WEIGHTED DISTRIBUTION OF THE 4–RANK OF CLASS GROUPS AND APPLICATIONS

ÉTIENNE FOUVRY AND JÜRGEN KLÜNERS

Abstract. We prove that the distribution of the values of the 4–rank of ideal class groups of quadratic fields is not affected when it is weighted by a divisor type function. We then give several applications concerning a new lower bound of the sums of class numbers of real quadratic fields with discriminant less than a bound tending to infinity and several questions of P. Sarnak concerning reciprocal geodesics.

1. Introduction

All along this paper the letter D, without index, will be reserved to denote a *fundamental discriminant*, that means the discriminant of a quadratic extension of $\mathbb{Q}$.

A fundamental discriminant D is said to be a *special discriminant* when it satisfies

$$D > 0 \text{ and } p \mid D \Rightarrow p \not\equiv 3 \bmod 4.$$

(As usual, the letter p is reserved for prime numbers.) In other words, a fundamental discriminant is special if and only if it is the sum of two squares. Recall also that if the fundamental unit ϵ_D of $\mathbb{Q}(\sqrt{D})$ has norm -1, then necessarily, D is special (see §1.1 below).

We are concerned with some aspects of the average behavior of the ideal class group (in the narrow sense) of the ring of integers $\mathcal{O}_D$ of the number field $\mathbb{Q}(\sqrt{D})$. We denote by $\mathcal{N}$ the norm on that field. Recall that two non zero ideals $\mathfrak{I}$ and $\mathfrak{J}$ of $\mathcal{O}_D$ are said to be *equivalent in the narrow sense*, (denoted by $\mathfrak{I} \sim \mathfrak{J}$) if and only if there exists $\alpha \in \mathcal{O}_D$, such that $\mathfrak{I} = (\alpha) \cdot \mathfrak{J}$ with $\mathcal{N}(\alpha) > 0$. We denote by C_D this class group and by $h(D)$ its cardinality (the *class number*).

We now say that the non zero ideals $\mathfrak{I}$ and $\mathfrak{J}$ are *equivalent in the ordinary sense*, if they satisfy $\mathfrak{I} = (\alpha) \cdot \mathfrak{J}$ for some $\alpha \in \mathcal{O}_D$, without any condition on the sign of $\mathcal{N}(\alpha)$. With this definition we build the *ordinary class group* Cl_D.

What is the structure of the finite abelian group C_D? Cohen and Lenstra have built a probabilistic model to guess the average behavior of C_D, in particular of the p–rank of that group, denoted by

$$\mathrm{rk}_p(\mathrm{C}_D) := \dim_{\mathbb{F}_p}\big(\mathrm{C}_D/\mathrm{C}_D^p\big).$$

Recall that the case $p = 2$ is entirely solved by a famous result of Gauss (see (10) below). The original so–called *heuristics of Cohen–Lenstra* (see [3]) only concerned the cases $p \geq 3$. These heuristics were extended and approached by Gerth [10] in the case of the 4–rank of C_D, which, by definition, is

$$\mathrm{rk}_4(\mathrm{C}_D) := \dim_{\mathbb{F}_2}\big(\mathrm{C}_D^2/\mathrm{C}_D^4\big).$$

Date: May 18, 2010.

1991 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R11.

Recently Fouvry and Klüners proved the Cohen–Lenstra–Gerth conjecture in the case of the 4–rank (see [6]). They also proved the analogous conjecture, due to Stevenhagen [25], on the distribution of the values of the function $D \mapsto \mathrm{rk}_4(\mathrm{C}_D)$ but when D now belongs to the set of special discriminants. They also applied their results to the frequency of the solvability of the negative Pell equation

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

when d is a squarefree integer (see [8]).

To state the above results of Fouvry & Klüners, we introduce the function η_k

$$\eta_k(t) := \prod_{j=1}^{k} (1 - t^{-j}), \tag{2}$$

which is defined for $|t| > 1$ and $k \in \{0, 1, 2, \dots, \infty\}$ and which frequently appears in the theory of partitions. With these conventions we proved (see [6, Theorem 3] & [8, Theorem 2]).

Theorem A. *For every integer $r \geq 0$ as $X \to \infty$, we have*

$$\sum_{\substack{0<D<X \\ \mathrm{rk}_4(\mathrm{C}_D)=r}} 1 \sim_r 2^{-r(r+1)} \cdot \frac{\eta_\infty(2)}{\eta_r(2)\,\eta_{r+1}(2)} \sum_{0<D<X} 1, \tag{3}$$

$$\sum_{\substack{0<-D<X \\ \mathrm{rk}_4(\mathrm{C}_D)=r}} 1 \sim_r 2^{-r^2} \cdot \frac{\eta_\infty(2)}{\eta_r(2)^2} \sum_{0<-D<X} 1, \tag{4}$$

and

$$\sum_{\substack{0<D<X,\, D \text{ special} \\ \mathrm{rk}_4(\mathrm{C}_D)=r}} 1 \sim_r 2^{-\frac{r(r+1)}{2}} \cdot \frac{\eta_\infty(2)}{\eta_\infty(4)\,\eta_r(2)} \sum_{0<D<X,\, D \text{ special}} 1. \tag{5}$$

$$\sum_{\substack{0<D<X,\, D \text{ special} \\ \mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{Cl}_D)=r}} 1 \sim_r 2^{\frac{-r(r+3)}{2}} \cdot \frac{\eta_\infty(2)}{\eta_\infty(4)\,\eta_r(2)} \sum_{0<D<X,\, D \text{ special}} 1. \tag{6}$$

Similar statements remain true if one restricts the summation over D to one of the following congruence classes

$$D \equiv 1 \bmod 4,\ D \equiv 12 \bmod 16 \text{ or } D \equiv 8 \bmod 16, \tag{7}$$

in the case of (3) and (4), and

$$D \equiv 1 \bmod 4 \text{ or } D \equiv 8 \bmod 16, \tag{8}$$

in the case of (5) and (6).

In other words, (3), (4) and (5) of Theorem A give the probability for a discriminant to have its associated 4–rank equal to r, when r is a fixed integer and when D is considered as an element of the set of positive fundamental discriminants, of negative fundamental discriminants, or of special discriminants, respectively. A similar interpretation can be given to (6).

Fouvry and Klüners also proved some partial result on the 8–rank of C_D, which by definition is

$$\mathrm{rk}_8(\mathrm{C}_D) := \dim_{\mathbb{F}_2}\big(\mathrm{C}_D^4/\mathrm{C}_D^8\big).$$

Theorem B. *([9, Theorem 2]) As $X \to \infty$, we have*

$$\sum_{\substack{0<D<X,\, D \text{ special} \\ \mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{Cl}_D)=1 \\ \mathrm{rk}_8(\mathrm{C}_D)=0}} 1 \sim \frac{1}{4} \cdot \frac{\eta_\infty(2)}{\eta_\infty(4)} \sum_{0<D<X,\, D \text{ special}} 1. \tag{9}$$

Similar statement remains true if one restricts the summation over D to one of the congruences classes written in (8).

Theorem B is used to improve our knowledge of the frequency of the solvability of (1) or equivalently, of the parity of period of the expansion of $\sqrt{d}$ in continued fractions for squarefree d.

As far as we know, Theorem B is the only result concerning the distribution law of the function $D \mapsto \mathrm{rk}_8(\mathrm{C}_D)$ (D special or not) since the function rk_8 seems very difficult to understand by algebraic properties that can be treated by the present methods of analytic number theory.

In April 2008, the second author visited Princeton University and P. Sarnak pointed out the interest of generalizing Theorems A & B by replacing the weight 1 (appearing in (3), (4), (5), (6) & (9)), by another weight. He mainly had in mind the weight $2^{\omega(|D|)}$, where $\omega(n)$ is the number of distinct prime divisors of the integer n. Recall the interpretation of that weight via the famous result of Gauss

$$2^{\omega(|D|)-1} = 2^{\mathrm{rk}_2(\mathrm{C}_D)} \Big(= \sharp\big\{\mathfrak{I} \in \mathrm{C}_D\,;\ \mathfrak{I}^2 \sim \mathcal{O}_D\big\}\Big), \tag{10}$$

(see [17, Theorem 8.8], for instance). Such a generalization would not be sterile since P. Sarnak pointed out precise applications in number theory. These applications concerned reciprocal geodesics and were presented in [23] & [24] (see §4 below for a description of these notions).

The main purpose of the present paper is to prove that the statements of Theorems A & B are not affected by the intrusion of a weight of the above type. We have decided to present this extension with the multiplicative weight

$$D \mapsto \kappa^{\omega(|D|)}, \quad \text{with } \kappa \in]0, +\infty[,$$

and, then present two types of applications, with the particular choice $\kappa = 2$.

We first write

Theorem 1. *For every integer r, for every $\kappa \in]0, \infty[$ and for $X \to \infty$, we have*

$$\sum_{\substack{0<D<X \\ \mathrm{rk}_4(\mathrm{C}_D)=r}} \kappa^{\omega(D)} \sim_{r,\kappa} 2^{-r(r+1)} \cdot \frac{\eta_\infty(2)}{\eta_r(2)\,\eta_{r+1}(2)} \sum_{0<D<X} \kappa^{\omega(D)}, \tag{11}$$

$$\sum_{\substack{0<-D<X \\ \mathrm{rk}_4(\mathrm{C}_D)=r}} \kappa^{\omega(|D|)} \sim_{r,\kappa} 2^{-r^2} \cdot \frac{\eta_\infty(2)}{\eta_r(2)^2} \sum_{0<-D<X} \kappa^{\omega(|D|)}, \tag{12}$$

and

$$\sum_{\substack{0<D<X,\, D \text{ special} \\ \mathrm{rk}_4(\mathrm{C}_D)=r}} \kappa^{\omega(D)} \sim_{r,\kappa} 2^{-\frac{r(r+1)}{2}} \cdot \frac{\eta_\infty(2)}{\eta_\infty(4)\,\eta_r(2)} \sum_{0<D<X,\, D \text{ special}} \kappa^{\omega(D)}, \tag{13}$$

$$\sum_{\substack{0<D<X,\, D \text{ special} \\ \mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{Cl}_D)=r}} \kappa^{\omega(D)} \sim_{r,\kappa} 2^{\frac{-r(r+3)}{2}} \cdot \frac{\eta_\infty(2)}{\eta_\infty(4)\eta_r(2)} \sum_{0<D<X,\, D \text{ special}} \kappa^{\omega(D)}. \tag{14}$$

Similar statements remain true if one restricts the summation over D to one of the congruence classes written in (7) in the case of (11) and (12), and to one of the congruence classes written in (8) in the case of (13) and (14).

We also have

Theorem 2. *For every $\kappa \in]0,\infty[$ and for $X \to \infty$, we have*

$$\sum_{\substack{0<D<X,\, D \text{ special}\\ \mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{Cl}_D)=1\\ \mathrm{rk}_8(\mathrm{C}_D)=0}} \kappa^{\omega(D)} \sim_\kappa \frac{1}{4}\cdot\frac{\eta_\infty(2)}{\eta_\infty(4)} \sum_{0<D<X,\, D \text{ special}} \kappa^{\omega(D)}. \tag{15}$$

A similar statement remains true if one restricts the summation over D to one of the congruences classes written in (8).

