# ON THE *SPIEGELUNGSSATZ* FOR THE 4–RANK

ÉTIENNE FOUVRY AND JÜRGEN KLÜNERS

Abstract. Let $d$ be a non square positive integer. We give the value of the natural probability that the narrow ideal class groups of the quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-d})$ have the same value for their 4–ranks.

## 1. Introduction

1.1. **Conventions and notations.** Throughout this work, the letter $D$ is reserved to denote a fundamental discriminant, *i.e* the discriminant of a quadratic extension of $\mathbb{Q}$. Let $K = \mathbb{Q}(\sqrt{D})$, $\mathcal{N}$ be the norm function on $K$ and let $\mathfrak{O}_K$ be the ring of integers of $K$. On the set of non zero ideals of $\mathfrak{O}_K$ we say that two ideals $\mathfrak{I}$ and $\mathfrak{J}$ are *equivalent in the narrow sense*, if there is an element $a \in \mathfrak{O}_K$, such that $\mathfrak{I} = (a)\mathfrak{J}$ and $\mathcal{N}(a) > 0$. By the multiplication of the ideal classes, we obtain the *(narrow) class group of* $K$, that we denote by $\mathrm{C}_D$. This is a finite abelian group.

We extend this definition of $\mathrm{C}_D$ in the following way: if $d$ is a non square integer, not necessarily a fundamental discriminant, we also denote by $\mathrm{C}_d$ the class group of the quadratic field $\mathbb{Q}(\sqrt{d})$. When $d$ is a non zero perfect square, we define $\mathrm{C}_d$ to be the trivial group.

We reserve the letter $p$ to prime numbers and, for $n \geq 1$, the number of distinct primes divisors of $n$ is denoted by $\omega(n)$. The Möbius function of $n$ is $\mu(n)$.

If $A$ is a finite multiplicative abelian group and $p$ a prime number, the *$p$–rank* is, by definition $\mathrm{rk}_p(A) := \dim_{\mathbb{F}_p}(A/A^p)$. More generally, if $k$ is an integer $\geq 1$, we define the *$p^k$–rank* of $A$, by $\mathrm{rk}_{p^k}(A) := \dim_{\mathbb{F}_p}(A^{p^{k-1}}/A^{p^k})$.

1.2. **Scholz' Theorem.** The original *Spiegelungssatz* concerned the 3–rank of $\mathrm{C}_D$ and was proved by Scholz [13] in the form of the double inequality

$$\mathrm{rk}_3(\mathrm{C}_d) \leq \mathrm{rk}_3(\mathrm{C}_{-3d}) \leq \mathrm{rk}_3(\mathrm{C}_d) + 1, \tag{1}$$

for any non square $d \geq 1$. With the above convention, it is straightforward to extend (1) to any $d \geq 1$.

Hence, when $d \geq 1$ is given, the integer $\mathrm{rk}_3(\mathrm{C}_{-3d})$ can only take two values: either $\mathrm{rk}_3(\mathrm{C}_d)$ or $\mathrm{rk}_3(\mathrm{C}_d)+1$. Each of these possibilities is well described in algebraic terms. But the natural question is to know the frequency of each of these events. Dutarte [6] further pushing the probabilistic model leading to the heuristics of Cohen–Lenstra [3], proposed a value of the second frequency. More precisely, he was led to conjecture

*Date*: October 2, 2008.
2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R11.

**Conjecture 1.** *([6, Formula(3) p. 8]) For every integer $a \geq 0$ we have*

$$\lim_{X\to+\infty} \frac{\sharp\big\{D\,;\ 0\leq D\leq X,\, \mathrm{rk}_3(\mathrm{C}_D)=a \text{ and } \mathrm{rk}_3(\mathrm{C}_{-3D})=a+1\big\}}{\sharp\big\{D\,;\ 0\leq D\leq X,\, \mathrm{rk}_3(\mathrm{C}_D)=a\big\}} = 3^{-(a+1)}. \tag{2}$$

The equality (2) can be seen as a conditional probability under the following convention: Let $\mathcal{A}$ be a subset of the set $\mathcal{D}^+$ of positive fundamental discriminants $D$, we define the probability of the event $D\in\mathcal{A}$ as being equal to the following limit (if it exists)

$$\mathbf{Prob}(\mathcal{A}) := \lim_{X\to+\infty}\Big(\sum_{\substack{0<D<X\\ D\in\mathcal{A}}} 1\Big)\Big/\Big(\sum_{0<D<X} 1\Big). \tag{3}$$

This probability also is the natural density of $\mathcal{A}$, considered as a subset of $\mathcal{D}^+$. With this definition, Conjecture 1 is only a statement concerning the existence and the value of a conditional probability. In other words, Dutarte thinks that for any $a\geq 0$ we have the equality

$$\mathbf{Prob}\Big(\mathrm{rk}_3(\mathrm{C}_{-3D})=a+1 \text{ and } \mathrm{rk}_3(\mathrm{C}_D)=a \,\Big|\, \mathrm{rk}_3(\mathrm{C}_D)=a\Big) = 3^{-a-1}. \tag{4}$$

Now we appeal to the following consequence of the heuristics of Cohen and Lenstra [3, (C 9) p. 57]

$$\mathbf{Prob}\big(\mathrm{rk}_3(\mathrm{C}_D)=a\big) = 3^{-a(a+1)}\,\eta_\infty(3)\,\eta_a^{-2}(3)\,(1-3^{-(a+1)})^{-1},$$

where the function $\eta_k(t)$ is defined in (8) below. Summing the equality (4) over all $a\geq 0$ we have

$$\begin{aligned}\mathbf{Prob}\big(\mathrm{rk}_3(\mathrm{C}_{-3D})=\mathrm{rk}_3(\mathrm{C}_D)+1\big) &= \sum_{a=0}^{\infty}\mathbf{Prob}\big(\mathrm{rk}_3(\mathrm{C}_{-3D})-1=\mathrm{rk}_3(\mathrm{C}_D)=a\big)\\ &= \eta_\infty(3)\sum_{a=0}^{\infty} 3^{-(a+1)^2}\,\eta_a^{-2}(3)\,(1-3^{-(a+1)})^{-1}\\ &= 0.283530\cdots\end{aligned} \tag{5}$$

But the equality (5) is conjectural for the moment, even if it has been tested on a computer (see [6, §4.2]). As far as we know, the only result around the conjectural value (5) is due to Belabas [1, Theorem 2.1] & [2], who proved the following equality

$$\frac{\displaystyle\sum_{\substack{0<D<X\\ \mathrm{rk}_3(\mathrm{C}_{-3D})=\mathrm{rk}_3(\mathrm{C}_D)+1}} 3^{\mathrm{rk}_3(\mathrm{C}_D)}}{\displaystyle\sum_{0<D<X} 3^{\mathrm{rk}_3(\mathrm{C}_D)}} = \frac{1}{4}+O\big(\exp(-\frac{1}{5}(\log X\log\log X)^{\frac{1}{2}})\big), \tag{6}$$

as $X$ tends to $+\infty$. The equality (6) can be seen as a weighted version of (5). These weights are chosen in order to easily apply the seminal work of Davenport & Heilbronn [4] concerning the average behavior of the 3–part of $\mathrm{C}_D$.

1.3. **Damey–Payan's Theorem and the contribution of Gerth.** We owe to Damey and Payan [5, Théorème II.9 & II.10] to have proved that a phenomenon similar to the 3–rank also holds for the 4–rank, that is

**Theorem A.** *("Spiegelungssatz for the 4–rank") For every $d\geq 1$ we have*

$$\mathrm{rk}_4(\mathrm{C}_d)\leq \mathrm{rk}_4(\mathrm{C}_{-d})\leq \mathrm{rk}_4(\mathrm{C}_d)+1. \tag{7}$$

Note the equality $\mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(\sqrt{-4d})$. We shall say that the fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-d})$ are *associated*.

As for the 3–rank, the natural question is to evaluate the frequency of each of the events "$\mathrm{rk}_4(\mathrm{C}_{-d}) = \mathrm{rk}_4(\mathrm{C}_d)$" and "$\mathrm{rk}_4(\mathrm{C}_{-d}) = \mathrm{rk}_4(\mathrm{C}_d) + 1$". The only paper concerning this question is due to Gerth [11]. In order to present his results we introduce several notations. For $k \in \mathbb{N} \cup \{\infty\}$ let $\eta_k$ be the function defined for $t > 1$ by

$$\eta_k(t) := \prod_{j=1}^{k} \big(1 - t^{-j}\big). \tag{8}$$

For $x \geq 1$ and $a, t \geq 0$ integers we introduce the two sets

$$A_{t;x} := \big\{m\,;\, m \text{ squarefree } \leq x, \text{ exactly } t \text{ primes ramify in } \mathbb{Q}(\sqrt{-m})/\mathbb{Q}\big\},$$

and

$$A^{=}_{t,a;x} := \big\{m\,;\, m \in A_{t,x},\ \mathrm{rk}_4(C_{-m}) = \mathrm{rk}_4(C_m) = a\big\}.$$

With these conventions, Gerth proved

**Theorem B.** *([11, p.2551]) For every integer $a \geq 0$, we have*

$$\lim_{t\to\infty}\ \lim_{x\to\infty} \frac{\sharp\ A^{=}_{t,a;x}}{\sharp\ A_{t;x}} = 2^{-a}\, 2^{-a^2}\, \eta_\infty(2)\eta_a(2)^{-2}. \tag{9}$$

In this statement, Gerth has chosen to list all the imaginary quadratic fields in the form $\mathbb{Q}(\sqrt{-m})$ with $m$ squarefree. Gerth could have adopted the other point of view of writing these imaginary fields in the form $\mathbb{Q}(\sqrt{D})$ with $D$ a negative fundamental discriminant. This is the point of view that we prefer to adopt in the present paper. Also remember that $D = -m$ or $D = -4m$ according to the cases $m \equiv 3 \bmod 4$ or $m \equiv 1$ or $2 \bmod 4$, and that exactly $\omega(|D|)$ primes ramify in $\mathbb{Q}(\sqrt{D})$.

More precisely, here is the variant of Theorem B that we have in mind and that could have been equally proved by Gerth in [11]:

**Theorem C.** *For any integer $a \geq 0$ we have*

$$\lim_{t\to\infty}\ \lim_{X\to\infty} \frac{\sharp\big\{D\,;\, 0 < -D < X,\, \omega(|D|) = t,\, \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) = a\big\}}{\sharp\big\{D\,;\, 0 < -D < X,\, \omega(|D|) = t\big\}} = 2^{-a}\, 2^{-a^2}\, \eta_\infty(2)\eta_a(2)^{-2}.$$

Theorems B & C appeal several commentaries. By mixing Theorem C with the central result of [10, Formula (1.5)], we get

**Corollary A.** *([11, p.2551]) For every integer $a \geq 0$*

$$\lim_{t\to\infty}\ \lim_{X\to\infty} \frac{\sharp\ \{D\,;\, 0 < -D \leq X,\, \omega(|D|) = t, \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) = a\}}{\sharp\ \{D\,;\, 0 < -D \leq X,\, \omega(|D|) = t, \mathrm{rk}_4(\mathrm{C}_D) = a\}} = 2^{-a}.$$

This corollary, roughly speaking, asserts that for an imaginary quadratic field with 4–rank equal to $a$, the probability (in the special sense introduced by Gerth) that its associated field has the same 4–rank is equal to $2^{-a}$. But the meaning of this probability cannot be reduced to the *natural* probability introduced in (3).

The second remark is when we sum the equality contained in Theorem C over all $a \geq 0$ we obtain

**Corollary B.** *(see* [11, Theorem 1]*)*

$$\lim_{t\to\infty}\lim_{X\to\infty}\frac{\sharp\,\{D\,;\,0<-D\le X,\,\omega(-D)=t,\mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{C}_{-D})\}}{\sharp\,\{D\,;\,0<-D\le X,\,\omega(|D|)=t\}}$$

$$=\sum_{a=0}^{\infty}2^{-a}\,2^{-a^2}\eta_\infty(2)\eta_a(2)^{-2}=0.610321\cdots\ .$$

This Corollary shows that certainly the behavior of the 4–ranks differs from the 3–rank as long as the Spiegelungssatz is concerned.

The third remark is that Gerth could have equally stated Theorem B by first considering the value $a$ of $\mathrm{rk}_4(\mathrm{C}_m)$ (instead of $\mathrm{rk}_4(\mathrm{C}_{-m})$). Then the value of the second part of the equalities contained in Theorems B, C and Corollary A would have been modified. Of course, the numerical constant appearing in Corollary B would have been unchanged.

The purpose of this paper is to prove the statements of Theorem C and Corollaries A & B, but in the context of the more natural space of probability, as defined in (3), but naturally transposed to the set of negative discriminants. This is far from being a simple transposition of the original proofs of Gerth, since he writes [11, p.2547]: *However, computing these limits appears to be very difficult.* The limits mentioned by Gerth are those which will appear in Theorem 1 below.

1.4. **Statement of the results.** The central result of our paper is

**Theorem 1.** *For every integer $r\ge 0$ we have*

(10)
$$\lim_{X\to\infty}\frac{\sharp\big\{D\,;\,0<-D<X,\,\mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{C}_{-D})=r\big\}}{\sharp\big\{D\,;\,0<-D<X\big\}}=2^{-r}\,2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2},$$

*and*

$$\lim_{X\to\infty}\frac{\sharp\big\{D\,;\,0<-D<X,\,\mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{C}_{-D})+1=r\big\}}{\sharp\big\{D\,;\,0<-D<X\big\}}=(1-2^{-r})\,2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2}. \tag{11}$$

*Similar statements remain true if, in the above expressions, we restrict to the negative fundamental $D$ congruent to* $1 \bmod 4$*, to* $0 \bmod 8$ *or to* $4 \bmod 8$.

Summing (10) or (11), we obtain

**Corollary 1.** *We have the equalities*

(12)
$$\lim_{X\to\infty}\frac{\sharp\big\{D\,;\,0<-D<X,\,\mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{C}_{-D})\big\}}{\sharp\big\{D\,;\,0<-D<X\big\}}=\sum_{r=0}^{\infty}2^{-r}\,2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2},$$

*and*

$$\lim_{X\to\infty}\frac{\sharp\big\{D\,;\,0<-D<X,\,\mathrm{rk}_4(\mathrm{C}_D)=\mathrm{rk}_4(\mathrm{C}_{-D})+1\big\}}{\sharp\big\{D\,;\,0<-D<X\big\}}=\sum_{r=0}^{\infty}(1-2^{-r})\,2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2}. \tag{13}$$

*Similar statements remain true if, in the above expressions, we restrict to the negative fundamental $D$ congruent to* $1 \bmod 4$*, to* $0 \bmod 8$ *or to* $4 \bmod 8$.

It is important to notice that the values appearing on the right sides of the equations (10), (11), (12) & (13) coincide with the values appearing in Theorem C and Corollary B, but the probabilistic models are not the same at all. However, these coincidences confirm an intuition of Gerth (see [11, p.2547]) expressed as: *Although the limits we compute are not guaranteed to equal the above limits, our results do provide some insight into this question.*

## 2. The theory of moments

A classical tool of analytic number theory in the study of the distribution of the values of an arithmetic function is the theory of moments of this function. Hence, as in [7, p.470], we introduce the quantities

$$S^-(X,k,a,q) := \sum_{\substack{0<-D<X \\ D\equiv a \bmod q}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}, \tag{14}$$

where $X \geq 2$ is a number and $a, k \geq 0$, and $q \geq 1$ are integers. In the present paper, we only deal with the cases

$$(a,q) \in \big\{(1,4),\,(0,8),\,(4,8)\big\}, \tag{15}$$

which corresponds to the classical partition of the set of fundamental discriminants, into three subsets, according to the highest power of 2 dividing $D$. The sum $S^-(X,k,a,q)$ is the moment of order $k$ of the function $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ on the set of negative discriminants congruent to $a \bmod q$. It is more efficient to work with the powers of $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ than with the powers of $\mathrm{rk}_4(\mathrm{C}_D)$ itself, since algebra furnishes a flexible formula for $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ (see (26) below).

