Étienne Fouvry and Jürgen Klüners

On the 4-rank of class groups of quadratic number fields

Oblatum date & date

Abstract We prove that the 4–rank of class groups of quadratic number fields behave as predicted in an extension due to Gerth of the Cohen–Lenstra heuristics.

Mathematics Subject Classification (2000) 11R29,11R11,11R45

1 Introduction and notations

In the whole paper D denotes a fundamental discriminant, i.e. a discriminant of a quadratic number field. Let $K = \mathbb{Q}(\sqrt{D})$ be the quadratic number field of discriminant D. Denote by Cl_D the ordinary class group of K and by C_D the narrow class group of K. We remark that these two groups are always the same if $D < 0$. For a prime p we denote by $\mathrm{rk}_p(A) := \dim_{\mathbb{F}_p}(A/A^p)$ the p–rank of an abelian group A. Furthermore we introduce the 4–rank $\mathrm{rk}_4(A) := \mathrm{rk}_2(A^2)$. In this paper we prove many properties about the average behavior of the 4–rank of class groups of quadratic number fields. In order to present the results we introduce the following

Definition 1 *Let $f(D)$ be a numerical function defined over the set of fundamental discriminants. We say that $f(D)$ has a mean value over positive discriminants, if there exists a real number $\mathscr{M}^+(f(D))$ such that, we have*

$$\frac{\sum_{0<D<X} f(D)}{\sum_{0<D<X} 1} \underset{X\to\infty}{\longrightarrow} \mathscr{M}^+(f(D)).$$

If f is the characteristic function of a subset of positive fundamental discriminants, we call $\mathscr{M}^+(f(D))$ the density of the subset.

E. Fouvry
Mathématique, Bât. 425, Univ. Paris–Sud, Campus d'Orsay, F–91405 Orsay Cedex, France, E-mail: Etienne.Fouvry@math.u-psud.fr

J. Klüners
Mathematisches Institut, Heinrich-Heine-Universität, Universitätsstr. 1, 40225 Düsseldorf, Germany, E-mail: klueners@math.uni-duesseldorf.de

The same definition extends to a mean value over negative discriminants (quoted $\mathscr{M}^-(f(D))$), and more generally to any infinite subset of the positive or of the negative discriminants.

Let us state two of the main conjectures stated in [2, (C6), (C10)] extended to $p=2$ by [7].

Conjecture 1 *For every prime number p and for every integer $\alpha \geq 0$ we have*

$$\mathrm{Conj}^-(p,\alpha) \qquad \mathscr{M}^-\Big(\prod_{0\leq i<\alpha}\big(p^{\mathrm{rk}_p(\mathrm{C}_D^2)}-p^i\big)\Big)=1$$

and

$$\mathrm{Conj}^+(p,\alpha) \qquad \mathscr{M}^+\Big(\prod_{0\leq i<\alpha}\big(p^{\mathrm{rk}_p(\mathrm{C}_D^2)}-p^i\big)\Big)=p^{-\alpha}.$$

Actually, Cohen and Lenstra enunciated Conjecture 1 for any odd p and with C_D^2 replaced by C_D (note the equality $\mathrm{rk}_p(\mathrm{C}_D^2)=\mathrm{rk}_p(\mathrm{C}_D)$ for odd p). By genus theory it is clear that $\mathrm{rk}_2(C_D)=\omega(D)-1$, where ω counts the number of prime factors. We remark that $\mathrm{rk}_2(C_D)-1\leq \mathrm{rk}_2(\mathrm{Cl}_D)\leq \mathrm{rk}_2(C_D)$ (for more details, see the discussion after Lemma 10). By averaging the corresponding expressions we get

$$\sum_{0<\pm D\leq X} 2^{\mathrm{rk}_2(\mathrm{Cl}_D)},\ \sum_{0<\pm D\leq X} 2^{\mathrm{rk}_2(C_D)} \sim cX\log X,$$

for some positive constant c and for X tending to infinity. Frank Gerth [7] put forward the idea to consider C_D^2 instead of C_D. For $p=2$ we get that $\mathrm{rk}_2(C_D^2)=\mathrm{rk}_4(C_D)$.

Of course, $\mathrm{Conj}^{\pm}(p,0)$ is true for any p. The case $\mathrm{Conj}^{\pm}(p,1)$ for odd primes p corresponds to the normal average:

$$\lim_{X\to\infty}\frac{\sum_{0<D\leq X} p^{\mathrm{rk}_p(C_D)}}{\sum_{0<D\leq X}1}=1+p^{-1}$$

and

$$\lim_{X\to\infty}\frac{\sum_{0<-D\leq X} p^{\mathrm{rk}_p(C_D)}}{\sum_{0<-D\leq X}1}=2,$$

where the sums are over discriminants D of quadratic fields. This result is only proven for $p=3$ as a consequence of the Davenport–Heilbronn theorem [3]. As a special case of Theorem 1 we will get this average for the 4–rank, i.e. for $p=2$:

$$\lim_{X\to\infty}\frac{\sum_{0<D\leq X} 2^{\mathrm{rk}_4(C_D)}}{\sum_{0<D\leq X}1}=1+1/2 \tag{1}$$

and

$$\lim_{X\to\infty}\frac{\sum_{0<-D\leq X} 2^{\mathrm{rk}_4(C_D)}}{\sum_{0<D\leq X}1}=2. \tag{2}$$

The aim of this paper is to prove the more general

Theorem 1 *The conjectures* $\mathrm{Conj}^+(2,\alpha)$ *and* $\mathrm{Conj}^-(2,\alpha)$ *are true for every integer* $\alpha \geq 0$.

In order to do this we first prove in Proposition 1 that Conjecture 1 is closely related to

Conjecture 2 *Let* p *be a prime number and* k *be an integer. Denote by* $\mathscr{N}(k,p)$ *the number of vector subspaces of* $\mathbb{F}_p^k$. *Then*

$$\mathrm{Conj}^-_{\mathrm{mod}}(p,k) \qquad \mathscr{M}^-(p^{k\mathrm{rk}_p(\mathrm{C}_D^2)}) = \mathscr{N}(k,p),$$

and

$$\mathrm{Conj}^+_{\mathrm{mod}}(p,k) \qquad \mathscr{M}^+(p^{k\mathrm{rk}_p(\mathrm{C}_D^2)}) = p^{-k}(\mathscr{N}(k+1,p)-\mathscr{N}(k,p)).$$

Then we show that Conjecture 2 is true for $p=2$ and any $k \geq 0$. Actually, we shall prove a more precise statement for each of the six families of

$$\begin{cases} D<0, D\equiv 1 \bmod 4 \\ D<0, D\equiv 0 \bmod 8 \\ D<0, D\equiv 4 \bmod 8 \end{cases} \qquad \begin{cases} D>0, D\equiv 1 \bmod 4 \\ D>0, D\equiv 0 \bmod 8 \\ D>0, D\equiv 4 \bmod 8. \end{cases} \tag{3}$$

For this we introduce the sums:

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

and

$$S^+(X,k,a,b) := \sum_{\substack{0<D<X \\ D\equiv a \bmod b}} 2^{k\mathrm{rk}_4(\mathrm{C}_D)}.$$

Then we show in Theorems 6–11 that for every positive integer k and every positive ε the following equalities are true, where $R(X,\varepsilon,k) := X(\log X)^{-2^{-k}+\varepsilon}$:

$$S^-(X,k,1,4) = \mathscr{N}(k,2)\Big(\sum_{\substack{0<-D<X \\ D\equiv 1 \bmod 4}} 1\Big) + O_{\varepsilon,k}(R(X,\varepsilon,k)) \tag{4}$$

$$S^+(X,k,1,4) = \frac{1}{2^k}\big(\mathscr{N}(k+1,2)-\mathscr{N}(k,2)\big)\Big(\sum_{\substack{0<D<X \\ D\equiv 1 \bmod 4}} 1\Big) + O_{\varepsilon,k}(R(X,\varepsilon,k)) \tag{5}$$

$$S^-(X,k,0,8) = \mathscr{N}(k,2)\Big(\sum_{\substack{0<-D<X \\ D\equiv 0 \bmod 8}} 1\Big) + O_{\varepsilon,k}(R(X,\varepsilon,k)) \tag{6}$$

$$S^+(X,k,0,8) = \frac{1}{2^k}\big(\mathscr{N}(k+1,2)-\mathscr{N}(k,2)\big)\Big(\sum_{\substack{0<D<X \\ D\equiv 0 \bmod 8}} 1\Big) + O_{\varepsilon,k}(R(X,\varepsilon,k)) \tag{7}$$

$$S^-(X,k,4,8) = \mathscr{N}(k,2)\Big(\sum_{\substack{0<-D<X \\ D\equiv 4 \bmod 8}} 1\Big) + O_{\varepsilon,k}(R(X,\varepsilon,k)) \tag{8}$$

$$S^+(X,k,4,8)=\frac{1}{2^k}\big(\mathscr{N}(k+1,2)-\mathscr{N}(k,2)\big)\Big(\sum_{\substack{0<D<X\\ D\equiv 4 \bmod 8}}1\Big)+O_{\varepsilon,k}(R(X,\varepsilon,k)). \quad (9)$$

These theorems, combined with (16) and Proposition 1 imply Theorem 1 directly.

Cohen–Lenstra heuristics contains also statements (see [2, (C5),(C9)]) about the density of fundamental discriminants D such that $\mathrm{rk}_p(C_D^2)=r$ for some integer r. Again, the conjecture for odd p was extended to $p=2$ by Gerth. In order to state the conjecture we need to introduce the function η_k:

$$\eta_k(t):=\prod_{j=1}^{k}(1-t^{-j}) \text{ for } k \text{ a non-negative integer or } +\infty.$$

Conjecture 3 *Let r be a non negative integer and p be a prime number. Then*

1. *The density of negative fundamental discriminants D such that $\mathrm{rk}_p(C_D^2)=r$ is equal to*
$$p^{-r^2}\eta_\infty(p)\eta_r(p)^{-2}.$$
2. *The density of positive fundamental discriminants D such that $\mathrm{rk}_p(C_D^2)=r$ is equal to*
$$p^{-r(r+1)}\eta_\infty(p)\eta_r(p)^{-1}\eta_{r+1}(p)^{-1}.$$

It is a very natural question if Conjecture 1 and 3 are related to each other. In [5] we prove by techniques different from those presented in this work the following theorem.

Theorem 2 *Let p be a prime number. If Conjecture 1 is true for p and all $\alpha\geq 0$ for positive fundamental discriminants, then Conjecture 3 for positive fundamental discriminants is true for p and all $r\geq 0$. The analogous statement holds for negative fundamental discriminants.*

We remark that in general it is not true that the knowledge of all k–moments is sufficient to get those average densities.

We apply this theorem for $p=2$ and together with Theorem 1 we proved:

Theorem 3 *Conjecture 3 is true for $p=2$ and all $r\geq 0$.*

1.1 Known results about 4–ranks

The 4–rank of class groups of quadratic fields was studied in several papers of Redei, e.g. [16,17]. In [16] he defines an explicit matrix (the Redei matrix) over $\mathbb{F}_2$ such that the rank corresponds to the 4–rank of C_D. This matrix is used in Gerth [6] to compute probabilities that the 4–rank is a given number if we only consider discriminants D with a fixed number of prime factors. Let us shortly describe these results. We define the following quantities for $m>0$ squarefree, i.e. $D=m$ or $4m$ in our notation.

$$A_t:=\{K=\mathbb{Q}(\sqrt{-m}) \mid \text{ exactly } t \text{ primes ramify in } K\},$$

$$A_{t;X}:=\{K\in A_t \mid m\leq X\},\ A_{t,r;X}:=\{K\in A_{t;X} \mid \mathrm{rk}_4(K)=r\}.$$

Gerth proves that the following limits exist (and computes their values):

$$d_{t,r} := \lim_{X\to\infty} \frac{|A_{t,r;X}|}{|A_{t;X}|} \text{ and } d_{\infty,r} := \lim_{t\to\infty} d_{t,r}.$$

Denote by $B_t, B_{t;X}, B_{t,r;X}, d'_{t,r}$, and $d'_{\infty,r}$ the corresponding quantities when we consider totally real fields. Then the main result of [6] is:

Theorem 4 (Gerth)

$$\begin{aligned} d_{\infty,r} &= 2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2} && \text{for } r = 0,1,2,\ldots \\ d'_{\infty,r} &= 2^{-r(r+1)}\eta_\infty(2)\eta_r(2)^{-1}\eta_{r+1}(2)^{-1} && \text{for } r = 0,1,2,\ldots. \end{aligned}$$

We remark that Theorem 4 gave a strong support for the correctness of Conjecture 3 for $p = 2$.

In order to prove the correctness of equations (1) and (2) we introduce the following symbols.

Definition 2 Let $(a|b) : \mathbb{Q}^* \times \mathbb{Q}^* \to \{0,1\}$, where $(a|b) = 1$ if and only if the equation $x^2 - ay^2 - bz^2 = 0$ has a solution $(0,0,0) \neq (x,y,z) \in \mathbb{Q}^3$.

The 4–rank of the narrow class group can be described by the following theorem.

Theorem 5

$$2^{\mathrm{rk}_4(C_D)} = \frac{1}{2}\#\{b \mid b > 0 \textit{ squarefree}, b \mid D,\ (b|-b') = 1\},$$

where $b' \in \mathbb{Z}$ is squarefree such that $bD = b'c^2$ for a suitable $c \in \mathbb{Z}$.

1.2 Sketch of the proof

The schedule of the proofs is as follows. The first quite new idea is to write, for any p, the Cohen–Lenstra Heuristics $\mathrm{Conj}^{\pm}(p,\alpha)$, in an equivalent form, where the cardinalities of sets of vector spaces over $\mathbb{F}_p$ have a crucial role (see Proposition 1 below). Such an interpretation shows that the geometry over finite fields is subjacent in these heuristics. We are now obliged to restrict ourselves to $p = 2$. In §3 we prove Theorem 5, which roughly speaking, establishes a strong link between $2^{\mathrm{rk}_4(C_D)}$ and the number of representations of D as $D = ab$, with a being a square modulo $|b|$ and b being a square modulo $|a|$ (see Lemma 6 (ii)). Then the symbol $(a|b)$ can easily be transformed in terms of Jacobi symbols (see Lemma 6 and equation (20), for instance for $D < 0$ and $\equiv 1 \bmod 4$). Since we are studying the k–moment of $2^{\mathrm{rk}_4(C_D)}$, we raise (20) to the k-th power. This transformation gives birth to a sum of products of 4^k Jacobi symbols, with numerator and denominator taken in a set of 4^k independent variables. This expression is very intricate (see (25)) and must be dealt in a global way. However, for small values of k ($k = 1,2,3$) it could be dealt by hand. One of the question is to know which Jacobi symbols appear and which do not appear. We owe to E. Kowalski to have suggested that the paper of Heath–Brown [10] would be useful to simplify our approach, since this author met the same type of difficulty. Hence, we have incorporated several

ideas contained in [10], in the present paper. The first one is to write variables as $D_{\mathbf{u}}$ with $\mathbf{u} \in \mathbb{F}_2^{2k}$ and to use an homogeneous quadratic polynomial $\Phi_k(\mathbf{u},\mathbf{v})$ in two variables in $\mathbb{F}_2^{2k}$ to detect which Jacobi symbols $(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}})$ are present in the formulas (see definition (27)). We are led to use some concepts of geometry in characteristic 2. The error terms come from oscillations of the Jacobi symbols and cause no trouble: as in [9,10], we appeal to Siegel–Walfisz Theorem and to a double averaging over sums of real characters (see Lemmata 13 and 15 below). (Note that the application of [9, Lemma 6] is erroneous on p. 180 : the inequality (6) $A_{ij} \geq \exp\{\kappa(\log\log X)^2\}$ does not allow to apply Lemma 6, because of the constraint " $q \leq \log^N x$ ", which is not always satisfied in that case. A modification of [9, (6)] into $A_{ij} \geq X^{\ddagger}$ (where $X^{\ddagger}$ is defined below in (36)) is sufficient to correct the proof. The same remark applies to [10, p. 343]).

The nature of the main term is highly combinatorial. As in [10], we check that it can only come from the contribution of terms associated to $(D_{\mathbf{u}})_{\mathbf{u}\in\mathbb{F}_2^{2k}}$ such that exactly 2^k variables $D_{\mathbf{u}}$ are not equal to 1 and large (see Proposition 3). In particular, the associated indices build a coset of a vector space of dimension k (*maximal unlinked subset of indices*, see Lemma 18), on which a (non symmetric) bilinear form L is identically equal to 0 (Lemmata 24 and 25). The proof is then reduced to count such subspaces (Lemma 26). The combinatorial study is harder for D such that the number -1 and 2 have a specific role, it is why the five last families of the list (3) are studied in Sections 6 to 10. Hence, our proof has similarities with [10] (for instance by the choice of the terminology) but the combinatorics and the underlying geometry are different in several aspects.

The analytic methods involved in our work can be easily generalized to show that the Cohen–Lenstra–Gerth heuristics for the 4–rank is true for more general sequences of fundamental discriminants D, e.g. when D belongs to a fixed arithmetic progression modulo an odd integer. Such extensions of this method should be motivated by algebraic applications.

2 Cohen–Lenstra heuristics and cardinality of sets of vector subspaces

2.1 Counting vector subspaces in characteristic p

The purpose of this section is to prove that $\mathrm{Conj}^{\pm}(p,\alpha)$ can be expressed in terms of the cardinality of vector subspaces of $\mathbb{F}_p^k$ for some k. Before proving this equivalent form, we first gather all the necessary properties of the function $\mathfrak{n}(k,\ell,p)$ which denotes the number of linear subspaces of dimension ℓ in $\mathbb{F}_p^k$. These properties will be also used in the combinatorial analysis of the main terms in the formulas of Theorems 6–11 to express them with the help of the function

$$\mathscr{N}(k,p) := \sum_{\ell=0}^{k} \mathfrak{n}(k,\ell,p),$$

which counts the number of the vector subspaces of $\mathbb{F}_p^k$ of any dimension. We have

Lemma 1 *Let k and ℓ be integers, then the function $\mathfrak{n}(k,\ell,p)$ satisfies the equalities*

- $\mathfrak{n}(k,\ell,p)=0$ *for* $k<0$, $\ell<0$ *or* $\ell>k$,
- $\mathfrak{n}(k,\ell,p)=\mathfrak{n}(k,k-\ell,p)$ *for* $k\geq 0$,
- $\mathfrak{n}(k,\ell,p)=\prod_{i=0}^{\ell-1}\frac{p^k-p^i}{p^\ell-p^i}=\prod_{i=1}^{\ell}\frac{p^{k-i+1}-1}{p^i-1}$ *for* $k\geq 0$ *and* $\ell\geq 0$,
- $\mathfrak{n}(k,\ell,p)=\mathfrak{n}(k-1,\ell-1,p)+p^\ell\mathfrak{n}(k-1,\ell,p)$ *for* $k\geq 1$ *and* $\ell\geq 0$.