The right hand sides of (11),....,(15) can be reduced to sums of multiplicative functions. Classical methods of analytic methods lead to the existence of positive constants c_κ and c'_κ such that

(16)
$$\sum_{0<\pm D<X} \kappa^{\omega(|D|)} \sim c_\kappa X(\log X)^{\kappa-1} \text{ and } \sum_{0<D<X,\ D \text{ special}} \kappa^{\omega(D)} \sim c'_\kappa X(\log X)^{\frac{\kappa}{2}-1},$$

as $X \to \infty$.

1.1. **List of applications.** The first application is an easy deduction from Theorems 1 & 2. It concerns the special discriminants, for which the fundamental unit ϵ_D of $\mathcal{O}_D$ satisfies

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

We have

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

$$\sum_{\substack{0<D<X,\, D \text{ special}\\ \mathcal{N}(\epsilon_D)=-1}} 2^{\omega(D)} \geqslant \Big(\frac{5}{4} - o(1)\Big)\cdot\frac{\eta_\infty(2)}{\eta_\infty(4)} \sum_{\substack{0<D<X\\ D \text{ special}}} 2^{\omega(D)}, \tag{17}$$

$$\sum_{\substack{0<D<X,\, D \text{ special}\\ \mathcal{N}(\epsilon_D)=-1}} 2^{\omega(D)} \leqslant \Big(\frac{2}{3} + o(1)\Big) \sum_{\substack{0<D<X\\ D \text{ special}}} 2^{\omega(D)}, \tag{18}$$

$$\sum_{\substack{0<D<X,\, D \text{ special}\\ \mathcal{N}(\epsilon_D)=1}} 2^{\omega(D)} \geqslant \Big(\frac{1}{3} - o(1)\Big) \sum_{\substack{0<D<X\\ D \text{ special}}} 2^{\omega(D)}, \tag{19}$$

and

$$\sum_{\substack{0<D<X,\, D \text{ special}\\ \mathcal{N}(\epsilon_D)=-1}} h(D) \geqslant \Big(\frac{3}{4} - o(1)\Big)\cdot\frac{\eta_\infty(2)}{\eta_\infty(4)} \sum_{\substack{0<D<X\\ D \text{ special}}} 2^{\omega(D)}. \tag{20}$$

Proof. For (17) and (20), we use the implication

$$\left.\begin{array}{c}\mathrm{rk}_4(\mathrm{C}_D)=0\\ \text{or}\\ \mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{Cl}_D)=1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D)=0\end{array}\right\} \Longrightarrow \mathcal{N}(\epsilon_D)=-1.$$

This implication is an easy consequence of the three following facts (see [9, §1.1], for instance).

• Cl_D is a factor group of C_D of index 1 or 2,
• for special D the two groups C_D and Cl_D have the same 2–rank,
• $\mathcal{N}(\epsilon_D) = -1$ if and only $\mathrm{C}_D = \mathrm{Cl}_D$.

Hence we have the inequality

$$\sum_{\substack{0<D<X,\, D \text{ special} \\ \mathcal{N}(\epsilon_D)=-1}} 2^{\omega(D)} \geq \Big(\sum_{\substack{0<D<X,\, D \text{ special} \\ \mathrm{rk}_4(\mathrm{C}_D)=0}} + \sum_{\substack{0<D<X,\, D \text{ special} \\ \mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{Cl}_D)=1 \\ \mathrm{rk}_8(\mathrm{C}_D)=0}} \Big) 2^{\omega(D)}.$$

It remains to apply (13) of Theorem 1 (with $r = 0$ and $\kappa = 2$) and (15) of Theorem 2 to complete the proof of (17).

For (20), the proof is the same after inserting the trivial inequality

$$h(D) \geq 2^{\mathrm{rk}_2(\mathrm{C}_D)} \cdot 2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2} \cdot 2^{\omega(D)} \cdot 2^{\mathrm{rk}_4(C_D)},$$

(see (10)), and replacing $\mathrm{rk}_4(\mathrm{C}_D)$ by 1 when applying Theorem 2.
The proof of (18) is a consequence of (14), Theorem 2, (10), and Lemma 3 in [8]. Furthermore note the equality

$$\sum_{r=0}^{\infty} 2^{\frac{-r(r+3)}{2}} \cdot \frac{\eta_\infty(2)}{\eta_\infty(4)\eta_r(2)} = \sum_{r=0}^{\infty} 2^{-r} \cdot \frac{\eta_\infty(2)}{\eta_\infty(4) \prod_{j=1}^{r}(2^j - 1)} = \frac{2}{3},$$

which was shown in the course of the proof of [8, Theorem 1 in §1.2].

For (19) note that $\mathcal{N}(\epsilon_D)$ is either 1 or -1. Hence (19) is a consequence of (18) by additivity. □

We shall postpone to §4 the interpretation of Corollary 1 in terms of the questions raised in [24, p.231] concerning reciprocal geodesics. This interpretation really was the starting point of the present paper.

The second application concerns an average lower bound of the function $h(D)$, more precisely let $\nabla(X)$ be the sum

$$\nabla(X) := \sum_{\substack{0<D<X \\ D\equiv 1 \bmod 4}} h(D). \tag{21}$$

In the definition of ∇, the summation is over positive fundamental discriminants D, however the restriction $D \equiv 1 \bmod 4$ is not obligatory at all, but it avoids several technical complications, which will be mentioned in §1.3. To state the central result in that direction, we introduce the Euler product

$$\Pi_0 := \prod_{p\geq 2} \Big(1 - \frac{3}{p^2} + \frac{2}{p^3}\Big) = .286\,747 \cdots \tag{22}$$

In §5.4, we shall prove

Theorem 3. *As $X \to \infty$, we have*

$$\sum_{\substack{1<D<X \\ D\equiv 1 \bmod 4}} h(D) \geq (c_0 - o(1))\, X \log X,$$

where the constant c_0 has the value

$$c_0 = \frac{71}{336} \cdot \Pi_0.$$

The trivial asymptotic lower bound is

$$\nabla(X) \geq \Big(\frac{1}{8}\cdot \Pi_0 - o(1)\Big)\, X \log X,\ \ (X\to\infty) \tag{23}$$

(see (68) and Proposition 2 below). Hence our result represents an improvement of 69% of the trivial lower bound. However, we are far from the conjectural value of $\nabla(X)$ (see Conjecture 1 below). We shall also indicate how to improve the value of the above constant c_0, by introducing arguments due to Hooley [14] which consists to carefully study the contribution of the D the associated regulators of which are small (see Theorem 5 below).

1.2. **Remarks.** Before embarking the proofs of Theorems 1 & 2, we make the following comments

(i) We did not find attractive applications of Theorems 1 & 2 for some $\kappa \neq 1, 2$. However for instance, the case $\kappa = 4$ would lead to a non trivial lower bound for the sum
$$\sum_{\substack{0<D<X\\ D\equiv 1 \bmod 4}} h^2(D).$$
But the lower bound that we obtain has not the expected asymptotic order of magnitude.

(ii) Another interesting case is
$$\kappa = -1.$$
By the methods that will be developed in §2 and which leads to Proposition 1, one can show that
$$\sum_{0<\pm D<X} (-1)^{\omega(|D|)}\cdot 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)} = o_k\Big(\sum_{0<\pm D<X} 1\Big).$$
Now, since $(1+(-1)^{\omega(|D|)})/2$ is the characteristic function of the set of discriminants D with an even number of prime divisors, we get the following extension of (3) & (4)
$$\sum_{\substack{0<D<X,\ 2\mid \omega(D)\\ \mathrm{rk}_4(\mathrm{C}_D)=r}} 1 \sim_r 2^{-r(r+1)-1}\cdot \frac{\eta_\infty(2)}{\eta_r(2)\,\eta_{r+1}(2)} \sum_{0<D<X} 1,$$
and
$$\sum_{\substack{0<-D<X,\ 2\mid \omega(|D|)\\ \mathrm{rk}_4(\mathrm{C}_D)=r}} 1 \sim_r 2^{-r^2-1}\cdot \frac{\eta_\infty(2)}{\eta_r(2)^2} \sum_{0<-D<X} 1,$$
for every integer $r\geq 0$. This shows that the value of the $\mathrm{rk}_4(\mathrm{C}_D)$ is statistically independent of the parity of $\omega(|D|)$.

1.3. **Organization of the paper.** The proof of Theorems 1 and 2 will be given in §2. We shall closely follow the proofs given in [6], [8] & [9] and only quote the parts which have to be modified in order to incorporate the weight $\kappa^{\omega(|D|)}$. To shorten this part, we shall even restrict ourselves to the case of odd negative fundamental D or of odd (positive) special D. As usual the prime 2 creates extra difficulty which is only of practical order, but not of theoretical one (the same phenomenon already appeared in [6], [8] & [9]). In §4, we shall develop some applications of Corollary 1 to some questions raised in [24]. This is the content of Theorem 4 below.

Finally, in §5, we shall prove Theorem 3. This proof is based on several sources of improvements, among which the richest one is Proposition 1 below, which implies Theorems 1 & 2. We shall also explain how to improve Theorem 3, this is the content of Theorem 5.

Acknowledgement. As written above, this paper was initiated in courses of conversations with P. Sarnak. The authors thank him for generously sharing his ideas.

2. Proof of theorems 1 and 2

As said above, Theorems 1 and 2 are only variations of results contained in [6], [8] and [9]. Our aim is to enumerate the modifications of the original proofs to incorporate the coefficient $\kappa^{\omega(|D|)}$. Actually, Theorem 1 contains ten results and Theorem 2 two results, if one considers the different cases of congruences modulo 8. The modifications due to these twelve cases have flagrant similarities, so we decided to only present the case D fundamental, negative and odd (in other words (12) when $D \equiv 1 \bmod 4$). This case is certainly the most typical one.

2.1. Basic concepts.

In [6, p.470], we introduced the moment of order k ($k \in \mathbb{N}$) of the arithmetical function $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ on the set of odd negative discriminants $D \equiv 1 \bmod 4$ by the formula

$$S^-(X,k,1,4) := \sum_{\substack{0<-D<X \\ D\equiv 1 \bmod 4}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}. \tag{24}$$

To make our proof more fluent, we shall systematically insert the index $_{\mathrm{w}}$, (as *weighted*) to quote the expression corresponding to our present question, when compared with [6]. So, in our case, we introduce the weighted moment of order k

$$S_{\mathrm{w}}^-(X,k,1,4) := \sum_{\substack{0<-D<X \\ D\equiv 1 \bmod 4}} \kappa^{\omega(|D|)} \cdot 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}, \tag{25}$$

and we want to study its asymptotic behavior, for $k \geq 1$, since the case $k = 0$ is trivial. This will be the content of Proposition 1 eq. (52).