It is natural to compare this moment to the corresponding counting function

$$\mathcal{D}^-(X,a,q) := S^-(X,0,a,q),$$

which is the cardinality of the set of negative fundamental discriminants $D$, congruent to $a \bmod q$, of absolute value less than $X$. These cardinalities are well known since we have

$$\mathcal{D}^-(X,1,4),\ 4\cdot\mathcal{D}^-(X,0,8)\ \&\ 4\cdot\mathcal{D}^-(X,4,8) = \frac{2}{\pi^2}X + O(\sqrt{X}), \tag{16}$$

uniformly for $X \geq 2$. The equalities (16) are only variations on the classical formula

$$\sum_{n\leq X}\mu^2(n) = \frac{6}{\pi^2}X + O(\sqrt{X}),$$

which counts the number of squarefree numbers up to $X$. We recall a notation introduced in [7, p.461]: $\mathbf{N}(k,2)$ denotes the total number of vector subspaces (of any dimension) of $\mathbb{F}_2^k$.

One of the central results of [7] is

**Theorem D.** *(see* [7, Thm. 6, 8 & 10]*) Let $(a,q)$ satisfying (15). Then for any integer $k \geq 0$ and for any $\epsilon > 0$ we have the equality*

$$S^-(X,k,a,q) = \mathbf{N}(k,2)\cdot\mathcal{D}^-(X,a,q) + O_{k,\epsilon}\Big(X(\log X)^{-2^{-k}+\epsilon}\Big)$$

*uniformly for $X \geq 2$.*

From Theorem D we deduced the following

**Corollary C.** *(see* [7, Theorem 3]*) Let* $(a,q)$ *satisfying (15). For every* $r\geq 0$ *we have*

$$\lim_{X\to\infty}\frac{\sharp\big\{D\,;\,0<-D<X,\,D\equiv a \bmod q,\,\mathrm{rk}_4(\mathrm{C}_D)=r\big\}}{\mathcal{D}^-(X,a,q)}=2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2}.$$

In order to trap the values of the pair of variables $(\mathrm{rk}_4(\mathrm{C}_D),\mathrm{rk}_4(\mathrm{C}_{-D}))$, we introduce the mixed moment

$$S^-_{\mathrm{mix}}(X,k,a,q):=\sum_{\substack{0<-D<X\\ D\equiv a \bmod q}}2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}\cdot 2^{\mathrm{rk}_4(\mathrm{C}_{-D})}. \tag{17}$$

Generally speaking, we should have to compute the sums corresponding to the terms $2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}\cdot 2^{\ell\,\mathrm{rk}_4(\mathrm{C}_{-D})}$, for all the integer exponents $(k,\ell)$. But the functions $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ and $2^{\mathrm{rk}_4(\mathrm{C}_{-D})}$ are highly constrained by Theorem A. Hence it is sufficient to compute the mixed moments for the exponents $(k,1)$ only (see (18) below). This remark avoids a huge amount of work, particularly in the combinatorial aspect. Such a situation already appeared in [9], where we studied the values of the pair of functions $(\mathrm{rk}_4(\mathrm{C}_D),\mathrm{rk}_4(\mathrm{Cl}_D))$, where $\mathrm{Cl}_D$ is the ordinary class group of the field $\mathbb{Q}(\sqrt{D})$, with $D>0$, divisible by no prime $\equiv 3 \bmod 4$.

Theorem 1 will be deduced from

**Theorem 2.** *Let* $(a,q)$ *satisfying (15). Then for any integer* $k\geq 0$ *and for any* $\epsilon>0$ *we have the equality*

$$S^-_{\mathrm{mix}}(X,k,a,q)=\frac{\mathbf{N}(k+1,2)+\mathbf{N}(k,2)}{2}\cdot\mathcal{D}^-(X,a,q)+O_{k,\epsilon}\Big(X(\log X)^{-2^{-k}+\epsilon}\Big)$$

*uniformly for* $X\geq 2$.

Theorems D & 2 imply that asymptotically the ratio

$$S^-_{\mathrm{mix}}(X,k,a,q)/S^-(X,k+1,a,q)$$

has a limit strictly less than 1 as $X$ tends to infinity. This means that frequently, the event $\mathrm{rk}_4(\mathrm{C}_{-D})=\mathrm{rk}_4(\mathrm{C}_D)-1$ happens. The theory of moments, *via* Theorem 2 is strong enough to deduce the frequency of such an event.

2.1. **From Theorem 2 to Theorem 1.** The structure of the proof is the same as the proof of [9, Theorem 2, see §2.2]. We shall restrict to the case $(a,q)=(1,4)$. The other cases $(a,q)=(0,8)$ and $(a,q)=(4,8)$ of (15) are exactly similar. To obtain the equalities (10) & (11), it suffices to sum the equalities corresponding to these three cases.

For $r$, $s$ integers $\geq 0$ and for $X\geq 5$ define the densities

$$\delta(r,s,X):=\frac{\sharp\big\{D\,;\,0<-D<X,\,D\equiv 1 \bmod 4,\mathrm{rk}_4(\mathrm{C}_D)=r,\mathrm{rk}_4(\mathrm{C}_{-D})=s\big\}}{\mathcal{D}^-(X,1,4)}.$$

Theorem A (Damey–Payan's Theorem) is equivalent to the following equality

$$\delta(r,s,X)=0 \text{ for } X>5 \text{ and for } s<r-1 \text{ or } s>r. \tag{18}$$

Corollary C and (18) imply the equality

$$\lim_{X\to\infty}\big(\delta(r,r,X)+\delta(r,r-1,X)\big)=2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2}. \tag{19}$$

From Theorem 2 we deduce Theorem 1 as follows.

*Proof.* Dividing by $\mathcal{D}^-(X,1,4)$, we write Theorem 2 in the weaker form

$$\lim_{X\to\infty}\sum_{r=0}^{\infty}\big(\delta(r,r,X)2^{(k+1)r}+\delta(r,r-1,X)2^{(k+1)r-1}\big)=\frac{\mathbf{N}(k+1,2)+\mathbf{N}(k,2)}{2},$$

for $k=0,\,1,\dots$. In an equivalent form we write this equality as

$$\sum_{r=0}^{\infty}\xi(r,X)\,2^{(k+1)r}=\big(\mathbf{N}(k+1,2)+\mathbf{N}(k,2)\big)+o_k(1), \tag{20}$$

for any $k\geq 0$ and $X\to\infty$. We have introduced

$$\xi(r,X):=2\delta(r,r,X)+\delta(r,r-1,X).$$

The function $\xi(r,X)$ takes its values between 0 and 2. Applying positivity to (20) we obtain

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

which leads to

$$0\leq\xi(r,X)=O_k\big(2^{-(k+1)r}\big), \tag{21}$$

uniformly for $X\geq 5$ and $r\geq 0$. By an infinite diagonal process, we build an infinite sequence of integers $\mathcal{M}$ and a sequence $(\xi_r)_{r\geq 0}$ of real numbers in $[0,2]$ such that

$$\lim_{\substack{m\to\infty\\ m\in\mathcal{M}}}\xi(r,m)=\xi_r,$$

for all $r\geq 0$. The relation (21) allows us to apply Lebesgue's dominated convergence theorem to (20), in order to deduce the equalities

$$\sum_{r=0}^{\infty}\xi_r\;2^{(k+1)r}=\mathbf{N}(k+1,2)+\mathbf{N}(k,2)\text{ for any }k\geq 0. \tag{22}$$

The equations (22) appear to be an infinite linear system in the positive unknowns $\xi_r$. The study of this system is divided in several steps.

**Lemma 1.** *The infinite linear system has at most one solution $(\xi_r)_{r\geq 0}$ in positive $\xi_r$.*

*Proof.* The system (22) is equivalent to the following system

$$\sum_{r=0}^{\infty}\xi'_r\,2^{k\,r}=C_k\;(k\geq 0), \tag{23}$$

with the new unknowns $\xi'_r=2^r\xi_r$ and $C_k=\mathbf{N}(k+1,2)+\mathbf{N}(k,2)$. The system (23) has the shape of the system studied in [8, §4.2]. By the explicit formula for $\mathbf{N}(k,2)$ (e.g. see [8, Lemma 1]), we see that $C_k$ satisfies

$$C_k\ll 2^{\frac{(k+1)^2}{4}}+2^{\frac{k^2}{4}}\ll 2^{\frac{k^2}{2}}.$$

We are exactly in the conditions of the application of [8, Prop. 3], the proof of which is based on Jensen's formula. Hence (23) has at most one solution in positive $\xi'_r$. From this we deduce that the system (22) has at most one solution in positive $\xi_r$. □

The second step is

**Lemma 2.** *The values*

$$\xi_r = (1+2^{-r})\,2^{-r^2}\,\eta_\infty(2)\,\eta_r^{-2}(2) \quad (r \geq 0)$$

*are a solution of the infinite linear system (22).*

*Proof.* By a proof based on formulas around the theory of partitions, we know [8, Prop.2] that the real numbers

$$y_r = 2^{-r^2}\eta_\infty(2)\eta_r^{-2}(2) \quad (r \geq 0),$$

satisfy the linear equations

$$\sum_{r=0}^{\infty} y_r\, 2^{k\,r} = \mathbf{N}(k,2),$$

for any integer $k \geq 0$. (This result was used to deduce Corollary C from Theorem D, see [7]). Applying this result twice, with a change of variable $k+1 \mapsto k$ and using linearity, we see that $y_r + 2^{-r}y_r$ is solution of (22). □

Now putting Lemmas 1 & 2 together, we deduce that the system (22) has only one solution in positive $(\xi_r)$ given by Lemma 2. This also implies that, for each $r$, the sequence $\xi(r,X)$ has only one limit point when $X \to \infty$. In other words, we know that

$$\lim_{X\to\infty}\big(2\delta(r,r,X)+\delta(r,r-1,X)\big) = (1+2^{-r})\,2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2}. \tag{24}$$

Putting together the relations (19) and (24), we deduce that each of the quantities $\delta(r,r,X)$ and $\delta(r,r-1,X)$ have limits when $X$ tends to $\infty$. These limits respectively have values $2^{-r}\,2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2}$ and $(1-2^{-r})\,2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2}$. This is exactly what is claimed in Theorem 1. □

2.2. **Possible extensions.** Due to its flexibility, the method presented in this paper may have several extensions. The first one is to rather count the positive discriminants when summing the moments, that is to evaluate

$$S^+(X,k,a,q) := \sum_{\substack{0<D<X\\ D\equiv a \bmod q}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}\cdot 2^{\mathrm{rk}_4(\mathrm{C}_{-D})}, \quad \text{for } (a,q) \text{ satisfying (15).} \tag{25}$$

This possibility was already mentioned at the end of §1.3. We could even restrict the summation in (25) to special discriminants $D$, which means that no prime $p \equiv 3 \bmod 4$ divides $D$ (see [9], for a study of the distribution law of the function $\mathrm{rk}_4(\mathrm{C}_D)$ on that set of discriminants with applications to the real quadratic fields, with a fundamental unit with norm $-1$). The interest of these two possible extensions will rely on the combinatorial question, which would lead to constant certainly different from the constant $(\mathbf{N}(k+1,2)+\mathbf{N}(k,2))/2$, appearing in Theorem 2.

## 3. Strategy of the proof of Theorem 2

Almost all of the tools required for the proof of this theorem are already in [7], since the problem has many similarities with one of the problems solved in that paper, namely to prove Theorem D.

The starting point is a formula for $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ in terms of sums of product of Jacobi symbols over divisors of $D$. When $D<0$ is $\equiv 1 \bmod 4$, we have

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

(see [7, Formula (20)]). Of course there are similar formulas where $D$ is positive or even, they are more complicated, because of the influence of the integers $-1$ and 2 (see [7, Formulas (77), (107), (111), (119) & (129)]).

In order to study the moment of order $k$ of $2^{\mathrm{rk}_4(\mathrm{C}_D)}$, it is necessary to raise (26) to the $k$–th power. Then the number of variables becomes $4^k$. To skirt round this technical difficulty, we exploit an idea introduced by Heath–Brown in [12]: take the indices in $\mathbb{F}_2^{2k}$ and use polynomials of degree two over $\mathbb{F}_2$ to detect which Jacobi symbols appear and which do not appear in the expansion of $2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}$. This idea was already exploited in [7]. Then we arrive at Lemmata 4, 14 or 19 below, according to the congruence of $D$ mod 8.

We multiply the expression by $2^{\mathrm{rk}_4(\mathrm{C}_{-D})}$ in terms of a quadruple sum, to finally arrive at an expression of $S^-_{\mathrm{mix}}(X,k,a,q)$ as a sum of dimension $4^{k+1}$, over variables $D_{\mathbf{w}}$, with $\mathbf{w}\in\mathbb{F}_2^{2(k+1)}$ (see Lemma 6, 16 & 21). We concentrate more on the case $D\equiv 1 \bmod 4$. Then the $D_{\mathbf{w}}$ are odd squarefree variables which satisfy the inequality $\prod_{\mathbf{w}\in\mathbb{F}_2^{2(k+1)}} D_{\mathbf{w}} \le X$. The Jacobi symbols appear in this expression of $S^-_{\mathrm{mix}}(X,k,a,q)$ in the form $\left(\frac{D_{\mathbf{w}}}{D_{\mathbf{w}'}}\right)^{\Phi_{k+1}(\mathbf{w};\mathbf{w}')}$, where $\Phi_{k+1}$ is some polynomial defined over $\mathbb{F}_2$. This expression has much to do with $S^-(X,k+1,1,4)$ defined in (14) and thoroughly studied in [7, §5]. In particular, analytic methods will take advantage of the oscillations of the character $\left(\frac{D_{\mathbf{w}}}{D_{\mathbf{w}'}}\right)$, provided $D_{\mathbf{w}}$ and $D_{\mathbf{w}'}$ satisfy some inequalities. But the question is to be sure that we effectively meet such a character, in other words, such a study has a meaning only if the indices $\mathbf{w}$ and $\mathbf{w}'$ satisfy the equality $\Phi_{k+1}(\mathbf{w};\mathbf{w}')+\Phi_{k+1}(\mathbf{w}';\mathbf{w})=1$. In that case, we follow an idea introduced in [12] and we say that these indices are *linked* (see the definition given in (31)). Then a combinatorial study proves that the main term can only come from the contribution from sets of indices $\{\mathbf{w}\}$ such that exactly $2^{k+1}$ of these form a vector space (or a translate of vector space) of unlinked indices called $\mathcal{U}$, and such that $D_{\mathbf{w}}=1$ if $\mathbf{w}\notin\mathcal{U}$. Gluing back the variables we arrive at Lemmata 7 & 13, where it remains to evaluate the coefficient of the main term. It is at that point that the proof of Theorem 2 really differs from the proof of Theorem D (for the parameter $k+1$), as done in [7]. Actually, some new cancellations appear in the coefficient of the main term. Their rôle is to testify that, oftenly, $\mathrm{rk}_4(\mathrm{C}_{-D})$ is less than $\mathrm{rk}_4(\mathrm{C}_D)$. As we said before, the analytic part of the present paper is almost the same as in [7]. It is useless to write it again. We ask the reader to refer to this paper, we have even chosen the same notations as far as possible.