Proof The three first equalities are classical. The fourth one is a direct consequence of the third one and of the equality $(p^k-1)=(p^\ell-1)+p^\ell(p^{k-\ell}-1)$, which is used in the case $0\leq\ell\leq k$. □

The proof of the following lemma is straightforward.

Lemma 2 *Let $k\geq 0$ and ℓ be integers. Let ξ be a non zero vector of $\mathbb{F}_p^k$. Then the number of vector subspaces of $\mathbb{F}_p^k$ of dimension ℓ containing ξ is equal to $\mathfrak{n}(k-1,\ell-1,p)$.*

Now we collect some properties of the function $\mathscr{N}(k,p)$.

Lemma 3 *For any $k\geq 1$, we have*

$$2\mathscr{N}(k,p)+(p^k-1)\mathscr{N}(k-1,p)=\mathscr{N}(k+1,p), \tag{10}$$

$$\sum_{\ell=0}^{k}p^{-\ell}\mathfrak{n}(k,\ell,p)=\frac{1}{p^k}\big(\mathscr{N}(k+1,p)-\mathscr{N}(k,p)\big), \tag{11}$$

and

$$\sum_{\ell=0}^{k}p^{\ell}\mathfrak{n}(k,\ell,p)=\mathscr{N}(k+1,p)-\mathscr{N}(k,p). \tag{12}$$

Proof By applying the third equality of Lemma 1 twice, we deduce the equality

$$(p^{k-\ell}-1)\mathfrak{n}(k,\ell,p)=(p^k-1)\mathfrak{n}(k-1,\ell,p),$$

which is equivalent to

$$2\mathfrak{n}(k,\ell,p)+(p^k-1)\mathfrak{n}(k-1,\ell,p)=(p^{k-\ell}+1)\mathfrak{n}(k,\ell,p).$$

Summing over all ℓ, we get

$$2\mathscr{N}(k,p)+(p^k-1)\mathscr{N}(k-1,p)=\sum_{\ell=0}^{k}(p^{k-\ell}+1)\,\mathfrak{n}(k,\ell,p). \tag{13}$$

We also have by symmetry (second equality of Lemma 1):

$$\sum_{\ell=0}^{k}(p^{k-\ell}+1)\mathfrak{n}(k,\ell,p)=\sum_{\ell=0}^{k}(p^{\ell}+1)\,\mathfrak{n}(k,\ell,p)=\sum_{\ell=0}^{k}p^{\ell}\mathfrak{n}(k,\ell,p)+\sum_{\ell=0}^{k+1}\mathfrak{n}(k,\ell-1,p),$$

and this is equal to

$$\sum_{\ell=0}^{k+1}\big(p^{\ell}\,\mathfrak{n}(k,\ell,p)+\mathfrak{n}(k,\ell-1,p)\big)=\mathscr{N}(k+1,p),$$

by the fourth equality of Lemma 1. Combining with (13), we get (10).

For the proof of (11), we use the second and the fourth equality of Lemma 1 to write

$$\sum_{\ell=0}^{k}p^{-\ell}\mathfrak{n}(k,\ell,p)=\frac{1}{p^k}\sum_{\ell=0}^{k}p^{\ell}\mathfrak{n}(k,\ell,p)=\frac{1}{p^k}\sum_{\ell=0}^{k}\big(\mathfrak{n}(k+1,\ell,p)-\mathfrak{n}(k,\ell-1,p)\big),$$

Hence the result. The proof of (12) works similarly. □

2.2 An equivalent form of Conjecture 1

We shall modify $\mathrm{Conj}^{\pm}(p,\alpha)$ by appealing to the function $\mathscr{N}$ and by proving

Proposition 1 *Let p be a prime number and $\alpha_0>0$. Then $\mathrm{Conj}^{+}(p,\alpha)$ is true for every $0\le\alpha\le\alpha_0$, if and only if $\mathscr{M}^{+}(p^{\alpha\,\mathrm{rk}_p(\mathrm{C}_D^2)})$ exists and has the value*

$$\mathrm{Conj}^{+}_{\mathrm{mod}}(p,\alpha):\qquad \mathscr{M}^{+}(p^{\alpha\,\mathrm{rk}_p(\mathrm{C}_D^2)})=p^{-\alpha}\big(\mathscr{N}(\alpha+1,p)-\mathscr{N}(\alpha,p)\big),$$

for every $0\le\alpha\le\alpha_0$.

Similarly, $\mathrm{Conj}^{-}(p,\alpha)$ is true for every $0\le\alpha\le\alpha_0$, if and only if the mean value $\mathscr{M}^{-}(p^{\alpha\,\mathrm{rk}_p(\mathrm{C}_D^2)})$ exists and has the value

$$\mathrm{Conj}^{-}_{\mathrm{mod}}(p,\alpha):\qquad \mathscr{M}^{-}(p^{\alpha\,\mathrm{rk}_p(\mathrm{C}_D^2)})=\mathscr{N}(\alpha,p),$$

for every $0\le\alpha\le\alpha_0$.

Proof It is an exercise in the theory of polynomials. Let $k\ge0$ and $Q_{k,p}(X)$ be the polynomial

$$Q_{k,p}(X)=\prod_{i=0}^{k-1}(X-p^i),$$

with the usual convention $Q_{0,p}\equiv1$. We have

Lemma 4 *For every prime p and every $n\ge0$, we have the equality*

$$X^n=\sum_{k=0}^{+\infty}\mathfrak{n}(n,k,p)\,Q_{k,p}(X).$$

Proof This lemma is true for $n = 0$. The proof is made by induction over n. By the hypothesis of induction, the definition of $Q_{k+1,p}$, and the fourth equality of Lemma 1, we have the equalities

$$\begin{aligned} X^{n+1} &= \sum_{k=0}^{+\infty} \mathfrak{n}(n,k,p)(X - p^k + p^k)\, Q_{k,p}(X) \\ &= \sum_{k=0}^{+\infty} \big(\mathfrak{n}(n,k-1,p) + p^k \mathfrak{n}(n,k,p)\big)\, Q_{k,p}(X) \\ &= \sum_{k=0}^{+\infty} \mathfrak{n}(n+1,k,p)\, Q_{k,p}(X). \end{aligned}$$

□

To prove Proposition 1, we first use Lemma 4 to write

$$p^{\alpha \mathrm{rk}_p(\mathrm{C}_D^2)} = \sum_{k=0}^{\alpha} \mathfrak{n}(\alpha,k,p) Q_{k,p}(p^{\mathrm{rk}_p(\mathrm{C}_D^2)}). \tag{14}$$

Hence, if each term of the right hand side of (14) has a mean value, the left hand side has also a mean value. By linearity of mean values, we have

$$\mathscr{M}^{\pm}\big(p^{\alpha \mathrm{rk}_p(\mathrm{C}_D^2)}\big) = \sum_{k=0}^{\alpha} \mathfrak{n}(\alpha,k,p) \mathscr{M}^{\pm}\big(Q_{k,p}(p^{\mathrm{rk}_p(\mathrm{C}_D^2)})\big). \tag{15}$$

Now we see that assuming the truth of $\mathrm{Conj}^{\pm}(p,k)$ for $k \leq \alpha$ implies the truth of $\mathrm{Conj}^{\pm}_{\mathrm{mod}}(p,\alpha)$ by the definition of $\mathscr{N}(\alpha,p)$, in the case of $\mathscr{M}^{-}$, or by (11), in the case of $\mathscr{M}^{+}$.

Reciprocally, suppose that $\mathrm{Conj}^{\pm}_{\mathrm{mod}}(p,\alpha)$ is true for every $0 \leq \alpha \leq \alpha_0$. Let $0 \leq \alpha \leq \alpha_0$ be the smallest number for which $\mathrm{Conj}^{\pm}(p,\alpha)$ is not true. Since $\mathfrak{n}(\alpha,\alpha,p) = 1$, the equality (15) then imply a contradiction. □

3 The 4–rank of class groups of quadratic fields

The goal of this section is to prove Theorem 5. Furthermore we study the relation between the ordinary and the narrow class group.

3.1 Properties of $(a|b)$

We start by collecting some properties of the symbol defined in Definition 2. We remark that $(a|b) = 1$ if and only if b is a norm in $\mathbb{Q}(\sqrt{a})$. Note that in the case that a is a square in $\mathbb{Q}$ the field $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}$ and any element is trivially a norm. We get the following easy properties:

Lemma 5 *Let $a,b,c \in \mathbb{Q}^*$. Then we have:*

1. $(a|b) = (b|a)$, $(a|1) = 1$, $(ac^2|b) = (a|b)$, $(a|-a) = 1$,

2. $(a|b) = (a|-ab)$.

Proof The first part is obvious from the definition. For the second part make the following change of variables in the definition: $x = ay', y = x', z = az'$ and divide by $-a$. □

The proof of the next lemma can be found in [18, Theorem 8, p. 41]. This is a particular case of Legendre's theorem for ternary quadratic forms.

Lemma 6 *Let a,b be squarefree and coprime integers with $b > 0$. Then the following statements are equivalent:*

1. $(a|b) = 1$.
2. *a is a square mod b and b is a square mod $|a|$.*

Since every odd number is a square modulo 2 we immediately get the following statement.

Lemma 7 *Let a,b be squarefree, odd, and coprime integers with $b > 0$. Then the following statements are equivalent:*

1. $(2a|2b) = 1$.
2. *$2a$ is a square mod b and $2b$ is a square mod $|a|$.*

For a non–zero integer b we denote by $[b]$ the squarefree integer with $[b] = bc^2$ for a suitable $c \in \mathbb{Q}^*$. Furthermore for a positive $b \mid D$ we define $b' := [bD] \in \mathbb{Z}$. We remark that $b' < 0$ if and only if $D < 0$. Using this we can prove the following lemma.

Lemma 8 *Let $b > 0$ be a squarefree divisor of D. Then $(D|b) = (b|-b')$.*

Proof Using Lemma 5 we get:

$$(b|-b') = (b|bb') = (b|b[bD]) = (b|[b^2D]) = (b|D) = (D|b).$$

□

3.2 The narrow class group

We start by proving Theorem 5 which is already implicitly contained in [16, p. 56]. Denote by P in C_D, the class of principal ideals generated by totally positive elements α. We remark that in a real quadratic field an element α with positive norm has the property that α or $-\alpha$ is totally positive.

We remark that all primes p which divide D are ramified. Furthermore all classes of order 2 are generated by prime ideals lying above these primes. We denote by $p_1, \dots, p_t$ the prime divisors of D and by $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O}_K$ the unique prime ideals of norm p_i in the maximal order $\mathcal{O}_K$ of K. In case $t > 1$ we get that these prime ideals have order 2 in C_D. Denote by $\tilde{D}$ the squarefree number with $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{\tilde{D}})$. Then there exists a principal ideal of norm $|\tilde{D}|$ generated by $\sqrt{\tilde{D}}$. Using this we get the only non–trivial relation of the group C_D/C_D^2 of order 2^{t-1} generated by $\mathfrak{p}_1, \dots, \mathfrak{p}_t$. If we look at the classes in C_D/C_D^2 represented by

$$\mathcal{B} := \{\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t} \mid e_i \in \{0,1\},\ 1 \le i \le t\},$$

then each class is represented exactly twice.

Lemma 9

1. $2^{\mathrm{rk}_4(C_D)} = \#\{B^2 \in C_D \mid B^4 = P\}$.
2. $2^{\mathrm{rk}_4(C_D)} = \frac{1}{2}\#\{\mathfrak{b} \in \mathscr{B} \mid \mathfrak{a}^2 = (\alpha)\mathfrak{b}$ *for suitable* $\mathfrak{a}$ *and totally positive* $\alpha\}$.

Proof The first part is obvious from the definition of the 4–rank. Using the first part and the above discussion we get the second part. □

Now we are able to prove Theorem 5.

Proof (Theorem 5) We use the second part of Lemma 9 and show that an ideal $\mathfrak{b} \in \mathscr{B}$ of norm b has the desired property if and only if $(b|-b') = 1$.

Now assume that a squarefree $b > 0$ dividing D has the property that $(b|-b') = 1 = (D|b)$ using Lemma 8. Therefore b is a norm in $K = \mathbb{Q}(\sqrt{D})$ and by clearing denominators we find an $\alpha \in \mathscr{O}_K$ such that $\mathscr{N}(\alpha) = bw^2$, where $\mathscr{N}$ denotes the norm function and $w \in \mathbb{N}$. Since $\mathscr{N}(\alpha) > 0$ we get that α or $-\alpha$ is totally positive. W.l.o.g. we can assume that $\alpha/p \notin \mathscr{O}_K$ for all prime numbers p. Ideals of norm p^2 are either principal ideals generated by p or a square of an ideal of norm p. Since $\alpha/p \notin \mathscr{O}_K$ no principal ideals generated by a prime p divide (α) and we get $(\alpha) = \mathfrak{b}\mathfrak{a}^2$, where $\mathfrak{b}$ is the unique ideal of norm b and $\mathscr{N}(\mathfrak{a}) = w$.

Now assume that $\mathfrak{a}^2 = (\alpha)\mathfrak{b}$ with the above properties. Then

$$\mathscr{N}(\alpha) = b\frac{\mathscr{N}(\mathfrak{a})^2}{b^2}.$$

Therefore $1 = (D|b) = (b|-b')$. □

3.3 The ordinary class group

In order to compute $\mathrm{rk}_4(\mathrm{Cl}_D)$ we need to know the relation between Cl_D and C_D. It is well known that we have an exact sequence

$$1 \to F_\infty \to C_D \to \mathrm{Cl}_D \to 1,$$

where $F_\infty \leq \mathbb{Z}/2\mathbb{Z}$. Furthermore $|F_\infty| = 2$ if and only if $D > 0$ and $\mathscr{N}(\varepsilon) = 1$, where ε is the fundamental unit of $\mathscr{O}_K$ (see e.g. [15, Corollary 2, p. 112]). To compare the structures of C_D and Cl_D we use the following result (see e.g. [15, Corollary 1, p. 457 and note 20, p. 483] and [13, Theorem 1, p. VII-6]).

Lemma 10 *Let $D > 0$ be a discriminant with $|F_\infty| = 2$. Then the following two statements are equivalent:*

1. $C_D \cong \mathbb{Z}/2\mathbb{Z} \times \mathrm{Cl}_D$.
2. *There exists a prime $p \mid D$ such that $p \equiv 3 \bmod 4$.*

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

This immediately implies that when all odd prime divisors of D are congruent to 1 mod 4 the 2–ranks of C_D and Cl_D coincide. If $\mathscr{N}(\varepsilon) = 1$, i.e. $|F_\infty| = 2$ this means that there exists an $r > 1$ such that $\mathrm{rk}_{2^r}(C_D) = \mathrm{rk}_{2^r}(\mathrm{Cl}_D) + 1$. We define $\varepsilon_D \in \{0,1\}$ by the equation $\mathrm{rk}_4(C_D) = \mathrm{rk}_4(\mathrm{Cl}_D) + \varepsilon_D$. We already proved that $\varepsilon_D = 0$ if there is a prime congruent to 3 mod 4 dividing D, or if the fundamental unit has norm -1.

Now we are able to prove that our main statements remain true if we replace C_D by Cl_D.

Corollary 1 *The equations* (4)–(9) *remain true when we replace C_D by the ordinary class group* Cl_D *in the definition of* $S^{\pm}(X,k,a,b)$.

Proof We have nothing to prove for negative discriminants or for discriminants $D \equiv 4 \mod 8$. For positive D we deduce from Lemma 10 the inequalities

$$\mathrm{rk}_4(C_D) - 1 \leq \mathrm{rk}_4(\mathrm{Cl}_D) \leq \mathrm{rk}_4(C_D)$$

and if the equality $\mathrm{rk}_4(C_D) - 1 = \mathrm{rk}_4(\mathrm{Cl}_D)$ holds, then all odd prime divisors of D are congruent to 1 mod 4. In the case $D \equiv 1 \mod 4$ we get using Hölder's inequality that the error is bounded above by

$$\sum_{\substack{0<D<X, D\equiv 1 \bmod 4 \\ p\mid D \Rightarrow p\equiv 1 \bmod 4}} 2^{k\,\mathrm{rk}_4(\mathrm{Cl}_D)} \leq \Big(\sum_{\substack{0<D<X, \\ p\mid D \Rightarrow p\equiv 1 \bmod 4}} 1\Big)^{1/a} \Big(\sum_{0<D<X, D\equiv 1 \bmod 4} 2^{bk\,\mathrm{rk}_4(\mathrm{Cl}_D)}\Big)^{1/b},$$

where $b \geq 2$ is an integer, and a satisfies $\frac{1}{a} + \frac{1}{b} = 1$. Using Landau's theorem (see e.g. [1, Satz 1.8.2]) and equality (5) we get that the above expression for the error is less than

$$\ll_{b,k} \left(\frac{X}{\sqrt{\log X}}\right)^{1/a} \cdot X^{1/b} \ll_{b,k} X(\log X)^{-\frac{1}{2a}} \ll_{\varepsilon,k} X(\log X)^{-\frac{1}{2}+\varepsilon}$$

for every positive ε, by choosing b large enough. A similar estimate can be given for the case $D \equiv 0 \mod 8$. □

4 Analytic tools

Let us first recall some well known counting formulas of fundamental discriminants

$$\begin{cases} \displaystyle\sum_{\substack{0<D<X \\ D\equiv 1 \bmod 4}} 1, \quad \sum_{\substack{0<-D<X \\ D\equiv 1 \bmod 4}} 1 = \frac{2}{\pi^2} X + O\big(X^{\frac{1}{2}}\big), \\ \displaystyle\sum_{\substack{0<D<X \\ D\equiv 0 \bmod 8}} 1, \quad \sum_{\substack{0<-D<X \\ D\equiv 0 \bmod 8}} 1, \quad \sum_{\substack{0<D<X \\ D\equiv 4 \bmod 8}} 1, \quad \sum_{\substack{0<-D<X \\ D\equiv 4 \bmod 8}} 1 = \frac{1}{2\pi^2} X + O\big(X^{\frac{1}{2}}\big), \end{cases} \tag{16}$$

which are extensions of the well known formula

$$\sum_{n\leq X} \mu^2(n) = \frac{6}{\pi^2} X + O(X^{\frac{1}{2}}),$$

which counts the number of squarefree integers $n \leq X$ (here μ is the Möbius function).