We first transform the coefficient $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ by the following formula (see [6, (20)]) based on a sum of products of Jacobi symbols

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(|D|)}} \sum_{-D=D_0D_1D_2D_3} \left(\frac{D_2}{D_0}\right)\left(\frac{D_1}{D_3}\right)\left(\frac{D_3}{D_0}\right)\left(\frac{D_0}{D_3}\right). \tag{26}$$

In that formula, the integers D with index are not necessarily fundamental discriminants, but they certainly are squarefree and coprime. We raise the formula (26) to the power k, and sum over all odd D between $-X$ and 0 giving (see [6, Lemma 17])

$$S^-(X,k,1,4) = 2^{-k} \sum_{(D_{\mathbf{u}})\in\mathcal{D}^-(X,k)} \Big(\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big) \prod_{\mathbf{u},\,\mathbf{v}} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\right)^{\Phi_k(\mathbf{u},\mathbf{v})},$$

where $\mathbf{u} = (u_1,\dots,u_{2k})$ and $\mathbf{v} = (v_1,\dots,v_{2k})$ are indices taken in $\mathbb{F}_2^{2k}$ ($\cong (\mathbb{F}_2^2)^k$), $\mathcal{D}^-(X,k)$ is the set of 4^k–tuples of squarefree, positive and coprime integers $(D_{\mathbf{u}})$

with $\mathbf{u} = (\mathbf{u}^{(1)}, \dots, \mathbf{u}^{(k)}) \in (\mathbb{F}_2^2)^k$ satisfying $\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} D_{\mathbf{u}} \leq X$ and $\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} D_{\mathbf{u}} \equiv -1 \bmod 4$. We also denote by $\Phi_k(\mathbf{u},\mathbf{v})$ the polynomial

$$\Phi_k(\mathbf{u},\mathbf{v}) = (u_1+v_1)(u_1+v_2)+\cdots+(u_{2k-1}+v_{2k-1})(u_{2k-1}+v_{2k}).$$

(Recall that all these combinatorics of [6] concerning the geometry over $\mathbb{F}_2$ were inspired by [12].) In our case, since we have $\omega(|D|) = \sum_{\mathbf{u}} \omega(D_{\mathbf{u}})$, we directly get the equality

(27)
$$S^-_{\mathrm{w}}(X,k,1,4) = 2^{-k} \sum_{(D_{\mathbf{u}})\in\mathcal{D}^-(X,k)} \Big(\prod_{\mathbf{u}} \kappa^{\,\omega(D_{\mathbf{u}})}\Big)\cdot\Big(\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big)\prod_{\mathbf{u},\,\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u},\mathbf{v})}.$$

2.2. **Error terms.** Our task is is to go through all the error terms appearing in [6, §5], in the proof of Theorem A to determine the effect of the newly inserted coefficient $\Big(\prod_{\mathbf{u}} \kappa^{\,\omega(D_{\mathbf{u}})}\Big)$. Compared with [6], the extra difficulty comes from the fact that this coefficient is unbounded when $\kappa > 1$ (see (29)). Let

$$\Omega_{\mathrm{w}} := \mathrm{e}\,\kappa\,4^k\,(\log\log X + B_0) + 1,$$

where B_0 is any constant which satisfies the Hardy–Ramanujan inequality [11], which asserts the inequality

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

for any $X \geq 2$ and $\ell \geq 1$ (see [6, Lemma 11]). Let $\Sigma_{1,\mathrm{w}}$ be the contribution to the right part of (27) of those $(D_{\mathbf{u}}) \in \mathcal{D}^-(X,k)$ which satisfy $\omega(D_{\mathbf{u_0}}) > \Omega_{\mathrm{w}}$ for at least one index $\mathbf{u_0} \in (\mathbb{F}_2^2)^k$. Then as in [6, (30)] or in [8, (61)], we get

$$\Sigma_{1,\mathrm{w}} \ll \frac{X}{\log X}, \tag{28}$$

for $k \geq 1$. This is acceptable as an error term in the formula (52), since we have $\Sigma^-_{\mathrm{w}}(X,k,1,4) \gg X(\log X)^{\kappa-1}$.

To shorten the formulas, we denote by κ_1 any constant ≥ 0, only depending on k and κ, such that we have

$$\max\big\{\kappa^{\omega(d)}\,;\ d \leq X,\, \omega(d) \leq \Omega_{\mathrm{w}}\big\} \leq (\log 2X)^{\kappa_1}\ (X \geq 2). \tag{29}$$

Now we introduce the dissection parameter

$$\Delta_{\mathrm{w}} := 1 + \log^{-\kappa\cdot 2^k} X,$$

and for each $\mathbf{u} \in \mathbb{F}_2^{2k}$, $A_{\mathbf{u}}$ denotes a number of the form 1, Δ_{w}, Δ_{w}^2, Δ_{w}^3,... For each $\mathbf{A} = (A_{\mathbf{u}})_{\mathbf{u}\in\mathbb{F}_2^{2k}}$ we define the restricted sum $S_{\mathrm{w}}(X,k,\mathbf{A})$ by the formula (compare with [6, (31)])

(30)
$$S_{\mathrm{w}}(X,k,\mathbf{A}) = 2^{-k} \sum_{(D_{\mathbf{u}})\in\mathcal{D}^-(X,k)} \Big(\prod_{\mathbf{u}} \kappa^{\,\omega(D_{\mathbf{u}})}\Big)\cdot\Big(\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big)\prod_{\mathbf{u},\,\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u},\mathbf{v})},$$

where the $(D_{\mathbf{u}})$ satisfies the conditions

$$(D_{\mathbf{u}}) \in \mathcal{D}^-(X,k),\ A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta_{\mathrm{w}} A_{\mathbf{u}},\ \omega(D_{\mathbf{u}}) \leq \Omega_{\mathrm{w}} \text{ for all } \mathbf{u} \in \mathbb{F}_2^{2k}. \tag{31}$$

By appealing to (28), the splitting process gives the equality

$$S_{\mathrm{w}}^{-}(X,k,1,4)=\sum_{\mathbf{A}} S_{\mathrm{w}}(X,k,\mathbf{A})+O\big(X(\log X)^{-1}\big), \tag{32}$$

where the sum is over all $\mathbf{A}$ such that $\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} A_{\mathbf{u}}\leq X$. Note that the sum in (31) contains $O((\log X)^{4^k(1+\kappa\cdot 2^k)})$ terms. The contribution of the $\mathbf{A}$ such that

$$\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} A_{\mathbf{u}}\geq \Delta_{\mathrm{w}}^{-4^k}X, \tag{33}$$

satisfies

$$\sum_{\mathbf{A}\text{ satisfies (33)}} |S_{\mathrm{w}}(X,k,\mathbf{A})|\ll X(\log X)^{-1}, \tag{34}$$

by a proof similar to [6, (34)], with the new choice of the dissection parameter Δ_{w}.

We introduce two parameters

$$X_{\mathrm{w}}^{\dagger}:=(\log X)^{3[1+4^k(1+\kappa_1+\kappa\cdot 2^k)]}$$

and

$$X_{\mathrm{w}}^{\ddagger}\text{ is the least power }\Delta_{\mathrm{w}}^{\ell}\geq\exp\big(\log^{\eta(k)}X\big),$$

where $\eta(k)$ is a small positive function of k (and κ) to be defined later, in order to obtain (43). The contribution of the $\mathbf{A}$, such that

$$\text{At most } 2^k-1 \text{ of the } A_{\mathbf{u}} \text{ are larger than } X_{\mathrm{w}}^{\ddagger} \tag{35}$$

satisfies

$$\sum_{\mathbf{A}\text{ satisfies (35)}} |S_{\mathrm{w}}(X,k,\mathbf{A})|\ll X(\log X)^{\kappa\cdot\eta(k)\cdot 2^k+\kappa-1-\kappa\cdot 2^{-k}}, \tag{36}$$

by a computation similar to [6, (38) & (39)].

We say that two indices $\mathbf{u}$ and $\mathbf{v}$ are *linked* if they satisfy

$$\Phi_k(\mathbf{u},\mathbf{v})+\Phi_k(\mathbf{v},\mathbf{u})=1.$$

With this convention, consider the condition

$$\begin{cases}\prod_{\mathbf{u}} A_{\mathbf{u}}\leq\Delta_{\mathrm{w}}^{-4^k}X\\ \text{and}\\ \text{there exists two linked indices } \mathbf{u} \text{ and } \mathbf{v} \text{ such that } A_{\mathbf{u}} \text{ and } A_{\mathbf{v}} \text{ are } \geq X_{\mathrm{w}}^{\dagger}.\end{cases} \tag{37}$$

By the definition of κ_1 (see (29)) and by a proof similar to [6, p.476], we can prove that, if $\mathbf{A}$ satisfies (37), we have

$$|S_{\mathrm{w}}(X,k,\mathbf{A})|\ll X\ (X_{\mathrm{w}}^{\dagger})^{-\frac{1}{3}}(\log X)^{\kappa_1\cdot 4^k},$$

then trivially summing over all possible $\mathbf{A}$, and by the definition of $X_{\mathrm{w}}^{\dagger}$, we get

$$\sum_{\mathbf{A}\text{ satisfies (37)}} |S_{\mathrm{w}}(X,k,\mathbf{A})|\ll X(X_{\mathrm{w}}^{\dagger})^{-\frac{1}{3}}\ (\log X)^{4^k(1+\kappa_1+\kappa\cdot 2^k)},$$

which reduces to

$$\sum_{\mathbf{A}\text{ satisfies (37)}} |S_{\mathrm{w}}(X,k,\mathbf{A})|\ll X(\log X)^{-1}, \tag{38}$$

by the definition of $X_{\mathrm{w}}^{\dagger}$.

The last contribution we look at, concerns those $\mathbf{A}$ such that

(39)
$$\begin{cases}\prod_{\mathbf{u}} A_{\mathbf{u}} \leq \Delta_{\mathrm{w}}^{-4^k} X,\\ \text{there exists no linked indices } \mathbf{u} \text{ and } \mathbf{v} \text{ such that } A_{\mathbf{u}} \text{ and } A_{\mathbf{v}} \text{ are} \geq X_{\mathrm{w}}^{\dagger}\\ \text{and}\\ \text{there exist two linked indices } \mathbf{u} \text{ and } \mathbf{v} \text{ such that } 2 \leq A_{\mathbf{v}} < X_{\mathrm{w}}^{\dagger} \text{ and } A_{\mathbf{u}} \geq X_{\mathrm{w}}^{\ddagger}.\end{cases}$$

As in [6, p.477–478], we apply the Siegel–Walfisz Theorem to the largest prime factor of $D_{\mathbf{u}}$, where the index $\mathbf{u}$ is defined in the last condition of (39), giving the inequality

$$|S_{\mathrm{w}}(X,k,\mathbf{A})| \ll_A X(X_{\mathrm{w}}^{\dagger})^{\frac{1}{2}}(\log X)^{\kappa_1\cdot 4^k - A\eta(k)/2},$$

where A is any positive constant. Then summing over possible $\mathbf{A}$ satisfying (39), and choosing $A = A(k,\kappa)$ very large, we get

$$\sum_{\mathbf{A} \text{ satisfies } (39)} |S_{\mathrm{w}}(X,k,\mathbf{A})| \ll X(\log X)^{-1}. \tag{40}$$

Recall that a subset $\mathcal{U}$ of $\mathbb{F}_2^{2k}$ is *maximal unlinked* when any pair of elements of $\mathcal{U}$ are unlinked and when $\mathcal{U}$ is maximal for inclusion. Actually, it is proved (see [6, Lemma 18]), that such maximal unlinked $\mathcal{U}$ are vector subspaces of dimension k of $\mathbb{F}_2^{2k}$ or cosets of such vector subspaces. In particular, the cardinality of each $\mathcal{U}$ is equal to 2^k.