3.1. **Conventions.** Before embarking the proof, we make the following conventions, which will apply for §4, 5 & 6, and we recall some easy facts. We have tried to follow the notations of [7], which were much inspired by [12]. We frequently introduced a subscript $_{\mathrm{mod}}$ under some symbols to mean that we have modified the definition of this symbol by comparison with [7].

First of all, some conventions in set theory:

• If $S$ and $T$ are two sets, we put $S\Delta T := (S \cup T) \setminus (S \cap T)$.
• If $S$ is a set, we denote by $\mathcal{P}(S)$, $\mathcal{P}^{\mathrm{odd}}(S)$ and $\mathcal{P}^{\mathrm{even}}(S)$ the set of all subsets of $S$, the set of all subsets of $S$ with odd cardinality and the set of all subsets of $S$ with even cardinality, respectively.
• Let $\ell \geq 1$ be an integer. If $A$ is a subset of $\mathbb{F}_2^\ell$, we denote by $\sigma(A)$ the sum of its elements. Hence $\sigma(A)$ belongs to $\mathbb{F}_2^\ell$. Note the equality $\sigma(A\Delta B) = \sigma(A) + \sigma(B)$ for all $A$ and $B \subset \mathbb{F}_2^\ell$.

Here are our definitions and conventions for geometry in characteristic 2:

• $k \geq 0$, will be an integer,
• $\mathbf{u} = (u_1, u_2, \dots, u_{2k})$ and $\mathbf{v} = (v_1, v_2, \dots, v_{2k})$ will be elements of $\mathbb{F}_2^{2k}$,
• $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$ and $\boldsymbol{\beta} = (\beta_1, \beta_2)$ will be elements of $\mathbb{F}_2^2$. Hence $(\mathbf{u}, \boldsymbol{\alpha})$ and $(\mathbf{v}, \boldsymbol{\beta})$ will be viewed as elements of $\mathbb{F}_2^{2(k+1)}$.
• $\mathbf{w} = (w_1, \dots, w_{2k+2})$, $\mathbf{w}' = (w'_1, \dots, w'_{2k+2})$ and $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_{2k+2})$ will be elements of $\mathbb{F}_2^{2(k+1)}$. In that vector space, an important point of our study will be $\boldsymbol{\rho} = (0, 1, \cdots, 0, 1)$.
• $\mathcal{C} := \{\vec{e}_1, \dots, \vec{e}_{2k+2}\}$ is the canonical base of $\mathbb{F}_2^{2(k+1)}$.
• For $0 \leq \ell \leq k$, define the new vectors $\vec{b}_{2\ell+1} = \vec{e}_{2\ell+1} + \vec{e}_{2\ell+2}$ and $\vec{b}_{2\ell+2} = \vec{e}_{2\ell+2}$ to introduce another basis of $\mathbb{F}_2^{2(k+1)}$ defined by $\mathcal{B} := \{\vec{b}_1, \dots, \vec{b}_{2k+2}\}$. Let $X$ (resp. $Y$) the subspace generated by the vectors $\vec{b}_1, \vec{b}_3, \dots, \vec{b}_{2k+1}$ (resp. $\vec{b}_2, \vec{b}_4, \dots, \vec{b}_{2k+2}$). The decomposition in direct sum $\mathbb{F}_2^{2(k+1)} = X \oplus Y$ defines the projection $\pi_X$ (resp. $\pi_Y$) on $X$, parallel to $Y$ (resp. on $Y$, parallel to $X$).
• We modify the $\vec{b}_j$ as follows: we put $\vec{b}'_j = \vec{b}_j$ for $1 \leq j \leq 2k$, $\vec{b}'_{2k+1} = \vec{b}_{2k+2}$ and $\vec{b}'_{2k+2} = \vec{b}_{2k+1}$. Then we define the modified basis $\mathcal{B}_{\mathrm{mod}} = \{\vec{b}'_1, \dots, \vec{b}'_{2k+2}\}$, the subspaces $X_{\mathrm{mod}}$ and $Y_{\mathrm{mod}}$ are respectively generated by $\vec{b}'_1, \vec{b}'_3, \dots, \vec{b}'_{2k+1}$ and $\vec{b}'_2, \vec{b}'_4, \dots, \vec{b}'_{2k+2}$. Then we define the projections $\pi_{X_{\mathrm{mod}}}$ and $\pi_{Y_{\mathrm{mod}}}$ as before.
• $\mathcal{H}$ is the hyperplane of $\mathbb{F}_2^{2(k+1)}$ defined by the equation $w_{2k+1} + w_{2k+2} = 0$ (in the basis $\mathcal{C}$).
• $\Phi_k$ is the polynomial in $4k$ variables over $\mathbb{F}_2$ defined by (see [7, Formula (27)]):

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

Similarly, we have

$$\Phi_{k+1}((\mathbf{u}, \boldsymbol{\alpha}); (\mathbf{v}, \boldsymbol{\beta})) = (u_1 + v_1)(u_1 + v_2) + \cdots + (u_{2k-1} + v_{2k-1})(u_{2k-1} + v_{2k}) + (\alpha_1 + \beta_1)(\alpha_1 + \beta_2).$$

• For $\mathcal{E} \subset \{1, \dots, k\}$ and $\mathbf{u} \in \mathbb{F}_2^{2k}$, we put

$$V_{\mathcal{E}}(\mathbf{u}) = \sum_{\ell \in \mathcal{E}} (u_{2\ell-1} + u_{2\ell} + 1).$$

By extension, for $(\mathbf{u}, \boldsymbol{\alpha}) \in \mathbb{F}_2^{2(k+1)}$, we also put

$$V_{\mathcal{E}}((\mathbf{u}, \boldsymbol{\alpha})) = \sum_{\ell \in \mathcal{E}} (u_{2\ell-1} + u_{2\ell} + 1).$$

• $A$ is the polynomial over $\mathbb{F}_2^{2(k+1)}$ defined by

$$A((\mathbf{u}, \boldsymbol{\alpha})) = \alpha_1 \alpha_2,$$

or equivalently by

$$A(\mathbf{w}) = w_{2k+1}w_{2k+2}.$$

• $B$ is the polynomial over $\mathbb{F}_2^{2(k+1)}$ defined by

$$B((\mathbf{u},\boldsymbol{\alpha})) = (\alpha_1+1)(\alpha_2+1),$$

or equivalently by

$$B(\mathbf{w}) = (w_{2k+1}+1)(w_{2k+2}+1).$$

• $\lambda_k$ is the second degree polynomial over $\mathbb{F}_2^{2k}$ defined by (see [7, Formula (79)])

$$\lambda_k(\mathbf{u}) = u_1u_2 + \cdots + u_{2k-1}u_{2k}.$$

• $\lambda_{k+1}$ is similarly defined, but on $\mathbb{F}_2^{2(k+1)}$.

• For $\mathbf{w}$ and $\mathbf{w}' \in \mathbb{F}_2^{2(k+1)}$, we define the bilinear form $L$ (see [7, Formula (60)])

$$L(\mathbf{w},\mathbf{w}') = \sum_{j=0}^{k} w_{2j+1}(w'_{2j+1} + w'_{2j+2}), \tag{27}$$

and its modification $L_{\mathrm{mod}}$

$$L_{\mathrm{mod}}(\mathbf{w},\mathbf{w}') = \sum_{j=0}^{k-1} w_{2j+1}(w'_{2j+1} + w'_{2j+2}) + (w_{2k+1}+w_{2k+2})w'_{2k+1}. \tag{28}$$

Let $\Lambda$ be the linear form (see [7, p. 484])

$$\Lambda(\mathbf{w}) = \sum_{j=0}^{k} w_{2j+1}.$$

We will use the following relations between these functions

$$\Phi_{k+1}(\mathbf{w};\mathbf{w}') = L(\mathbf{w}+\mathbf{w}',\mathbf{w}') + \Lambda(\mathbf{w}+\mathbf{w}'), \tag{29}$$

and

$$L_{\mathrm{mod}}(\mathbf{w},\mathbf{w}') = L(\mathbf{w},\mathbf{w}') + A(\mathbf{w}) + A(\mathbf{w}') + A(\mathbf{w}+\mathbf{w}'). \tag{30}$$

• $\mathbf{w}$ and $\mathbf{w}'$ are said to be *unlinked* if and only if they satisfy

$$\Phi_{k+1}(\mathbf{w};\mathbf{w}') + \Phi_{k+1}(\mathbf{w}';\mathbf{w}) = 0.$$

Otherwise, $\mathbf{w}$ and $\mathbf{w}'$ are said to be *linked*.

• $\mathcal{U} \subset \mathbb{F}_2^{2(k+1)}$ is said to be an *unlinked subset* (for $\Phi_{k+1}$), if for any $\mathbf{w}$ and $\mathbf{w}' \in \mathcal{U}$, we have

$$\Phi_{k+1}(\mathbf{w};\mathbf{w}') + \Phi_{k+1}(\mathbf{w}';\mathbf{w}) = 0. \tag{31}$$

By (29) this condition is equivalent to

$$L(\mathbf{w}+\mathbf{w}',\mathbf{w}+\mathbf{w}') = 0. \tag{32}$$

and also equivalent to

$$L_{\mathrm{mod}}(\mathbf{w}+\mathbf{w}',\mathbf{w}+\mathbf{w}') = 0. \tag{33}$$

Any translate of an unlinked subset is also unlinked. We say that $\mathcal{U}$ is *maximal unlinked* when it is maximal for the inclusion. In that case, its cardinality is $2^{k+1}$ and $\mathcal{U}$ is the translate of some unlinked vector subspace $\mathcal{U}_0$ of dimension $k+1$ (For the proof, see [7, Lemma 18]).

• A vector subspace $\mathcal{V}$ of $\mathbb{F}_2^{2(k+1)}$ is said to be *good* for $L$ (resp. for $L_{\mathrm{mod}}$), if it has dimension $k+1$ and if the restriction to $\mathcal{V}\times\mathcal{V}$ of the bilinear form $L$ (resp.

$L_{\mathrm{mod}}$) is identically equal to zero. A direct consequence of (31), (32) & (33) is the following implication:

(34) $\mathcal{V}$ is a good vector subspace for $L$ or $L_{\mathrm{mod}} \Rightarrow \mathcal{V}$ is maximal unlinked.

Finally, some facts concerning counting of vector subspaces in characteristic $p$:
• $\mathfrak{n}(k,\ell,p)$ is the number of vector subspaces of $\mathbb{F}_p^k$ of dimension $\ell$. We recall some identities (see [7, Lemma 3])

$$\sum_{\ell=0}^{k} p^{\ell}\,\mathfrak{n}(k,\ell,p) = \mathbf{N}(k+1,p) - \mathbf{N}(k,p)\ (k\geq 0), \tag{35}$$

and

$$\mathbf{N}(k+1,p) = 2\,\mathbf{N}(k,p) + (p^k-1)\,\mathbf{N}(k-1,p)\ (k\geq 1). \tag{36}$$

3.2. **Counting good vector subspaces.** As in [7], the factor $\mathbf{N}(k,2)$ appearing in the formula of Theorem 2 has its origin in the counting of some good vector subspaces. The following lemma gathers all that we shall require in this counting process. It is only an extension of [7, Lemma 26].

**Lemma 3.** *Let $k\geq 0$.*
*(i) There is a one–to–one correspondence between vector subspaces $\mathcal{U}_0$ of $\mathbb{F}_2^{2(k+1)}$, good for $L$, and vector subspaces of $X$. More precisely, if $F$ is a vector subspace of $X$, there is only one good vector subspace $\mathcal{U}_0$ of $L$ such that $\pi_X(\mathcal{U}_0)=F$. It is given by*

$$\mathcal{U}_0 = F\oplus F^{\perp}, \tag{37}$$

*where $F^{\perp} := \{\vec{y}\in Y\,;\, L(\vec{x},\vec{y})=0 \text{ for all } \vec{x}\in F\}$.*
*(ii) A similar statement holds for vector subspaces $F'$ of $Y$.*
*(iii) Similar statements are also true for the subspaces $\mathcal{U}_0$ good for $L_{\mathrm{mod}}$, with the modification that we replace the vector subspaces $X$ and $Y$ by $X_{\mathrm{mod}}$ and $Y_{\mathrm{mod}}$, respectively.*
*(iv) In $\mathbb{F}_2^{2(k+1)}$ there are $\mathbf{N}(k+1,2)$ vector subspaces good for $L$ and $\mathbf{N}(k+1,2)$ vector subspaces good for $L_{\mathrm{mod}}$.*

*Proof. (i)* Let $F=\pi_X(\mathcal{U}_0)$. Decompose each element $\mathbf{w}$ and $\mathbf{w}'\in\mathcal{U}_0$ in the form $\mathbf{w}=\mathbf{w}_X+\mathbf{w}_Y$ and $\mathbf{w}'=\mathbf{w}'_X+\mathbf{w}'_Y$ according to the direct sum $\mathbb{F}_2^{2(k+1)}=X\oplus Y$. Since $\mathcal{U}_0$ is good for $L$, we obtain the equalities $L(\mathbf{w}_X,\mathbf{w}'_Y)=L(\mathbf{w}'_X,\mathbf{w}_Y)=0$, this is an easy consequence of the fact that, in $\mathcal{B}$, $L(\mathbf{w},\mathbf{w}')=x_1x'_2+\cdots+x_{2k+1}x'_{2k+2}$, if $(x_i)$ and $(x'_i)$ are the coordinates of $\mathbf{w}$ and $\mathbf{w}'$ in this basis. This expression shows also that $\dim F^{\perp}=k+1-\dim F$. Hence, since $\mathbf{w}_X$ belongs to $F$, $\mathbf{w}_Y$ belongs to the vector subspace $F^{\perp}$ of dimension at most $k+1-\dim F$. Since we impose to $\mathcal{U}_0$ to have its dimension equal to $k+1$, necessarily we have $\pi_Y(\mathcal{U}_0)=F^{\perp}$. This gives (37).

*(ii)* This item is evident.

*(iii)* It is sufficient to notice that, $L_{\mathrm{mod}}(\mathbf{w},\mathbf{w}')=x_1x'_2+\cdots+x_{2k+1}x'_{2k+2}$, if $(x_i)$ and $(x'_i)$ are now the coordinates of $\mathbf{w}$ and $\mathbf{w}'$ in the basis $\mathcal{B}_{\mathrm{mod}}$.