Our proof will start by a technical preparation of the integer variables. E.g. we shall eliminate those with too many prime factors by appealing to a classical result of Hardy and Ramanujan [8, Lemma A, p. 265]:

Lemma 11 *There exists an absolute constant B_0, such that for every $X \geq 3$, for every $\ell \geq 0$, we have*

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

We shall frequently use the classical result:

Lemma 12 *Let γ be a positive real number. Then we have*

$$\sum_{X-Y<n\leq X} \gamma^{\omega(n)} \ll Y(\log X)^{\gamma-1},$$

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

Proof Consider the Dirichlet series $F(s) := \sum \gamma^{\omega(n)} n^{-s}$, use the classical zero–free region for the Riemann zeta–function to express $F(s)$ in terms of $\zeta^\gamma(s)$ and perform a complex integration with Perron formula. □

For stronger results, see [19, Theorem 1] for instance.

We appeal to one of numerous forms of Siegel–Walfisz theorem [14, Corollary 5.29]:

Lemma 13 *For every $q \geq 2$, for every primitive character $\chi \bmod q$, and for every $A > 0$ we have*

$$\sum_{y\leq p\leq x} \chi(p) \ll_A \sqrt{q}x(\log x)^{-A},$$

uniformly for $x \geq y \geq 2$.

We shall also benefit from double oscillation of characters by using the following result of Heath–Brown [11, Corollary 4, p. 238]. (However, some weaker result having its origin in [12] would be sufficient for our purpose.)

Lemma 14 *Let a_m and b_n be complex numbers of modulus less than 1. Then for every $M, N \geq 1$ and for every positive ε we have*

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

This result covers many of the cases we will encounter. However, to circumvent the extra factor $(MN)^\varepsilon$ which causes trouble when M and N are of completely different sizes, we shall also use

Lemma 15 *Let a_m and b_n be complex numbers of modulus less than 1. Then, for every $M, N \geq 1$ we have*

$$\sum_{m\leq M}\sum_{n\leq N} a_m b_n \mu^2(2m)\mu^2(2n)\Big(\frac{n}{m}\Big) \ll MN\min\big\{\big(M^{-\frac{1}{2}} + (N/M)^{-\frac{1}{2}}\big), \big(N^{-\frac{1}{2}} + (M/N)^{-\frac{1}{2}}\big)\big\}, \quad (17)$$

and for every positive ε, we have

$$\sum_{m\leq M}\sum_{n\leq N} a_m b_n \mu^2(2m)\mu^2(2n)\Big(\frac{n}{m}\Big) \ll_\varepsilon MN\big(M^{-\frac{1}{2}+\varepsilon} + N^{-\frac{1}{2}+\varepsilon}\big). \quad (18)$$

Proof Formula (17) is a consequence of the large sieve for primitive characters (see [14, Theorem 7.13], for instance). By Cauchy–Schwarz inequality and positivity, we have

$$\begin{aligned}
&\Big|\sum_{m\leq M}\sum_{n\leq N} a_m b_n \mu^2(2m)\mu^2(2n)\big(\frac{n}{m}\big)\Big| \\
&\leq M^{\frac{1}{2}}\Big\{\sum_{m\leq M}\mu^2(2m)\Big|\sum_{n\leq N}\mu^2(2n)b_n\big(\frac{n}{m}\big)\Big|^2\Big\}^{\frac{1}{2}} \\
&\leq M^{\frac{1}{2}}\Big\{\sum_{m\leq M}\sum_{\chi \text{ prim mod } m}\Big|\sum_{n\leq N}\mu^2(2n)b_n\chi(n)\Big|^2\Big\}^{\frac{1}{2}} \ll M^{\frac{1}{2}}\big((M^2+N)N\big)^{\frac{1}{2}},
\end{aligned}$$

since, for odd squarefree positive m, the application $n\mapsto\big(\frac{n}{m}\big)$ is a primitive character of conductor m. The other part of the inequality of Lemma 15 comes from an application of Cauchy–Schwarz inequality to $\sum_n|\sum_m|$, from large sieve inequality and from the fact that for odd squarefree positive n the application $m\mapsto\big(\frac{n}{m}\big)$ is a primitive character of conductor n or $4n$.

Now (18) is an easy consequence of Lemma 14 and of (17). By symmetry, we can suppose the inequality $M\leq N$. Then if $M\leq N\leq M^2$, we apply Lemma 14 and notice that $(MN)^{\varepsilon}\leq M^{3\varepsilon}$. Finally, for $N>M^2$, (17) gives the bound

$$\ll MN\big(M^{-\frac{1}{2}}+(N/M)^{-\frac{1}{2}}\big)\ll MN\cdot M^{-\frac{1}{2}+\varepsilon}.$$

□

5 Proof of Theorem 1 in the case of odd negative discriminants.

5.1 From 4–ranks to products of Jacobi symbols.

In that section, we shall restrict to fundamental discriminant D satisfying

$$D<0,\ \ D\equiv 1 \bmod 4. \tag{19}$$

This is the simplest case since it does not take into account the quadratic structure of -1 and 2 modulo p. In Sections 6 to 10, we shall indicate how to extend these results to other fundamental discriminants, negative or positive, odd or even.

We plan to study the moments of the quantity $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ over the set of D satisfying (19), which means to study the sum

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

for k a positive integer and for $X\to+\infty$. We shall prove

Theorem 6 *For every positive integer k and every positive ε, we have*

$$S^-(X,k,1,4)=\mathscr{N}(k,2)\Big(\sum_{\substack{0<-D<X\\ D\equiv 1 \bmod 4}}1\Big)+O_{\varepsilon,k}\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big),$$

uniformly for $X\geq 2$.

With the words of Definition 1, we shall prove that $\mathscr{N}(k,2)$ is the mean value of $2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}$ on the set of negative odd fundamental discriminants D.

When D satisfies (19), we easily deduce from Theorem 5 and Lemma 6 the following

Lemma 16 *Let D be a fundamental discriminant satisfying* (19)*. Then we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2}\,\#\big\{(a,b) \mid a,b \geq 1, -D = ab, \textit{ a is a square } \bmod b \\ \textit{and b is a square } \bmod a\big\}.$$

Now we use the Jacobi symbol $\left(\frac{a}{b}\right)$ (for odd $b \geq 1$) to detect if a is a square $\bmod\ b$ with the formula

$$\frac{1}{2^{\omega(b)}}\prod_{p\mid b}\left(1+\left(\frac{a}{p}\right)\right) = \frac{1}{2^{\omega(b)}}\sum_{c\mid b}\left(\frac{a}{c}\right).$$

Using Lemma 16 we get

$$2^{\mathrm{rk}_4(C_D)} = \frac{1}{2\cdot 2^{\omega(-D)}}\sum_{-D=ab}\left(\sum_{c\mid b}\left(\frac{a}{c}\right)\right)\left(\sum_{d\mid a}\left(\frac{b}{d}\right)\right),$$

which gives us with the change of variables $a = D_2D_3$, $b = D_0D_1$, $c = D_0$, and $d = D_3$ the following:

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(-D)}}\sum_{-D=D_0D_1D_2D_3}\left(\frac{D_2}{D_0}\right)\left(\frac{D_1}{D_3}\right)\left(\frac{D_3}{D_0}\right)\left(\frac{D_0}{D_3}\right), \tag{20}$$

always under the assumption that D satisfies (19).

Note that we do not yet appeal to the quadratic reciprocity law. We follow the idea of Heath–Brown [10], to use the field $\mathbb{F}_2$ to create indices for the variables on the right–hand side of (20) and then make geometry in characteristic 2. We replace each index 0, 1, 2 and 3 by its expansion in basis 2 : 00, 01, 10, 11, which are viewed as elements of $\mathbb{F}_2^2$. For $(\mathbf{u},\mathbf{v}) = (u_1,u_2,v_1,v_2) \in \mathbb{F}_2^2\times\mathbb{F}_2^2$, we consider the polynomial

$$\Phi_1(\mathbf{u},\mathbf{v}) := (u_1+v_1)(u_1+v_2).$$

This polynomial can be seen as the analogue of B used by Heath–Brown [10, p. 338]. The function Φ_1 is useful to detect which Jacobi symbols appear in (20). We have

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(-D)}}\sum_{-D=D_{00}D_{01}D_{10}D_{11}}\ \prod_{(\mathbf{u},\mathbf{v})\in\mathbb{F}_2^4}\left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\right)^{\Phi_1(\mathbf{u},\mathbf{v})}, \tag{21}$$

since the equation $\Phi_1(\mathbf{u},\mathbf{v}) = 1$ has only solutions for the quadruples $(1,0,0,0)$, $(0,1,1,1)$, $(1,1,0,0)$ and $(0,0,1,1)$. In (21), we interpret the exponents 0 and $1\in\mathbb{F}_2$ as 0 and $1\in\mathbb{N}$, with the convention $0^0 = 1$. Since we study the k–moment,

our next task is to raise (21) to the k–th power. Hence we have to parameterize the solutions of the k–fold equation

$$-D=\prod_{\mathbf{u}^{(1)}\in\mathbb{F}_2^2}D^{(1)}_{\mathbf{u}^{(1)}}=\cdots=\prod_{\mathbf{u}^{(k)}\in\mathbb{F}_2^2}D^{(k)}_{\mathbf{u}^{(k)}}. \tag{22}$$

To perform this we introduce the greatest common divisor (g.c.d.) of variables:

$$D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(k)}}:=\text{g.c.d.}\big(D^{(1)}_{\mathbf{u}^{(1)}},\dots,D^{(k)}_{\mathbf{u}^{(k)}}\big)$$

to write the factorization

$$D^{(\ell)}_{\mathbf{u}^{(\ell)}}=\prod_{\substack{1\leq n\leq k\\ n\neq\ell}}\prod_{\mathbf{u}^{(n)}\in\mathbb{F}_2^2}D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(\ell)},\dots,\mathbf{u}^{(k)}}. \tag{23}$$

These are the solutions of (22), provided that the $D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(k)}}$ satisfy the equality

$$-D=\prod_{1\leq n\leq k}\prod_{\mathbf{u}^{(n)}\in\mathbb{F}_2^2}D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(k)}}. \tag{24}$$

Reciprocally, starting from the decomposition (24) of $-D$ into the product of 4^k integers, we deduce solutions to (22), by grouping variables as in (23). Raising (21) to the k–th power, we get

$$\begin{aligned}2^{k\mathrm{rk}_4(\mathrm{C}_D)}&=\frac{1}{2^k\cdot 2^{k\omega(-D)}}\\&\times\sum_{D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(k)}}}\cdots\sum\prod_{(\mathbf{u}^{(1)},\mathbf{v}^{(1)})\in\mathbb{F}_2^4}\Big(\frac{D^{(1)}_{\mathbf{u}^{(1)}}}{D^{(1)}_{\mathbf{v}^{(1)}}}\Big)^{\Phi_1(\mathbf{u}^{(1)},\mathbf{v}^{(1)})}\cdots\prod_{(\mathbf{u}^{(k)},\mathbf{v}^{(k)})\in\mathbb{F}_2^4}\Big(\frac{D^{(k)}_{\mathbf{u}^{(k)}}}{D^{(k)}_{\mathbf{v}^{(k)}}}\Big)^{\Phi_1(\mathbf{u}^{(k)},\mathbf{v}^{(k)})},\end{aligned}$$

where the $D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(k)}}$ satisfy (24), and the $D^{(\ell)}_{\mathbf{u}^{(\ell)}}$ and the $D^{(\ell)}_{\mathbf{v}^{(\ell)}}$ are defined by (23).

By the multiplicative properties of Jacobi symbols and the decomposition given by equality (23), we obtain the equality

$$\begin{aligned}2^{k\mathrm{rk}_4(\mathrm{C}_D)}=&\frac{1}{2^k\cdot 2^{k\omega(-D)}}\\&\times\sum_{D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(k)}}}\cdots\sum\prod_{\substack{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(k)}\\ \mathbf{v}^{(1)},\dots,\mathbf{v}^{(k)}}}\left(\frac{D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(k)}}}{D_{\mathbf{v}^{(1)},\dots,\mathbf{v}^{(k)}}}\right)^{\Phi_1(\mathbf{u}^{(1)},\mathbf{v}^{(1)})+\cdots+\Phi_1(\mathbf{u}^{(k)},\mathbf{v}^{(k)})}.\end{aligned} \tag{25}$$

We now introduce the elements of $(\mathbb{F}_2^2)^k$, $\mathbf{u}=(\mathbf{u}^{(1)},\dots,\mathbf{u}^{(k)})=(u_1,\cdots,u_{2k})$ and $\mathbf{v}=(\mathbf{v}^{(1)},\dots,\mathbf{v}^{(k)})=(v_1,\cdots,v_{2k})\in\mathbb{F}_2^{2k}$, and we sum the formula (25) over all the $-D\leq X$ satisfying (19), to finally obtain

Lemma 17 *For every positive X we have the equality*

$$S^-(X,k,1,4) = 2^{-k} \sum_{(D_{\mathbf{u}})\in\mathscr{D}^-(X,k)} \Big(\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big) \prod_{\mathbf{u},\mathbf{v}} \Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u},\mathbf{v})}, \tag{26}$$

where $\mathscr{D}^-(X,k)$ is the set of 4^k–tuples of squarefree, positive and coprime integers $(D_{\mathbf{u}})$, with $\mathbf{u} = (\mathbf{u}^{(1)},\dots,\mathbf{u}^{(k)}) \in \mathbb{F}_2^{2k}$ satisfying

$$\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} D_{\mathbf{u}} \le X, \quad \prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} D_{\mathbf{u}} \equiv -1 \bmod 4,$$

and

$$\begin{aligned}\Phi_k(\mathbf{u},\mathbf{v}) &= \Phi_1(\mathbf{u}^{(1)},\mathbf{v}^{(1)}) + \cdots + \Phi_1(\mathbf{u}^{(k)},\mathbf{v}^{(k)}) \\ &= (u_1+v_1)(u_1+v_2) + \cdots + (u_{2k-1}+v_{2k-1})(u_{2k-1}+v_{2k}).\end{aligned} \tag{27}$$

5.2 Linked variables.

Inspired by [10, p. 338], we say that the variables $D_{\mathbf{u}}$ and $D_{\mathbf{v}}$ (or the indices $\mathbf{u}$ and $\mathbf{v}$) are *linked*, if they satisfy the equality

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

In other words, this means that in (26), exactly one of the symbols $\left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\right)$ or $\left(\frac{D_{\mathbf{v}}}{D_{\mathbf{u}}}\right)$ appears with exponent 1. Let P be the quadratic form over $\mathbb{F}_2^{2k}$ defined by

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

The quadratic form P satisfies the equality $P(\mathbf{u}+\mathbf{v}) = \Phi_k(\mathbf{u},\mathbf{v}) + \Phi_k(\mathbf{v},\mathbf{u})$. Hence, $D_{\mathbf{u}}$ and $D_{\mathbf{v}}$ are linked if and only if $P(\mathbf{u}+\mathbf{v}) = 1$. They are unlinked if and only if $P(\mathbf{u}+\mathbf{v}) = 0$.

5.3 Number of prime factors of the variables.

Let

$$\Omega = \mathrm{e}\,4^k(\log\log X + B_0), \tag{28}$$

with B_0 defined in Lemma 11. Denote by $\tau_k(n)$ the number of ways of writing the integer n as product of k positive integers.

Let Σ_1 be the contribution to the right part of (26) of the $(D_{\mathbf{u}})_{\mathbf{u}\in\mathbb{F}_2^{2k}}$ which do not satisfy

$$\omega(D_{\mathbf{u}}) \le \Omega, \text{for all } \mathbf{u} \in \mathbb{F}_2^{2k}. \tag{29}$$

We write $n=\prod_{\mathbf{u}} D_{\mathbf{u}}$, and we use the Cauchy–Schwarz inequality to see that

$$\begin{aligned}\Sigma_1 &\ll \sum_{\substack{n\leq X\\ \omega(n)\geq \Omega}} \mu^2(n)\tau_{4^k}(n)2^{-k\omega(n)} \ll \sum_{\substack{n\leq X\\ \omega(n)\geq \Omega}} \mu^2(n)\tau_{2^k}(n)\\ &\ll \Big(\sum_{\substack{n\leq X\\ \omega(n)\geq \Omega}} \mu^2(n)\Big)^{\frac{1}{2}}\Big(\sum_{n\leq X} 4^{k\omega(n)}\Big)^{\frac{1}{2}}.\end{aligned}$$

By Lemmata 11 and 12 and by Stirling's formula, this contribution also satisfies

$$\begin{aligned}\Sigma_1 &\ll \Big(\frac{X}{\log X}\sum_{\ell>\Omega}\frac{(\log\log X+B_0)^\ell}{\ell!}\Big)^{\frac{1}{2}}\Big(X(\log X)^{4^k-1}\Big)^{\frac{1}{2}}\\ &\ll X(\log X)^{2^{2k-1}-1}\Big(\sum_{\ell>\Omega}\big(\frac{\log\log X+B_0}{\ell/\mathrm{e}}\big)^\ell\Big)^{\frac{1}{2}} \ll X(\log X)^{2^{2k-1}-1}\Big(\sum_{\ell>\Omega}4^{-k\ell}\Big)^{\frac{1}{2}}\\ &\ll X2^{-k\Omega}(\log X)^{2^{2k-1}-1},\end{aligned}$$

which, for $k\geq 1$, finally gives

$$\Sigma_1 \ll X(\log X)^{-1}, \tag{30}$$

by the choice (28).