Using the properties of these subsets (see [6, Lemma 18]) and gathering (32), (34), (36), (38) & (40), we arrive at (compare with [6, Prop.3]

$$S_{\mathrm{w}}^{-}(X,k,1,4) = \sum_{\mathbf{A} \text{ satisfies } (42)} S_{\mathrm{w}}(X,k,\mathbf{A}) + O\Big(X_{\mathrm{w}}(\log X)^{\kappa\cdot\eta(k)\cdot 2^k - \kappa\cdot 2^{-k}}\Big) \tag{41}$$

with

$$\begin{cases}\prod_{\mathbf{u}} A_{\mathbf{u}} \leq \Delta_{\mathrm{w}}^{-4^k} X,\\ \mathcal{U} := \{\mathbf{u}\,;\ A_{\mathbf{u}} > X_{\mathrm{w}}^{\ddagger}\} \text{ is a maximal subset of unlinked indices and}\\ A_{\mathbf{u}} = 1 \text{ for } \mathbf{u} \notin \mathcal{U}.\end{cases} \tag{42}$$

and

$$X_{\mathrm{w}} := \sum_{\substack{0 < -D \leq X\\ D \equiv 1 \bmod 4}} \kappa^{\omega(|D|)},$$

which naturally appears as a scale of comparison in this problem with weights. Recall that X_{w} satisfies (see (16))

$$X_{\mathrm{w}} \sim c_\kappa X(\log X)^{\kappa-1},\ (X \mapsto \infty)$$

for some positive c_κ. Choosing $\eta(k)$ sufficiently small in terms of k and κ, we simplify (41) into

$$S_{\mathrm{w}}^{-}(X,k,1,4) = \sum_{\mathbf{A} \text{ satisfies } (42)} S_{\mathrm{w}}(X,k,\mathbf{A}) + o_k(X_{\mathrm{w}}). \tag{43}$$

Replacing the weight 1 by $\kappa^{\omega(|D|)}$ and using (16), we easily extend the proof of [6, Lemma 19], to write

Lemma 1. *Let κ be a positive number. For $\nu = \pm 1 \bmod 4$, for every $A \geq 0$ and for $Y \geq y \geq 1$, we have the equality*

$$\sum_{\substack{y \leq n \leq Y \\ n \equiv \nu \bmod 4 \\ \omega(n)=\ell}} \mu^2(n_0 n)\, \kappa^{\omega(n)} = \frac{1}{2} \sum_{\substack{y \leq n \leq Y \\ (2,n)=1 \\ \omega(n)=\ell}} \mu^2(n_0 n)\, \kappa^{\omega(n)} + O_A\Big((\ell+1)^{A+1}\, Y\, (\log 2Y)^{\kappa-1-A} + \omega(n_0)\, Y^{1-\frac{1}{\ell}}\, (\log 2Y)^{\kappa-1}\Big),$$

uniformly for $\ell \geq 1$ and for odd squarefree integer n_0.

This lemma shows the equidistribution of the function $\kappa^{\omega(n)}$ in reduced congruences modulo 4, when the number of prime factors of n is fixed. It allows to transform (41) into the following formula (compare with [6, Prop. 5])

$$S_{\mathrm{w}}^{-}(X,k,1,4) = 2^{1-k-2^k} \cdot \Big(\sum_{\mathcal{U}} \gamma(\mathcal{U})\Big) \cdot X_{\mathrm{w}} + o_k(X_{\mathrm{w}}), \tag{44}$$

where the sum is over all maximal unlinked subsets $\mathcal{U} \subset \mathbb{F}_2^{2k}$, and where

$$\gamma(\mathcal{U}) := \sum_{(h_{\mathbf{u}})} \Big(\prod_{\mathbf{u},\,\mathbf{v}} (-1)^{\Phi_k(\mathbf{u},\mathbf{v})\cdot \frac{h_{\mathbf{u}}-1}{2} \cdot \frac{h_{\mathbf{v}}-1}{2}}\Big).$$

In the above line, the product is over unordered pairs $\{\mathbf{u},\, \mathbf{v}\} \subset \mathcal{U}$ and $(h_{\mathbf{u}})_{\mathbf{u}\in\mathcal{U}} \in \{\pm 1 \bmod 4\}^{2^k}$ satisfies $\prod_{\mathbf{u}} h_{\mathbf{u}} \equiv -1 \bmod 4$.

The coefficient of the main term of (44) is computed in [6, (74) & Lemma 26]. Then, introducing $\mathbf{N}(m,p)$ to denote the total number of vector subspaces (of any dimension) of $\mathbb{F}_p^m$, we obtain the equality

$$S_{\mathrm{w}}^{-}(X,k,1,4) = \mathbf{N}(k,2) \cdot X_{\mathrm{w}} + o_k(X_{\mathrm{w}}), \tag{45}$$

which has to be compared with [6, Theorem 6].

This study of the weighted moments can be easily adapted to the other situations present in Theorem 1. Hence following the proofs of [6, Theorems 7, 8, 9, 10 & 11], [8, Theorems 3 & 4] and [9, Theorem 3], we obtain the evaluation of the corresponding weighted moments. To state our results in a global way, we introduce the following moments

$$S_{\mathrm{w}}^{\pm}(X,k,a,q) := \sum_{\substack{0 < \pm D < X \\ D \equiv a \bmod q}} \kappa^{\omega(|D|)} \cdot 2^{k\, \mathrm{rk}_4(\mathrm{C}_D)}, \tag{46}$$

$$S_{\mathrm{w}}^{\mathrm{spec}}(X,k,a,q) := \sum_{\substack{0 < D < X,\ D \text{ special} \\ D \equiv a \bmod q}} \kappa^{\omega(D)} \cdot 2^{k\, \mathrm{rk}_4(\mathrm{C}_D)}, \tag{47}$$

$$S_{\mathrm{w}}^{\mathrm{mix}}(X,k,a,q) := \sum_{\substack{0 < D < X,\ D \text{ special} \\ D \equiv a \bmod q}} \kappa^{\omega(D)} \cdot 2^{k\, \mathrm{rk}_4(\mathrm{C}_D)} \cdot 2^{\mathrm{rk}_4(\mathrm{Cl}_D)}, \tag{48}$$

and

$$S_{\mathrm{w}}^{\mathrm{mix},\lambda}(X,k,a,q) := \sum_{\substack{0 < D < X,\ D \text{ special} \\ D \equiv a \bmod q}} \kappa^{\omega(D)} \cdot 2^{k\, \mathrm{rk}_4(\mathrm{C}_D)} \cdot 2^{\lambda_D}, \tag{49}$$

for integers a, q and $k \geq 0$. In (49), by definition we have

$$2^{\lambda_D} = \sharp\,\big\{(D_1,D_2)\,;\ D = D_1 D_2,\ D_1 \text{ and } D_2 \text{ are special discriminants},\ [D_1,D_2]_4 = 1\big\},$$

where the symbol $[a,b]_4$ is defined, for coprime positive a and b, as a multiplicative function of b and satisfies, for p odd

$$[a,p]_4 = \begin{cases} 1 & \text{if } a \text{ is a fourth power } \bmod p, \\ -1 & \text{if } a \text{ is a square but not a fourth power } \bmod p, \\ 0 & \text{if } a \text{ is not a square } \bmod p, \end{cases}$$

and

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

The crucial property of λ_D for special D is to satisfy the inequality $\mathrm{rk}_8(\mathrm{C}_D) \leq \lambda_D$, and this inequality becomes an equality when $\mathrm{rk}_4(\mathrm{C}_D) \leq 1$ (see [9, Theorem 3]).

To approximate these moments, we introduce the following expressions which generalizes X_{w} introduced above

$$\Sigma_{\mathrm{w}}^{\pm}(X,a,q) := \sum_{\substack{0<\pm D<X \\ D\equiv a \bmod q}} \kappa^{\omega(|D|)}, \tag{50}$$

$$\Sigma_{\mathrm{w}}^{\mathrm{spec}}(X,a,q) := \sum_{\substack{0<D<X,\ D \text{ special} \\ D\equiv a \bmod q}} \kappa^{\omega(D)}. \tag{51}$$

Extending the proof of (45) to the other situations, we can finally write

Proposition 1. *Let κ be a fixed positive real number. Then for every $k \geq 0$, for every $\epsilon > 0$ and for $(a,q) = (1,4),\ (4,8)$ or $(0,8)$, we have*

$$S_{\mathrm{w}}^{-}(X,k,a,q) = (1+o_k(1)) \cdot \mathbf{N}(k,2) \cdot \Sigma_{\mathrm{w}}^{-}(X,a,q), \tag{52}$$

and

$$S_{\mathrm{w}}^{+}(X,k,a,q) = (1+o_k(1)) \cdot \Big\{ \frac{1}{2^k}\big(\mathbf{N}(k+1,2) - \mathbf{N}(k,2)\big)\Big\} \cdot \Sigma_{\mathrm{w}}^{+}(X,a,q), \tag{53}$$

when $X \to \infty$.
For every $k \geq 0$, for every $\epsilon > 0$ and for $(a,q) = (1,4)$ or $(0,8)$, we have

$$S_{\mathrm{w}}^{\mathrm{spec}}(X,k,a,q) = (1+o_k(1)) \cdot \prod_{j=0}^{k-1}(2^j+1) \cdot \Sigma_{\mathrm{w}}^{\mathrm{spec}}(X,a,q), \tag{54}$$

$$S_{\mathrm{w}}^{\mathrm{mix}}(X,k,a,q) = (1+o_k(1)) \cdot (2^{k-1}+1) \cdot \prod_{j=0}^{k-1}(2^j+1) \cdot \Sigma_{\mathrm{w}}^{\mathrm{spec}}(X,a,q), \tag{55}$$

and

$$S_{\mathrm{w}}^{\mathrm{mix},\lambda}(X,k,a,q) = (1+o_k(1)) \cdot (2^{k-2}+1) \cdot \prod_{j=0}^{k-1}(2^j+1) \cdot \Sigma_{\mathrm{w}}^{\mathrm{spec}}(X,a,q), \tag{56}$$

when $X \to \infty$.

From the asymptotic expansions of these moments for any integral order k, we deduce Theorems 1 & 2 as it was done in [6], [8] & [9], using tools presented in [7]. This completes the proof of these theorems.

3. Some easy formulas

In this section we want to compute the asymptotics of some functions which will be used below.

Lemma 2. *Let χ be the non principal character modulo 4. Then for $X \to \infty$ we have*

$$\sum_{\substack{0<D<X\\ D \text{ special}}} 2^{\omega(D)} \sim \beta X, \text{ where}$$

$$\beta := \frac{5\pi}{32} \prod_{p\geq 3}\left(1 - \frac{2+\chi(p)}{p^2} + \frac{1+\chi(p)}{p^3}\right) \approx 0.3617230. \tag{57}$$

Proof. This is a direct application of Ikehara's theorem. Note that each special D can be written as $D = 2^a p_1 \cdots p_r$, where the p_i are pairwise different and congruent to 1 mod 4, and $a \in \{0, 3\}$. Hence

$$F(s) := \sum_{\substack{0<D<X\\ \text{D special}}} \frac{2^{\omega(D)}}{D^s} = (1+\frac{2}{2^{3s}}) \prod_{p\equiv 1 \bmod 4}\left(1+\frac{2}{p^s}\right) = (1+\frac{2}{2^{3s}}) \prod_{p\geq 3}\left(1+\frac{1+\chi(p)}{p^s}\right).$$

Introducing the ζ–function we get

$$\begin{aligned} F(s) &= \zeta(s)(1-\frac{1}{2^s})(1+\frac{2}{2^{3s}}) \prod_{p\geq 3}\left(1+\frac{1+\chi(p)}{p^s}\right)\left(1-\frac{1}{p^s}\right) \\ &= \zeta(s)\left(1-\frac{1}{2^s}+\frac{2}{8^s}-\frac{2}{16^s}\right) \prod_{p\geq 3}\left(1+\frac{\chi(p)}{p^s}-\frac{1+\chi(p)}{p^{2s}}\right) \\ &= \zeta(s)\left(1-\frac{1}{2^s}+\frac{2}{8^s}-\frac{2}{16^s}\right) L(s,\chi) \prod_{p\geq 3}\left(1-\frac{2+\chi(p)}{p^{2s}}+\frac{1+\chi(p)}{p^{3s}}\right). \end{aligned}$$

Since $L(1, \chi) \neq 0$ we have

$$\sum_{\substack{0<D<X\\ \text{D special}}} 2^{\omega(D)} \sim \frac{5}{8} L(1,\chi) \prod_{p\geq 3}\left(1-\frac{2+\chi(p)}{p^2}+\frac{1+\chi(p)}{p^3}\right) X.$$

Recall the classical formula $L(1, \chi) = \pi/4$ which finishes the proof. □

The proof of the following lemma is obvious by applying Lemma 2 and (17).