*(iv)* This is a direct consequence of the bijection with the vector subspaces of $X$ or of $X_{\mathrm{mod}}$ which are both of dimension $k+1$. □

## 4. Proof of Theorem 2. The case of odd negative $D$

4.1. **Beginning of the proof.** In this section we deal with the sum $S^-_{\rm mix}(X,k,1,4)$ introduced in (17). If $D$ is a negative fundamental discriminant $\equiv 1 \bmod 4$, then $-4D$ is the fundamental discriminant of the associated field $\mathbb{Q}(\sqrt{-D})$. To transform the first term $2^{k\,{\rm rk}_4({\rm C}_D)}$, we appeal to

**Lemma 4.** *For any $k \geq 0$ and for every odd negative fundamental discriminant $D$ we have the equality*

$$2^{k\,{\rm rk}_4({\rm C}_D)} = \frac{1}{2^k \cdot 2^{k\,\omega(-D)}} \sum_{(D_{\mathbf{u}})_{\mathbf{u}\in\mathbb{F}_2^{2k}}} \prod_{\mathbf{u}} \prod_{\mathbf{v}} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\right)^{\Phi_k(\mathbf{u};\mathbf{v})},$$

*where the sum is over all the $2^{2k}$–tuples $(D_{\mathbf{u}})$ such that*

$$\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} D_{\mathbf{u}} = -D. \tag{38}$$

*Proof.* See [7, Formula (25)]. □

To deal with the other factor $2^{{\rm rk}_4({\rm C}_{-D})} = 2^{{\rm rk}_4({\rm C}_{-4D})}$, we use the following formula

**Lemma 5.** *For any positive fundamental discriminant $D$ congruent to $4 \bmod 8$, we have the equality*

(39)

$$2^{{\rm rk}_4({\rm C}_D)} = \frac{1}{2\cdot 2^{\omega(D/4)}} \sum_{(D_{\boldsymbol{\alpha}})} \Big[\prod_{\boldsymbol{\alpha}} \prod_{\boldsymbol{\beta}} \left(\frac{D_{\boldsymbol{\alpha}}}{D_{\boldsymbol{\beta}}}\right)^{(\alpha_1+\beta_1)(\alpha_1+\beta_2)}\Big] \cdot \Big[\prod_{\boldsymbol{\alpha}} \left(\frac{-1}{D_{\boldsymbol{\alpha}}}\right)^{\alpha_1\alpha_2}\Big] \times \Big[1+\prod_{\boldsymbol{\alpha}} \left(\frac{2}{D_{\boldsymbol{\alpha}}}\right)^{\alpha_1+\alpha_2+1}\Big],$$

*where the first sum, is over the 4–tuples $(D_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\mathbb{F}_2^2}$ such that*

$$\prod_{\boldsymbol{\alpha}} D_{\boldsymbol{\alpha}} = D/4. \tag{40}$$

*Proof.* See [7, Formula (129)]. □

We apply Lemma 4 for $D \equiv 1 \bmod 4$ and $D<0$ and Lemma 5 to the value $-4D$. We are led to simultaneously solve (38) and (40), in other words

$$\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} D_{\mathbf{u}} = \prod_{\boldsymbol{\alpha}\in\mathbb{F}_2^2} D_{\boldsymbol{\alpha}} = -D.$$

Let $D_{\mathbf{u},\boldsymbol{\alpha}} = {\rm g.c.d.}(D_{\mathbf{u}}, D_{\boldsymbol{\alpha}})$. Then we have $D_{\mathbf{u}} = \prod_{\boldsymbol{\alpha}} D_{\mathbf{u},\boldsymbol{\alpha}}$ and $D_{\boldsymbol{\alpha}} = \prod_{\mathbf{u}} D_{\mathbf{u},\boldsymbol{\alpha}}$. Using the multiplicative properties of the Jacobi symbols we deduce the following equality which is true for any negative $D \equiv 1 \bmod 4$:

(41)

$$2^{k\,{\rm rk}_4({\rm C}_D)}.2^{{\rm rk}_4({\rm C}_{-D})} = \frac{1}{2^{k+1}\cdot 2^{(k+1)\omega(-D)}} \sum_{(D_{\mathbf{u},\boldsymbol{\alpha}})} \left[\prod_{\mathbf{u},\boldsymbol{\alpha}} \prod_{\mathbf{v},\boldsymbol{\beta}} \left(\frac{D_{\mathbf{u},\boldsymbol{\alpha}}}{D_{\mathbf{v},\boldsymbol{\beta}}}\right)^{\Phi_{k+1}\left((\mathbf{u},\boldsymbol{\alpha});(\mathbf{v},\boldsymbol{\beta})\right)}\right] \times \left[\prod_{\mathbf{u},\boldsymbol{\alpha}} \left(\frac{-1}{D_{\mathbf{u},\boldsymbol{\alpha}}}\right)^{A((\mathbf{u},\boldsymbol{\alpha}))}\right] \times \left[1+\prod_{\mathbf{u},\boldsymbol{\alpha}} \left(\frac{2}{D_{\mathbf{u},\boldsymbol{\alpha}}}\right)^{(A+B)((\mathbf{u},\boldsymbol{\alpha}))}\right],$$

where the sum is over all the $4^{k+1}$–tuples $(D_{\mathbf{u},\boldsymbol{\alpha}})$ satisfying

$$\prod_{\mathbf{u},\boldsymbol{\alpha}} D_{\mathbf{u},\boldsymbol{\alpha}} = -D.$$

Summing (41) over the set of $D \equiv 1 \bmod 4$ satisfying $0 < -D < X$, and replacing the variables of summation $(\mathbf{u}, \alpha)$ and $(\mathbf{v}, \beta)$ by $\mathbf{w}$ and $\mathbf{w}'$ ($\in \mathbb{F}_2^{2(k+1)}$), resp., we get:

**Lemma 6.** *For every $k \geq 0$ and every $X \geq 2$ we have the equality*

$$S^-_{\mathrm{mix}}(X,k,1,4) = \frac{1}{2^{k+1}} \sum_{(D_{\mathbf{w}})} \Big[\prod_{\mathbf{w}} 2^{-(k+1)\omega(D_{\mathbf{w}})}\Big] \times \Big[\prod_{\mathbf{w}} \prod_{\mathbf{w}'} \Big(\frac{D_{\mathbf{w}}}{D_{\mathbf{w}'}}\Big)^{\Phi_{k+1}(\mathbf{w};\mathbf{w}')}\Big] \times \Big[\prod_{\mathbf{w}} \Big(\frac{-1}{D_{\mathbf{w}}}\Big)^{A(\mathbf{w})}\Big] \times \Big[1 + \prod_{\mathbf{w}} \Big(\frac{2}{D_{\mathbf{w}}}\Big)^{(A+B)(\mathbf{w})}\Big] \tag{42}$$

*where the sum is over all the $4^{k+1}$–tuples $(D_{\mathbf{w}})$ of coprime, squarefree and positive integers satisfying*

$$\prod_{\mathbf{w}} D_{\mathbf{w}} \leq X \text{ and } \prod_{\mathbf{w}} D_{\mathbf{w}} \equiv 3 \bmod 4.$$

Note that in (42), the $D_{\mathbf{w}}$ are not necessarily fundamental discriminants. We decompose $S^-_{\mathrm{mix}}(X,k,1,4)$ into two terms

$$S^-_{\mathrm{mix}}(X,k,1,4) = \Sigma_1(X) + \Sigma_2(X), \tag{43}$$

where $\Sigma_1(X)$ and $\Sigma_2(X)$, resp. correspond to the contributions of the terms 1 and $\prod_{\mathbf{w}} \Big(\frac{2}{D_{\mathbf{w}}}\Big)^{(A+B)(\mathbf{w})}$ contained in the term $\Big[1 + \prod_{\mathbf{w}} \Big(\frac{2}{D_{\mathbf{w}}}\Big)^{(A+B)(\mathbf{w})}\Big]$ appearing in the right part of (42).

4.2. **Study of $\Sigma_1(X)$.** The beginning of the proof is the same as in [7, Lemma 28 & Prop. 6]. We introduce the following notation: for $\nu = 0$ or $1 \bmod 2$ and $\mathcal{U}$ a maximal unlinked subset in $\mathbb{F}_2^{2(k+1)}$, let

$$\gamma^+(\mathcal{U},\nu) := \sum_{(h_{\mathbf{w}})} \Big[\prod_{\mathbf{w}\in\mathcal{U}} (-1)^{A(\mathbf{w})\cdot\frac{h_{\mathbf{w}}-1}{2}}\Big] \times \Big[\prod_{\substack{\mathbf{w}\in\mathcal{U}\\ \mathbf{w}'\in\mathcal{U}}} (-1)^{\Phi_{k+1}(\mathbf{w};\mathbf{w}')\cdot\frac{h_{\mathbf{w}}-1}{2}\cdot\frac{h_{\mathbf{w}'}-1}{2}}\Big]. \tag{44}$$

In (44) the sum is over $(h_{\mathbf{w}})_{\mathbf{w}\in\mathcal{U}} \in \{\pm 1 \bmod 4\}^{2^{k+1}}$, satisfying

$$\prod_{\mathbf{w}\in\mathcal{U}} h_{\mathbf{w}} \equiv (-1)^{\nu} \bmod 4. \tag{45}$$

We follow the proof leading to [7, Prop. 6]. The only differences are the substitutions $k \mapsto k+1$, $\lambda_k \mapsto A$ and $\nu = 0 \mapsto \nu = 1$ in (45). Finally, we arrive at

**Lemma 7.** *For every $k \geq 0$ and every $\epsilon > 0$ we have uniformly for $X \geq 2$ the equality*

$$\Sigma_1(X) = \frac{2^{2-(k+1)-2^{k+1}}}{\pi^2} \cdot \Big(\sum_{\mathcal{U}} \gamma^+(\mathcal{U},1)\Big) \cdot X + O_\epsilon\big(X(\log X)^{-2^{-k-1}+\epsilon}\big),$$

*where the sum is over all the maximal unlinked subsets $\mathcal{U} \subset \mathbb{F}_2^{2(k+1)}$.*

Using (16), we write Lemma 7 in the equivalent form

$$\Sigma_1(X) = 2^{-k-2^{k+1}} \cdot \Gamma_1 \cdot \mathcal{D}^-(X,1,4) + O_\epsilon\big(X(\log X)^{-2^{-k-1}+\epsilon}\big), \tag{46}$$

with

$$\Gamma_1 = \sum_{\mathcal{U}} \gamma^+(\mathcal{U},1). \tag{47}$$

4.2.1. *Study of the main coefficient $\Gamma_1$. Preliminary steps.* We are now concerned by the study of $\Gamma_1$. Let $\mathcal{U}$ be a maximal unlinked subset of $\mathbb{F}_2^{2(k+1)}$, let $\big(h_{\mathbf{w}}\big)_{\mathbf{w}\in\mathcal{U}}$ be a family of congruence classes satisfying (45) for $\nu = 1$. Let $S$ be the subset of $\mathcal{U}$ consisting of the indices $\mathbf{w} \in \mathcal{U}$ such that $h_{\mathbf{w}} \equiv 3 \bmod 4$. By (45), we know that $S$ has odd cardinality. Inverting the summations, we can write (44) in the form

$$\gamma^+(\mathcal{U},1) = \sum_{\substack{S\subset\mathcal{U}\\ \sharp S \text{ odd}}} (-1)^{e^+_{\mathrm{mod}}(S)},$$

where

$$e^+_{\mathrm{mod}}(S) = \sum_{\mathbf{w}\in S} A(\mathbf{w}) + \sum_{\substack{\mathbf{w}\in S\\ \mathbf{w}'\in S}} \Phi_{k+1}\big(\mathbf{w};\mathbf{w}'\big), \tag{48}$$

where the double sum is made over unordered pairs of elements of $S$.

The study of $\gamma^+(\mathcal{U},1)$ will mimic the study made in [7, §6.1]. Later on, we shall require results on $\gamma^+(\mathcal{U},0)$. It is natural to generalize our study by considering for $\nu = 0$ or $1 \bmod 2$ the equality

$$\gamma^+(\mathcal{U},\nu) = \sum_{\substack{S\subset\mathcal{U}\\ \sharp S \equiv \nu \bmod 2}} (-1)^{e^+_{\mathrm{mod}}(S)}, \text{ for } \nu = 0 \text{ or } 1. \tag{49}$$

Note that our function $e^+_{\mathrm{mod}}(S)$ slightly differs from the function $e^+(S)$ defined in [7, Formula (83)]. Hence the way of treating it is very similar. For $S$ and $T \subset \mathcal{U}$, we define

$$e^+_{\mathrm{mod}}(S,T) := e^+_{\mathrm{mod}}(S) + e^+_{\mathrm{mod}}(T) + e^+_{\mathrm{mod}}(S\Delta T), \tag{50}$$

and define

$$e(S) := \sum_{\substack{\mathbf{w}\in S\\ \mathbf{w}'\in S}} \Phi_{k+1}\big(\mathbf{w};\mathbf{w}'\big) \quad \big(= e^+_{\mathrm{mod}}(S) + \sum_{\mathbf{w}\in S} A(\mathbf{w})\big). \tag{51}$$

The function $e(S)$ exactly coincides with the function introduced in [7, Formula (57)], but in dimension $k+1$. Also let

$$e(S,T) := e(S) + e(T) + e(S\Delta T), \tag{52}$$

which also coincides with the function $e(S,T)$ introduced in [7, Formula (62)]. This quantity satisfies the equality

$$e(S,T) = e^+_{\mathrm{mod}}(S,T), \tag{53}$$

which is an easy consequence of the equality

$$\sum_{\mathbf{w}\in S} A(\mathbf{w}) + \sum_{\mathbf{w}\in T} A(\mathbf{w}) + \sum_{\mathbf{w}\in S\Delta T} A(\mathbf{w}) = 0.$$

Squaring (49), inverting summation and following the proof of [7, Formula (89)], we get the equality

$$\big[\gamma^+(\mathcal{U},\nu)\big]^2 = 2^{2^{k+1}-1} \sum_{T\in\mathcal{T}} (-1)^{e^+_{\mathrm{mod}}(T)+\nu\left(\Lambda(\sigma(T))+L(\sigma(T),\mathbf{c})\right)}, \tag{54}$$

where
– $\nu \in \{0, 1 \bmod 2\}$,
– $L, \Lambda$ and $\sigma$ are defined in §3.1,
– $\mathcal{T}$ is the set of subsets $T \subset \mathcal{U}$ of even cardinality such that

$$L(\sigma(T), \sigma(S_0)) = 0,$$

for every subset $S_0$ of $\mathcal{U}$ with even cardinality, (note that $\mathcal{T}$ contains the subsets $T$ of even cardinality satisfying $\sigma(T) = 0$),
– $\mathbf{c}$ is any point of $\mathbb{F}_2^{2(k+1)}$, such that $\mathcal{U} = \mathbf{c} + \mathcal{U}_0$, where $\mathcal{U}_0$ is a vector subspace. Note that $(\mathcal{T}, \Delta)$ is a commutative group.

Now we recall some facts taken from [7].

**Lemma 8.** *Let $\mathcal{U}$ be a maximal unlinked subset of $\mathbb{F}_2^{2(k+1)}$. For all subsets $S$ and $T$ of $\mathcal{U}$, we have the equalities*

$$\begin{aligned} e(S,T) &= e^+_{\mathrm{mod}}(S,T) \\ &= L\big(\sigma(S),\sigma(T)\big) + \sharp S \cdot \Big(\sum_{\mathbf{w}\in T} L(\mathbf{w},\mathbf{w})\Big) + \sharp T \cdot \Lambda\big(\sigma(S)\big) + \sharp S \cdot \Lambda\big(\sigma(T)\big). \end{aligned} \tag{55}$$

*If $\sharp S$ is even and if $\mathbf{c}$ is a point of $\mathcal{U}$, we have the equality*

$$e(\{\mathbf{c}, \mathbf{c} + \sigma(S)\}) = L(\sigma(S), \mathbf{c}) + \Lambda(\sigma(S)). \tag{56}$$

*Proof.* Combine (53) and [7, Lemma 21 & Formula (61)] to obtain the first equality. The second one is [7, Formula (72)]. □

Lemma 8 implies that $e^+_{\mathrm{mod}}(T, T') = 0$ for every $T$ and $T' \in \mathcal{T}$. This equality combined with (52) implies the equality $e^+_{\mathrm{mod}}(T\Delta T') = e^+_{\mathrm{mod}}(T) + e^+_{\mathrm{mod}}(T')$ (for all $T$ and $T' \in \mathcal{T}$), from which we deduce the fact that the application

$$T \mapsto (-1)^{e^+_{\mathrm{mod}}(T)+\nu\left(\Lambda(\sigma(T))+L(\sigma(T),\mathbf{c})\right)},$$

is a multiplicative character on $(\mathcal{T}, \Delta)$. From this property and from (54) we easily deduce

**Lemma 9.** *Let $\nu \in \{0, 1 \bmod 2\}$ and let $\mathcal{U}$ a maximal unlinked subset of $\mathbb{F}_2^{2(k+1)}$, such that $\gamma^+(\mathcal{U}, \nu) \neq 0$. Then we have*

$$e^+_{\mathrm{mod}}(T) = 0,$$

*for every subset $T$ of $\mathcal{U}$, satisfying $\sharp T$ even and $\sigma(T) = 0$.*

Lemma 9 appears to be the analogue of Lemma 29 of [7]. Now we prove an analogue of Lemma 30 of [7].