5.4 Order of magnitude of the variables.

We dissect the set of variations of the variables $D_{\mathbf{u}}$ in the definition of $\mathscr{D}^-(X,k)$ to control their orders of magnitude and to mollify the constraint $\prod D_{\mathbf{u}}\leq X$. We first introduce the dissection parameter

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

and for each $\mathbf{u}\in\mathbb{F}_2^{2k}$, a number $A_{\mathbf{u}}$ of the form 1, Δ, Δ^2, Δ^3,...

For $\mathbf{A}=(A_{\mathbf{u}})_{\mathbf{u}\in\mathbb{F}_2^{2k}}$, we define the restricted sum $S(X,k,\mathbf{A})$ by the formula

$$S(X,k,\mathbf{A}) = 2^{-k}\sum_{(D_{\mathbf{u}})}\Big(\prod_{\mathbf{u}}2^{-k\,\omega(D_{\mathbf{u}})}\Big)\prod_{\mathbf{u},\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u},\mathbf{v})}, \tag{31}$$

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

$$(D_{\mathbf{u}})\in\mathscr{D}^-(X,k),\ A_{\mathbf{u}}\leq D_{\mathbf{u}}<\Delta A_{\mathbf{u}},\ \omega(D_{\mathbf{u}})\leq\Omega \text{ for all } \mathbf{u}\in\mathbb{F}_2^{2k}.$$

Recall that $\mathscr{D}^-(X,k)$ is defined in Lemma 17. Using equation (30) we decompose $S^-(X,k,1,4)$ by the formula

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

where $\mathbf{A}$ is such that $\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}}A_{\mathbf{u}}\leq X$. We remark that the sum in (32) contains $O\big((\log X)^{4^k(1+2^k)}\big)$ terms.

We now define four families of $\mathbf{A}$ and prove that their contributions to the right part of (32) are negligible.

The first family is defined by:

$$\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} A_{\mathbf{u}} \geq \Delta^{-4^k} X. \tag{33}$$

By Lemma 12 and by the definition of Δ, we see that

$$\begin{aligned}\sum_{\mathbf{A}\text{ satisfies (33)}} \left|S(X,k,\mathbf{A})\right| &\leq \sum_{\Delta^{-4^k}X\leq n\leq X} \mu^2(n)\tau_{4^k}(n)2^{-k\omega(n)}\\ &\ll \sum_{\Delta^{-4^k}X\leq n\leq X} 2^{k\omega(n)}\\ &\ll (1-\Delta^{-4^k})X(\log X)^{2^k-1}.\end{aligned}$$

Using the expansion $(1+x)^\alpha = 1+\alpha x+O(x^2)$ for $x\to 0$ we get:

$$\Delta^{-4^k} = (1+\log^{-2^k}X)^{-4^k} = 1-4^k\log^{-2^k}X+O(\log^{-2^{k+1}}X).$$

Putting the last two formulas together we finally get:

$$\sum_{\mathbf{A}\text{ satisfies (33)}} \left|S(X,k,\mathbf{A})\right| \ll X(\log X)^{-1}. \tag{34}$$

Note that if (33) is not satisfied, the conditions $A_{\mathbf{u}}\leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}}$ imply $\prod_{\mathbf{u}} D_{\mathbf{u}} \leq X$ automatically. This means that the sizes of the $D_{\mathbf{u}}$ are mutually independent now.

To define the three other families we introduce two numbers $X^\dagger$ and $X^\ddagger$ defined by

$$X^\dagger = (\log X)^{3[1+4^k(1+2^k)]} \tag{35}$$

$$X^\ddagger \text{ is the least } \Delta^\ell \geq \exp(\log^{\eta(k)}X). \tag{36}$$

We shall choose $\eta(k)$ as a small positive function of k (see its definition before the statement of Proposition 5). The second family is defined by

$$\text{At most } 2^k-1 \text{ of the } A_{\mathbf{u}} \text{ are larger than } X^\ddagger. \tag{37}$$

It is easy to see the inequality

$$\sum_{\mathbf{A}\text{ satisfies (37)}} \left|S(X,k,\mathbf{A})\right| \leq \sum_{\substack{(D_{\mathbf{u}})\\ \prod D_{\mathbf{u}}\leq X}} \prod_{\mathbf{u}} 2^{-k\omega(D_{\mathbf{u}})}, \tag{38}$$

where the sum is over the 4^k–tuples $(D_{\mathbf{u}})$ which are squarefree, coprime and are such that at most 2^k-1 are larger than $X^\ddagger$. We dissect the above sum according to the number $r\leq 2^k-1$ of $D_{\mathbf{u}}$ which are larger than $X^\ddagger$. Let n be the product of

those $D_{\mathbf{u}}$ which are larger than $X^{\ddagger}$, and m the product of the remaining ones. With these conventions and with Lemma 12, we transform (38) into

$$\begin{aligned}
&\sum_{\mathbf{A}\text{ satisfies (37)}} \big|S(X,k,\mathbf{A})\big| \\
&\leq \sum_{0\leq r\leq 2^k-1} \sum_{m\leq (X^{\ddagger})^{4^k-r}} \mu^2(m)\tau_{4^k-r}(m)2^{-k\omega(m)} \sum_{n\leq X/m} \mu^2(n)\tau_r(n)2^{-k\omega(n)} \\
&\ll \sum_{0\leq r\leq 2^k-1} \sum_{m\leq (X^{\ddagger})^{4^k-r}} \mu^2(m)\tau_{4^k-r}(m)2^{-k\omega(m)}(X/m)\big(\log X\big)^{r2^{-k}-1} \\
&\ll X\Big(\sum_{0\leq r\leq 2^k-1} \big(\log X\big)^{r2^{-k}-1}\Big)\Big(\sum_{m\leq (X^{\ddagger})^{4^k}} \frac{2^{k\omega(m)}}{m}\Big).
\end{aligned}$$

By Mertens formula, we finally get

$$\sum_{\mathbf{A}\text{ satisfies (37)}} \big|S(X,k,\mathbf{A})\big| \ll X(\log X)^{2^k\eta(k)-2^{-k}}. \tag{39}$$

The third family of $\mathbf{A}$ is defined by

$$\begin{cases} \text{The condition (33) is not satisfied and} \\ \\ \text{there exist two linked indices } \mathbf{u} \text{ and } \mathbf{v} \text{ such that } A_{\mathbf{u}} \text{ and } A_{\mathbf{v}} \text{ are } \geq X^{\dagger}. \end{cases} \tag{40}$$

In that case the bound for $S(X,k,\mathbf{A})$ will be obtained as a consequence of the double oscillations of the character $(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}})$ when $D_{\mathbf{u}}$ and $D_{\mathbf{v}}$ vary independently (see Lemma 15). If $\mathbf{A}$ satisfies (40), there exist two indices $\mathbf{u}$ and $\mathbf{v}$ such that $\Phi_k(\mathbf{u},\mathbf{v})+\Phi_k(\mathbf{v},\mathbf{u})=1$. Hence we can write the inequality

$$\begin{aligned}
&|S(X,k,\mathbf{A})| \leq \\
&\sum_{(D_{\mathbf{w}})_{\mathbf{w}\neq\mathbf{u},\mathbf{v}}} \prod_{\mathbf{w}\neq\mathbf{u},\mathbf{v}} 2^{-k\omega(D_{\mathbf{w}})} \Big|\sum_{D_{\mathbf{u}}}\sum_{D_{\mathbf{v}}} a(D_{\mathbf{u}},(D_{\mathbf{w}})_{\mathbf{w}\neq\mathbf{u},\mathbf{v}})a(D_{\mathbf{v}},(D_{\mathbf{w}})_{\mathbf{w}\neq\mathbf{u},\mathbf{v}})\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)\Big|,
\end{aligned} \tag{41}$$

where

$$a(D_{\mathbf{u}},(D_{\mathbf{w}})_{\mathbf{w}\neq\mathbf{u},\mathbf{v}}) = 2^{-k\omega(D_{\mathbf{u}})} \prod_{\mathbf{w}\neq\mathbf{u},\mathbf{v}} \Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{w}}}\Big)^{\Phi_k(\mathbf{u},\mathbf{w})} \prod_{\mathbf{w}\neq\mathbf{u},\mathbf{v}} \Big(\frac{D_{\mathbf{w}}}{D_{\mathbf{u}}}\Big)^{\Phi_k(\mathbf{w},\mathbf{u})}$$

and $a(D_{\mathbf{v}},(D_{\mathbf{w}})_{\mathbf{w}\neq\mathbf{u},\mathbf{v}})$ is defined similarly. The coefficients a are always less than 1 in absolute value and the variables of summation $D_{\mathbf{w}}$ are coprime, squarefree and satisfy the conditions

$$\prod_{\mathbf{w}\in\mathbb{F}_2^{2k}} D_{\mathbf{w}} \equiv -1 \bmod 4,\ \omega(D_{\mathbf{w}}) \leq \Omega \text{ and } A_{\mathbf{w}} \leq D_{\mathbf{w}} < \Delta A_{\mathbf{w}}\ (\mathbf{w}\in\mathbb{F}_2^{2k}),$$

with $A_{\mathbf{u}},A_{\mathbf{v}}\geq X^{\dagger}$. By fixing the class ±1 mod 4 of each $D_{\mathbf{w}}$, and by applying (18) to the inner double sum of (41), we get the inequality

$$\big|S(X,k,\mathbf{A})\big|\ll\Big(\prod_{\mathbf{w}\neq\mathbf{u},\mathbf{v}}A_{\mathbf{w}}\Big)\big(A_{\mathbf{u}}A_{\mathbf{v}}(A_{\mathbf{u}}^{-\frac{1}{3}}+A_{\mathbf{v}}^{-\frac{1}{3}})\big)\ll X(X^{\dagger})^{-\frac{1}{3}}.$$

It remains to sum over the $O\big((\log X)^{4^k(1+2^k)}\big)$ possible $\mathbf{A}$ and to use the definition of $X^{\dagger}$ to finally get

$$\sum_{\mathbf{A}\text{ satisfies (40)}}\big|S(X,k,\mathbf{A})\big|\ll X(\log X)^{-1}. \tag{42}$$

The fourth family of $\mathbf{A}$ is defined by

$$\begin{cases}\text{The condition (33) is not satisfied and there exist}\\ \\ \text{two linked indices }\mathbf{u}\text{ and }\mathbf{v}\text{ such that }2\leq A_{\mathbf{v}}<X^{\dagger}\text{ and }A_{\mathbf{u}}\geq X^{\ddagger}.\end{cases} \tag{43}$$

To deal with such cases, we introduce κ in the following equations in order to satisfy the condition $\prod_{\mathbf{u}}D_{\mathbf{u}}\equiv-1$ mod 4. Since (43) is satisfied, we have the inequality

$$\big|S(X,k,\mathbf{A})\big|\leq 2\max_{\kappa=\pm1\bmod 4}\sum_{(D_{\mathbf{w}})_{\mathbf{w}\neq\mathbf{u},\mathbf{v}}}\sum_{D_{\mathbf{v}}}\Big|\sum_{D_{\mathbf{u}}}\frac{\mu^2\big(2\prod_{\mathbf{w}}D_{\mathbf{w}}\big)}{2^{k\omega(D_{\mathbf{u}})}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)\Big|, \tag{44}$$

where $A_{\mathbf{w}}\leq D_{\mathbf{w}}<\Delta A_{\mathbf{w}}$ ($\mathbf{w}\in\mathbb{F}_2^{2k}$) and $D_{\mathbf{u}}\equiv\kappa$ mod 4 and $\omega(D_{\mathbf{u}})\leq\Omega$, with the inequalities $A_{\mathbf{u}}\geq X^{\ddagger}$ and $2\leq A_{\mathbf{v}}<X^{\dagger}$. Fixing the value ℓ of $\omega(D_{\mathbf{u}})$ and writing $D_{\mathbf{u}}=p_1\cdots p_{\ell}$ in ascending order, we transform (44) into

$$\big|S(X,k,\mathbf{A})\big|\ll\max_{\kappa=\pm1\bmod 4}\sum_{(D_{\mathbf{w}})_{\mathbf{w}\neq\mathbf{u},\mathbf{v}}}\sum_{D_{\mathbf{v}}}\sum_{0\leq\ell\leq\Omega}\frac{1}{2^{k\ell}}\Big|\sum_{\substack{\omega(D_{\mathbf{u}})=\ell\\ D_{\mathbf{u}}\equiv\kappa\bmod 4}}\mu^2\big(2\prod_{\mathbf{w}}D_{\mathbf{w}}\big)\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)\Big|, \tag{45}$$

and the inner sum satisfies

$$\begin{aligned}&\Big|\sum_{\substack{\omega(D_{\mathbf{u}})=\ell\\ D_{\mathbf{u}}\equiv\kappa\bmod 4}}\mu^2\big(2\prod_{\mathbf{w}}D_{\mathbf{w}}\big)\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)\Big|\\ &\qquad\leq 2\max_{\kappa'=\pm1\bmod 4}\sum_{p_1\cdots p_{\ell-1}}\Big|\sum_{p_{\ell}\equiv\kappa'\bmod 4}\mu^2\big(2p_1\cdots p_{\ell}\prod_{\mathbf{w}\neq\mathbf{u}}D_{\mathbf{w}}\big)\Big(\frac{p_{\ell}}{D_{\mathbf{v}}}\Big)\Big|,\end{aligned} \tag{46}$$

and p_{ℓ} satisfies $A_{\mathbf{u}}\leq p_1\cdots p_{\ell}<\Delta A_{\mathbf{u}}$. Since ℓ is not too large ($\ell\leq\Omega$), the variable p_{ℓ} satisfies $p_{\ell}\geq A_{\mathbf{u}}^{\frac{1}{\ell}}$, the interval of variation for p_{ℓ} is large enough, compared with the modulus $4D_{\mathbf{v}}\leq 8X^{\dagger}$, since we have $A_{\mathbf{u}}^{\frac{1}{\ell}}\geq\exp\big(\log^{\eta(k)/2}X\big)$. Applying Lemma 13 with $q=4D_{\mathbf{v}},x=\frac{\Delta A_{\mathbf{u}}}{p_1\cdots p_{\ell-1}}$, and A large we have

$$\Big|\sum_{p_{\ell}\equiv\kappa'\bmod 4}\mu^2\big(2p_1\cdots p_{\ell}\prod_{\mathbf{w}\neq\mathbf{u}}D_{\mathbf{w}}\big)\Big(\frac{p_{\ell}}{D_{\mathbf{v}}}\Big)\Big|\ll A_{\mathbf{v}}^{\frac{1}{2}}\frac{A_{\mathbf{u}}}{p_1\cdots p_{\ell-1}}\big(\log X\big)^{-A\eta(k)/2}+\Omega.$$

We remark that the Ω–term comes from the μ^2–term, which may be zero, if p_ℓ divides one of the $D_{\mathbf{w}}$. Inserting this bound in (46), summing over p_1, ..., $p_{\ell-1}$, and then in (45), we finally get the inequality

$$\big|S(X,k,\mathbf{A})\big| \ll A_{\mathbf{u}} A_{\mathbf{v}}^{\frac{3}{2}} \Big(\prod_{\mathbf{w}\neq\mathbf{u},\mathbf{v}} A_{\mathbf{w}} \Big) \big(\log X\big)^{-A\eta(k)/2} \ll X \big(X^{\dagger}\big)^{\frac{1}{2}} \big(\log X\big)^{-A\eta(k)/2}.$$

Now summing over all the $\mathbf{A}$ satisfying (43), and choosing A very large in terms of k, we proved

$$\sum_{\mathbf{A} \text{ satisfies (43)}} \big|S(X,k,\mathbf{A})\big| \ll X(\log X)^{-1}. \tag{47}$$

It is now easy to deduce from (32), (34), (39), (42) and (47):

Proposition 2 *For every $k \geq 1$, we have the equality*

$$S^{+}(X,k,1,4) = \sum_{\mathbf{A} \text{ satisfies (48)}} S(X,k,\mathbf{A}) + O\Big((X(\log X)^{2^k\eta(k)-2^{-k}} \Big),$$

where

$$\begin{cases} \displaystyle\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} A_{\mathbf{u}} < \Delta^{-4^k} X \\ \text{At least } 2^k \text{ indices } \mathbf{u} \text{ satisfy } A_{\mathbf{u}} > X^{\ddagger}, \\ \text{Two indices } \mathbf{u} \text{ and } \mathbf{v} \text{ with } A_{\mathbf{u}}, A_{\mathbf{v}} > X^{\dagger} \text{ are always unlinked}, \\ \text{If } A_{\mathbf{u}} \text{ and } A_{\mathbf{v}} \text{ with } A_{\mathbf{v}} \leq A_{\mathbf{u}} \text{ are linked, then} \\ \quad \text{either } A_{\mathbf{v}} = 1 \text{ or } (2 \leq A_{\mathbf{v}} < X^{\dagger} \text{ and } A_{\mathbf{v}} \leq A_{\mathbf{u}} < X^{\ddagger}). \end{cases} \tag{48}$$

Actually, in proving Proposition 2, we did not enter into the properties of linked indices. It is the purpose of the following subsection, to simplify the conditions (48).

5.5 Geometry of unlinked indices.

We first prove

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

Proof We follow the proof of [10, Lemmata 7–8]. It is easy to see that if $\mathscr{U}$ is a set of unlinked indices, then $\mathbf{c}+\mathscr{U}$ has the same property. We introduce the symmetric bilinear form

$$p(\mathbf{u},\mathbf{v}) = P(\mathbf{u}+\mathbf{v}) - P(\mathbf{u}) - P(\mathbf{v}) = \sum_{j=0}^{k-1} (u_{2j+1}v_{2j+2} + u_{2j+2}v_{2j+1}).$$

Note that if $\mathbf{u}$ and $\mathbf{v}$ are unlinked with $\mathbf{0}$, then $\mathbf{u}$ and $\mathbf{v}$ are unlinked if and only if we have $p(\mathbf{u},\mathbf{v})=0$.

