ is the privileged factorization of E_i.

10.1. **Study of $G(X,k)$.** Starting from (132), and by applying the same process as in §8.3 & 8.4 we introduce

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

for $r\in\mathcal{Q}^k$ and $i\in\mathcal{Q}$, to finally write the even analogue of (100):

(133)

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

where

- the indices $\mathbf{r}$ and $\mathbf{s}$ belong to $\mathcal{Q}^k$,
- the indices i and j belong to $\mathcal{Q}$,
- the 4^{k+1}–tuples $(D_{\mathbf{r},i})$ satisfy

$$D_{\mathbf{r},i}\in\mathcal{D}_{\mathrm{odd}}\cup\{1\} \text{ and } \prod_{\mathbf{r}\in\mathcal{Q}^k}\prod_{i\in\mathcal{Q}} D_{\mathbf{r},i}\le X/8, \tag{134}$$

- $D_{\mathbf{r},i} = \mathfrak{D}_{\mathbf{r},i}\overline{\mathfrak{D}}_{\mathbf{r},i}$ is the privileged factorization of $D_{\mathbf{r},i}$.

Our next task is to detect the main terms in (133), by following the path of §8.3. However, there is a big difference in the present situation since there is no more

symmetry between the pairs of indices $\{0,1\}$ and $\{2,3\}$. By the same approach, leading to (120), we have

$$G(X,k)=\frac{1}{2}\big(G_{0,1}(X,k)+G_{2,3}(X,k)\big)+O\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big), \tag{135}$$

with

(136)

$$G_{0,1}(X,k)=\sum_{D_{\mathbf{r},0}}\sum_{D_{\mathbf{r},1}}\mu^2\Big(\prod_{\mathbf{r}}D_{\mathbf{r},0}D_{\mathbf{r},1}\Big)\Big(\prod_{\mathbf{r}}2^{-(k+1)\omega(D_{\mathbf{r},0}D_{\mathbf{r},1})}\Big)$$
$$\times\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},0}D_{\mathbf{r},1}}{D_{\mathbf{s},0}D_{\mathbf{s},1}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\}\Big(\prod_{\mathbf{r}}\Big(\frac{2}{D_{\mathbf{r},0}\,D_{\mathbf{r},1}}\Big)^{L_k(\mathbf{r})}\Big),$$

and

$$G_{2,3}(X,k)=\sum_{D_{\mathbf{r},2}}\sum_{D_{\mathbf{r},3}}\mu^2\Big(\prod_{\mathbf{r}}D_{\mathbf{r},2}D_{\mathbf{r},3}\Big)\Big(\prod_{\mathbf{r}}2^{-(k+1)\omega(D_{\mathbf{r},2}D_{\mathbf{r},3})}\Big) \tag{137}$$
$$\times\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},2}D_{\mathbf{r},3}}{D_{\mathbf{s},2}D_{\mathbf{s},3}}\Big)^{\kappa_k(\mathbf{r},\mathbf{s})}\Big\}\Big(\prod_{\mathbf{r}}\Big(\frac{2}{D_{\mathbf{r},2}D_{\mathbf{r},3}}\Big)^{L_k(\mathbf{r})}\Big)$$
$$\times\Big(\prod_{\mathbf{r}}\Big(\frac{2}{\mathfrak{D}_{\mathbf{r},2}\overline{\mathfrak{D}}_{\mathbf{r},3}}\Big)_4\Big)\Big[\prod_{\mathbf{r}}D_{\mathbf{r},2}D_{\mathbf{r},3},2\Big]_4,$$

where the variables of summations satisfy (134).

In (136), we write $D_{\mathbf{r}}=D_{\mathbf{r},0}D_{\mathbf{r},1}$ and we see at once the equality (see Lemma 47):

$$G_{0,1}(X,k)=S_{\mathrm{even}}(X,k)+O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big). \tag{138}$$

But $G_{2,3}(X,k)$ is an error term because of the oscillations of the symbols containing 2. To prove this, we argue as in §8.2 and §8.3. First of all, we split the summations in (137) in order to make the variables $D_{\mathbf{r},i}$ ($i=2$ or 3) independent. This means that we split the summation into subsums corresponding to the extra inequalities

$$A_{\mathbf{r},i}\le D_{\mathbf{r},i}<\Delta A_{\mathbf{r},i},\ \omega(D_{\mathbf{r},i})\le\Omega'\ (i=2,3)$$

with an admissible error (Ω' is defined in (102)). We may also suppose

$$X^{\frac{1}{2}}\le\prod_{\mathbf{r}}A_{\mathbf{r},2}A_{\mathbf{r},3}\le\Delta^{-4^{k+1}}X/8 \tag{139}$$

with an admissible error.