**Lemma 10.** *Let $\nu \in \{0,\ 1 \bmod 2\}$ and let $\mathcal{U}$ a maximal unlinked subset of $\mathbb{F}_2^{2(k+1)}$, such that $\gamma^+(\mathcal{U},\nu) \neq 0$. Then for any $S \subset \mathcal{U}$ we have the equality*

$$e^+_{\rm mod}(S) = A\big(\sigma(S)\big) + \big(1 + \sharp\, S\big)\Big(L_{\rm mod}(\sigma(S),\mathbf{c}) + \Lambda(\sigma(S))\Big).$$

*In that expression $\mathbf{c}$ is any point such that $\mathcal{U} = \mathbf{c}+\mathcal{U}_0$, where $\mathcal{U}_0$ is a vector subspace of $\mathbb{F}_2^{2(k+1)}$ and $L_{\rm mod}$ is defined in (28).*

*Proof.* It mimics the proof of [7, Lemma 30]. We discuss on the parity of $\sharp\, S$.

• If $\sharp\, S$ is odd, we have $\sigma(S) \in \mathcal{U}$. By Lemma 9 applied to the subset $T$ of $\mathcal{U}$ defined by $T := S\,\Delta\,\{\sigma(S)\}$ (which satisfies $\sharp\, T \equiv 0 \bmod 2$ and $\sigma(T) = 0$), we obtain

$$e^+_{\rm mod}(T) = 0. \tag{57}$$

By the definition of $T$, by equations (57) and (50) we have

$$0 = e^+_{\rm mod}(S) + e^+_{\rm mod}(\{\sigma(S)\}) + e^+_{\rm mod}(S,\{\sigma(S)\}). \tag{58}$$

The equality (55) of Lemma 8 gives the equality $e^+_{\rm mod}(S,\{\sigma(S)\}) = 0$. The definition (48) produces $e^+(\{\sigma(S)\}) = A(\sigma(S))$. Inserting these two equalities into (58), we obtain the proof of Lemma 10 in the case $2 \nmid \sharp\, S$.

• If $\sharp\, S$ is even and $\sigma(S) = 0$, Lemma 9 gives Lemma 10 in that case.

• Now suppose $\sharp\, S$ even and $\sigma(S) \neq 0$. Then $\sigma(S)$ belongs to $\mathcal{U}_0$. We consider $T = S\,\Delta\,\{\mathbf{c}, \mathbf{c}+\sigma(S)\}$. Then $T$ is a subset of $\mathcal{U}$ satisfying $\sharp\, T$ even and $\sigma(T) = 0$. By Lemma 9 we also have (57). By the choice of $T$ and by (50), we deduce from (57) the equality

$$0 = e^+_{\rm mod}(S) + e^+_{\rm mod}(\{\mathbf{c}, \mathbf{c}+\sigma(S)\}) + e^+_{\rm mod}(S,\{\mathbf{c}, \mathbf{c}+\sigma(S)\}). \tag{59}$$

By (56) of Lemma 8 and by (51) we have

$$e^+_{\rm mod}(\{\mathbf{c}, \mathbf{c}+\sigma(S)\}) = A(\mathbf{c}) + A(\mathbf{c}+\sigma(S)) + L(\sigma(S),\mathbf{c}) + \Lambda(\sigma(S)). \tag{60}$$

By (55) of Lemma 8 we obtain

$$e^+_{\rm mod}(S,\{\mathbf{c}, \mathbf{c}+\sigma(S)\}) = L(\sigma(S),\sigma(S)) = 0, \tag{61}$$

since $\sigma(S)$ and 0 both belong to the maximal unlinked subset $\mathcal{U}_0$ (see (32)).

By (59), (60) & (61), we have

$$e^+_{\rm mod}(S) = A(\mathbf{c}) + A(\mathbf{c}+\sigma(S)) + L(\sigma(S),\mathbf{c}) + \Lambda(\sigma(S))$$

To finish the proof of Lemma 10, it remains to check the equality

$$A\big(\sigma(S)\big) + L_{\rm mod}(\sigma(S),\mathbf{c}) + \Lambda(\sigma(S)) \\ = A(\mathbf{c}) + A(\mathbf{c}+\sigma(S)) + L(\sigma(S),\mathbf{c}) + \Lambda(\sigma(S)).$$

This directly follows from (30). □

Now we prove an analogue of Lemma 31 of [7].

**Lemma 11.** *Let $\nu \in \{0,\ 1 \bmod 2\}$. Let $\mathcal{U}$ be a maximal unlinked subset of $\mathbb{F}_2^{2(k+1)}$, written in the form $\mathcal{U} = \mathbf{c}+\mathcal{U}_0$, such that $\gamma^+(\mathcal{U},\nu) \neq 0$. Then $\mathcal{U}_0$ is good for $L_{\rm mod}$.*

*Proof.* Let $\sigma$ and $\tau$ be two non zero elements of $\mathcal{U}_0$. Then $S := \{\mathbf{c}, \mathbf{c}+\sigma\}$ and $T := \{\mathbf{c}, \mathbf{c}+\tau\}$ are two subsets of $\mathcal{U}$ with even cardinalities. By Lemma 10, we get the three equalities

$$\begin{aligned} e^+_{\mathrm{mod}}(S) &= A(\sigma) + L_{\mathrm{mod}}(\sigma, \mathbf{c}) + \Lambda(\sigma), \\ e^+_{\mathrm{mod}}(T) &= A(\tau) + L_{\mathrm{mod}}(\tau, \mathbf{c}) + \Lambda(\tau), \\ e^+_{\mathrm{mod}}(S\Delta T) &= A(\sigma+\tau) + L_{\mathrm{mod}}(\sigma+\tau, \mathbf{c}) + \Lambda(\sigma+\tau). \end{aligned}$$

We sum these three equalities, use linearity and the definition (50), to arrive at the equality

$$e^+_{\mathrm{mod}}(S, T) = A(\sigma) + A(\tau) + A(\sigma+\tau). \tag{62}$$

By (55) of Lemma 8, we know that $e^+(S, T) = L(\sigma, \tau)$. Combining this with (62) we get the equality

$$A(\sigma) + A(\tau) + A(\sigma+\tau) + L(\sigma, \tau) = 0.$$

Thanks to (30), we recognize $L_{\mathrm{mod}}(\sigma, \tau)$ in the right part of the above equality. This proves that the restriction to $\mathcal{U}_0 \times \mathcal{U}_0$ of $L_{\mathrm{mod}}$ is identically equal to zero. □

From Lemma 11 we deduce an analogue of [7, Lemma 32]. It is an extension of Lemma 10.

**Lemma 12.** *Let $\mathcal{U} = \mathbf{c} + \mathcal{U}_0$ be a maximal unlinked subset of $\mathbb{F}_2^{2(k+1)}$ such that $\mathcal{U}_0$ is good for $L_{\mathrm{mod}}$. Then for every $S \subset \mathcal{U}$ we have*

$$e^+_{\mathrm{mod}}(S) = A\big(\sigma(S)\big) + \big(1 + \sharp S\big)\Big(L_{\mathrm{mod}}(\sigma(S), \mathbf{c}) + \Lambda(\sigma(S))\Big). \tag{63}$$

*Proof.* We prove it by induction on $\sharp S$.
• If $S = \emptyset$, then $\sigma(S) = 0$ and the result is trivial by (48).
• If $S$ consists of exactly one element, say $\mathbf{w}$, the Definition (48) gives the equality $e^+_{\mathrm{mod}}(S) = A(\mathbf{w})$ which proves (63) in that case.
• Suppose now that $S = \{\mathbf{w}, \mathbf{w}'\}$. By Definition (48), and by the relations (29) & (30), we have in that case

$$\begin{aligned} e^+_{\mathrm{mod}}(S) &= A(\mathbf{w}) + A(\mathbf{w}') + \Phi_{k+1}(\mathbf{w}; \mathbf{w}') \\ &= A(\mathbf{w}) + A(\mathbf{w}') + L(\mathbf{w}+\mathbf{w}', \mathbf{w}') + \Lambda(\mathbf{w}+\mathbf{w}') \\ &= A(\mathbf{w}+\mathbf{w}') + L_{\mathrm{mod}}(\mathbf{w}, \mathbf{w}') + L(\mathbf{w}', \mathbf{w}') + \Lambda(\mathbf{w}+\mathbf{w}'). \end{aligned} \tag{64}$$

By (30) we have

$$L(\mathbf{w}', \mathbf{w}') = L_{\mathrm{mod}}(\mathbf{w}', \mathbf{w}'). \tag{65}$$

Since $\mathbf{w}+\mathbf{w}'$ and $\mathbf{c}+\mathbf{w}'$ belong to $\mathcal{U}_0$, which is good for $L_{\mathrm{mod}}$, we have

$$L_{\mathrm{mod}}(\mathbf{w}+\mathbf{w}', \mathbf{c}+\mathbf{w}') = 0. \tag{66}$$

Putting together (64), (65) & (66) and using linearity, we obtain the equality

$$e^+_{\mathrm{mod}}(S) = A(\mathbf{w}+\mathbf{w}') + L_{\mathrm{mod}}(\mathbf{w}+\mathbf{w}', \mathbf{c}) + \Lambda(\mathbf{w}+\mathbf{w}'),$$

which is exactly (63) in that case.

• Now suppose that $S$ contains at least three elements. Let $T$ be a subset of $S$ with exactly two elements. Let $S' = S \,\Delta\, T$. By the hypothesis of the induction, concerning (63), applied to $S'$ and $T$, we have the two equalities

$$e^+_{\rm mod}(S') = A(\sigma(S')) + (1 + \sharp\, S')\big(L_{\rm mod}(\sigma(S'), \mathbf{c}) + \Lambda(\sigma(S'))\big), \tag{67}$$

$$e^+_{\rm mod}(T) = A(\sigma(T)) + \big(L_{\rm mod}(\sigma(T), \mathbf{c}) + \Lambda(\sigma(T))\big). \tag{68}$$

By (55) of Lemma 8 we write

$$e^+_{\rm mod}(T, S') = L(\sigma(T), \sigma(S')) + \sharp\, S' \cdot \Lambda(\sigma(T)). \tag{69}$$

Combining (67), (68) & (69) with (50) then using linearity and (30), we can write

$$e^+_{\rm mod}(S) = A(\sigma(S)) + (1 + \sharp\, S)\Lambda(\sigma(S)) + \Omega(S), \tag{70}$$

where

$$\Omega(S) = (1 + \sharp\, S)\big(L_{\rm mod}(\sigma(S'), \mathbf{c})\big) + L_{\rm mod}(\sigma(T), \mathbf{c}) + L_{\rm mod}(\sigma(T), \sigma(S')).$$

Now we appeal to the fact that $\mathcal{U}_0$ is good to modify $\Omega(S)$ as follows:

– If $\sharp\, S$ is even, then $\sigma(T)$ and $\sigma(S')$ both belong to $\mathcal{U}_0$. Hence $L_{\rm mod}(\sigma(T), \sigma(S')) = 0$, and, by linearity we deduce the equality

$$\Omega(S) = (1 + \sharp\, S)\, L_{\rm mod}(\sigma(S), \mathbf{c}). \tag{71}$$

Combining this with (70) we obtain (63) in that case.

– If $\sharp\, S$ is odd, then $\sigma(T)$ and $\mathbf{c} + \sigma(S')$ both belong to $\mathcal{U}_0$. Hence $L_{\rm mod}(\sigma(T), \mathbf{c} + \sigma(S')) = 0$. This implies the equality $\Omega(S) = 0$, which means that $\Omega(S)$ also satisfies (71). We recover (63) again. □

4.2.2. *Study of the main coefficient* $\Gamma_1$. *The final step.* We are now in position to compute the coefficient $\Gamma_1$ defined in (47). Of course, in (47), we can restrict the summation to $\mathcal{U}$, such that $\gamma^+(\mathcal{U}, 1)$ is non zero. This was the purpose of Lemma 11 which, combined with (34), implies the equality

$$\Gamma_1 = \sum_{\substack{\mathcal{U}\,;\ \mathcal{U}_0 \text{ good} \\ \text{for } L_{\rm mod}}} \gamma^+(\mathcal{U}, 1) = \frac{1}{2^{k+1}} \sum_{\substack{\mathcal{U}_0 \text{ good} \\ \text{for } L_{\rm mod}}} \sum_{\mathbf{c} \in \mathbb{F}_2^{2(k+1)}} \gamma^+(\mathbf{c} + \mathcal{U}_0, 1). \tag{72}$$

Now we use (49) and Lemma 12 in order to write

$$\gamma^+(\mathbf{c} + \mathcal{U}_0, 1) = \sum_{\substack{S \subset \mathbf{c} + \mathcal{U}_0 \\ \sharp\, S \text{ odd}}} (-1)^{A(\sigma(S))}. \tag{73}$$

Note that in the expression $(-1)^{A(\sigma(S))}$, $S$ only appears by the sum of its terms. The application $S \mapsto \sigma(S)$ is a surjective morphism from $(\mathcal{P}^{\rm even}(\mathcal{U}_0), \Delta)$ onto $(\mathcal{U}_0, +)$. Hence, for every $\boldsymbol{\sigma} \in \mathcal{U}_0$, the equation

$$\sigma(S) = \boldsymbol{\sigma}, \tag{74}$$

has $2^{2^{k+1}}/(2 \cdot 2^{k+1})$ solutions in $S \in \mathcal{P}^{\rm even}(\mathcal{U}_0)$. Considering the application $S \mapsto S \,\Delta\, \{0\}$, we deduce that the equation (74) has the same number of solutions $S \in \mathcal{P}^{\rm odd}(\mathcal{U}_0)$. Using now the translation by $\mathbf{c}$, we see that the equation $\sigma(S) = \mathbf{c} + \boldsymbol{\sigma}$ has the same number of solutions in $S \in \mathcal{P}^{\rm odd}(\mathbf{c} + \mathcal{U}_0)$. This allows us to transform (73) into

$$\gamma^+(\mathbf{c} + \mathcal{U}_0, 1) = 2^{2^{k+1} - k - 2} \sum_{\boldsymbol{\sigma} \in \mathcal{U}_0} (-1)^{A(\mathbf{c} + \boldsymbol{\sigma})}. \tag{75}$$

Putting this expression into (72) and inverting summations we obtain

$$\Gamma_1 = 2^{2^{k+1}-2k-3} \sum_{\substack{\mathcal{U}_0 \text{ good} \\ \text{for } L_{\mathrm{mod}}}} \sum_{\boldsymbol{\sigma}\in\mathcal{U}_0} \sum_{\mathbf{c}\in\mathbb{F}_2^{2(k+1)}} (-1)^{A(\mathbf{c}+\boldsymbol{\sigma})}. \tag{76}$$

Let $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_{2k+2})$ and $\mathbf{c} = (c_1, \dots, c_{2k+2})$. First write the equality $(-1)^{A(\mathbf{c}+\boldsymbol{\sigma})} = (-1)^{(c_{2k+1}+\sigma_{2k+1})(c_{2k+2}+\sigma_{2k+2})}$, and check that, for any $(\sigma_{2k+1}, \sigma_{2k+2}) \in \mathbb{F}_2^2$, the following equality holds

$$\sum_{(c_{2k+1},c_{2k+2})\in\mathbb{F}_2^2} (-1)^{(c_{2k+1}+\sigma_{2k+1})(c_{2k+2}+\sigma_{2k+2})} = 2.$$