Let $\mathscr{U}$ be a subset of unlinked indices. Hence for any $\mathbf{u}$ and $\mathbf{v}\in\mathscr{U}$ we have $P(\mathbf{u}+\mathbf{v})=0$ and therefore $\mathbf{u}+\mathbf{v}$ is unlinked with $\mathbf{0}$. Since the property of being unlinked is stable under translation, we may suppose that $\mathbf{0}\in\mathscr{U}$. Hence, under the assumption $\mathbf{0}\in\mathscr{U}$ we have $p(\mathbf{u},\mathbf{v})=0$ for any $\mathbf{u}$ and $\mathbf{v}\in\mathscr{U}$ and $p(\mathbf{u}+\mathbf{v},\mathbf{w})=p(\mathbf{u},\mathbf{w})+p(\mathbf{v},\mathbf{w})=0$ for any $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}\in\mathscr{U}$. Then we deduce that $\mathbf{u}+\mathbf{v}$ is unlinked with any $\mathbf{w}\in\mathscr{U}$. If we suppose that $\mathscr{U}$ is maximal, we see that $\mathscr{U}$ is closed under addition, and is a vector subspace of $\mathbb{F}_2^{2k}$.

We now appeal to some results concerning the theory of bilinear forms on vector spaces over fields with characteristic 2 (see [4, p.33 & 34] for instance). To follow the the terminology of that theory, $\mathscr{U}$ is a *singular* space for the non degenerate quadratic form P (which means that $P\equiv 0$ on $\mathscr{U}$). It follows that $\dim\mathscr{U}\leq k$.

By [4, p. 23.4 & p.36] we know that all the maximal singular spaces have the same dimension. We know the singular space of dimension k which is generated by the vectors $(1,1,0,\dots,0),(0,0,1,1,0\dots,0),\dots,(0,0,\dots,0,1,1)$. Hence it is a maximal singular space and all the maximal singular spaces have dimension k.

□

Now we can simplify the conditions of summation (48). Let $\mathbf{A}=(\mathbf{A_u})$ satisfying (48) and let $\mathscr{U}$ be the set of indices $\mathbf{u}$, such that $A_{\mathbf{u}}>X^{\ddagger}$. This is a set of unlinked indices of cardinality $\geq 2^k$. By Lemma 18 we know that its cardinality is equal to 2^k. Furthermore, by this lemma, it is also a maximal subset of unlinked indices. Hence, for any $\mathbf{v}\notin\mathscr{U}$, there exists $\mathbf{u}\in\mathscr{U}$, such that $\mathbf{u}$ and $\mathbf{v}$ are linked. From the last condition in (48), we deduce that $A_{\mathbf{v}}=1$.

From this discussion,we simplify Proposition 2 into

Proposition 3 *For every $k\geq 1$, we have the equality*

$$S^{-}(X,k,1,4)=\sum_{\mathbf{A}\ \textit{satisfies}\ (49)} S(X,k,\mathbf{A})+O\big(X(\log X)^{2^k\eta(k)-2^{-k}}\big)$$

where

$$\begin{cases}\displaystyle\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} A_{\mathbf{u}}\leq \Delta^{-4^k}X,\\ \mathscr{U}=\{\mathbf{u}\,;A_{\mathbf{u}}>X^{\ddagger}\}\ \textit{is a maximal subset of unlinked indices},\\ A_{\mathbf{u}}=1\ \textit{for}\ \mathbf{u}\notin\mathscr{U}.\end{cases}\tag{49}$$

Following the notations of Heath–Brown [10], we reserve the letter $\mathscr{U}$ for any subset of 2^k unlinked indices, taken in $\mathbb{F}_2^{2k}$. We say that $\mathbf{A}=(A_{\mathbf{u}})_{\mathbf{u}\in\mathbb{F}_2^{2k}}$ is *admissable* for $\mathscr{U}$, if it satisfies

$$\begin{cases}A_{\mathbf{u}}>X^{\ddagger}\Leftrightarrow\mathbf{u}\in\mathscr{U}\\ A_{\mathbf{u}}=1\Leftrightarrow\mathbf{u}\notin\mathscr{U}\\ \prod A_{\mathbf{u}}\leq\ \Delta^{-4^k}X.\end{cases}\tag{50}$$

We remark that $A_{\mathbf{u}}=1$ implies $D_{\mathbf{u}}=1$. For $\mathbf{u}\in\mathscr{U}$, let $h_{\mathbf{u}}\in\{\pm 1 \bmod 4\}$ such that

$$\prod_{\mathbf{u}\in\mathscr{U}} h_{\mathbf{u}}\equiv -1 \bmod 4.\tag{51}$$

Let $\mathbf{A}$ be admissable for $\mathscr{U}$. The definition of unlinked indices, the quadratic reciprocity law and the definition (31) imply the equality ($\Phi_k(\mathbf{u},\mathbf{v}) = \Phi_k(\mathbf{v},\mathbf{u})$ for $\mathbf{u},\mathbf{v}$ unlinked):

$$S(X,k,\mathbf{A}) = 2^{-k}\sum_{(h_{\mathbf{u}})}\Big(\sum_{(D_{\mathbf{u}})}\mu^2(\prod_{\mathbf{u}\in\mathscr{U}}D_{\mathbf{u}})\prod_{\mathbf{u}\in\mathscr{U}}2^{-k\omega(D_{\mathbf{u}})}\Big)\Big(\prod_{\mathbf{u},\mathbf{v}}(-1)^{\Phi_k(\mathbf{u},\mathbf{v})\cdot\frac{h_{\mathbf{u}}-1}{2}\cdot\frac{h_{\mathbf{v}}-1}{2}}\Big), \tag{52}$$

where the first sum is over $h_{\mathbf{u}}$ satisfying (51) and the second sum is over $(D_{\mathbf{u}})_{\mathbf{u}\in\mathscr{U}}$ such that

$$A_{\mathbf{u}} \le D_{\mathbf{u}} < \Delta A_{\mathbf{u}},\ D_{\mathbf{u}} \equiv h_{\mathbf{u}} \bmod 4,\ \omega(D_{\mathbf{u}}) \le \Omega,$$

and the last product is over unordered pairs $\{\mathbf{u},\mathbf{v}\}$ of elements of $\mathscr{U}$.

We now appeal to the following lemma, which is a consequence of the equidistribution of primes in fixed arithmetic progressions.

Lemma 19 *For $\kappa = \pm 1 \bmod 4$, for every $A \ge 0$ and for $Y \ge y \ge 1$, we have the equality*

$$\sum_{\substack{y\le n\le Y\\ n\equiv\kappa \bmod 4\\ \omega(n)=\ell}}\mu^2(n_0n) = \frac{1}{2}\sum_{\substack{y\le n\le Y\\ \omega(n)=\ell}}\mu^2(2n_0n) + O_A\Big((\ell+1)^{A+1}Y(\log 2Y)^{-A} + \omega(n_0)Y^{1-\frac{1}{\ell}}\Big),$$

uniformly for an odd squarefree integer n_0, and $\ell \ge 0$.

Note that this lemma is of poor quality when ℓ is large and trivial for $\ell = 0$.

Proof We suppose $\ell \ge 1$ and write $n = p_1\cdots p_\ell$ the decomposition of n in increasing odd primes. Note that we have the inequality $Y/(p_1\cdots p_{\ell-1}) \ge Y^{\frac{1}{\ell}}$, otherwise the sum is empty. Hence, we have the equality

$$\sum_{\substack{y\le n\le Y, n\equiv\kappa \bmod 4\\ \omega(n)=\ell}}\mu^2(n_0n) = \sum_{p_1\cdots p_{\ell-1}\le Y^{1-\frac{1}{\ell}}}\mu^2(n_0p_1\cdots p_{\ell-1})\sum_{\substack{\max(p_{\ell-1},y/(p_1\cdots p_{\ell-1}))<p_\ell\le Y/(p_1\cdots p_{\ell-1})\\ p_\ell\equiv\kappa/(p_1\cdots p_{\ell-1}) \bmod 4}}\mu^2(2n_0p_\ell). \tag{53}$$

By the prime number theorem in arithmetic progressions modulo 4 written in the form

$$\sum_{\substack{Z_1<p\le Z_2\\ p\equiv a \bmod 4}}1 = \frac{1}{2}\sum_{Z_1<p\le Z_2}1 + O\big(Z_2(\log 2Z_2)^{-A}\big),$$

uniformly for a odd and $1 < Z_1 < Z_2$ (see Lemma 13, with $q = 4$), we see that the sum over p_ℓ in (53) is equal to

$$\frac{1}{2}\sum_{\substack{\max(p_{\ell-1},y/(p_1\cdots p_{\ell-1}))<p_\ell\\ p_\ell\le Y/(p_1\cdots p_{\ell-1})}}\mu^2(2n_0p_\ell) + O\Big(\omega(n_0) + \frac{Y}{p_1\cdots p_{\ell-1}}(\log^{-A}(2Y^{\frac{1}{\ell}}))\Big),$$

then, summing this expression over $p_1\cdots p_{\ell-1} \le Y^{1-\frac{1}{\ell}}$, we finish the proof of Lemma 19. □

This lemma is used to transform the inner sum over $(D_{\mathbf{u}})$ in (52) in the following way. We momentarily suppose that the set $\mathscr{U}$ is written in the form

$$\mathscr{U} = \{u_m\,;\, 1 \le m \le 2^k\},$$

with $u_m \in \mathbb{F}_2^{2k}$. Then we have

$$\sum_{(D_{\mathbf{u}})} \mu^2\Big(\prod_{\mathbf{u}\in\mathscr{U}} D_{\mathbf{u}}\Big) \prod_{\mathbf{u}\in\mathscr{U}} 2^{-k\omega(D_{\mathbf{u}})} = \sum_{D_{u_1}} 2^{-k\,\omega(D_{u_1})} \times \Big(\sum_{D_{u_2}} 2^{-k\,\omega(D_{u_2})}\Big(\cdots\Big(\sum_{D_{u_{2^k}}} \mu^2(D_{u_1}\cdots D_{u_{2^k}})2^{-k\,\omega(D_{u_{2^k}})}\Big)\cdots\Big)\Big), \tag{54}$$

where, for each $1 \le i \le 2^k$, the sum over D_{u_i} satisfies

$$A_{u_i} \le D_{u_i} < \Delta A_{u_i},\, D_{u_i} \equiv h_{u_i} \bmod 4,\, \omega(D_{u_i}) \le \Omega.$$

By fixing the value $\omega(D_{u_{2^k}}) = \ell$, applying Lemma 19 with $y = A_{u_{2^k}}$ and $Y = \Delta A_{u_{2^k}}$, and then summing over $\ell \le \Omega$, we get the equality

$$\sum_{D_{u_{2^k}}} \mu^2(D_{u_1}\cdots D_{u_{2^k}})2^{-k\,\omega(D_{u_{2^k}})} = \frac{1}{2}\sum_{\substack{A_{u_{2^k}} \le D_{u_{2^k}} < \Delta A_{u_{2^k}} \\ \omega(D_{u_{2^k}})\le\Omega}} \mu^2(2D_{u_1}\cdots D_{u_{2^k}})2^{-k\,\omega(D_{u_{2^k}})} + O\big(A_{u_{2^k}}(\log X)^{-1-4^k(1+2^k)}\big).$$

Note that the congruence condition for $D_{u_{2^k}}$ has disappeared and that we used the lower bound $\log(2Y) \ge \log A_{u_{2^k}} \ge (\log X)^{\eta(k)}$. Inserting this formula into (54), inverting summations, and applying the same lemma to the variable $D_{u_{2^k-1}}$ and so on, we finally get the equality

$$\sum_{(D_{\mathbf{u}})} \mu^2\Big(\prod_{\mathbf{u}\in\mathscr{U}} D_{\mathbf{u}}\Big) \prod_{\mathbf{u}\in\mathscr{U}} 2^{-k\omega(D_{\mathbf{u}})} = \frac{1}{2^{2^k}} \sum_{\substack{(D_{\mathbf{u}}),\, A_{\mathbf{u}} \le D_{\mathbf{u}} < \Delta A_{\mathbf{u}} \\ \omega(D_{\mathbf{u}})<\Omega}} \mu^2\Big(2\prod_{\mathbf{u}\in\mathscr{U}} D_{\mathbf{u}}\Big) \prod_{\mathbf{u}\in\mathscr{U}} 2^{-k\omega(D_{\mathbf{u}})} + O\Big(X(\log X)^{-1-4^k(1+2^k)}\Big).$$

Inserting this formula into (52) and summing over all **A** admissible for a fixed $\mathscr{U}$ and satisfying (49), we get

$$\sum_{\mathbf{A}\text{ admissible for }\mathscr{U}} S(X,k,\mathbf{A}) = 2^{-k-2^k}\Big\{\sum_{(h_{\mathbf{u}})}\Big(\prod_{\mathbf{u},\mathbf{v}}(-1)^{\Phi_k(\mathbf{u},\mathbf{v})\cdot\frac{h_{\mathbf{u}}-1}{2}\cdot\frac{h_{\mathbf{v}}-1}{2}}\Big)\Big\} \times \Big\{\sum_{(D_{\mathbf{u}})} \mu^2(2\prod_{\mathbf{u}\in\mathscr{U}} D_{\mathbf{u}}) \prod_{\mathbf{u}\in\mathscr{U}} 2^{-k\omega(D_{\mathbf{u}})}\Big\} + O\big(X(\log X)^{-1}\big), \tag{55}$$

where the sum is over the $(D_{\mathbf{u}})$ such that $\omega(D_{\mathbf{u}}) \leq \Omega$ and such that there is an $\mathbf{A} = (A_{\mathbf{u}})$ satisfying (50) and $A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}}$.

By a computation similar to the proof of (30), we can drop the condition of $\omega(D_{\mathbf{u}}) \leq \Omega$ with an error term in $O\big(X(\log X)^{-1}\big)$.

By a computation already done to obtain (39) and (34), we transform the right–hand side of (55) into

$$\begin{aligned}\sum_{(D_{\mathbf{u}})} \mu^2(2\prod_{\mathbf{u}\in\mathscr{U}} D_{\mathbf{u}}) \prod_{\mathbf{u}\in\mathscr{U}} 2^{-k\omega(D_{\mathbf{u}})} &= \sum_{n\leq X} \mu^2(2n)\tau_{2^k}(n)2^{-k\omega(n)} + O(X(\log X)^{-1}) \\ &\quad + O\Big(\sum_{1\leq \ell\leq X^{\ddagger}} 2^{-k\omega(\ell)} \sum_{1\leq m\leq X/\ell} 2^{-k\omega(m)}(2^k-1)^{\omega(m)}\Big) \\ &= \sum_{n\leq X} \mu^2(2n) + O\Big(X(\log X)^{\eta(k)2^{-k}-2^{-k}}\Big).\end{aligned}$$

The first error term comes from equation (34). In the second error term we count the numbers which have at least one factor $\ell \leq X^{\ddagger}$. The sum over m is computed by Lemma 9 using $\gamma = 1-2^{-k}$ and the final sum using Mertens formula. By this expression, by (16), and by (55) we get

Proposition 4 *For every k, and for every maximal unlinked subset $\mathscr{U} \subset \mathbb{F}_2^{2k}$, we have*

$$\sum_{\mathbf{A}\ \text{admissable for}\ \mathscr{U}} S(X,k,\mathbf{A}) = 2^{-k-2^k}\,\gamma(\mathscr{U})\frac{4X}{\pi^2} + O\Big(X(\log X)^{\eta(k)2^{-k}-2^{-k}}\Big),$$

with

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

where the product is over unordered pairs $\{\mathbf{u},\mathbf{v}\} \subset \mathscr{U}$, and where $(h_{\mathbf{u}})_{\mathbf{u}\in\mathscr{U}} \in \{\pm 1 \bmod 4\}^{2^k}$ satisfy (51).

Now we sum over all maximal unlinked sets $\mathscr{U}$ in Proposition 4, use Proposition 3 and chose $\eta(k) = 2^{-k}\varepsilon$, to finally write

Proposition 5 *For every $k \geq 1$ and for every positive ε, we have the equality*

$$S^-(X,k,1,4) = \frac{2^{2-k-2^k}}{\pi^2}\Big(\sum_{\mathscr{U}} \gamma(\mathscr{U})\Big)\cdot X + O\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big),$$

where the sum is over the set of maximal unlinked sets $\mathscr{U} \subset \mathbb{F}_2^{2k}$.

5.6 Study of the coefficient of the main term.

By Proposition 5, the proof of Theorem 6 is reduced to the study the quantity $\sum_{\mathscr{U}} \gamma(\mathscr{U})$. This is the purpose of this section, in which we follow the strategy of the proof of [10]. By Lemma 18, we write $\mathscr{U}$ as $\mathscr{U} = \mathbf{c} + \mathscr{U}_0$, with $\mathbf{c} \in \mathbb{F}_2^{2k}$ and $\mathscr{U}_0$ a vector subspace of $\mathbb{F}_2^{2k}$ of dimension k. Note that $\mathscr{U}_0$ is also a maximal unlinked vector subspace.