Lemma 3.

$$\sum_{\substack{0<D<X,\, D \text{ special}\\ \mathcal{N}(\epsilon_D)=-1}} 2^{\omega(D)} \geqslant \left(\frac{5}{4}-o(1)\right) \cdot \frac{\eta_\infty(2)}{\eta_\infty(4)} \beta X \geq 0.1896434\ X.$$

Note that the constant

$$\frac{\eta_\infty(2)}{\eta_\infty(4)} = \prod_{j=1}^{\infty} \frac{1}{1+2^{-j}} \approx 0.4194224$$

is often denoted by α, e.g. see [8, (5)].

Let us prove the corresponding lower bound when we sum over special discriminants which have a fundamental unit of positive norm.

Lemma 4.

$$\sum_{\substack{0<D<X,\, D \text{ special} \\ \mathcal{N}(\epsilon_D)=1}} 2^{\omega(D)} \geqslant \left(\frac{1}{3} - o(1)\right) \beta\ X \geq 0.1205743\ X.$$

Proof. Apply Lemma 2 and (19). □

4. Applications to reciprocal geodesics

In this section we would like to introduce the necessary notations and facts given in [24]. For more details we refer the reader to [24] or to the corresponding review of Popa in Mathematical Reviews.

Denote by $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$ the special projective group. Reciprocal geodesics are closed geodesics on the modular surface $\mathbb{H}/\Gamma$ which are equivalent to themselves when their orientation is reversed.

These are in one-to-one correspondence to

- conjugacy classes of hyperbolic elements $\gamma \in \Gamma$ which are conjugate to their inverse, i.e. $\gamma^{-1} = S\gamma S^{-1}$.
- conjugacy classes of maximal dihedral subgroups of Γ.
- the equivalence classes of integral, primitive, binary quadratic forms f of non-square discriminant which are equivalent to $-f$ under the action of Γ.

The latter characterization is the best one for our applications. Denote by $\mathcal{F}_d$ the set of those forms which have discriminant $d > 0$, where d is not a square. It is well known that the narrow class group of a quadratic order of discriminant d is in bijection with $\mathcal{F}_d$. As usual, the narrow class group is the group of invertible fractional ideals modulo the principal ideals which are generated by elements which are totally positive. In case d is fundamental this coincides with the previous definition of C_d.

In his note Sarnak is interested in the asymptotic behavior of reciprocal elements ordered by their length, as well ordered by their discriminant. The first ordering is more natural in the geometric interpretation, where the discriminant ordering is more natural in the number field setting.

Let us remark that in the geometric ordering all the interesting asymptotics can be computed, see formulas (11–15) in [24]. In more details, denote by Π the set of conjugacy classes of primitive hyperbolic elements of Γ. We have three interesting automorphisms of order 2 which act on Γ:

- $\Phi_R(\gamma) = \gamma^{-1}$,
- $\Phi_w(\gamma) = w^{-1}\gamma w$, where $w = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$,
- $\Phi_A = \Phi_R \circ \Phi_w = \Phi_w \circ \Phi_A$.

Note that Φ_w is an outer automorphism induced by the action coming from $\mathrm{PGL}(2,\mathbb{Z})$. Denote by e the trivial automorphism and let H be a subgroup of the Klein group of order 4 given by $\{e, \Phi_R, \Phi_w, \Phi_A\}$. We define:

$$\Pi_H := \{\{p\} \in \Pi \mid \Phi(\{p\}) = \{p\} \text{ for } \Phi \in H\}.$$

Therefore we have:

- $\Pi_{\{e\}} = \Pi$,
- $\Pi_{\langle \Phi_R \rangle} = \rho$, which is the set of conjugacy classes of reciprocal elements.

Let us call elements in $\Pi_{\langle\Phi_A\rangle}$ *ambiguous classes* and elements in $\Pi_{\langle\Phi_w\rangle}$ *inert classes.*

Let $p \in \Gamma$ be a primitive hyperbolic element. Then the length of the corresponding primitive closed geodesics (which only depends on the conjugacy class) is $\log(((t(p)+\sqrt{t(p)^2-4})/2)^2)$, where $t(p)$ denotes the trace of p. Ordering these elements (conjugacy classes) by their length is therefore equivalent to ordering them by their trace $t(p)$. Like in (10) in [24] we define:

$$\Pi_H(x) := \sum_{\{p\}\in\Pi_H, t(p)\le x} 1.$$

Then we get for $x \to \infty$ the formulas (11–15) in [24].

When we interpret the formulas (11–15) in [24] in this way, we can e.g. say that the asymptotic cardinality of the set of reciprocal classes is the square root of the cardinality of the set of all primitive classes while that the asymptotic cardinality of the set of classes which are simultaneously reciprocal, ambiguous, and inert, is the fourth root of the cardinality of the set of all primitive classes. All these statements refer to the geometric ordering by the length of the geodesics.

Let us now come to the ordering which is more natural in the number field setting, i.e. we order by discriminant. The action of our automorphisms on quadratic forms is given via:

- $\Phi_R : f \mapsto -f$,
- $\Phi_w \sim * : [a,b,c]^* = [-a,b,-c]$,
- $\Phi_A \sim {}' : [a,b,c]' = [a,-b,c]$.

Let us reformulate the above properties in the language of quadratic forms. Denote by $\mathcal{D} := \{d \mid d > 0, d \equiv 0, 1 \bmod 4, d \text{ not a square}\}$ the set of positive discriminants of quadratic orders. We get that the primitive hyperbolic conjugacy classes are in 1-1 correspondence with classes of forms of discriminants $d \in \mathcal{D}$. For a given d there exist $h(d)$ forms of discriminant d, where $h(d)$ denotes the (narrow) class number. In order to parameterize the ambiguous classes we have (more or less) to count the elements of order 2 in the above class group and the number of elements is given by $\nu(d)$, where the definition of $\nu(d)$ can be found in [24, formula (6')]. Denote by $\mathcal{D}_R \subseteq \mathcal{D}$ the set of special discriminants d, i.e. odd primes dividing d are congruent to 1 mod 4 and the prime 2 can only occur with exponent $0, 2, 3$. This set quite naturally occurs when looking at the negative Pell equation. For $d \in \mathcal{D}_R$ the definition of $\nu(d)$ is easier to state:

$$\nu(d) := \begin{cases} 2^{\omega(d)-1} & \text{if } 2 \nmid d \text{ or } 2^3 || d \\ 2^{\omega(d)-2} & \text{if } 2^2 || d. \end{cases} \tag{58}$$

Some computations show that reciprocal elements can only occur when $d \in \mathcal{D}_R$. The set $\mathcal{D}_R$ has the nice property that there is no local obstruction for the Pell equation:

$$t^2 - du^2 = -4. \tag{59}$$

Note that the solvability of (59) is equivalent to the statement that the order of discriminant d has a unit of norm -1.

We write $\mathcal{D}_R = \mathcal{D}_R^+ \dot\cup \mathcal{D}_R^-$, where the latter set contains exactly those d, where the above Pell equation is solvable. The reciprocal classes are inert (and therefore ambiguous) if and and only if $d \in \mathcal{D}_R^-$. Here we see why it is interesting to study the asymptotics of such d, where the negative Pell equation is solvable.

Denote by $\Psi_H(x)$ the number of classes of quadratic forms with discriminant bounded by x which are invariant under the automorphisms in H (compare (71) in [24]). When we order by discriminant we arrive at formulas (72–76) of [24], these are equations (60)–(64) in this paper. Note that $G = \{e, \Phi_A, \Phi_R, \Phi_w\}$ is the Klein four group. So we have

$$\Psi_{\{e\}}(x) = \sum_{d\in\mathcal{D}, d\le x} h(d), \tag{60}$$

$$\Psi_{\langle\Phi_A\rangle}(x) = \sum_{d\in\mathcal{D}, d\le x} \nu(d) \qquad \Big(\sim \frac{3}{2\pi^2} x\log x,\ \text{as } x\to\infty\Big), \tag{61}$$

$$\Psi_{\langle\Phi_R\rangle}(x) = \sum_{d\in\mathcal{D}_R, d\le x} \nu(d) \qquad \Big(\sim \frac{3}{4\pi} x,\ \text{as } x\to\infty\Big), \tag{62}$$

$$\Psi_{\langle\Phi_w\rangle}(x) = \sum_{d\in\mathcal{D}_R^-, d\le x} h(d), \tag{63}$$

$$\Psi_G(x) = \sum_{d\in\mathcal{D}_R^-, d\le x} \nu(d). \tag{64}$$

Our methods are sufficient to give upper and lower bounds for (64) which are of the same asymptotic size. In other words, our results show that a positive density of reciprocal elements are inert (and therefore ambiguous), too. On the other hand we give an improvement of the constant in (79) of [24], which is based on the trivial fact that $\Psi_{\{e\}}(x) \ge \Psi_{\langle\Phi_A\rangle}(x)$. However, we are obliged to restrict ourselves to the subset of fundamental discriminants D instead of the whole set $\mathcal{D}$ defined above. This is the content of Theorem 3.

Theorem 4. *As $x\to\infty$ we have the following inequalities:*

(i) $\Psi_G(x) \ge \big(\frac{5}{8} - o(1)\big)\frac{\eta_\infty(2)}{\eta_\infty(4)}\beta\ x \approx 0.0948217\ x$.

(ii) $\Psi_G(x) \le \Big(\frac{3}{4\pi} - \frac{\beta}{6} + o(1)\Big)\ x \approx 0.1784452\ x$.

(iii) $\Psi_{\langle\Phi_w\rangle}(x) \ge \big(\frac{3}{4} - o(1)\big)\frac{\eta_\infty(2)}{\eta_\infty(4)}\beta\ x \approx 0.1137861\ x$.