Using this remark we transform (76) into

$$\Gamma_1 = 2^{2^{k+1}-2k-3} \cdot 2^{k+1} \cdot 2^{2k} \cdot 2 \cdot \sum_{\substack{\mathcal{U}_0 \text{ good} \\ \text{for } L_{\mathrm{mod}}}} 1 = 2^{2^{k+1}+k-1} \sum_{\substack{\mathcal{U}_0 \text{ good} \\ \text{for } L_{\mathrm{mod}}}} 1. \tag{77}$$

Now we appeal to Lemma 3 *(iv)* in order to transform (77) into

$$\Gamma_1 = 2^{2^{k+1}+k-1}\, \mathbf{N}(k+1, 2). \tag{78}$$

4.3. **Study of $\Sigma_2(X)$.** This second sum is defined in (43) and the study has many similarities with $\Sigma_1(X)$. But a new phenomenon appears: the oscillations of the symbol $\left(\frac{2}{D_{\mathbf{w}}}\right)^{(A+B)(\mathbf{w})}$, if the associated exponent, *i.e.* $(A+B)(\mathbf{w})$, is non zero. To be more precise, if the congruence modulo 4 of $D_{\mathbf{w}}$ is fixed ($D_{\mathbf{w}} \equiv +1 \bmod 4$ or $D_{\mathbf{w}} \equiv -1 \bmod 4$, say), the symbol $\left(\frac{2}{D_{\mathbf{w}}}\right) = (-1)^{\frac{D_{\mathbf{w}}^2-1}{8}}$ takes the values $+1$ and $-1$ with equal frequencies, and then gives birth to an error term. This idea was exploited in the proof of [7, Proposition 7]. By the same technique, we arrive at the following analogue of Lemma 7:

**Lemma 13.** *For every $k \geq 0$ and for every $\epsilon > 0$ we have uniformly for $X \geq 2$ the equality*

$$\Sigma_2(X) = \frac{2^{2-(k+1)-2^{k+1}}}{\pi^2} \cdot \Big(\sum_{\mathcal{U}} \gamma^+(\mathcal{U}, 1)\Big) \cdot X + O_\epsilon\big(X(\log X)^{-2^{-k-1}+\epsilon}\big),$$

*where the sum is over all the maximal unlinked subsets $\mathcal{U} \subset \mathbb{F}_2^{2(k+1)}$, such that the function $(A+B)$ is identically zero on it. The function $\gamma^+$ is defined in (44).*

The analogue of (46) is the equality

$$\Sigma_2(X) = 2^{-k-2^{k+1}} \cdot \Gamma_2 \cdot \mathcal{D}^-(X, 1, 4) + O_\epsilon\big(X(\log X)^{-2^{-k-1}+\epsilon}\big) \tag{79}$$

with

$$\Gamma_2 = \sum_{\mathcal{U}} \gamma^+(\mathcal{U}, 1), \tag{80}$$

where now the sum is over all the maximal unlinked subsets $\mathcal{U}$ on which the affine function $A+B$ is zero identically. By Lemma 11 we restrict the sum to the $\mathcal{U}$ of the form $\mathcal{U} = \mathbf{c} + \mathcal{U}_0$, with $\mathcal{U}_0$ good for $L_{\mathrm{mod}}$. By the easy equality

$$(A+B)(\mathbf{w}) = w_{2k+1} + w_{2k+2} + 1,$$

which is true for any $\mathbf{w} \in \mathbb{F}_2^{2(k+1)}$, we see that $\mathcal{U} = \mathbf{c} + \mathcal{U}_0$ (with $\mathcal{U}_0$ good for $L_{\mathrm{mod}}$) participates to the summation in (80) if and only if $\mathcal{U}_0$ is included in the vector

hyperplane $\mathcal{H}$ (defined in §3.1) and if $\mathbf{c}$ satisfies $c_{2k+1}+c_{2k+2}=1$. Also note the implication

$$(A+B)(\mathbf{w})=0 \Rightarrow A(\mathbf{w})=0. \tag{81}$$

If $\mathcal{U}$ is as above, every subset $S$ of it, with odd cardinality satisfies $\sigma(S)\in\mathcal{U}$. Hence, by Lemma 12 and by (81) we have the equality

$$e^{+}_{\mathrm{mod}}(S)=0.$$

After all these considerations we transform (80) into

$$\Gamma_2 = 2^{-k-1}\sum_{\substack{\mathcal{U}_0 \text{ good for } L_{\mathrm{mod}}\\ \mathcal{U}_0\subset\mathcal{H}}}\ \sum_{\substack{\mathbf{c}\\ (A+B)(\mathbf{c})=0}}\ \sum_{\substack{S\subset\mathbf{c}+\mathcal{U}_0\\ \sharp\, S \text{ odd}}} 1 \tag{82}$$
$$= 2^{2^{k+1}+k-1}\ \sharp\,\{\mathcal{U}_0\,;\ \mathcal{U}_0 \text{ good for } L_{\mathrm{mod}}\subset\mathcal{H}\}.$$

Lemma 3 implies the equality

$$\sharp\,\{\mathcal{U}_0\,;\ \mathcal{U}_0 \text{ good for } L_{\mathrm{mod}}\subset\mathcal{H}\}=\mathbf{N}(k,2), \tag{83}$$

as follows. Let $(x_1,\dots,x_{2k+2})$ be the coordinates of a general point of $\mathbb{F}_2^{2(k+1)}$ in the basis $\mathcal{B}_{\mathrm{mod}}$ introduced in §3.1. The hyperplane $\mathcal{H}$ has the equation $x_{2k+1}=0$. We remark that $Y_{\mathrm{mod}}\subset\mathcal{H}$. By Lemma 3 we know that a good subspace $\mathcal{U}_0$ for $L_{\mathrm{mod}}$ is characterized by $\pi_{X_{\mathrm{mod}}}(\mathcal{U}_0)$, hence the equality

$$\sharp\,\{\mathcal{U}_0\,;\ \mathcal{U}_0 \text{ good for } L_{\mathrm{mod}}\subset\mathcal{H}\}=\sharp\,\{F';\ F' \text{ vector subspace of } \mathcal{H}\cap X_{\mathrm{mod}}\},$$

which directly leads to (83), since $\dim(\mathcal{H}\cap X_{\mathrm{mod}})=k$. Inserting the equality (83) into (82) we obtain the equality

$$\Gamma_2 = 2^{2^{k+1}+k-1}\mathbf{N}(k,2). \tag{84}$$

4.4. **End of the proof.** It suffices to put together (43), (46), (78), (79) & (84) to finish the proof of Theorem 2, in the case $(a,q)=(1,4)$.

## 5. Proof of Theorem 2. The case of negative $D$ divisible by 8

In that section we are concerned with negative fundamental $D$, which are divisible by 8. The goal is to evaluate the sum $S^{-}_{\mathrm{mix}}(X,k,0,8)$ defined in (17). Note that $-D$ is also a fundamental discriminant and that $-D/8$ is squarefree and congruent to $\pm1$ mod 4. Here also, we shall highly benefit from the combinatorics elaborated in [7]. In order to replace Lemma 4 we use

**Lemma 14.** *For any $k\geq 0$ and for every negative fundamental discriminant $D$ divisible by 8 we have the equality*

$$2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}=\frac{1}{2^{k\,\omega(-D/8)}}\sum_{(D_{\mathbf{u}})_{\mathbf{u}\in\mathbb{F}_2^{2k}}}\Big[\prod_{\mathbf{u}}\prod_{\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u};\mathbf{v})}\Big]\cdot\Big[\prod_{\mathbf{u}}\Big(\frac{2}{D_{\mathbf{u}}}\Big)^{\lambda_k(\mathbf{u})}\Big],$$

*where the sum is over all the $2^{2k}$–tuples $(D_{\mathbf{u}})$ such that*

$$\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} D_{\mathbf{u}}=-D/8. \tag{85}$$

*Proof.* See [7, Formulas (107) & (108)]. □

We replace Lemma 5 by

**Lemma 15.** *For any positive fundamental discriminant $D$ divisible by 8 we have the equality*

(86)
$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D/8)}} \sum_{(D_{\boldsymbol{\alpha}})} \Big[\prod_{\boldsymbol{\alpha}}\prod_{\boldsymbol{\beta}} \Big(\frac{D_{\boldsymbol{\alpha}}}{D_{\boldsymbol{\beta}}}\Big)^{(\alpha_1+\beta_1)(\alpha_1+\beta_2)}\Big] \cdot \Big[\prod_{\boldsymbol{\alpha}} \Big(\frac{2}{D_{\boldsymbol{\alpha}}}\Big)^{\alpha_1\alpha_2}\Big] \times \Big[\prod_{\boldsymbol{\alpha}} \Big(\frac{-1}{D_{\boldsymbol{\alpha}}}\Big)^{\alpha_1\alpha_2} + \prod_{\boldsymbol{\alpha}} \Big(\frac{-1}{D_{\boldsymbol{\alpha}}}\Big)^{(\alpha_1+1)(\alpha_2+1)}\Big],$$

*where the first sum is over the 4–tuples $(D_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\mathbb{F}_2^2}$ such that*

$$\prod_{\boldsymbol{\alpha}} D_{\boldsymbol{\alpha}} = D/8. \tag{87}$$

*Proof.* See [7, Formula (112)]. □

As we did in §4.1, we parametrize the solutions of the system of the equations (85) & (87), sum over all the $D \equiv 0 \bmod 8$, satisfying $0 < -D < X$ to arrive at the following lemma (compare with Lemma 6 above):

**Lemma 16.** *For every $k \geq 0$ and for every $X \geq 2$ we have the equality*

(88)
$$S^-_{\mathrm{mix}}(X,k,0,8) = \frac{1}{2}\sum_{(D_{\mathbf{w}})} \Big[\prod_{\mathbf{w}} 2^{-(k+1)\omega(D_{\mathbf{w}})}\Big] \times \Big[\prod_{\mathbf{w}}\prod_{\mathbf{w}'} \Big(\frac{D_{\mathbf{w}}}{D_{\mathbf{w}'}}\Big)^{\Phi_{k+1}(\mathbf{w};\mathbf{w}')}\Big] \times \Big[\prod_{\mathbf{w}} \Big(\frac{2}{D_{\mathbf{w}}}\Big)^{\lambda_{k+1}(\mathbf{w})}\Big] \times \Big[\prod_{\mathbf{w}} \Big(\frac{-1}{D_{\mathbf{w}}}\Big)^{A(\mathbf{w})} + \prod_{\mathbf{w}} \Big(\frac{-1}{D_{\mathbf{w}}}\Big)^{B(\mathbf{w})}\Big],$$

*where the sum is over all the $4^{k+1}$–tuples $(D_{\mathbf{w}})$ of coprime, squarefree and positive integers satisfying*

$$\prod_{\mathbf{w}} D_{\mathbf{w}} \leq X/8 \text{ and } \prod_{\mathbf{w}} D_{\mathbf{w}} \equiv \pm 1 \bmod 4$$

*and where the indices $\mathbf{w}$ and $\mathbf{w}'$ belong to $\mathbb{F}_2^{2(k+1)}$.*

We split $S^-_{\mathrm{mix}}(X,k,0,8)$ into

$$S^-_{\mathrm{mix}}(X,k,0,8) = \Sigma_3(X) + \Sigma_4(X), \tag{89}$$

where $\Sigma_3(X)$ and $\Sigma_4(X)$ correspond to the contribution of the first and of the second term inside the symbol $[\cdots + \cdots]$ appearing in (88), respectively.

5.1. **Study of $\Sigma_3(X)$.** Recall the definition (44). The analogue of Lemma 7 is

**Lemma 17.** *For every $k \geq 0$ and every $\epsilon > 0$ we have uniformly for $X \geq 2$ the equality*

$$\Sigma_3(X) = \frac{2^{1-2^{k+1}}}{\pi^2} \cdot \Big(\sum_{\mathcal{U}} \{\gamma^+(\mathcal{U},0) + \gamma^+(\mathcal{U},1)\}\Big) \cdot \frac{X}{8} + O_\epsilon\big(X(\log X)^{-2^{-k-1}+\epsilon}\big),$$

*where the sum is over all the maximal unlinked subsets $\mathcal{U} \subset \mathbb{F}_2^{2(k+1)}$ such that $\lambda_{k+1}$ is identically equal to zero on $\mathcal{U}$.*

*Proof.* See the proof of [7, Proposition 7]. We point out that, as in Lemma 13, the condition $\lambda_{k+1} \equiv 0$ on $\mathcal{U}$ is to avoid oscillations of the character $\left(\frac{2}{D_{\mathbf{w}}}\right)^{\lambda_{k+1}(\mathbf{w})}$. □

Again using (16), we write Lemma 17 in the equivalent form

$$\Sigma_3(X) = 2^{-2^{k+1}-1} \cdot \left(\Gamma_3^{(0)} + \Gamma_3^{(1)}\right) \cdot \mathcal{D}^-(X,0,8) + O_\epsilon\big(X(\log X)^{-2^{-k-1}+\epsilon}\big), \tag{90}$$

with

$$\Gamma_3^{(\nu)} = \sum_{\mathcal{U}} \gamma^+(\mathcal{U},\nu), \quad \text{for } \nu = 0 \text{ or } 1,$$

where the summation over $\mathcal{U}$ is the same as in Lemma 17.

5.1.1. *Study of* $\Gamma_3^{(1)}$. It is very similar to the study of $\Gamma_1$ made in §4.2.2. We use (75) to write an analogue of (76):

$$\Gamma_3^{(1)} = 2^{2^{k+1}-2k-3} \sum_{\substack{\mathcal{U}_0 \text{ good} \\ \text{for } L_{\mathrm{mod}}}} \sum_{\boldsymbol{\sigma}\in\mathcal{U}_0} \sum_{\mathbf{c}\in\mathbb{F}_2^{2(k+1)}} (-1)^{A(\mathbf{c}+\boldsymbol{\sigma})}, \tag{91}$$

where $\mathbf{c}$ satisfies the extra condition

$$\lambda_{k+1} \equiv 0 \text{ on } \mathbf{c}+\mathcal{U}_0. \tag{92}$$

We use the following result of linear algebra, where $\boldsymbol{\rho}$ is defined in §3.1.

**Lemma 18.** *Let $\mathcal{U}_0$ be a vector subspace of $\mathbb{F}_2^{2(k+1)}$ which has the property to be good for $L_{\mathrm{mod}}$. Let $\mathbf{c}$ be a point of $\mathbb{F}_2^{2(k+1)}$. Then the condition (92) is satisfied if and only if*

$$\mathbf{c}+\mathcal{U}_0 = \boldsymbol{\rho}+\mathcal{U}_0.$$

*Proof.* The proof is similar to the proof of [7, Lemma 36], with the difference that it is concerned with subspaces which are good for the bilinear form $L$. The transcription to $L_{\mathrm{mod}}$ is standard. □

Coming back to (91) we deduce from Lemma 18 the equality

$$\Gamma_3^{(1)} = 2^{2^{k+1}-k-2} \sum_{\substack{\mathcal{U}_0 \text{ good} \\ \text{for } L_{\mathrm{mod}}}} \sum_{\boldsymbol{\sigma}\in\mathcal{U}_0} (-1)^{A(\boldsymbol{\rho}+\boldsymbol{\sigma})}. \tag{93}$$

Note the direct consequence of the definition of $A$

$$A(\boldsymbol{\rho}+\boldsymbol{\sigma}) = \sigma_{2k+1}(\sigma_{2k+2}+1),$$

for $\boldsymbol{\sigma} = (\sigma_1,\dots,\sigma_{2k+2})$.