Let $S = S(\mathscr{U},(h_{\mathbf{u}}))$ be the set

$$S = \{\mathbf{u} \in \mathscr{U}\,;\, h_{\mathbf{u}} \equiv -1 \bmod 4\}.$$

By (51), the cardinality s of S is odd. We directly obtain

$$\gamma(\mathscr{U}) = \sum_{\substack{S\subset\mathscr{U}\\ s \text{ odd}}} (-1)^{e(S)}, \tag{56}$$

with

$$e(S) = \sum_{\mathbf{u},\mathbf{v}} \Phi_k(\mathbf{u},\mathbf{v}), \tag{57}$$

where the sum is over unordered pairs $\{\mathbf{u},\mathbf{v}\} \subset S$. Of course, since $e(S) \in \mathbb{F}_2$, we interpret $(-1)^{e(S)}$ as an element of $\mathbb{Z}$, in the natural way. For the purpose of the next sections, we generalize $\gamma(\mathscr{U})$ by introducing for $\nu = 0$ or 1 mod 2, the following

$$\gamma(\mathscr{U},\nu) = \sum_{\substack{S\subset\mathscr{U}\\ s\equiv\nu \bmod 2}} (-1)^{e(S)}. \tag{58}$$

Now we decompose the polynomial Φ_k in a sum of a bilinear form, the quadratic form P and two linear forms, in the following way

$$\Phi_k(\mathbf{u},\mathbf{v}) = L(\mathbf{u},\mathbf{v}) + P(\mathbf{v}) + \Lambda(\mathbf{u}) + \Lambda(\mathbf{v}), \tag{59}$$

with

$$L(\mathbf{u},\mathbf{v}) = \sum_{j=0}^{k-1} u_{2j+1}(v_{2j+1} + v_{2j+2}), \tag{60}$$

$$P(\mathbf{v}) = \sum_{j=0}^{k-1} v_{2j+1}(v_{2j+1} + v_{2j+2}),$$

and

$$\Lambda(\mathbf{u}) = \sum_{j=0}^{k-1} u_{2j+1}^2 = \sum_{j=0}^{k-1} u_{2j+1}.$$

Note that

$$L(\mathbf{u},\mathbf{u}) = P(\mathbf{u}) \ (\forall \mathbf{u} \in \mathbb{F}_2^{2k}). \tag{61}$$

The quadratic form P is almost linear in the following sense:

Lemma 20 *Let S be a subset of $\mathscr{U}$ of cardinality s and $\sigma := \sum_{\mathbf{u}\in S}\mathbf{u}$. Then*

1. *For s odd we get that $P(\sigma) = L(\sigma,\sigma) = \sum_{\mathbf{u}\in S} P(\mathbf{u})$.*
2. $L(\sigma,\sigma) + s\left(\sum_{\mathbf{u}\in S} P(\mathbf{u})\right) = 0.$

Proof When $s=1$, (i) is a consequence of (61). For other odd s, this is a consequence of the general formula true for any quadratic form Q over $\mathbb{F}_2^{2k}$, and for every $\mathbf{u}$, $\mathbf{v}$, and $\mathbf{w}$:

$$Q(\mathbf{u}+\mathbf{v}+\mathbf{w}) = Q(\mathbf{u}+\mathbf{v})+Q(\mathbf{u}+\mathbf{w})+Q(\mathbf{v}+\mathbf{w})+Q(\mathbf{u})+Q(\mathbf{v})+Q(\mathbf{w}),$$

which for $Q=P$ and $\mathbf{u}$, $\mathbf{v}$, and $\mathbf{w}\in\mathscr{U}$ gives

$$P(\mathbf{u}+\mathbf{v}+\mathbf{w}) = P(\mathbf{u})+P(\mathbf{v})+P(\mathbf{w}),$$

where we used $P(\mathbf{u}+\mathbf{v})=0$ for $\mathbf{u}$ and $\mathbf{v}$ unlinked. This proves the second equality for s odd. In the even case we note that $\sigma\in\mathscr{U}_0$ and $P(\sigma+\mathbf{0})=0$ since $\mathbf{u}$ and $\mathbf{0}$ are unlinked. □

We now want to evaluate the function $e(S)$ defined in (57) in a suitable way.

We shall require some notations from set theory : if $\mathscr{X}$ is a set, we denote by $\mathscr{P}(\mathscr{X})$ the set of subsets of $\mathscr{X}$. For $\mathscr{X}$ finite and for $\nu=0$ or 1 mod 2, $\mathscr{P}_\nu(\mathscr{X})$ is the set of subsets of $\mathscr{X}$, with cardinalities $\equiv\nu$ mod 2. The symmetric difference operator is denoted by Δ, and shall frequently use the facts that $\mathscr{P}(\mathscr{X})$ and $\mathscr{P}_0(\mathscr{X})$ are abelian groups with the law Δ, and that $\mathscr{P}_0(\mathscr{X})$ operates on $\mathscr{P}_1(\mathscr{X})$ by the law Δ in a simply transitive way.

For any S and $T\in\mathscr{P}(\mathscr{U})$, with cardinalities odd or even, we define

$$e(S,T) := e(S)+e(T)+e(S\Delta T). \tag{62}$$

Then we have

$$e(S,T) = \sum_{\mathbf{u}\in S}\sum_{\mathbf{v}\in T}\Phi_k(\mathbf{u},\mathbf{v}). \tag{63}$$

The proof of (63) is in [10, p. 351]. Another direct proof is to check that (63) is correct for $S=T=\emptyset$ and to prove it by induction on the cardinality of $S\cup T$. In other words, we check that for any $\mathbf{w}\in\mathscr{U}$ but $\mathbf{w}\notin S\cup T$, the equality (63) remains true if we replace S and T respectively by $S\cup\{\mathbf{w}\}$ and T, by S and $T\cup\{\mathbf{w}\}$, or by $S\cup\{\mathbf{w}\}$ and $T\cup\{\mathbf{w}\}$. We only require the properties that $\Phi_k(\mathbf{u},\mathbf{u})=0$ and $\Phi_k(\mathbf{u},\mathbf{v})=\Phi_k(\mathbf{v},\mathbf{u})$ for any $\mathbf{u}$ and $\mathbf{v}\in\mathscr{U}$.

In the following σ and τ always denote the sum of elements in S and T, respectively. Furthermore the size of S and T is denoted by s and t, which will be interpreted as elements in $\mathbb{F}_2$ by reducing mod 2.

Lemma 21 *For all subsets S and T of $\mathscr{U}$ we have:*

$$e(S,T) = L(\sigma,\tau)+s\left(\sum_{\mathbf{v}\in T}P(\mathbf{v})\right)+t\Lambda(\sigma)+s\Lambda(\tau).$$

Proof This follows directly from (59) and (63) using linearity. □

Squaring (58), we have the equality

$$\begin{aligned}\gamma^2(\mathscr{U},\nu) &= \sum_{\substack{S,S'\subset\mathscr{U}\\ s,s'\equiv\nu \bmod 2}}\sum (-1)^{e(S)+e(S')}\\ &= \sum_{\substack{S,S'\subset\mathscr{U}\\ s,s'\equiv\nu \bmod 2}}\sum (-1)^{e(S\Delta S')+e(S',S)}.\end{aligned} \tag{64}$$

Instead of summing over S', we sum over $T = S\Delta S'$, which has even cardinality. By Lemma 21, by linearity and by t even, we have

$$\begin{aligned} e(S\Delta T,S) &= L(\sigma+\tau,\sigma)+(s+t)\Big(\sum_{\mathbf{u}\in S}P(\mathbf{u})\Big)+s\Lambda(\sigma+\tau)+(s+t)\Lambda(\sigma) \\ &= L(\tau,\sigma)+L(\sigma,\sigma)+s\sum_{\mathbf{u}\in S}P(\mathbf{u})+s\Lambda(\tau) \end{aligned} \tag{65}$$

since

$$\sum_{\mathbf{u}\in S\Delta T}\mathbf{u}=\sum_{\mathbf{u}\in S}\mathbf{u}+\sum_{\mathbf{u}\in T}\mathbf{u}=\sigma+\tau.$$

Using Lemma 20 we can even more simplify:

$$e(S',S)=e(S\Delta T,S)=L(\tau,\sigma)+s\Lambda(\tau). \tag{66}$$

By (66), (64), and using $T = S\Delta S'$ we get

$$\gamma^2(\mathscr{U},\nu)=\sum_{T\subset\mathscr{U},\,t\text{ even}}(-1)^{e(T)+\nu\Lambda(\tau)}\Sigma(T,\nu), \tag{67}$$

where

$$\Sigma(T,\nu)=\sum_{S\subset\mathscr{U},s\equiv\nu \bmod 2}(-1)^{L(\tau,\sigma)}. \tag{68}$$

For every $S_0\in\mathscr{P}_0(\mathscr{U})$ and corresponding sum σ_0 we get by linearity the equality

$$\Sigma(T,\nu)=\sum_{S\subset\mathscr{U},s\equiv\nu \bmod 2}(-1)^{L(\tau,\sigma+\sigma_0)}$$

which gives us the equation

$$\Sigma(T,\nu)=(-1)^{L(\tau,\sigma_0)}\Sigma(T,\nu)$$

for every $S_0\in\mathscr{P}_0(\mathscr{U})$. Hence $\Sigma(T,\nu)=0$ unless

$$L(\tau,\sigma_0)=0 \text{ for every } S_0\in\mathscr{P}_0(\mathscr{U}). \tag{69}$$

If (69) is satisfied, then with the choice $S_0=\{\mathbf{c}\}\Delta S$, we have $L(\tau,\sigma)=L(\tau,\mathbf{c})$ for every $S\in\mathscr{P}_1(\mathscr{U})$. This implies that $L(\tau,\sigma)=sL(\tau,\mathbf{c})$, for any $S\subset\mathscr{U}$, with s odd or even. Since $\mathscr{P}_0(\mathscr{U})$ and $\mathscr{P}_1(\mathscr{U})$ have cardinality equal to 2^{2^k-1}, we get the equality (still assuming (69)):

$$\Sigma(T,\nu)=2^{2^k-1}(-1)^{\nu L(\tau,\mathbf{c})},$$

which transforms (67) into

$$\gamma^2(\mathscr{U},\nu)=2^{2^k-1}\sum_{T\in\mathscr{T}}(-1)^{e(T)+\nu\left(\Lambda(\tau)+L(\tau,\mathbf{c})\right)}, \tag{70}$$

where $\mathscr{T}$ is the set of subsets T of $\mathscr{U}$ with even cardinality such that (69) is satisfied.

Note that $\mathscr{T}$ contains all subsets T of $\mathscr{U}$, with t even and $\tau = 0$, and that $\mathscr{T}$ is a group with symmetric difference operator. Note also that Lemma 21 implies $e(T, T') = 0$ for every T and $T' \in \mathscr{T}$ and by the way using (62), the application

$$T \mapsto (-1)^{e(T)}$$

is a multiplicative character on that group, and also the map

$$T \mapsto (-1)^{e(T)+\nu\left(\Lambda(\tau)+L(\tau,\mathbf{c})\right)}.$$

From (70) we deduce that $\gamma(\mathscr{U}, \nu)$ vanishes unless

$$e(T) = \nu\big(L(\tau, \mathbf{c}) + \Lambda(\tau)\big),$$

for all $T \in \mathscr{T}$. By restriction to the $T \in \mathscr{T}$ with $\tau = 0$, we proved

Lemma 22 *Let $\mathscr{U}$ be a maximal unlinked subset of $\mathbb{F}_2^{2k}$. Then we have*

$$\big(\gamma(\mathscr{U}, 0) \text{ or } \gamma(\mathscr{U}, 1) \neq 0\big) \Rightarrow \big(e(T) = 0 \ \forall T \subset \mathscr{U} \text{ with } t \text{ even and } \tau = 0\big).$$

This lemma is a weak form of the following

Lemma 23 *Let $\mathscr{U}$ be a maximal unlinked set of $\mathbb{F}_2^{2k}$ written in the form $\mathscr{U} = \mathbf{c} + \mathscr{U}_0$. Then we have*

$$\big(\gamma(\mathscr{U}, 0) \text{ or } \gamma(\mathscr{U}, 1) \neq 0\big) \Rightarrow \big(e(S) = (1+s)\big(L(\sigma, \mathbf{c}) + \Lambda(\sigma)\big) \ \forall S \subset \mathscr{U}\big).$$

Proof We suppose that $\gamma(\mathscr{U}, \nu) \neq 0$ for $\nu = 0$ or for $\nu = 1 \bmod 2$. Let $S \subset \mathscr{U}$ such that s is odd. We fix $T = S\Delta\{\sigma\}$. Since s is odd, σ is an element of $\mathscr{U}$. We also have $\tau = \sigma + \sigma = 0$. By Lemma 22, we have $e(T) = 0$ and by Lemma 21 we get

$$e(S, \{\sigma\}) = L(\sigma, \sigma) + sP(\sigma) + \Lambda(\sigma) + s\Lambda(\sigma) = 0.$$

Combining this relation with (62), we get

$$e(S) = e(\{\sigma\}) + e(T) + e(S, \{\sigma\}) = 0,$$

which gives Lemma 23 when s is odd.

We now consider the case when s is even. If $\sigma = 0$, then Lemma 22 implies that $e(S) = 0$ and Lemma 23 is correct in that case. Now, if $\sigma \neq 0$, we consider the set $T = S\Delta\{\mathbf{c}, \mathbf{c} + \sigma\}$, which satisfies t even and $\tau = 0$. Lemma 22 gives

$$e(T) = 0. \tag{71}$$

By definition (57), by (61) and by linearity, we have

$$\begin{aligned} e(\{\mathbf{c}, \mathbf{c}+\sigma\}) &= \Phi_k(\mathbf{c}, \mathbf{c}+\sigma) \\ &= L(\mathbf{c}, \mathbf{c}+\sigma) + P(\mathbf{c}+\sigma) + \Lambda(\mathbf{c}) + \Lambda(\mathbf{c}+\sigma) \\ &= L(\mathbf{c}+\mathbf{c}+\sigma, \mathbf{c}+\sigma) + \Lambda(\sigma) = L(\sigma, \sigma) + L(\sigma, \mathbf{c}) + \Lambda(\sigma), \end{aligned}$$

which gives the equality

$$e(\{\mathbf{c}, \mathbf{c}+\sigma\}) = L(\sigma, \mathbf{c}) + \Lambda(\sigma), \tag{72}$$

since $\sigma \in \mathscr{U}_0$ and $L(\sigma,\sigma) = P(\sigma+\mathbf{0}) = 0$ (s even). By applying Lemma 21 we get (s and t are even):

$$e(S,\{\mathbf{c},\mathbf{c}+\sigma\}) = L(\sigma,\sigma) = 0. \tag{73}$$

Using (62) and the three equalities (71), (72), (73), we get that

$$\begin{aligned} e(S) &= e(S,\{\mathbf{c},\mathbf{c}+\sigma\}) + e(\{\mathbf{c},\mathbf{c}+\sigma\}) + e(T) \\ &= L(\sigma,\mathbf{c}) + \Lambda(\sigma), \end{aligned}$$

which finishes the proof of Lemma 23. □

We push further the study of subsets $\mathscr{U}$ such that $\gamma(\mathscr{U},v) \neq 0$:

Lemma 24 *Let $\mathscr{U}$ be a maximal unlinked subset of $\mathbb{F}_2^{2k}$ written in the form $\mathscr{U} = \mathbf{c}+\mathscr{U}_0$. Then we have*

$$\big(\gamma(\mathscr{U},0) \neq 0 \text{ or } \gamma(\mathscr{U},1) \neq 0\big) \Rightarrow L_{|\mathscr{U}_0\times\mathscr{U}_0} \equiv 0.$$

Proof Let σ and τ be two non zero elements of $\mathscr{U}_0$. We see that they are the sums of the elements of the following subsets of $\mathscr{U}$: $S := \{\mathbf{c},\mathbf{c}+\sigma\}$ and $T := \{\mathbf{c},\mathbf{c}+\tau\}$. These two subsets have even cardinality. By Lemma 21 and equation (62) we deduce

$$\begin{aligned} L(\sigma,\tau) &= e(S,T) = e(S)+e(T)+e(S\Delta T) \\ &= \big(L(\sigma,\mathbf{c})+\Lambda(\sigma)\big) + \big(L(\tau,\mathbf{c})+\Lambda(\tau)\big) + \big(L(\sigma+\tau,\mathbf{c})+\Lambda(\sigma+\tau)\big), \end{aligned}$$

the last line being a triple application of Lemma 23. By linearity, we finally get that $L(\sigma,\tau) = 0$. □

As Heath–Brown [10, p.354], we say that the vector subspace $\mathscr{U}_0$ of $\mathbb{F}_2^{2k}$ is *good*, when it has dimension k and when the bilinear form L is identically zero on $\mathscr{U}_0 \times \mathscr{U}_0$. Note the implication

$$\mathscr{U}_0 \text{ good} \Rightarrow \mathbf{c}+\mathscr{U}_0 \text{ is maximal unlinked for all } \mathbf{c} \in \mathbb{F}_2^{2k},$$

since, for every $\mathbf{u}$ and $\mathbf{v} \in \mathscr{U}_0$, we have

$$P\big((\mathbf{c}+\mathbf{u})+(\mathbf{c}+\mathbf{v})\big) = P(\mathbf{u}+\mathbf{v}) = L(\mathbf{u}+\mathbf{v},\mathbf{u}+\mathbf{v}) = 0.$$

We extend Lemma 23 in the following way:

Lemma 25 *Let $\mathscr{U} = \mathbf{c}+\mathscr{U}_0$ be a maximal unlinked subset of $\mathbb{F}_2^{2k}$. Then we have the implication*

$$\mathscr{U}_0 \textit{ good } \Rightarrow e(S) = (1+s)\big(L(\sigma,\mathbf{c})+\Lambda(\sigma)\big)\ \forall S \subset \mathscr{U}.$$

In particular, if s is odd, we have $e(S) = 0$.