Proof. For the lower bound we restrict to fundamental special discriminants

$$\Psi_G(x) = \sum_{d\in\mathcal{D}_R^-, d\le x} \nu(d) \ge \sum_{\substack{0<D<X,\ D \text{ special} \\ \mathcal{N}(\epsilon_D)=-1}} \nu(D).$$

Noting the equality $\nu(D) = 2^{\mathrm{rk}_2(\mathrm{C}_D)} = 2^{\omega(D)-1}$ we get the desired bound by applying Lemma 3. For the upper bound recall that $\mathcal{D}_R = \mathcal{D}_R^+ \dot\cup \mathcal{D}_R^-$. Denote by $\mathcal{D}_R^{+f}$ the subset of fundamental discriminants of $\mathcal{D}_R^+$. These are exactly the fields of special discriminant D such that the fundamental unit has positive norm. Therefore, by Lemma 4, we have:

$$\begin{aligned}
\Psi_G(x) &= \sum_{d\in\mathcal{D}_R^-, d\le x} \nu(d) = \sum_{d\in\mathcal{D}_R, d\le x} \nu(d) - \sum_{d\in\mathcal{D}_R^+, d\le x} \nu(d) \\
&\le \sum_{d\in\mathcal{D}_R, d\le x} \nu(d) - \sum_{D\in\mathcal{D}_R^{+f}, D\le x} \nu(D) \\
&\le \left(\frac{3}{4\pi} + o(1)\right)\ x - \left(\frac{1}{6} - o(1)\right)\beta\ x = \left(\frac{3}{4\pi} - \frac{\beta}{6} + o(1)\right)\ x.
\end{aligned}$$

The proof of the last statement is analogous to the proof of the first statement when we use (20) and Lemma 2. □

Also note that the trivial upper bound (see (62)) is given by

$$\Psi_G(x) \leq \Psi_{\langle\Phi_R\rangle}(x) \simeq 0.2387324\ x.$$

Playing with that constant and the constants appearing in Theorem 4 (i) and (ii), we deduce the following result that we voluntarily express in natural words.

Corollary 2. *In the set of reciprocal classes of quadratic forms, ordered by the increasing value of the discriminants, the percentage of those classes which are inert (and therefore ambiguous) is asymptotically larger than 39 % and smaller than 75 %.*

Using $\Psi_{\langle\Phi_A\rangle}(x) \leq \Psi_{\{e\}}(x)$ and $\Psi_G(x) \leq \Psi_{\langle\Phi_w\rangle}(x)$ we get the trivial lower asymptotic bounds for $\Psi_{\{e\}}(x)$ and $\Psi_{\langle\Phi_w\rangle}(x)$. The 3rd part of Theorem 4 improves the trivial lower bound by a constant factor. We remark that applying Theorem 3 and the trivial equality

$$\Psi_{\{e\}}(x) \geq \nabla(x) + \sum_{\substack{d\leq x \\ d \text{ non fund. discr.}}} \nu(d)$$

gives also an improvement for the trivial lower bound. Note that we defined $\nabla(x)$ in (21) for odd fundamental discriminants.

Let us remark that for all improvements in Theorem 4 we only used non-trivial information coming from the set of fundamental discriminants, which is a subset (with positive density) of the set of all discriminants. Unfortunately, introducing non-fundamental discriminants is more than a slight modification of our previous results. We refer the reader to our short discussion around Lemma 1 in [9]. We have

Lemma 5. *Let d be an integer and p be an odd divisor of d. Then the following are equivalent:*

(i) $t^2 - du^2 = -1$ *is solvable for* $t, u \in \mathbb{Z}$.
(ii) $t^2 - p^2du^2 = -1$ *is solvable for* $t, u \in \mathbb{Z}$.

Proof. This is Lemma 1 in [9]. □

Lemma 6. *Let d be an integer and p be an odd divisor of d. Then the following are equivalent:*

(i) $t^2 - du^2 = -4$ *is solvable for* $t, u \in \mathbb{Z}$.
(ii) $t^2 - p^2du^2 = -4$ *is solvable for* $t, u \in \mathbb{Z}$.

Proof. (ii) implies (i) is trivial. For the other direction note that $d \in \mathcal{D}_R$ and therefore there exists an order R of discriminant d. Since (i) is solvable, R has an unit ϵ of norm -1. Since $p \mid d$ and p odd, we have that ϵ^p has norm -1 and ϵ^p is an element of the order of discriminant dp^2. The latter is equivalent to the solvability of (ii). □

We can use this Lemma to improve the lower bound of Theorem 4 (i). Another easy statement is that when $t^2 - du^2 = -1$ is unsolvable for d, then it is also unsolvable when we replace d by dp^2 for an arbitrary p. This might be useful to improve the upper bound in Theorem 4 (ii).

5. Applications to the class number of real quadratic fields

The purpose of this section is to prove Theorem 3. In other words, we are concerned by the following question about the function ∇ defined in (21)

What is the asymptotic behavior of $\nabla(X)$ *as* $X \to \infty$ *?*

The authors are convinced that the following is true

Conjecture 1. *There exists a positive constant* c_1*, such that, as* $X \to \infty$*, one has*

$$\nabla(X) \sim c_1 X \log^2 X.$$

Such a conjecture seems quite deep and, if it is correct, it shows that on average, the class number of real quadratic fields is much smaller than the class number of imaginary quadratic fields. Conjecture 1, which apparently is new in these terms, can be seen as a transcription – in the scenery of real quadratic fields – of a conjecture due to Hooley [14] concerning the sum

$$\widetilde{\nabla}(X) := \sum_{d<X} H(d). \tag{65}$$

Here $H(d)$ is the number of properly primitive classes of indefinite forms $ax^2 + 2bxy + cy^2$ satisfying $d = b^2 - ac$. Hooley [14, Theorem 2] was the first to prove a lower bound of the form $\widetilde{\nabla}(X) \geq \tilde{c}_2 X \log X$ with a non trivial $\tilde{c}_2$ by considering the contribution of the d with a small regulator (hence a large value of $H(d)$). Pushing his arguments further, he was led to propose the conjectural asymptotic value [14, Conjecture 7]

$$\widetilde{\nabla}(X) \sim \frac{25}{12\pi^2} \cdot X \log^2 X \text{ for } X \to +\infty, \tag{66}$$

which inspirated our Conjecture 1.

Actually, the work of Hooley around this subject was anticipated by a result of Sarnak [21], which is of great interest. The author proves an asymptotic formula for the sum $\sum_{\epsilon_d<x} H(d)$, where d now is the discriminant of the more general quadratic form $ax^2+bxy+cy^2$ and ϵ_d is the associated regulator. In other words, surprisingly, when one sums $H(d)$ according to the the size of the fundamental solution ϵ_d of the Pell equation $t^2 - du^2 = \pm 4$ (and not on the size of d, which is the natural way of ordering of the discriminants), one finds and proves some regularity. One can summarize Sarnak's result in saying that $H(d)$ and ϵ_d have the same order of magnitude, when one uses the ordering by the size of ϵ_d. (For a generalization and a transposition of the results of [21] to the case of arithmetic progressions and of fundamental discriminants, see [20]). In [22, Conjecture 1], Sarnak also proposes a conjecture to guess the statistical size of $h(D)$ with D fundamental. It is also very valuable to bring Sarnak's and Hooley's approaches face to face with the Cohen–Lenstra heuristics, leading, for instance, to the conjecture

$$\sum_{\substack{p \leq X \\ p \equiv 1 \bmod 4}} h(p) \sim \frac{X}{8}$$

(see [3], [14], [15, p.96], [22], [24],...). It is also interesting to numerically test the conjecture (66) and related conjectures (see [16] & [18]).

We prefer to work on $\nabla(X)$ rather than on $\widetilde{\nabla}(X)$, the main reason being that we want to directly benefit from the algebraic number theory related to the ring of integers $\mathcal{O}_D$.

5.1. **The trivial lower bound for $\nabla(X)$.** The first result in the direction of Conjecture 1 is well known but very weak, it is a consequence of the inequality:

$$h(D) \geq 2^{\mathrm{rk}_2(\mathrm{C}_D)} = 2^{\omega(D)-1}, \tag{67}$$

already mentioned in (10). Then we deduce the following inequality (that we want to call *trivial lower bound*)

$$\nabla(X) \geq \nabla_2(X) \ (X \geq 1), \tag{68}$$

with

$$\nabla_2(X) = \sum_{\substack{0<D<X \\ D\equiv 1 \bmod 4}} 2^{\mathrm{rk}_2(\mathrm{C}_D)} \ \Big(= \frac{1}{2} \sum_{\substack{0<D<X \\ D\equiv 1 \bmod 4}} 2^{\omega(D)}\Big). \tag{69}$$

To treat $\nabla_2(X)$, let χ be the non principal Dirichlet character modulo 4 (see Lemma 4). We now consider the Dirichlet series

$$F(s) := \sum_{D\equiv 1 \bmod 4} \frac{2^{\omega(D)}}{D^s} \ \Big(= \sum_{n\geq 1} \frac{a_n}{n^s} \text{ say}\Big).$$

One has the equality

$$F(s) = \frac{1}{2} \sum_{n \text{ odd}} \frac{2^{\omega(n)}\mu^2(n)}{n^s} + \frac{1}{2} \sum_{n} \frac{2^{\omega(n)}\mu^2(n)\chi(n)}{n^s},$$

which in terms of Euler products gives the equality

$$\begin{aligned} F(s) &= \frac{1}{2} \prod_{p\geq 3} \Big(1 + \frac{2}{p^s}\Big) + \frac{1}{2} \prod_{p\geq 3} \Big(1 + \frac{2\chi(p)}{p^s}\Big) \\ &:= F_1(s) + F_2(s), \end{aligned}$$

say. Introducing the ζ–function and the function $L(s,\chi)$ one has the equalities ($\Re s > 1$)

$$F_1(s) = \frac{1}{2}\zeta^2(s)\, G_1(s),$$

$$F_2(s) = \frac{1}{2}L(s,\chi)^2\, G_2(s),$$

with

$$G_1(s) = (1 - \frac{1}{2^s}\Big)^2 \prod_{p\geqslant 3} \Big(1 - \frac{3}{p^{2s}} + \frac{2}{p^{3s}}\Big),$$

and

$$G_2(s) = \prod_{p\geqslant 3} \Big(1 - \frac{3}{p^{2s}} + \frac{2\chi(p)}{p^{3s}}\Big).$$

The products defining the functions $G_1(s)$ are $G_2(s)$ are convergent for $\Re s > 1/2$. By the classical properties of ζ and $L(s,\chi)$, one deduces that $F(s)$ has a meromorphic continuation in the open half plane $\{s \in \mathbb{C}\,;\ \Re s > 1/2\}$, where $F(s)$ has only one pole. It is of second order and it is located at $s = 1$. By classical integration techniques (mainly based on Perron's formula), one gets the equality

$$2\,\nabla_2(X) = \sum_{n<X} a_n = \frac{1}{2\pi\imath}\int_{\Re s=\frac{3}{2}} F(s)\frac{X^s}{s}\,\mathrm{d}s.$$

Moving the line of integration to the left and inserting classical bounds in vertical strips of $\zeta(s)$ and $L(s,\chi)$, one gets the formula

$$\sum_{n\le X} a_n \sim \frac{1}{2}\cdot G_1(1)\,X\,\log X,$$

as X tends to infinity. Hence we get

$$\nabla_2(X) \sim \frac{1}{8}\cdot \Pi_0\,X\,\log X\quad (X\to\infty), \tag{70}$$

where Π_0 is defined in (22). Note that (70) could have been equally proved by variations of the Dirichlet hyperbola method for the divisor function. Hence we proved

Proposition 2. *As $X \to \infty$, the following holds*

$$\nabla_2(X) \sim c_3 X\log X, \tag{71}$$

where

$$c_3 = \frac{1}{8}\cdot\Pi_0 = 0.035843\cdots. \tag{72}$$

Combining this Proposition with (68) we obtain (23), which is the starting point of our investigations on $\nabla(X)$. We shall see that its improvements will require rather involved tools. The authors are convinced that the proof of the equality

$$\overline{\lim}\frac{\nabla(X)}{X\log X} = +\infty, \tag{73}$$

which is much weaker than Conjecture 1, would give a new light on our understanding of the function $h(D)$. Our modest goal is to improve the value of c_3 appearing in the lower bound $\nabla(X) \ge (c_3 - o(1))X\log X$ (see (23)).