5.1.2. *Study of* $\Gamma_3^{(0)}$. Now we use Lemma 12 with $\sharp S$ even. Hence for any $S$ with even cardinality, included in $\boldsymbol{\rho}+\mathcal{U}_0$, with $\mathcal{U}_0$ good, we have

$$e^+_{\mathrm{mod}}(S) = A(\sigma(S)) + L_{\mathrm{mod}}(\sigma(S),\boldsymbol{\rho}) + \Lambda(\sigma(S)) = \sigma_{2k+1}(S)(\sigma_{2k+2}(S)+1)$$

by writing

$$\sigma(S) = (\sigma_1(S),\dots,\sigma_{2k+2}(S)).$$

By summing as above according to the value of $\boldsymbol{\sigma} = \sigma(S)$ (see the proof of (75)) we arrive at the equality

$$\Gamma_3^{(1)} = 2^{2^{k+1}-k-2} \sum_{\mathcal{U}_0 \text{ good}} \sum_{\boldsymbol{\sigma}\in\mathcal{U}_0} (-1)^{\sigma_{2k+1}(\sigma_{2k+2}+1)}.$$

This combined with (93) gives

$$\Gamma_3^{(0)}+\Gamma_3^{(1)}=2^{2^{k+1}-k-1}\sum_{\mathcal{U}_0\text{ good}}\ \sum_{\boldsymbol{\sigma}\in\mathcal{U}_0}(-1)^{\sigma_{2k+1}(\sigma_{2k+2}+1)}. \tag{94}$$

5.2. **Study of $\Sigma_4(X)$.** Similarly to (90) we have the equality

$$\Sigma_4(X)=2^{-2^{k+1}}\cdot\Big(\Gamma_4^{(0)}+\Gamma_4^{(1)}\Big)\cdot\mathcal{D}^-(X,0,8)+O_\epsilon\big(X(\log X)^{-2^{-k-1}+\epsilon}\big) \tag{95}$$

with

$$\Gamma_4^{(\nu)}=\sum_{\mathcal{U}}\ \tilde{\gamma}(\mathcal{U},\nu),\quad\text{for }\nu=0\text{ or }1, \tag{96}$$

where the summation is over all the maximal unlinked subsets $\mathcal{U}$, such that $\lambda_{k+1}$, defined in §3.1, is identically equal to zero on $\mathcal{U}$. We have put

$$\tilde{\gamma}(\mathcal{U},\nu)=\sum_{\substack{S\subset\mathcal{U}\\ \sharp\, S\equiv\nu\bmod 2}}(-1)^{\tilde{e}(S)}, \tag{97}$$

where the function $\tilde{e}$ slightly differs from $e^+_{\mathrm{mod}}$ (defined in (48)), since it is equal to

$$\begin{aligned}\tilde{e}(S)&:=\sum_{\mathbf{w}\in S}B(\mathbf{w})+\sum_{\substack{\mathbf{w}\in S\\ \mathbf{w}'\in S}}\Phi_{k+1}\big(\mathbf{w};\mathbf{w}'\big)\\ &=e^+_{\mathrm{mod}}(S)+\sigma_{2k+1}(S)+\sigma_{2k+2}(S)+\sharp\, S.\end{aligned} \tag{98}$$

In the first line of (98), the second sum is over unordered pairs of elements of $S$. A variant of Lemma 11 adapted to the function $\tilde{e}(S)$ gives

$$\tilde{\gamma}(\mathcal{U},\nu)\neq 0\text{ for }\nu=0\text{ or }1\Rightarrow\mathcal{U}_0\text{ good for }L_{\mathrm{mod}}.$$

Hence, in (96) we can restrict the sum to the $\mathcal{U}$ of the form $\mathbf{c}+\mathcal{U}_0$, with $\mathcal{U}_0$ good (for $L_{\mathrm{mod}}$). By Lemma 18, we restrict this summation to the $\mathcal{U}$ of the form $\boldsymbol{\rho}+\mathcal{U}_0$, with $\mathcal{U}_0$ good. After these considerations, we apply Lemma 12 to simplify (98) into

$$\tilde{e}(S)=(\sigma_{2k+1}(S)+1)(\sigma_{2k+2}(S)+\sharp\, S), \tag{99}$$

for any subset $S$ of $\mathcal{U}$ as above. Summing over the values of $\boldsymbol{\sigma}=\sigma(S)$ ($\boldsymbol{\sigma}\in\mathcal{U}_0$, $\sharp\, S\equiv 0\bmod 2$), as we did for (75), we obtain for such a $\mathcal{U}$ the equality

$$\begin{aligned}\tilde{\gamma}(\mathcal{U},0)&=\sum_{\substack{S\subset\mathcal{U}\\ \sharp\, S\equiv 0\bmod 2}}(-1)^{(\sigma_{2k+1}(S)+1)\sigma_{2k+2}(S)}\\ &=2^{2^{k+1}-k-2}\sum_{\boldsymbol{\sigma}\in\mathcal{U}_0}(-1)^{(\sigma_{2k+1}+1)\sigma_{2k+2}}.\end{aligned} \tag{100}$$

Similarly, summing over the values of $\boldsymbol{\rho}+\boldsymbol{\sigma}=\sigma(S)$ ($\boldsymbol{\sigma}\in\mathcal{U}_0$, $\sharp\, S\equiv 1\bmod 2$) we also obtain

$$\begin{aligned}\tilde{\gamma}(\mathcal{U},1)&=\sum_{\substack{S\subset\mathcal{U}\\ \sharp\, S\equiv 1\bmod 2}}(-1)^{(\sigma_{2k+1}(S)+1)(\sigma_{2k+2}(S)+1)}\\ &=2^{2^{k+1}-k-2}\sum_{\boldsymbol{\sigma}\in\mathcal{U}_0}(-1)^{(\sigma_{2k+1}+1)\sigma_{2k+2}}.\end{aligned} \tag{101}$$

By (96), (100) & (101) we write

$$\Gamma_4^{(0)}+\Gamma_4^{(1)}=2^{2^{k+1}-k-1}\sum_{\substack{\mathcal{U}_0\text{ good}\\ \text{for }L_{\mathrm{mod}}}}\ \sum_{\boldsymbol{\sigma}\in\mathcal{U}_0}(-1)^{(\sigma_{2k+1}+1)\sigma_{2k+2}}. \tag{102}$$

Gathering (94) and (102) we have

$$\Gamma_3^{(0)}+\Gamma_3^{(1)}+\Gamma_4^{(0)}+\Gamma_4^{(1)} = 2^{2^{k+1}-k-1}\sum_{\substack{\mathcal{U}_0 \text{ good}\\ \text{for } L_{\rm mod}}}\ \sum_{\boldsymbol{\sigma}\in\mathcal{U}_0}\Big[(-1)^{\sigma_{2k+1}(\sigma_{2k+2}+1)}+(-1)^{(\sigma_{2k+1}+1)\sigma_{2k+2}}\Big]. \tag{103}$$

Now we easily remark

$$(-1)^{\sigma_{2k+1}(\sigma_{2k+2}+1)}+(-1)^{(\sigma_{2k+1}+1)\sigma_{2k+2}} = \begin{cases} 0, & \text{if } \sigma_{2k+1}+\sigma_{2k+2}=1,\\ 2, & \text{if } \sigma_{2k+1}+\sigma_{2k+2}=0.\end{cases}$$

Hence, if the $\mathcal{U}_0$ (good for $L_{\rm mod}$) is included in the hyperplane $\mathcal{H}$ (defined in §3.1) we have

$$\sum_{\boldsymbol{\sigma}\in\mathcal{U}_0}\Big[(-1)^{\sigma_{2k+1}(\sigma_{2k+2}+1)}+(-1)^{(\sigma_{2k+1}+1)\sigma_{2k+2}}\Big] = 2^{k+2}. \tag{104}$$

By (83) we know that there are exactly $\mathbf{N}(k,2)$ such $\mathcal{U}_0$.

In the other direction, if $\mathcal{U}_0$ is not included in $\mathcal{H}$ we have $\sharp\,(\mathcal{U}_0\cap\mathcal{H}) = 2^k$ and also the equality

$$\sum_{\boldsymbol{\sigma}\in\mathcal{U}_0}\Big[(-1)^{\sigma_{2k+1}(\sigma_{2k+2}+1)}+(-1)^{(\sigma_{2k+1}+1)\sigma_{2k+2}}\Big] = 2^{k+1}. \tag{105}$$

Combining Lemma 3 with (83) we know that there are exactly $\mathbf{N}(k+1,2)-\mathbf{N}(k,2)$ subspaces $\mathcal{U}_0$ which are good for $L_{\rm mod}$ and not included in $\mathcal{H}$. Putting together (103), (104) & (105) we have

$$\begin{aligned}\Gamma_3^{(0)}+\Gamma_3^{(1)}+\Gamma_4^{(0)}+\Gamma_4^{(1)} &= 2^{2^{k+1}-k-1}\Big\{2^{k+2}\mathbf{N}(k,2)+2^{k+1}\big(\mathbf{N}(k+1,2)-\mathbf{N}(k,2)\big)\Big\}\\ &= 2^{2^{k+1}+1}\cdot\frac{\mathbf{N}(k+1,2)+\mathbf{N}(k,2)}{2}. \end{aligned}\tag{106}$$

5.3. **End of the proof.** Put together (89), (90), (95) & (106), to exhibit the asymptotic expansion of $S^{-}_{\rm mix}(X,k,0,8)$ announced in Theorem 2.

## 6. The case of even negative $D$ not divisible by 8

In this last section we deal with negative fundamental discriminants$D$, which are $\equiv 4 \bmod 8$ in order to evaluate the sum $S^{-}_{\rm mix}(X,k,4,8)$. Note that the integer $-D/4$ now is squarefree and congruent to 1 mod 4, hence it is the discriminant of the associated field to $\mathbb{Q}(\sqrt{D})$.

6.1. **Reduction of the proof.** We have

**Lemma 19.** *For any $k\geq 0$ and for every negative fundamental discriminant $D$, congruent to 4 modulo 8, we have the equality*

$$2^{k\,\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2^k\cdot 2^{k\,\omega(-D/4)}}\sum_{\mathcal{E}\subset\{1,\dots,k\}} U_{\mathcal{E}}$$

*where*

$$U_{\mathcal{E}} = \sum_{(D_{\mathbf{u}})_{\mathbf{u}\in\mathbb{F}_2^{2k}}}\Big[\prod_{\mathbf{u}}\prod_{\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u};\mathbf{v})}\Big]\cdot\Big[\prod_{\mathbf{u}}\Big(\frac{2}{D_{\mathbf{u}}}\Big)^{V_{\mathcal{E}}(\mathbf{u})}\Big],$$

*where the sum is over all the $2^{2k}$–tuples $(D_{\mathbf{u}})$ such that*

$$\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} D_{\mathbf{u}} = -D/4. \tag{107}$$

*Proof.* See [7, Formula (120) & Lemma 41], with a slight change of notation concerning the affine function $V_{\mathcal{E}}$ defined in §3.1. □

We also use

**Lemma 20.** *For any positive fundamental discriminant $D \equiv 1 \bmod 4$ we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D)}} \sum_{(D_{\boldsymbol{\alpha}})} \Big[\prod_{\boldsymbol{\alpha}}\prod_{\boldsymbol{\beta}} \Big(\frac{D_{\boldsymbol{\alpha}}}{D_{\boldsymbol{\beta}}}\Big)^{(\alpha_1+\beta_1)(\alpha_1+\beta_2)}\Big] \cdot \Big[\prod_{\boldsymbol{\alpha}} \Big(\frac{-1}{D_{\boldsymbol{\alpha}}}\Big)^{\alpha_1\alpha_2}\Big], \tag{108}$$

*where the first sum is over the 4–tuples $(D_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\mathbb{F}_2^2}$ such that*

$$\prod_{\boldsymbol{\alpha}} D_{\boldsymbol{\alpha}} = D. \tag{109}$$

*Proof.* See [7, Formula (78)]. □

As we did before, we parametrize the solutions of the simultaneous equations (107) & (109), then sum over all $D$ satisfying $0 < -D < X$ and $D \equiv 4 \bmod 8$ to arrive at

**Lemma 21.** *For every $X \geq 2$ we have the equality*

$$S^{-}_{\mathrm{mix}}(X,k,4,8) = \frac{1}{2^{k+1}} \sum_{\mathcal{E}\subset\{1,\dots,k\}} T_{\mathcal{E}}(X) \tag{110}$$

*with*

$$\begin{aligned} T_{\mathcal{E}}(X) := \sum_{(D_{\mathbf{w}})} \Big[\prod_{\mathbf{w}} 2^{-(k+1)\omega(D_{\mathbf{w}})}\Big] \times \Big[\prod_{\mathbf{w}}\prod_{\mathbf{w}'} \Big(\frac{D_{\mathbf{w}}}{D_{\mathbf{w}'}}\Big)^{\Phi_{k+1}(\mathbf{w};\mathbf{w}')}\Big] \\ \times \Big[\prod_{\mathbf{w}} \Big(\frac{2}{D_{\mathbf{w}}}\Big)^{V_{\mathcal{E}}(\mathbf{w})}\Big] \times \Big[\prod_{\mathbf{w}} \Big(\frac{-1}{D_{\mathbf{w}}}\Big)^{A(\mathbf{w})}\Big], \end{aligned} \tag{111}$$

*where the sum is over all the $4^{k+1}$–tuples $(D_{\mathbf{w}})$ of coprime, squarefree and positive integers satisfying*

$$\prod_{\mathbf{w}} D_{\mathbf{w}} \leq X/4 \text{ and } \prod_{\mathbf{w}} D_{\mathbf{w}} \equiv 1 \bmod 4.$$

Using symmetries we write (110) in the form

$$S^{-}_{\mathrm{mix}}(X,k,4,8) = \frac{1}{2^{k+1}} \sum_{\ell=0}^{k} \binom{k}{\ell} T_{\{1,\dots,\ell\}}(X) \tag{112}$$

The same analysis as for Lemma 7 leads to

**Lemma 22.** *For every $k \geq 0$, for every $\epsilon > 0$ and for every $\mathcal{E} \subset \{1, \dots, k\}$ we have uniformly for $X \geq 2$ the equality*

$$T_{\mathcal{E}}(X) = \frac{2^{2-2^{k+1}}}{\pi^2} \cdot \Big(\sum_{\mathcal{U}} \gamma^+(\mathcal{U}, 0)\Big) \cdot \frac{X}{4} + O_\epsilon\big(X(\log X)^{-2^{-k-1}+\epsilon}\big),$$

*where the sum is over all the maximal unlinked subsets $\mathcal{U} \subset \mathbb{F}_2^{2(k+1)}$ such that $V_{\mathcal{E}}$ is identically equal to zero on $\mathcal{U}$.*

Recall that $\gamma^+(\mathcal{U}, 0)$ is defined in (49). As before, we appeal to Lemma 11 in order to restrict the summation to the $\mathcal{U} = \mathbf{c} + \mathcal{U}_0$, such that $\mathcal{U}_0$ is good for $L_{\mathrm{mod}}$. With the help of (16), we write Lemma 22 in the following equivalent manner

$$T_{\mathcal{E}}(X) = T_{\mathcal{E}} \cdot \mathcal{D}^-(X, 4, 8) + O_\epsilon\big(X(\log X)^{-2^{-k-1}+\epsilon}\big) \tag{113}$$

with

$$T_{\mathcal{E}} = 2^{1-2^{k+1}} \cdot \Big(\sum_{\mathcal{U}} \gamma^+(\mathcal{U}, 0)\Big) \tag{114}$$

and the same conditions of summation for $\mathcal{U}$ as in Lemma 22. Considering (112) & (113) we see that the proof of Theorem 2 in the case $(a, q) = (4, 8)$ is reduced to prove the equality

$$\frac{1}{2^{k+1}} \sum_{k_0=0}^{k} \binom{k}{k_0} T_{\{1,\dots,k_0\}} = \frac{\mathbf{N}(k+1, 2) + \mathbf{N}(k, 2)}{2} \tag{115}$$

for every $0 \leq k_0 \leq k$.