Proof This lemma is true for $s=0$ or 1, since $e(S)=0$ in both cases. For $s=2$, it is a consequence of (72). The rest of the proof is made by induction. Let $S\subset\mathscr{U}$ with $s\geq 2$. We decompose $S=T\Delta S'$, with $s'=s-2$, $t=2$, and $\sum_{u\in S'}u=\sigma'$. By definition (62), by induction hypothesis and by Lemma 21, we have

$$\begin{aligned}e(S)&=e(T\Delta S')=e(T)+e(S')+e(T,S')\\&=\big(L(\tau,\mathbf{c})+\Lambda(\tau)\big)+(1+s')\big(L(\sigma',\mathbf{c})+\Lambda(\sigma')\big)+\big(L(\tau,\sigma')+s'\Lambda(\tau)\big)\\&=\big(L(\tau,\mathbf{c})+(1+s')L(\sigma',\mathbf{c})+L(\tau,\sigma')\big)+(1+s')\Lambda(\sigma).\end{aligned}$$

If s and s' are odd we get:

$$e(S)=L(\tau,\mathbf{c})+L(\tau,\sigma')=L(\tau,\mathbf{c}+\sigma')=0$$

since $\tau,\mathbf{c}+\sigma'\in\mathscr{U}_0$. If s and s' are even we get:

$$e(S)=L(\tau,\mathbf{c})+L(\sigma',\mathbf{c})+L(\tau,\sigma')+\Lambda(\sigma)=L(\sigma,\mathbf{c})+\Lambda(\sigma)$$

because $\tau+\sigma'=\sigma$ and $L(\tau,\sigma')=0$ since $\tau,\sigma'\in\mathscr{U}_0$. □

In order to precise the main term in Proposition 5, we must study the coefficient $\sum_{\mathscr{U}}\gamma(\mathscr{U})=\sum_{\mathscr{U}}\gamma(\mathscr{U},1)$. By decomposition and by Lemma 24, we have

$$\begin{aligned}\sum_{\mathscr{U}}\gamma(\mathscr{U})&=\sum_{\mathscr{U}_0\text{ good}}\sum_{\substack{\mathscr{U}\\ \text{coset of }\mathscr{U}_0}}\gamma(\mathscr{U})+\sum_{\mathscr{U}_0\text{ not good}}\sum_{\substack{\mathscr{U}\\ \text{coset of }\mathscr{U}_0}}\gamma(\mathscr{U})\\&=\sum_{\mathscr{U}_0\text{ good}}\sum_{\substack{\mathscr{U}\\ \text{coset of }\mathscr{U}_0}}\gamma(\mathscr{U}).\end{aligned}$$

By Lemma 25, we know that each $S\in\mathscr{P}_1(\mathbf{c}+\mathscr{U}_0)$ with $\mathscr{U}_0$ is good, satisfies $e(S)=0$. From this, we deduce

$$\sum_{\mathscr{U}}\gamma(\mathscr{U})=\sum_{\mathscr{U}_0\text{ good}}\sum_{\substack{\mathscr{U}\\ \text{coset of }\mathscr{U}_0}}\#\{S\subset\mathscr{U}\,;s\text{ odd}\}=2^k\cdot 2^{2^k-1}\sum_{\mathscr{U}_0\text{ good}}1,$$

which finally gives the equality

$$\sum_{\mathscr{U}}\gamma(\mathscr{U})=2^{2^k+k-1}\#\{\mathscr{U}_0\text{ good}\}. \tag{74}$$

5.7 Counting the number of good subspaces

As in [10, Lemma 6], we are now led to a problem of linear algebra and we prove

Lemma 26 *Let $k\geq 1$, and consider the vector space $\mathscr{E}=\mathbb{F}_2^{2k}$. Let L be the bilinear form defined on $\mathscr{E}\times\mathscr{E}$ by the formula*

$$L(\mathbf{u},\mathbf{v})=\sum_{j=0}^{k-1}u_{2j+1}(v_{2j+1}+v_{2j+2}).$$

Let $\emptyset\neq\Gamma\subseteq\{1,\dots,k\}$. Then the following holds:

(i) There is a bijection between the set of good vector subspaces $\mathscr{U}_0$ of $\mathscr{E}$ as defined before Lemma 25, and the set of vector subspaces of $\mathbb{F}_2^k$.
(ii) The number of good subspaces in $\mathscr{E}$ is equal to $\mathscr{N}(k,2)$.
(iii) The number of good subspaces $\mathscr{U}_0$ in $\mathscr{E}$ such that $\sum_{\ell\in\Gamma}(u_{2\ell-1}+u_{2\ell})=0$ for all $\mathbf{u}\in\mathscr{U}_0$ is equal to $\mathscr{N}(k-1,2)$.
(iv) The number of good subspaces $\mathscr{U}_0$ in $\mathscr{E}$ such that $\sum_{\ell\in\Gamma}u_{2\ell-1}=0$ for all $\mathbf{u}\in\mathscr{U}_0$ is equal to $\mathscr{N}(k-1,2)$.

Proof Let $\{e_1,\dots,e_{2k}\}$ be the canonical basis of $\mathscr{E}$, and let $\mathscr{B}$ the basis defined by $\mathscr{B}=\{b_1,\dots,b_{2k}\}=\{e_1+e_2,e_2,\dots,e_{2k-1}+e_{2k},e_{2k}\}$ of $\mathscr{E}$. In this new basis, we have

$$L(\mathbf{u},\mathbf{v})=\sum_{j=0}^{k-1}x_{2j+1}y_{2j+2},$$

where (x_i) and (y_j) are the components of $\mathbf{u}$ and $\mathbf{v}$ in $\mathscr{B}$. Let X and Y be the subspaces of $\mathscr{E}$ defined by

$$X=\Big\{\sum_{j=0}^{k-1}x_{2j+1}b_{2j+1}\mid x_{2j+1}\in\mathbb{F}_2\Big\},$$

and

$$Y=\Big\{\sum_{j=0}^{k-1}y_{2j+2}b_{2j+2}\mid y_{2j+2}\in\mathbb{F}_2\Big\}.$$

From the decomposition $\mathscr{E}=X\oplus Y$, we define two projections π_X and π_Y over X and Y, respectively. Note the general identity

$$L\big(\pi_X(\mathbf{u}),\pi_Y(\mathbf{v})\big)=L(\mathbf{u},\mathbf{v}). \tag{75}$$

We now prove that, for any subspace F of X there is exactly one subspace $\mathscr{U}_0\subset\mathscr{E}$ of dimension k, such that $L_{|\mathscr{U}_0\times\mathscr{U}_0}\equiv 0$ and $\pi_X(\mathscr{U}_0)=F$. Suppose $\mathscr{U}_0$ has this property. By (75), we obtain that

$$L\big(\pi_X(\mathbf{u}),\pi_Y(\mathbf{v})\big)=0,$$

for all $\mathbf{u}$ and $\mathbf{v}\in\mathscr{U}_\mathbf{0}$. This implies that $\pi_Y(\mathscr{U}_0)\subset F^\perp$, where $F^\perp$ is the vector subspace of Y with $\dim F^\perp=k-\dim F$, defined by

$$F^\perp=\big\{\mathbf{v}\in Y\ ;\ L(\mathbf{u},\mathbf{v})=0\ \forall\mathbf{u}\in F\big\}.$$

We deduce $\mathscr{U}_0\subset\pi_X(\mathscr{U}_0)\oplus\pi_Y(\mathscr{U}_0)\subset F\oplus F^\perp$, hence, by reasoning on dimensions, we see that $\mathscr{U}_0=F\oplus F^\perp$ and $\mathscr{U}_0$ is uniquely determined. The application $\mathscr{U}_0\leftrightarrow\pi_X(\mathscr{U}_0)$ is the bijection claimed in the first part. We remark that the inverse mapping is given by $F\mapsto\mathscr{U}_0:=F\oplus F^\perp$.

The second part follows immediately by the first part and the definition of $\mathscr{N}(k,2)$.

For the third part we note that **u** has the following coordinates in the new basis: $z_{2\ell-1} := u_{2\ell-1}$ and $z_{2\ell} := u_{2\ell-1} + u_{2\ell}$ for $\ell = 1,\dots,k$. Therefore the condition becomes:

$$\sum_{\ell\in\Gamma} z_{2\ell} = 0 \text{ for all } \mathbf{u} \in \mathscr{U}_0.$$

This is equivalent to the fact that the vector

$$\sum_{\ell\in\Gamma} b_{2\ell-1}$$

belongs to $\mathscr{U}_0$. This vector certainly also belongs to X which by the bijection of the first part means that we have to count all vector subspaces of X containing one given vector. Using Lemma 2 we get the desired result.

For the fourth part of the lemma we get the following condition in the new basis:

$$\sum_{\ell\in\Gamma} z_{2\ell-1} = 0 \text{ for all } \mathbf{u} \in \mathscr{U}_0.$$

Since this introduces one relation, the number of vector subspaces of X satisfying this condition is equal to $\mathscr{N}(k-1,2)$. □

To prove Theorem 6, it remains to put together Proposition 5, Lemma 26, (16) and (74).

6 The case of odd positive discriminants.

The purpose of this section is to modify the methods of §5 to treat the case of fundamental discriminants D satisfying

$$D > 0,\ D \equiv 1 \bmod 4, \tag{76}$$

and to prove an analogue of Theorem 6 for the sum

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

We shall prove

Theorem 7 *For every positive integer k and every positive ε, we have*

$$S^+(X,k,1,4) = \frac{1}{2^k}\big(\mathscr{N}(k+1,2)-\mathscr{N}(k,2)\big)\Big(\sum_{\substack{0<D<X\\ D\equiv 1 \bmod 4}} 1\Big) + O_{\varepsilon,k}\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big),$$

uniformly for $X \geq 2$. The same expansion remains true if we replace the narrow class group C_D by the ordinary class group Cl_D, in the definition of $S^+(X,k,1,4)$.

As before, the starting point of the proof of Theorem 7 is Theorem 5 and Lemma 6. Therefore Lemma 16 has to be modified into

Lemma 27 *Let D be a fundamental discriminant satisfying* (76)*. Then we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2}\,\#\big\{(a,b) \mid a,b \geq 1, D = ab,\ -a \text{ is a square } \bmod b \\ \text{and } b \text{ is a square } \bmod a\big\}.$$

When we use Jacobi symbols, we now introduce the symbol $(\frac{-1}{\cdot})$ and (20) is modified into

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=D_0D_1D_2D_3} \Big(\frac{-1}{D_0}\Big)\Big(\frac{D_2}{D_0}\Big)\Big(\frac{D_1}{D_3}\Big)\Big(\frac{D_3}{D_0}\Big)\Big(\frac{D_0}{D_3}\Big) \\ = \frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=D_0D_1D_2D_3} \Big(\frac{-1}{D_3}\Big)\Big(\frac{D_2}{D_0}\Big)\Big(\frac{D_1}{D_3}\Big)\Big(\frac{D_3}{D_0}\Big)\Big(\frac{D_0}{D_3}\Big), \qquad (77)$$

for D satisfying (76). Let

$$\lambda_1(\mathbf{u}) = u_1u_2,$$

be the two variable polynomial over $\mathbb{F}_2$. The analogue of (21) is now

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D)}} \sum_{D=D_{00}D_{01}D_{10}D_{11}} \Big\{\prod_{\mathbf{u}\in\mathbb{F}_2^2}\Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{\lambda_1(\mathbf{u})}\Big\}\Big\{\prod_{(\mathbf{u},\mathbf{v})\in\mathbb{F}_2^4}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_1(\mathbf{u},\mathbf{v})}\Big\}. \qquad (78)$$

Let λ_k be the polynomial in $2k$ variables

$$\lambda_k(\mathbf{u}) = \sum_{j=1}^{k} \lambda_1(\mathbf{u}^{(j)}) = \sum_{j=0}^{k-1} u_{2j+1}u_{2j+2}, \qquad (79)$$

with $\mathbf{u} = (\mathbf{u}^{(1)},\cdots,\mathbf{u}^{(k)})$ and $\mathbf{u}^{(j)} \in \mathbb{F}_2^2$. The analogue of Lemma 17 is

Lemma 28 *For every positive X we have the equality*

$$S^+(X,k,1,4) = 2^{-k} \sum_{(D_{\mathbf{u}})\in\mathscr{D}^+(X,k)} \Big(\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big)\Big(\prod_{\mathbf{u}}\Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{\lambda_k(\mathbf{u})}\Big)\prod_{\mathbf{u},\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u},\mathbf{v})}, \qquad (80)$$

where $\mathscr{D}^+(X,k)$ is the set of 4^k–tuples of squarefree, positive and coprime integers $(D_{\mathbf{u}})$, with $\mathbf{u} = (\mathbf{u}^{(1)},\ldots,\mathbf{u}^{(k)}) \in \mathbb{F}_2^{2k}$ satisfying

$$\prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} D_{\mathbf{u}} \leq X,\ \prod_{\mathbf{u}\in\mathbb{F}_2^{2k}} D_{\mathbf{u}} \equiv 1 \bmod 4.$$

The analysis of the error terms is the same as above, however remark that, in the proof of the analogues of (42) and (47), the values of $(\frac{-1}{D_{\mathbf{u}}})$ is fixed, since we have blocked the congruence class of $D_{\mathbf{u}}$ modulo 4. In the same way, we use the notion of maximal unlinked subsets $\mathscr{U}$ of $\mathbb{F}_2^{2k}$. We also define for such an $\mathscr{U}$,

$$\gamma^+(\mathscr{U}) = \sum_{(h_{\mathbf{u}})} \Big(\prod_{\mathbf{u}\in\mathscr{U}} (-1)^{\lambda_k(\mathbf{u})\cdot\frac{h_{\mathbf{u}}-1}{2}}\Big)\Big(\prod_{\mathbf{u},\mathbf{v}} (-1)^{\Phi_k(\mathbf{u},\mathbf{v})\cdot\frac{h_{\mathbf{u}}-1}{2}\cdot\frac{h_{\mathbf{v}}-1}{2}}\Big), \qquad (81)$$

where the sum is over $(h_{\mathbf{u}})_{\mathbf{u}\in\mathscr{U}} \in \{\pm 1 \bmod 4\}^{2^k}$ now satisfying

$$\prod_{\mathbf{u}\in\mathscr{U}} h_{\mathbf{u}} \equiv 1 \bmod 4, \tag{82}$$

and the product is over unordered pairs $\{\mathbf{u},\mathbf{v}\} \subset \mathscr{U}$.

With these conventions the analogue of Proposition 5 is

Proposition 6 *For every $k \geq 1$ and for every positive ε, we have the equality*

$$S^+(X,k,1,4) = \frac{2^{2-k-2^k}}{\pi^2}\Big(\sum_{\mathscr{U}} \gamma^+(\mathscr{U})\Big)\cdot X + O\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big),$$

where the sum is over the set of maximal unlinked sets $\mathscr{U} \subset \mathbb{F}_2^{2k}$.

6.1 Analysis of the coefficient of the main term.

We follow the study already made in §5.6 but we have to take into account the coefficient $\lambda_k(\mathbf{u})$ and also the fact that the set $S \subset \mathscr{U}$ of indices $\mathbf{u}$ where $h_{\mathbf{u}} \equiv -1 \bmod 4$ has a cardinality s, which is now even, because of (82). Let $S \in \mathscr{P}(\mathscr{U})$ with sum of elements σ and cardinality s. We define $e^+(S)$ by the formula

$$e^+(S) := \sum_{\mathbf{u}\in S} \lambda_k(\mathbf{u}) + \sum_{\mathbf{u},\mathbf{v}} \Phi_k(\mathbf{u},\mathbf{v}), \tag{83}$$

where the last sum is over unordered pairs $\{\mathbf{u},\mathbf{v}\} \subset S$. With this definition, (81) is written as

$$\gamma^+(\mathscr{U}) = \sum_{\substack{S\subset\mathscr{U}\\ s \text{ even}}} (-1)^{e^+(S)}.$$

For any $S,T \subset \mathscr{U}$ we define

$$e^+(S,T) := e^+(S) + e^+(T) + e^+(S\Delta T). \tag{84}$$

Using the fact that

$$\sum_{\mathbf{u}\in S} \lambda_k(\mathbf{u}) + \sum_{\mathbf{u}\in T} \lambda_k(\mathbf{u}) + \sum_{\mathbf{u}\in S\Delta T} \lambda_k(\mathbf{u}) = 0,$$

for any S and T subsets of $\mathscr{U}$, we have the equalities

$$e^+(S,T) = e(S,T), \tag{85}$$

and

$$e^+(S) = e(S) + \sum_{\mathbf{u}\in S} \lambda_k(\mathbf{u}), \tag{86}$$

where $e(S)$ and $e(S,T)$ are defined in (57) and (62).

More generally, for $\nu = 0$ or $1 \bmod 2$ and for $\mathscr{U}$ maximal unlinked, we study the quantity

$$\gamma^+(\mathscr{U},\nu) := \sum_{\substack{S\subset\mathscr{U}\\ s\equiv\nu \bmod 2}} (-1)^{e^+(S)}. \tag{87}$$

Similarly as (64), by squaring (87) we have

$$\gamma^{+2}(\mathscr{U},\nu)=\sum_{S\in\mathscr{P}_\nu(\mathscr{U})}\sum_{S'\in\mathscr{P}_\nu(\mathscr{U})}(-1)^{e^+(S\Delta S')}(-1)^{e^+(S',S)}.$$

Instead of summing over S', we sum over $T=S\Delta S'$ which has even cardinality. Hence

$$\begin{aligned}\gamma^{+2}(\mathscr{U},\nu)&=\sum_{\substack{T\subset\mathscr{U}\\ t\equiv 0 \bmod 2}}(-1)^{e^+(T)}\sum_{\substack{S\subset\mathscr{U}\\ s\equiv\nu \bmod 2}}(-1)^{e^+(S\Delta T,S)}\\&=\sum_{\substack{T\subset\mathscr{U}\\ t\equiv 0 \bmod 2}}(-1)^{e^+(T)}\sum_{\substack{S\subset\mathscr{U}\\ s\equiv\nu \bmod 2}}(-1)^{e(S\Delta T,S)}\\&=\sum_{\substack{T\subset\mathscr{U}\\ t\equiv 0 \bmod 2}}(-1)^{\nu\Lambda(\tau)+e^+(T)}\,\Sigma(T,\nu),\end{aligned}\tag{88}$$

by appealing to (66), (68) and (85). In particular, (88) can be written as

$$\gamma^{+2}(\mathscr{U},\nu)=2^{2^k-1}\sum_{T\in\mathscr{T}}(-1)^{e^+(T)+\nu\left(\Lambda(\tau)+L(\tau,\mathbf{c})\right)},\tag{89}$$

which is the analogue of (70). By (84), (85) and Lemma 21, we get the equalities

$$e^+(T\Delta T')=e^+(T)+e^+(T')+e(T,T')=e^+(T)+e^+(T')$$

which are true for any T and $T'\in\mathscr{T}$, where $\mathscr{T}$ is defined after (70). This implies that the application

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

is a multiplicative character on the group $(\mathscr{T},\Delta)$. From this remark and from (89), we obtain the analogue of Lemma 22:

Lemma 29 *Let $\mathscr{U}$ be a maximal unlinked subset of $\mathbb{F}_2^{2k}$. Then we have*

$$\left(\gamma^+(\mathscr{U},0)\ \textit{or}\ \gamma^+(\mathscr{U},1)\neq 0\right)\Rightarrow\left(e^+(T)=0\ \forall T\subset\mathscr{U}\ \textit{with t even and}\ \tau=0\right).$$

We now wish an analogue of Lemma 23. It is given by

Lemma 30 *Let $\mathscr{U}$ be a maximal unlinked subspace of $\mathbb{F}_2^{2k}$ written in the form $\mathscr{U}=\mathbf{c}+\mathscr{U}_0$. Then we have*

$$\left(\gamma^+(\mathscr{U},0)\ \textit{or}\ \gamma^+(\mathscr{U},1)\neq 0\right)$$

$$\Rightarrow\left(e^+(S)=\lambda_k(\sigma)+(1+s)\left(L(\mathbf{c},\sigma)+\Lambda(\sigma)\right)\ \forall S\subset\mathscr{U}\right).$$

Note the inversion of the arguments inside $L(.,.)$ by comparison with Lemma 23.