We shall follow four paths, which we can describe in terms of the new implemented ideas:

(i) Incorporate results the 3–part of C_D;
(ii) Incorporate results on the 4–part of C_D, in other words benefit from (11) of Theorem 1, (actually (53) of Proposition 1 with $k = 1$ and $\kappa = 2$ will be sufficient);
(iii) Finally mix the two tools mentioned above, to complete the proof of Theorem 3;
(iv) Give improvement by the use of ideas of Hooley [14] on the size of the regulator.

Each of these items is described in the next four subsections.

5.2. **Inserting results on the 3–rank.** We shall use a better inequality than (67), where now both 2 and 3–ranks are taken into account, that is

$$h(D) \geq 2^{\mathrm{rk}_2(\mathrm{C}_D)} \cdot 3^{\mathrm{rk}_3(\mathrm{C}_D)} = 2^{\omega(D)-1} \cdot 3^{\mathrm{rk}_3(\mathrm{C}_D)}. \tag{74}$$

which implies the lower bound

$$\nabla(X) \geq \nabla_{2,3}(X)\ (X \geq 1), \tag{75}$$

with

$$\nabla_{2,3}(X) := \sum_{\substack{0<D<X \\ D\equiv 1 \bmod 4}} 2^{\mathrm{rk}_2(\mathrm{C}_D)} \cdot 3^{\mathrm{rk}_3(\mathrm{C}_D)}. \tag{76}$$

Let τ be the usual divisor function. Since D is squarefree, we have $2^{\omega(D)} = \tau(D)$, from which we deduce the equality

$$2^{\mathrm{rk}_2(\mathrm{C}_D)} \cdot 3^{\mathrm{rk}_3(\mathrm{C}_D)} = \tau(D) \cdot \frac{3^{\mathrm{rk}_3(\mathrm{C}_D)} - 1}{2} + \frac{2^{\omega(D)}}{2}. \tag{77}$$

We now insert the equality

$$\tau(D) = 2 \sum_{q|D,\, q\leq\sqrt{D}} 1,$$

which is the key of Dirichlet's hyperbola method. By (76) & (77), we get

$$\begin{aligned}\nabla_{2,3}(X) &= 2 \sum_{\substack{q<\sqrt{X} \\ q \text{ odd}}} \Big(\sum_{\substack{q^2\leq D\leq X \\ q|D}} \frac{3^{\mathrm{rk}_3(\mathrm{C}_D)} - 1}{2} \Big) + \frac{1}{2} \sum_{D<X} 2^{\omega(D)} \\ &\geq 2 \sum_{\substack{q<Y \\ q \text{ odd}}} \Big(\sum_{\substack{q^2\leq D\leq X \\ q|D}} \frac{3^{\mathrm{rk}_3(\mathrm{C}_D)} - 1}{2} \Big) + \nabla_2(X). \end{aligned} \tag{78}$$

In the above summations, we always assumed the condition $D \equiv 1 \bmod 4$ and Y is any parameter $\leq \sqrt{X}$. By the classical upper bound (see [17, Prop. 8.7], for instance)

$$\frac{3^{\mathrm{rk}_3(\mathrm{C}_D)} - 1}{2} < h(D) < D^{\frac{1}{2}}.$$

we simplify (78) into

$$\begin{aligned}\nabla_{2,3}(X) &\geq 2 \sum_{\substack{q<Y \\ q \text{ odd}}} \Big(\sum_{\substack{D\leq X \\ D\equiv 1 \bmod 4,\ q|D}} \frac{3^{\mathrm{rk}_3(\mathrm{C}_D)} - 1}{2} \Big) + \nabla_2(X) - O(Y^3) \\ &\geq 2 \cdot \mho(X,Y) + \nabla_2(X) - O(Y^3), \end{aligned} \tag{79}$$

by definition. If we choose $Y = 1$ in (79) and appeal to (75), we recover (68). Hence, if for some $Y \leq \sqrt{X}$ one finds a non trivial lower bound of $\mho(X,Y)$, one immediately improves the lower bound (23). Producing such a lower bound is the object of the end of that subsection.

At that point we appeal to a result of Belabas & Fouvry [1, Théorème 2], based on the famous result of Davenport & Heilbronn ([4]).

Lemma 7. *Let ν be the unique multiplicative function defined on the set of square-free integers such that $\nu(p) = \frac{p}{p+1}$, for every prime p. Then, for every positive ϵ, we have the equality*

$$\sum_{q \leq X^{\frac{2}{7}-\epsilon}} \mu^2(q) \Big| \sum_{\substack{D \leq X \\ q|D}} \frac{3^{\mathrm{rk}_3(\mathrm{C}_D)} - 1}{2} - \frac{\nu(q)}{q} \cdot \frac{X}{2\pi^2} \Big| = O_\epsilon\Big(\frac{X}{\log X \log\log X}\Big),$$

uniformly for $X \geq 3$.

To apply this lemma to $\mho(X, Y)$ defined in (79), we first notice the trivial identity

$$\sum_{\substack{D<X \\ D \equiv 1 \bmod 4,\, q|D}} f(D) = \sum_{\substack{D<X \\ q|D}} f(D) - \sum_{\substack{D<X \\ 2q|D}} f(D),$$

(which is true for any function f and any odd q) and we fix $Y = Y_0 = X^{\frac{2}{7}-\epsilon}$. This gives the equality

$$\mho(X, Y_0) = \Big(\sum_{\substack{q \leq Y_0 \\ q \text{ odd}}} \mu^2(q) \cdot \frac{\nu(q)}{q} - \sum_{\substack{q \leq Y_0 \\ q \text{ odd}}} \mu^2(q) \cdot \frac{\nu(2q)}{2q}\Big) \cdot \frac{X}{2\pi^2} + O(X)$$

$$= \frac{2}{3}\Big(\sum_{\substack{q \leq Y_0 \\ q \text{ odd}}} \mu^2(q) \cdot \frac{\nu(q)}{q}\Big) \cdot \frac{X}{2\pi^2} + O(X). \tag{80}$$

Now a standard lemma coming from complex analysis asserts

Lemma 8. *As Z tends to infinity, we have*

$$\sum_{\substack{q \leq Z \\ q \text{ odd}}} \mu^2(q) \cdot \frac{\nu(q)}{q} \sim \frac{1}{2} \prod_{p \geq 3}\Big(1 - \frac{2}{p(p+1)}\Big) \log Z.$$

Proof. For $\Re s > 1$, consider the Dirichlet series

$$F_3(s) := \sum_{n \geq 1} \frac{\mu^2(2n)\nu(n)}{n^s} = \prod_{p \geq 3}\Big(1 + \frac{p/(p+1)}{p^s}\Big) = \zeta(s)\, G_3(s),$$

with

$$G_3(s) = (1 - \frac{1}{2^s}) \prod_{p \geq 3}\Big(1 - \frac{1}{(p+1)p^s} - \frac{1}{(p+1)p^{2s-1}}\Big).$$

Since G_3 has an holomorphic continuation in $\Re s > 1/2$, we can apply classical tools. For instance the Hardy–Littlewood–Karamata Theorem (see [26, Theorem 8 p. 227]) implies that the sum in consideration is $\sim G_3(1) \log Z$. □

Combining Lemma 8 with (79) and (80), we obtain the inequality

$$\nabla_{2,3}(X) \geq \frac{2 - o(1)}{21 \cdot \pi^2} \prod_{p \geq 3}\Big(1 - \frac{2}{p(p+1)}\Big) X \log X + \nabla_2(X). \tag{81}$$

Recall the classical formula

$$\frac{6}{\pi^2} = \prod_{p \geq 2}\Big(1 - \frac{1}{p^2}\Big),$$

which transforms (81) into

$$\nabla_{2,3}(X) \geq \Big(\frac{1}{42} - o(1)\Big) \cdot \Pi_0\, X \log X + \nabla_2(X).$$

It remains to combine with (71) to finally write

Proposition 3. *As $X \to \infty$, the following holds*

$$\nabla_{2,3}(X) \geq \big(c_4 - o(1)\big) X \log X,$$

where

$$c_4 = \frac{25}{168} \cdot \Pi_0 \ \big(= \frac{25}{21} \cdot c_3\big).$$

Comparing the numerical values of c_4 and c_3, we may say that Proposition 3 combined with (75) improves the trivial lower bound (23) by 19 %, approximately.

5.3. **Inserting results on the 4–rank.** Instead of working with (74), we start from the other trivial inequality

$$h(D) \geq 2^{\mathrm{rk}_2(\mathrm{C}_D)} \cdot 2^{\mathrm{rk}_4(\mathrm{C}_D)} = 2^{\omega(D)-1} \cdot 2^{\mathrm{rk}_4(\mathrm{C}_D)}, \tag{82}$$

which gives

$$\nabla(X) \geq \nabla_{2,4}(X), \tag{83}$$

with

$$\nabla_{2,4}(X) := \sum_{\substack{0<D<X \\ D\equiv 1 \bmod 4}} 2^{\mathrm{rk}_2(\mathrm{C}_D)} \cdot 2^{\mathrm{rk}_4(\mathrm{C}_D)}. \tag{84}$$

This function has been already met in §2, this is exactly half of the weighted moment of order 1, i.e. $S_{\mathrm{w}}^{+}(X, 1, 1, 4)$, with $\kappa = 2$ (see (46)). Appealing to (53) of Proposition 1 and dividing by 2, we have

$$\nabla_{2,4}(X) \sim \frac{\mathbf{N}(2,2) - \mathbf{N}(1,2)}{2} \cdot \nabla_2(X) = \frac{3}{2} \cdot \nabla_2(X). \tag{85}$$

Combining with (71) we finally proved

Proposition 4. *As $X \to \infty$, one has*

$$\nabla_{2,4}(X) = \big(c_5 + o(1)\big) \cdot X \log X,$$

with $c_5 = \frac{3}{16} \cdot \Pi_0 = \frac{3}{2} \cdot c_3$.

Clearly, Proposition 4 combined with (83) improves the trivial lower bound (23) by 50%.

5.4. **Mixing the two methods : the proof of Theorem 3.** We start from a most intricate lower bound

$$h(D) \geq 2^{\mathrm{rk}_2(\mathrm{C}_D)} \cdot 3^{\mathrm{rk}_3(\mathrm{C}_D)} \cdot 2^{\mathrm{rk}_4(\mathrm{C}_D)},$$

which gives the inequality

$$\nabla(X) \geq \nabla_{2,3,4}(X), \tag{86}$$

where

$$\nabla_{2,3,4}(X) = \sum_{\substack{0<D<X \\ D\equiv 1 \bmod 4}} 2^{\mathrm{rk}_2(\mathrm{C}_D)} \cdot 3^{\mathrm{rk}_3(\mathrm{C}_D)} \cdot 2^{\mathrm{rk}_4(\mathrm{C}_D)}. \tag{87}$$

It seems difficult to control simultaneously the 3–rank and the 4-rank. So we separate these quantities by appealing to the following lower bound

$$tu \geq t + u - 1 \ (t \,\&\, u \geq 1),$$

which we apply with $t = 3^{\mathrm{rk}_3(\mathrm{C}_D)}$ and $u = 2^{\mathrm{rk}_4(\mathrm{C}_D)}$. Multiplying by $2^{\mathrm{rk}_2(\mathrm{C}_D)}$, summing over all $D \leq X$, congruent to 1 mod 4, and introducing the already defined summatory functions ∇, ∇_2, $\nabla_{2,3}$ and $\nabla_{2,4}$, we deduce from (87) the inequality

$$\nabla_{2,3,4}(X) \geq \nabla_{2,3}(X) + \nabla_{2,4}(X) - \nabla_2(X).$$

It remains to apply Propositions 2, 3 and 4 to get

Proposition 5. *As $X \to \infty$, one has*

$$\nabla_{2,3,4}(X) \geq \big(c_0 - o(1)\big) \cdot X \log X,$$

with

$$c_0 = \frac{71}{336} \cdot \Pi_0 \ (= \frac{71}{42} \cdot c_3).$$

Combining with (86), we complete the proof of Theorem 3.