For notational simplicity, we suppose that the largest $A_{\mathbf{r},i}$ is of the form $A_{\mathbf{r_0},2}$, hence it is greater than $X^{4^{-(k+1)}}$. We consider two cases:

• There is an index $(\mathbf{s_0},2)$ satisfying

$$A_{\mathbf{r_0},2}>\ A_{\mathbf{s_0},2}>(\log X)^{100\cdot 10^k}\text{ and }\kappa_k(\mathbf{r_0},\mathbf{s_0})+\kappa_k(\mathbf{s_0},\mathbf{r_0})\equiv 1\bmod 2. \tag{140}$$

The last condition means that the indices $\mathbf{r_0}$ and $\mathbf{s_0}$ are linked. The symbol $\Big(\frac{D_{\mathbf{r_0},2}}{D_{\mathbf{s_0},2}}\Big)$ is really present in (137) and the associated variables are large. Hence Lemma 33 is efficient. The same holds if the index $(\mathbf{s_0},2)$ is replaced by $(\mathbf{s_0},3)$.

• All the variables which are linked with $D_{\mathbf{r_0},2}$ are small (which means that their sizes do not satisfy the inequality in (140)). Let d be the product of these variables.

Note that $d \equiv 1 \bmod 4$ is an integer. This integer d may be equal to 1 but it is less than some power of $\log X$. The sum we are studying can be written as

$$S := \sum_d \sum_\ell \alpha_{d,\ell} \sum_{D_{\mathbf{r_0},2}} 2^{-(k+1)\,\omega(D_{\mathbf{r_0},2})} \left(\frac{D_{\mathbf{r_0},2}}{d}\right)\left(\frac{2}{\mathfrak{D}_{\mathbf{r_0},2}}\right)_4 \big[d\ell D_{\mathbf{r_0},2}, 2\big]_4, \tag{141}$$

or as its conjugate, according to the value of $L_k(\mathbf{r_0})$. In (141), $\alpha_{d,\ell}$ is some complex number with modulus less than one, the product $d\ell D_{\mathbf{r_0},2}$ replaces $\prod_{\mathbf{r}} D_{\mathbf{r},2} D_{\mathbf{r},3}$. We apply the last part of Proposition 7 to the largest prime privileged divisor of $D_{\mathbf{r_0},2}$ (as we did several times before) by using the equality

$$\left(\frac{D_{\mathbf{r_0},2}}{d}\right) = \left(\frac{\mathfrak{D}_{\mathbf{r_0},2}}{d}\right)_4^2$$

This leads to

$$S \ll \Big(\prod_{\mathbf{r}} A_{\mathbf{r},2} A_{\mathbf{r},3}\Big)(\log X)^{-B} \ll X(\log X)^{-B},$$

for any constant B. Summing over all the $A_{\mathbf{r},i}$ satisfying (139), we get

$$G_{2,3}(X,k) = O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big). \tag{142}$$

Inserting (138) and (142) in (135), we get

$$\begin{aligned} G(X,k) &= \frac{1}{2}\cdot S_{\mathrm{even}}(X,k) + O_{k,\epsilon}\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big), \\ &= \frac{1}{2}\prod_{j=0}^{k-1}(2^j+1)\cdot \mathcal{D}_{\mathrm{even}}(X) + O\big(X(\log X)^{-\frac{1}{2}-\frac{1}{2^{k+2}}+\epsilon}\big). \end{aligned}$$

by Proposition 13. It remains to insert this equality into (131), to apply Proposition 13 to $S_{\mathrm{even}}(X,k+1)$ and to sum the coefficients of the main terms to conclude the proof of Proposition 15.

References

[1] V. Blomer, On the negative Pell equation. *preprint,* 2006.

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

[3] H. Cohen and H.W. Lenstra, Heuristics on class groups of number fields. *in* Number Theory, Noordwijkerhout 1983. *Lecture Notes in Math.*, vol. 1068: 33–62, Springer, Berlin, 1984.

[4] H. Cohn, A Classical Invitation to Algebraic Numbers and Class Fields. Springer, New York-Heidelberg-Berlin, 1978.

[5] L. Comtet, Advanced Combinatorics *(Revised and enlarged edition)*, D. Reidel Publishing Company, 1974.