6.2. **Transformation of the fundamental sum.** By Lemma 12, we have the equality

$$e^+_{\mathrm{mod}}(S) = A(\sigma(S)) + L_{\mathrm{mod}}(\sigma(S), \mathbf{c}) + \Lambda(\sigma(S)),$$

for every $S$, with an even cardinality, included in $\mathcal{U} = \mathbf{c} + \mathcal{U}_0$, such that $\mathcal{U}_0$ is good for $L_{\mathrm{mod}}$. For such an $S$, the sum $\sigma(S)$ belongs to $\mathcal{U}_0$, then, summing over the values of $\boldsymbol{\sigma} = \sigma(S)$, as we did for (75), we obtain

$$\gamma^+(\mathcal{U}, 0) = 2^{2^{k+1}-k-2} \sum_{\boldsymbol{\sigma} \in \mathcal{U}_0} (-1)^{J(\boldsymbol{\sigma}, \mathbf{c})}, \tag{116}$$

with

$$\begin{aligned} J(\boldsymbol{\sigma}, \mathbf{c}) &:= A(\boldsymbol{\sigma}) + L_{\mathrm{mod}}(\boldsymbol{\sigma}, \mathbf{c}) + \Lambda(\boldsymbol{\sigma}) \\ &= \sigma_1(c_1 + c_2 + 1) + \cdots + \sigma_{2k-1}(c_{2k-1} + c_{2k} + 1) \\ &\quad + c_{2k+1}(\sigma_{2k+1} + \sigma_{2k+2}) + \sigma_{2k+1}(1 + \sigma_{2k+2}). \end{aligned}$$

Inserting (116) into (114), and inverting summations, we have the equality

$$T_{\mathcal{E}} = 2^{-2k-2} \sum_{\substack{\mathcal{U}_0 \text{ good} \\ \text{for } L_{\mathrm{good}}}} \sum_{\boldsymbol{\sigma} \in \mathcal{U}_0} \sum_{\mathbf{c}} (-1)^{J(\boldsymbol{\sigma}, \mathbf{c})}, \tag{117}$$

where the sum is over all the $\mathbf{c}$ such that

$$V_{\mathcal{E}} \equiv 0 \text{ on } \mathbf{c} + \mathcal{U}_0. \tag{118}$$

6.3. **The case $\mathcal{E}=\emptyset$.** In that case, the condition (118) is empty. Summing over $\mathbf{c}$ first, we see that the sum $\sum_{\mathbf{c}}(-1)^{J(\boldsymbol{\sigma},\mathbf{c})}$ is equal to $2^{2(k+1)}$ if and only if

$$\sigma_1=\sigma_3=\cdots=\sigma_{2k-1}=\sigma_{2k+1}+\sigma_{2k+2}=0. \tag{119}$$

Otherwise, this sum is equal to zero. Now we work in the basis $\mathcal{B}_{\mathrm{mod}}$ defined in §3.1. Let $(x_i)$ be the coordinates in $\mathcal{B}_{\mathrm{mod}}$ of $\boldsymbol{\sigma}$. Then (119) is equivalent to

$$x_1=x_3=\cdots=x_{2k-1}=x_{2k+1}=0. \tag{120}$$

So we have the equality

$$T_{\emptyset}=\sum_{\substack{\mathcal{U}_0 \text{ good}\\ \text{for } L_{\mathrm{mod}}}} \sharp\{\boldsymbol{\sigma}\in\mathcal{U}_0\,;\ x_1=x_3=\cdots=x_{2k+1}=0\}. \tag{121}$$

Now we apply Lemma 3. In the decomposition $\mathcal{U}_0=\pi_{X_{\mathrm{mod}}}(\mathcal{U}_0)\oplus\pi_{Y_{\mathrm{mod}}}(\mathcal{U}_0)$, only the elements of $F':=\pi_{Y_{\mathrm{mod}}}(\mathcal{U}_0)$ satisfy the condition (120). Their number is $2^{\dim F'}$. Since $F'$ characterizes $\mathcal{U}_0$, by summing over $\ell:=\dim F'$, we obtain the equality

$$T_{\emptyset}=\sum_{\ell=0}^{k+1}2^{\ell}\cdot\mathfrak{n}(k+1,\ell,2). \tag{122}$$

6.4. **The case $\sharp\mathcal{E}=1$.** We continue to investigate all the $T_{\mathcal{E}}$ participating to (110). The second step concerns the case when $\mathcal{E}$ has only one element. Hence we are led to study the quantity $T_{\{1\}}$. The condition (118) is simply

$$\begin{cases} c_1+c_2+1 &=0\\ w_1+w_2 &=0 \text{ for all } \mathbf{w}\in\mathcal{U}_0.\end{cases}$$

It is easy to see that the sum $\sum_{\mathbf{c}}(-1)^{J(\boldsymbol{\sigma},\mathbf{c})}$, appearing in (117) is equal to $2^{2k+1}$ if and only if we have

$$\sigma_3=\sigma_5=\cdots=\sigma_{2k-1}=0 \text{ and } \sigma_{2k+1}+\sigma_{2k+2}=0. \tag{123}$$

Otherwise this sum is equal to 0. Now we use the coordinates $x_i$ in the basis $\mathcal{B}_{\mathrm{mod}}$. With the above observations we have the equalities

$$\begin{aligned} T_{\{1\}}&=\frac{1}{2}\sum_{\mathcal{U}_0}\sharp\{\boldsymbol{\sigma}\in\mathcal{U}_0\,;\ x_3=\cdots=x_{2k-1}=x_{2k+1}=0\},\\ &=\frac{1}{2}\sum_{\mathcal{U}_0}\sharp\{\boldsymbol{\sigma}\in\mathcal{U}_0\,;\ x_1=x_3=\cdots=x_{2k-1}=x_{2k+1}=0\}\\ &+\frac{1}{2}\sum_{\mathcal{U}_0}\sharp\{\boldsymbol{\sigma}\in\mathcal{U}_0\,;\ x_1=1 \text{ and } x_3=\cdots=x_{2k-1}=x_{2k+1}=0\},\end{aligned} \tag{124}$$

where the sum is over all the subspaces $\mathcal{U}_0$ of $\mathbb{F}_2^{2(k+1)}$, which are good for $L_{\mathrm{mod}}$ and which are contained in the hyperplane $\mathcal{H}_1$ with equation $x_2=0$. Now we go back to Lemma 3, particularly to the decomposition

$$\mathcal{U}_0=\pi_{X_{\mathrm{mod}}}(\mathcal{U}_0)\oplus\pi_{Y_{\mathrm{mod}}}(\mathcal{U}_0):=F\oplus F'. \tag{125}$$

It is easy to see that $\mathcal{U}_0\subset\mathcal{H}_1$ if and only if $F'\subset\mathcal{H}_1$. Since $F$ and $F'$ are perpendicular, relatively to $L_{\mathrm{mod}}$, this last statement is equivalent to $\vec{b}_1'\in F$. We

deduce that the translation by $\vec{b}'_1$ is an involution of $\mathcal{U}_0$, so we can simplify (124) into

$$T_{\{1\}} = \sum_{\mathcal{U}_0} \sharp\{\boldsymbol{\sigma} \in \mathcal{U}_0\,;\, x_1 = x_3 = \cdots = x_{2k-1} = x_{2k+1} = 0\}. \tag{126}$$

In order to conclude the above discussion, we sum over $\ell = \dim F'$, where $F'$ is a vector subspace of $\mathcal{H}_1 \cap Y_{\mathrm{mod}}$ (which is of dimension $k$) to finally transform (126) into

$$T_{\{1\}} = \sum_{\ell=0}^{k} 2^{\ell} \cdot \mathfrak{n}(k, \ell, 2). \tag{127}$$

6.5. **The case $\sharp\,\mathcal{E} \geq 2$.** Now we are considering the case $\mathcal{E} = \{1, \ldots, k_0\}$, where $k_0$ now satisfies $2 \leq k_0 \leq k$. This case has much to do with the case $\sharp\,\mathcal{E} = \{1\}$. Now the constraint (118) becomes

$$\begin{cases} \displaystyle\sum_{\ell=1}^{k_0} (c_{2\ell-1} + c_{2\ell} + 1) = 0 \\ \\ \displaystyle\sum_{\ell=1}^{k_0} (w_{2\ell-1} + w_{2\ell}) = 0 \text{ for all } \mathbf{w} \in \mathcal{U}_0. \end{cases} \tag{128}$$

Under that constraint $J(\boldsymbol{\sigma}, \mathbf{c})$ is now

$$\begin{aligned} J(\boldsymbol{\sigma}, \mathbf{c}) = {} & (\sigma_1 + \sigma_{2k_0-1})(c_1 + c_2 + 1) + \cdots + (\sigma_{2k_0-3} + \sigma_{2k_0-1})(c_{2k_0-3} + c_{2k_0-2} + 1) \\ & + \sigma_{2k_0+1}(c_{2k_0+1} + c_{2k_0+2} + 1) + \cdots + \sigma_{2k-1}(c_{2k-1} + c_{2k} + 1) \\ & + c_{2k+1}(\sigma_{2k+1} + \sigma_{2k+2}) + \sigma_{2k+1}(1 + \sigma_{2k+2}). \end{aligned}$$

Now it is easy to see that the sum $\sum_{\mathbf{c}} (-1)^{J(\boldsymbol{\sigma}, \mathbf{c})}$, appearing in (117) is equal to $2^{2k+1}$ if and only if we have

$$\sigma_1 = \sigma_3 = \cdots = \sigma_{2k_0-1},\ \sigma_{2k_0+1} = \cdots = \sigma_{2k-1} = 0 \text{ and } \sigma_{2k+1} + \sigma_{2k+2} = 0. \tag{129}$$

Otherwise it is zero. Now we use the coordinates $x_i$ in the basis $\mathcal{B}_{\mathrm{mod}}$. With the above observations we have the equalities

(130)

$$\begin{aligned} T_{\{1,\ldots,k_0\}} &= \frac{1}{2} \sum_{\mathcal{U}_0} \sharp\{\boldsymbol{\sigma} \in \mathcal{U}_0\,;\, x_1 = \cdots = x_{2k_0-1},\ x_{2k_0+1} = \cdots = x_{2k-1} = x_{2k+1} = 0\}, \\ &= \frac{1}{2} \sum_{\mathcal{U}_0} \sharp\{\boldsymbol{\sigma} \in \mathcal{U}_0\,;\, x_1 = x_3 = \cdots = x_{2k-1} = x_{2k+1} = 0\} \\ &\quad + \frac{1}{2} \sum_{\mathcal{U}_0} \sharp\{\boldsymbol{\sigma} \in \mathcal{U}_0\,;\, x_1 = \cdots = x_{2k_0-1} = 1,\ x_{2k_0+1} = \cdots = x_{2k+1} = 0\}, \end{aligned}$$

where the sum is over all the subspaces $\mathcal{U}_0$ of $\mathbb{F}_2^{2(k+1)}$, which are good for $L_{\mathrm{mod}}$ and which are contained in the hyperplane $\mathcal{H}_{k_0}$ with equation $x_2 + x_4 + \cdots x_{2k_0} = 0$. One more time, we use the decomposition (125). It is easy to see that $\mathcal{U}_0 \subset \mathcal{H}_{k_0}$ if and only if $F' \subset \mathcal{H}_{k_0}$. Since $F$ and $F'$ are perpendicular, this last statement

is equivalent to $\vec{b}'_1 + \vec{b}'_3 + \cdots + \vec{b}'_{2k_0-1} \in F$. The translation by this vector is an involution of $\mathcal{U}_0$, so we can simplify (130) into

$$T_{\{1,\dots,k_0\}} = \sum_{\mathcal{U}_0} \sharp\{\boldsymbol{\sigma} \in \mathcal{U}_0\,;\, x_1 = x_3 = \cdots = x_{2k-1} = x_{2k+1} = 0\}. \tag{131}$$

We recognize an expression already met in (126). Hence by (127), we also have

$$T_{\{1,\dots,k_0\}} = \sum_{\ell=0}^{k} 2^\ell \cdot \mathfrak{n}(k,\ell,2) \quad (k_0 \geq 2). \tag{132}$$

6.6. **The final step.** We put together (122), (127) & (132) in order to write the equality

$$\sum_{k_0=0}^{k} \binom{k}{k_0} T_{\{1,\dots,k_0\}} = \sum_{\ell=0}^{k+1} 2^\ell \cdot \mathfrak{n}(k+1,\ell,2) + (2^k-1) \sum_{\ell=0}^{k} 2^\ell \cdot \mathfrak{n}(k,\ell,2). \tag{133}$$

Using (35) we deduce from (133) the equality

$$\sum_{k_0=0}^{k} \binom{k}{k_0} T_{\{1,\dots,k_0\}} = \big(\mathbf{N}(k+2,2) - \mathbf{N}\,(k+1,2)\big) + (2^k-1)\big(\mathbf{N}(k+1,2) - \mathbf{N}\,(k,2)\big). \tag{134}$$

Now we appeal to (36) to replace $\mathbf{N}\,(k+2,2)$ by $2\,\mathbf{N}(k+1,2) + (2^{k+1}-1)\,\mathbf{N}(k,2)$ in (134). This finally gives the equality

$$\sum_{k_0=0}^{k} \binom{k}{k_0} T_{\{1,\dots,k_0\}} = 2^k\,\mathbf{N}(k+1,2) + 2^k\,\mathbf{N}(k,2).$$

This proves (115). The proof of Theorem 2 is now complete in the case $(a,q) = (4,8)$, which was the final case to consider.

## References


[1] K. Belabas, On the mean 3–rank of quadratic fields. *Comp. Math.*, 118: 1–9, 1999.

[2] K. Belabas, Corrigendum: On the mean 3–rank of quadratic fields. *Comp. Math.*, 140: 1221, 2004.

[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] P. Damey and J–J. Payan, Existence et construction des extensions galoisiennes et non–abéliennes de degré 8 d'un corps de caractéristique différente de 2. *J. für reine Angew. Math*, 244 : 37–54, 1970.

[6] P. Dutarte, Compatibilité avec le Spiegelungssatz de propriétés conjecturales sur le $p$–rang du groupe de classes. Mémoire de D.E.A. *Théorie des Nombres. Université de Besançon*, 1983–1984.

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

[8] 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.

[9] E. Fouvry and J. Klüners, On the negative Pell equation. *to appear in Annals of Math.*, 2008.

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

[11] F. Gerth III, Comparison of 4–class ranks of certain quadratic fields. *Proc. Amer. Math. Soc.*, 129 (n. 9) : 2547–2552, 2001.(*electronic*)

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

[13] A. Scholz, Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. *J. für reine Angew. Math.*, 166 : 201–203, 1932.

Univ. Paris–Sud, Laboratoire de Mathématiques d'Orsay, CNRS, F-91405 Orsay Cedex, France
*E-mail address*: Etienne.Fouvry@math.u-psud.fr

Mathematisches Institut, Heinrich–Heine–Universität, Universitätstr., 40225 Düsseldorf, Germany.
*E-mail address*: klueners@mathematik.uni-duesseldorf.de