5.5. **Further improvements.** We want to show how to incorporate the ideas that were introduced by Hooley in [14] to improve the lower bound of the function $\tilde{\nabla}(X)$ as defined in (65) above. His idea essentially consists in searching for discriminants d with small regulators (which means less than $d^{\frac12+\alpha}$ for some small positive α). This set of d corresponds to the case where the equation

$$T^2 - dU^2 = \pm 4,$$

has a primitive solution η_d, written as $T + U\sqrt{d}$ satisfying $\sqrt{d} \leq \eta_d \leq d^{\frac12+\alpha}$. If α is not too large, the cardinality of such $d \leq X$ is $\asymp \sqrt{X}\log^2 X$. This set of discriminants has some regularity, since one can prove that the attached L–function is constant, on average, at the point 1. By the Dirichlet class number formula (see [14, form. (3)] for instance), the class number of these d, is $\asymp \sqrt{d}/\log d$, on average. We easily see that the contribution of this set of discriminants to the sum $\tilde{\nabla}(X)$ is $\asymp X \log X$, which is exactly the order of magnitude of the trivial lower bound of $\tilde{\nabla}(X)$. Here is the origin of the improvement stated in [14, Theorem 2].

In our context of positive fundamental discriminants $D \equiv 1 \bmod 4$, let ϵ_D be the fundamental unit of the group of units $\mathbb{U}_D$ of $\mathcal{O}_D$ (in other words, ϵ_D is the unique unit > 1 such that $\mathbb{U}_D$ can be written as $\mathbb{U}_D = \{\pm\epsilon_D^n\,; n \in \mathbb{Z}\}$). For $\alpha > 0$ define

$$\mathcal{E}(X,\alpha) := \big\{0 < D \leq X\,;\ D \equiv 1 \bmod 4,\ D^{\frac12} \leq \epsilon_D \leq D^{\frac12+\alpha}\big\}.$$

We can prove

Proposition 6. *There exists three positive constants α_0, β_0 and γ_0, such that, as $X \to \infty$, one has*

$$\sharp\,\mathcal{E}(X,\alpha_0) \sim \beta_0\, X^{\frac12} \log^2 X, \tag{88}$$

and

$$\sum_{D \in \mathcal{E}(X,\alpha_0)} h(D) \sim \gamma_0 \cdot \Pi_0 \cdot X \log X. \tag{89}$$

Proof. The proof mimics [14, p. 98–123]. We give some hints about the strategy we have to follow in our context. Searching for small ϵ_D can be reduced to finding solutions to the equation

$$T^2 - DU^2 = \pm 4,$$

with the constraint $T + U\sqrt{D} \leq 2D^{\frac{1}{2}+\alpha_0}$, and $D \leq X$. By an easy argument, we are led to study the pairs (T, U) of positive integers, satisfying some inequalities (in terms of X and α_0) and such that

$$(T^2 \pm 4)/U^2,$$

is an integer which is congruent to 1 mod 4 and which is squarefree. This last condition is new, when compared with [14] and is far from being an innocent condition. However, since we are working with polynomials of degree 2, a sieve of dimension 0 is sufficient. This gives (88). The study of the average value of $L(1, \left(\frac{D}{\cdot}\right))$, for $D \in \mathcal{E}(X, \alpha_0)$, looks like [14, §6]. By appealing to the class number formula for $h(D)$ (see [2, Prop. 5.6.9]), we get (89).

Our computations (not published) show that in Proposition 6, we can choose any positive $\alpha_0 < 1/4$. The associated γ_0 has the value

$$\gamma_0 = \frac{1}{6}\big(\alpha_0 - \frac{1}{2}\log(1 + 2\alpha_0)\big). \tag{90}$$

Taking α_0 arbitrarily close to $1/4$, one obtains

$$\gamma_0 = .007\,877\cdots$$

It is an interesting problem to prove Proposition 6 for values of $\alpha_0 > 1/4$. Such an improvement will certainly depend on sophisticated techniques of analytic number theory. □

We now explain how to improve the result of Theorem 3 with the help of the results of Proposition 6.

Theorem 5. *Let α_0, β_0 and γ_0 be three positive constants as in Proposition 6. Then we have*

$$\nabla(X) \geq \big(\frac{71}{336} + \gamma_0 - o(1)\big) \cdot \Pi_0 \cdot X \log X$$

Proof. We start from the relations

$$\begin{aligned}
\nabla(X) &= \sum_{D \in \mathcal{E}(X,\alpha_0)} h(D) + \sum_{\substack{D \notin \mathcal{E}(X,\alpha_0) \\ D \equiv 1 \bmod 4,\, D \leq X}} h(D) \\
&\geq \sum_{D \in \mathcal{E}(X,\alpha_0)} h(D) + \sum_{\substack{D \notin \mathcal{E}(X,\alpha_0) \\ D \equiv 1 \bmod 4,\, D \leq X}} 2^{\mathrm{rk}_2(\mathrm{C}_D)} \cdot 3^{\mathrm{rk}_3(\mathrm{C}_D)} \cdot 2^{\mathrm{rk}_4(\mathrm{C}_D)} \\
&\geq \sum_{D \in \mathcal{E}(X,\alpha_0)} h(D) + \nabla_{2,3,4}(X) - O\Big(X^{\epsilon}\, \sharp\mathcal{E}(X,\alpha_0) \max_{D \leq X} 3^{\mathrm{rk}_3(\mathrm{C}_D)}\Big). \qquad (91)
\end{aligned}$$

By Proposition 6, we know that the first term on the right of (91) is

$$\sim \gamma_0 \cdot \Pi_0 \cdot X \log X. \tag{92}$$

By Proposition 5, we know that the second term is

$$\geq \big(c_0 - o(1)\big) \cdot X \log X. \tag{93}$$

Finally, appealing to the deep results of [19], [5] or [13], we know the existence of a positive δ_0, such that

$$3^{\mathrm{rk}_3(\mathrm{C}_D)} \ll |D|^{\frac{1}{2}-\delta_0},$$

for every fundamental D, positive or negative. This inequality combined with (88) proves that the error term in the right part of (91) is

$$\ll X. \tag{94}$$

Gathering (91),..., (94), we complete the proof of Theorem 5. □

Remarks

(i) It is worth noticing that the introduction of the constant γ_0 (corresponding to α_0 slightly less than 1/4) only produces an improvement of 6.3 % on the trivial lower bound for $\nabla(X)$. This is much smaller than the improvements coming from the study of the 3 and 4–ranks. This situation would change if we could take for α_0, values much larger than 1/4 in Proposition 6. However, for larger values of α_0, it is not sure that the definition of γ_0 continues to be given by (90) (for a discussion on that subject see [14]).

(ii) The authors think that a proof of (73) could pass through an improvement of the inequality (86) where infinitely many powers of primes would appear or through the study of the contribution of the D with ϵ_D larger than any fixed power of D. These two approaches seem quite difficult.

References

[1] K. Belabas and E. Fouvry, Sur le 3–rang des corps quadratiques de discriminant premier ou presque premier. *Duke Math. J.*, 98: 217–268, 1999.

[2] H. Cohen, A Course in Computational Algebraic Number Theory. *Grad. Texts in Math. 138* Springer, 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. Davenport and H. Heilbronn, On the density of discriminants of cubic fields (ii). *Proc. Roy. Soc. London A*, 322: 405–420, 1971.

[5] J.S. Ellenberg and A. Venkatesh, Reflection principles and bounds for class group torsion. *Int. Math. Res. Not. IMRN*, no. 1, Art. ID rnm002, 18 pp, 2007.

[6] E. Fouvry and J. Klüners, On the 4–rank of quadratic number fields. *Inv. Math.*, 167 : 455–516, 2007.

[7] E. Fouvry and J. Klüners, Cohen-Lenstra heuristics of quadratic number fields. *Algorithmic number theory, Lecture Notes in Comput. Sci.,* 4076 : 40–55, Springer, Berlin, 2006.

[8] E. Fouvry and J. Klüners, On the negative Pell equation. *Annals of Math.*, (to appear).

[9] E. Fouvry and J. Klüners, The parity of the period of the continued fraction of $\sqrt{d}$. *Proc. London Math. Soc.*, (to appear).

[10] F. Gerth III, The 4–class ranks of quadratic fields. *Inv. Math.*, 77 : 489–515, 1984.

[11] 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.

[12] D.R. Heath–Brown, The size of Selmer groups for the congruent number problem. II. *Inv. Math.*, 118 : 331-370, 1994.

[13] H. Helfgott and A. Venkatesh, Integral points on elliptic curves and 3–torsion in class groups. *J. American Math. Soc.*, 19 no. 3: 527–550, 2006.

[14] C. Hooley, On the Pellian equation and the class number of indefinite quadratic forms. *J. für reine Angew. Math.*, 353 : 98–131, 1984.

[15] C. Hooley, Some recent advances in analytical number theory. *Proceedings of the International Congress of Mathematicians*, Vol. 1, 2 (Warsaw, 1983), PWN, Warsaw: 85–97, 1984.

[16] S. Kwon, On the average class numbers. *Undergraduate Thesis*, Princeton University, 2006.

[17] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers (Second edition). Springer, 1990.

[18] I.N. Petrov, Numerical evidence of a conjecture of Hooley. *Undergraduate Thesis*, Princeton University, 2007.

[19] L. Pierce, The 3–part of class numbers of quadratic fields. *J. London Math. Soc. (2)*, 71: 579–598, 2005.

[20] N. Raulf, Asymptotics of class numbers for progressions and for fundamental discriminants. *Forum Math.*, 21: 221–257, 2009.

[21] P. Sarnak, Class numbers of indefinite binary quadratic forms. *J. Number Theory*, 15: 229–247, 1982. & Corrigenda *J. Number Theory*, 16: 284, 1983.

[22] P. Sarnak, Class numbers of indefinite binary quadratic forms. II. *J. Number Theory*, 21: 333–346, 1985.

[23] P. Sarnak, Letter to J. Davis about reciprocal geodesics (unpublished), 2005.

[24] P. Sarnak, Reciprocal geodesics. *Analytic Number Theory. Clay Math. Proc.*, American Math. Soc., Providence, R.I., vol. 7 : 217–237, 2007.

[25] P. Stevenhagen, The number of real quadratic fields with units of negative norms. *Experiment. Math.*, 2: 121–136, 1993.

[26] G. Tenenbaum, Introduction to Analytic and Probabilistic Number Theory. *Cambridge Studies in Advanced mathematics* vol. 46. C.U.P., 1995.

Univ Paris-Sud, Laboratoire de Mathématiques, UMR8628, Orsay, F-91405; CNRS, Orsay, F-91405

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

Universität Paderborn, Institut für Mathematik, D-33095 Paderborn, Germany.

E-mail address: klueners@math.uni-paderborn.de