[6] H. Davenport, Multiplicative Number Theory (Second Edition). *Graduate Texts in Mathematics*, 74, Springer–Verlag, 1980.

[7] J. Dieudonné, La Géométrie des Groupes Classiques (Troisième Edition). Springer, 1971.

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

[9] T. Esterman, Introduction to modern Prime Number Theory. *Cambridge Tracts in Mathematics and Mathematical Physics*, 41, Cambridge at the University Press, 1952.

[10] E. Fouvry and J. Klüners, Cohen–Lenstra heuristics of quadratic number fields. In : F. Hess, S. Pauli, and M. Pohst (ed.) *ANTS Proceedings Berlin,* LNCS 4076 : 40–55, 2006.

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

[12] J. Friedlander and H. Iwaniec, The polynomial X^2+Y^4 captures its primes. *Annals of Math.*, 148 : 945–1040, 1998.

[13] F. Gerth III, The 4–rank class of quadratic fields *Inv. Math.*, 77(3) : 489–515, 1984.

[14] L.J. Goldstein, A generalization of the Siegel–Walfisz theorem *Trans. A.M.S.*, 149 : 417–429, 1970.

[15] 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.
[16] H. Hasse, Number Theory, *Grundlehren der mathematischen Wissenschaften. 229*, Springer, 1978.
[17] D.R. Heath–Brown, The size of Selmer groups for the congruent number problem, II *Inv. Math.*, 118 : 331–370, 1994.
[18] D.R. Heath–Brown, A mean value estimate for real character sums. *Acta Arith.*, 72 : 235–275, 1995.
[19] D.R. Heath–Brown, Kummer's conjecture for cubic Gauss sums. *Israel Journal of Math.*, 120 : 67–124, 2000.
[20] E. Hecke, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. II. *Math. Zeit.*, 6 : 11–51, 1920.
[21] E. Hecke, Lectures on the theory of algebraic numbers. Springer, 1981.
[22] H. Heilbronn, On the averages of some arithmetic functions of two variables. *Mathematika*, 5 : 1–7, 1958.
[23] C. Hooley, On the Pellian equation and the class number of indefinite binary quadratic forms. J. Reine Angew. Math., 353:98–131 (1984).
[24] K. Ireland and M. Rosen, A classical introduction to modern number theory (Second edition). *Graduate texts in Mathematics*, 84, Springer, 1990.
[25] H. Iwaniec and E. Kowalski, Analytic Number Theory. *Colloquium Publications*, 53, AMS, 2004.
[26] G. Janusz, Algebraic Number Fields. Graduate Studies in Mathematics, 2nd edition, AMS, 1996.
[27] M. Karoubi and T. Lambre, Sur la K-théorie du foncteur norme. *J. Algebra*, to appear.
[28] F. Lemmermeyer, The 4–class group of real quadratic number fields. Preprint, http://www.rzuser.uni-heidelberg.de/∼hb3/rank4.ps
[29] S. Louboutin, Groupes des classes d'idéaux triviaux. *Acta Arithmetica*, 54: 61–74, 1989.
[30] T. Mitsui, Generalized Prime Number Theorem. *Japanese Journal of Math.*, 26 : 1–42, 1956.
[31] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers (Second edition). Springer, 1990.
[32] 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.
[33] L. Redei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.* 171 : 55–60, 1934.
[34] 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.
[35] 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.
[36] G. J. Rieger, Über die Anzahl der als Summe von zwei Quadraten darstellbaren und in einer primen Restklasse gelegenen Zahlen unterhalb einer positiven Schranke. II. *J. reine angew. Math.*, 217: 200–216, 1965.
[37] J.-P. Serre, Local Fields, Springer, Berlin, 1979.
[38] A. Scholz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, Math. Z. **39**, 95–111 (1935).
[39] P. Shiu, A Brun–Titchmarsh theorem for multiplicative functions. *J. reine angew. Math.* 313: 161–170, 1980
[40] P. Stevenhagen, The number of real quadratic fields with units of negative norms. *Experiment. Math.*, 2: 121–136, 1993.
[41] A. Weil, Number Theory: An approach through History. Birkhäuser, Boston, 1984.

Univ. Paris-Sud, Laboratoire de Mathématiques d'Orsay, CNRS, F-91405 Orsay Cedex, France.
E-mail address: Etienne.Fouvry@math.u-psud.fr

Universität Paderborn, Institut für Mathematik, 33095 Paderborn, Germany
E-mail address: klueners@math.uni-paderborn.de