Proof We discuss on the parity of s.
• If $S \in \mathscr{P}_1(\mathscr{U})$, we have $\sigma \in \mathscr{U}$. We apply Lemma 29 with $T = S\Delta\{\sigma\}$ (hence t is even and $\tau = 0$) and obtain

$$e^+(T) = 0. \tag{90}$$

However, by the definition (84) and (85) we have

$$e^+(S) = e^+(T) + e^+(\{\sigma\}) + e(T, \{\sigma\}). \tag{91}$$

We trivially have

$$e^+(\{\sigma\}) = \lambda_k(\sigma), \tag{92}$$

and by Lemma 21, we have

$$e(T, \{\sigma\}) = L(0, \sigma) + \Lambda(0) = 0. \tag{93}$$

Gathering (90), (91), (92) and (93), we obtain the truth of Lemma 30 for odd s.
• If $S \in \mathscr{P}_0(\mathscr{U})$ and $\sigma = 0$, Lemma 29 gives Lemma 30 in that case.
• If $S \in \mathscr{P}_0(\mathscr{U})$ and $\sigma \neq 0$, we consider $T = S\Delta\{\mathbf{c}, \mathbf{c}+\sigma\}$. Such a T satisfies $T \subset \mathscr{U}$, t even and $\tau = 0$. By the definition (84) and by (85), we have the equality

$$e^+(S) = e^+(T) + e^+(\{\mathbf{c}, \mathbf{c}+\sigma\}) + e(T, \{\mathbf{c}, \mathbf{c}+\sigma\}). \tag{94}$$

By Lemma 29, we have (90) again and

$$e(T, \{\mathbf{c}, \mathbf{c}+\sigma\}) = 0, \tag{95}$$

by Lemma 21. By (72) and (86) we get:

$$e^+(\{\mathbf{c}, \mathbf{c}+\sigma\}) = \lambda_k(\mathbf{c}) + \lambda_k(\mathbf{c}+\sigma) + L(\sigma, \mathbf{c}) + \Lambda(\sigma). \tag{96}$$

To see that (94), (95) and (96) imply Lemma 30 in the case s even and $\sigma \neq 0$, it remains to prove the equality

$$L(\sigma, \mathbf{c}) + L(\mathbf{c}, \sigma) = \lambda_k(\mathbf{c}) + \lambda_k(\sigma) + \lambda_k(\mathbf{c}+\sigma).$$

The above equality is a particular case of the general equality

$$L(\mathbf{u}, \mathbf{v}) + L(\mathbf{v}, \mathbf{u}) = \lambda_k(\mathbf{u}) + \lambda_k(\mathbf{v}) + \lambda_k(\mathbf{u}+\mathbf{v}), \tag{97}$$

which is true for any $\mathbf{u}$ and $\mathbf{v} \in \mathbb{F}_2^{2k}$. A direct proof of (97), is to use the explicit definitions of L and λ_k (see (60) and (79)). The proof of Lemma 30 is now complete. □

The analogue of Lemma 24 is the following

Lemma 31 *Let $\mathscr{U}$ be a maximal unlinked subset of $\mathbb{F}_2^{2k}$ written in the form $\mathscr{U} = \mathbf{c} + \mathscr{U}_0$. Then we have*

$$\big(\gamma^+(\mathscr{U}, 0) \neq 0 \text{ or } \gamma^+(\mathscr{U}, 1) \neq 0\big) \Rightarrow L_{|\mathscr{U}_0 \times \mathscr{U}_0} \equiv 0.$$

Proof Let σ and τ be two non zero elements of $\mathscr{U}_0$. We apply Lemma 30 with the choices $S=\{\mathbf{c},\mathbf{c}+\sigma\}$ and $T=\{\mathbf{c},\mathbf{c}+\tau\}$, which are subsets of $\mathscr{U}$ with even cardinalities. We have the three equalities

$$\begin{aligned} e^+(S) &= \lambda_k(\sigma)+L(\mathbf{c},\sigma)+\Lambda(\sigma),\\ e^+(T) &= \lambda_k(\tau)+L(\mathbf{c},\tau)+\Lambda(\tau),\\ e^+(S\Delta T) &= \lambda_k(\sigma+\tau)+L(\mathbf{c},\sigma+\tau)+\Lambda(\sigma+\tau). \end{aligned}$$

Summing these three equalities, using linearity and (84), we get the equality

$$e^+(S,T)=\lambda_k(\sigma)+\lambda_k(\tau)+\lambda_k(\sigma+\tau).$$

Lemma 21 and (85) imply that $e^+(S,T)=e(S,T)=L(\sigma,\tau)$ and we get

$$L(\sigma,\tau)=\lambda_k(\sigma)+\lambda_k(\tau)+\lambda_k(\sigma+\tau).$$

This implies

$$L(\tau,\sigma)=0,$$

by combination with (97). □

We recall that a subspace $\mathscr{U}_0$ of dimension k of $\mathbb{F}_2^{2k}$ is said to be *good* if $L_{|\mathscr{U}_0\times\mathscr{U}_0}\equiv 0$. We now prove an extension of Lemma 30. It is also an analogue of Lemma 25 and shows that $e^+(S)$ depends on σ only, under some assumptions.

Lemma 32 *Let $\mathscr{U}=\mathbf{c}+\mathscr{U}_0$ a maximal unlinked subset of $\mathbb{F}_2^{2k}$. Then we have*

$$\mathscr{U}_0 \text{ good } \Rightarrow e^+(S)=\lambda_k(\sigma)+(1+s)\big(L(\mathbf{c},\sigma)+\Lambda(\sigma)\big)\ \forall S\subset\mathscr{U}.$$

Proof We prove it by induction on s. It is true for $s=0$ and $s=1$ by definition (83) of $e^+(S)$. Let $S=\{\mathbf{u},\mathbf{v}\}$ be a subset of $\mathscr{U}$. By definition (83) and by (59), we have

$$\begin{aligned} e^+(S) &= \lambda_k(\mathbf{u})+\lambda_k(\mathbf{v})+\Phi_k(\mathbf{u},\mathbf{v})\\ &= \lambda_k(\mathbf{u})+\lambda_k(\mathbf{v})+L(\mathbf{u},\mathbf{v})+P(\mathbf{v})+\Lambda(\sigma)\\ &= \big\{\lambda_k(\sigma)+L(\mathbf{u},\mathbf{v})+L(\mathbf{v},\mathbf{u})\big\}+L(\mathbf{u}+\mathbf{v},\mathbf{v})+\Lambda(\sigma), \end{aligned} \tag{98}$$

the last line being a consequence of (61) and (97). Using linearity, and the facts that $\mathscr{U}_0$ is good and that $\mathbf{u}+\mathbf{v}\in\mathscr{U}_0$, we get that $L(\mathbf{u},\mathbf{v})+L(\mathbf{v},\mathbf{u})+L(\mathbf{u}+\mathbf{v},\mathbf{v})=L(\mathbf{u},\mathbf{u}+\mathbf{v})=L(\mathbf{c},\sigma)$. Inserting this equality into (98), we complete the proof of Lemma 32 for $s=2$.

Now let $S\subset\mathscr{U}$ with cardinality $s\geq 3$. Let T be a subset of S with cardinality 2. We decompose S into $S=S'\Delta T$. By assumption of induction, we have

$$\begin{aligned} e^+(S') &= \lambda_k(\sigma')+(1+s)\big(L(\mathbf{c},\sigma')+\Lambda(\sigma')\big),\\ e^+(T) &= \lambda_k(\tau)+L(\mathbf{c},\tau)+\Lambda(\tau). \end{aligned}$$

We also have by Lemma 21 and (85) the equality

$$e^+(T,S')=e(T,S')=L(\tau,\sigma')+s\Lambda(\tau).$$

By (84) and the three above equalities we deduce

$$e^+(S)=\lambda_k(\sigma')+\lambda_k(\tau)+(1+s)L(\mathbf{c},\sigma')+L(\mathbf{c},\tau)+L(\tau,\sigma')+(1+s)\Lambda(\sigma). \quad (99)$$

We now appeal to (97) and linearity to transform (99) into

$$e^+(S)=\lambda_k(\sigma)+L(\sigma',\tau)+(1+s)L(\mathbf{c},\sigma')+L(\mathbf{c},\tau)+(1+s)\Lambda(\sigma).$$

It is now clear that, in order to complete the proof of Lemma 32, it remains to check the equality

$$L(\sigma',\tau)+(1+s)L(\mathbf{c},\sigma')+L(\mathbf{c},\tau)=(1+s)L(\mathbf{c},\sigma). \quad (100)$$

• If s is odd, $\mathbf{c}+\sigma'$ and τ are elements of $\mathscr{U}_0$, this implies the equality $L(\sigma',\tau)+L(\mathbf{c},\tau)=L(\mathbf{c}+\sigma',\tau)=0$, since $\mathscr{U}_0$ is good. Hence, (100) is true for s odd.
• If s is even, then σ' and τ belong to $\mathscr{U}_0$, hence $L(\sigma',\tau)=0$. By linearity, we also have $L(\mathbf{c},\sigma')+L(\mathbf{c},\tau)=L(\mathbf{c},\sigma)$. Hence, (100) is true for s even.

The proof of Lemma 32 is complete. □

The coefficient of the main term of Proposition 6 is (see definition (87)):

$$\sum_{\mathscr{U}}\gamma^+(\mathscr{U})=\sum_{\mathscr{U}}\gamma^+(\mathscr{U},0)=\sum_{\mathscr{U}}\sum_{\substack{S\subset\mathscr{U}\\ s\text{ even}}}(-1)^{e^+(S)}.$$

By decomposing with good subspaces and by applying Lemma 31, we have

$$\begin{aligned}\sum_{\mathscr{U}}\gamma^+(\mathscr{U})&=\sum_{\mathscr{U}_0\text{ good}}\sum_{\substack{\mathscr{U}\\ \text{coset of }\mathscr{U}_0}}\gamma^+(\mathscr{U},0)+\sum_{\mathscr{U}_0\text{ not good}}\sum_{\substack{\mathscr{U}\\ \text{coset of }\mathscr{U}_0}}\gamma^+(\mathscr{U},0)\\&=\sum_{\mathscr{U}_0\text{ good}}\sum_{\substack{\mathscr{U}\\ \text{coset of }\mathscr{U}_0}}\sum_{\substack{S\subset\mathscr{U}\\ s\text{ even}}}(-1)^{e^+(S)}.\end{aligned}$$

We write $\mathscr{U}=\mathbf{c}+\mathscr{U}_0$, apply Lemma 32, and sum over all the $\mathbf{c}\in\mathbb{F}_2^{2k}$ to write

$$\sum_{\mathscr{U}}\gamma^+(\mathscr{U})=2^{-k}\sum_{\mathscr{U}_0\text{ good}}\sum_{\mathbf{c}\in\mathbb{F}_2^{2k}}\sum_{\substack{S\subset\mathbf{c}+\mathscr{U}_0\\ s\text{ even}}}(-1)^{\lambda_k(\sigma)+L(\mathbf{c},\sigma)+\Lambda(\sigma)}. \quad (101)$$

The application $S\mapsto\mu(S):=\sigma$ is a group homomorphism between the groups $\big(\mathscr{P}_0(\mathbf{c}+\mathscr{U}_0),\Delta\big)$ and $(\mathscr{U}_0,+)$. Since $\sigma\in\mathscr{U}_0,\sigma\neq 0$ satisfies $\sigma=\mu(\{\mathbf{c},\mathbf{c}+\sigma\})$, μ is a surjective application. This implies that the equation $\mu(S)=\mathbf{x}$, with $\mathbf{x}$ given in $\mathscr{U}_0$ has exactly $2^{2^k-1}/2^k$ solutions in $S\in\mathscr{P}_0(\mathbf{c}+\mathscr{U}_0)$. This simplifies (101) into

$$\sum_{\mathscr{U}}\gamma^+(\mathscr{U})=2^{2^k-2k-1}\sum_{\mathscr{U}_0\text{ good}}\sum_{\sigma\in\mathscr{U}_0}\sum_{\mathbf{c}\in\mathbb{F}_2^{2k}}(-1)^{\lambda_k(\sigma)+L(\mathbf{c},\sigma)+\Lambda(\sigma)}. \quad (102)$$

We sum over $\mathbf{c}$ first. It is a $2k$–dimensional geometric progression. Most of the time the sum over $\mathbf{c}$ is zero, unless we have

$$\sigma_1+\sigma_2=\cdots=\sigma_{2k-1}+\sigma_{2k}=0. \quad (103)$$

Note that the assumption (103) implies $\lambda_k(\sigma)+\Lambda(\sigma)=0$. With these remarks we simplify (102) into

$$\sum_{\mathscr{U}}\gamma^+(\mathscr{U})=2^{2^k-1}\sum_{\mathscr{U}_0\text{ good}}\#\{\sigma\in\mathscr{U}_0\ ;\ \sigma\text{ satisfies (103)}\}. \tag{104}$$

We go back to the proof of Lemma 26 in §5.7 and follow the notations introduced there. Recall that a good subspace $\mathscr{U}_0$ is characterized by its projection $F=\pi_X(\mathscr{U}_0)$. In $\mathscr{U}_0$ we want to count the elements σ satisfying (103). This condition is equivalent to $\sigma\in X$. The only elements of $\mathscr{U}_0$ which satisfy (103) are the elements of F, which is an $\mathbb{F}_2$–vector space of dimension ℓ. With these observations, we transform (104) into

$$\sum_{\mathscr{U}}\gamma^+(\mathscr{U})=2^{2^k-1}\sum_{\ell=0}^{k}2^\ell\,\mathfrak{n}(k,\ell,2)=2^{2^k-1}\big(\mathscr{N}(k+1,2)-\mathscr{N}(k,2)\big), \tag{105}$$

by appealing to (12).

Putting (105) into Proposition 6, and using (16), we complete the proof of the first part of Theorem 7.

To pass from the function C_D to Cl_D, we use Corollary 1. This ends the proof of Theorem 7.

7 Negative discriminants divisible by 8

We are now concerned with fundamental discriminants D satisfying

$$D<0,\ D\equiv 0 \bmod 8, \tag{106}$$

in other words with the sum

$$S^-(X,k,0,8)=\sum_{\substack{0<-D<X\\ D\equiv 0 \bmod 8}}2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}.$$

We want to prove

Theorem 8 *For every positive integer k and every positive ε, we have*

$$S^-(X,k,0,8)=\mathscr{N}(k,2)\Big(\sum_{\substack{0<-D<X\\ D\equiv 0 \bmod 8}}1\Big)+O_{\varepsilon,k}\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big),$$

uniformly for $X\geq 2$.

The strategy is as above. Using Theorem 5 and Lemma 7, we see that the analogue of Lemma 16 now is

Lemma 33 *Let D be a fundamental discriminant satisfying* (106)*. Then we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{C}_D)}=\#\big\{(a,b)\mid a,b\geq 1,-D=8ab,\ 2a\text{ is a square }\bmod b \text{ and } b\text{ is a square }\bmod a\big\}.$$

Using now Jacobi symbols, the analogue of (20) is

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2^{\omega(-D/8)}} \sum_{-D=8D_0D_1D_2D_3} \Big(\frac{2}{D_3}\Big)\Big(\frac{D_2}{D_0}\Big)\Big(\frac{D_1}{D_3}\Big)\Big(\frac{D_3}{D_0}\Big)\Big(\frac{D_0}{D_3}\Big), \tag{107}$$

and the analogue of Lemmata 17 and 28 is

Lemma 34 *For every positive X we have the equality*

$$S^-(X,k,0,8) = \sum_{(D_{\mathbf{u}})\in\mathscr{D}^{\pm}(X/8,k)} \Big(\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big)\ \Big(\prod_{\mathbf{u}} \Big(\frac{2}{D_{\mathbf{u}}}\Big)^{\lambda_k(\mathbf{u})}\Big)\ \prod_{\mathbf{u},\mathbf{v}} \Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u},\mathbf{v})}, \tag{108}$$

where $\mathscr{D}^{\pm}(X,k) = \mathscr{D}^{+}(X,k) \cup \mathscr{D}^{-}(X,k)$.

Note that there is no more coefficient 2^{-k} in front of the right hand side of (108), and that λ_k is defined in (79). By recalling the definition (58), we write the analogue of Proposition 5.

Proposition 7 *For every $k \geq 1$ and for every positive ε, we have the equality*

$$S^-(X,k,0,8) = \frac{2^{2-2^k}}{\pi^2}\Big\{\sum_{\mathscr{U}} \big(\gamma(\mathscr{U},0)+\gamma(\mathscr{U},1)\big)\Big\}\cdot\frac{X}{8} + O\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big), \tag{109}$$

where the sum is over the set of maximal unlinked sets $\mathscr{U} \subset \mathbb{F}_2^{2k}$, such that $\lambda_k(\mathbf{u}) = 0$, for all $\mathbf{u} \in \mathscr{U}$.

Proof We follow the proof of Proposition 5 and give quick indications of the modifications to incorporate. The first one is to notice that we are summing over $(D_{\mathbf{u}})_{\mathbf{u}\in\mathscr{U}}$ such that their product is congruent to ± 1 mod 4, we must consider subsets S of $\mathscr{U}$, with even or odd cardinalities. The second one concerns the effect of the symbol $\Big(\frac{2}{D_{\mathbf{u}}}\Big)^{\lambda_k(\mathbf{u})}$. Suppose we have $\lambda_k(\mathbf{u}) = 1$ for some $\mathbf{u} \in \mathscr{U}$. Then we meet the sum

$$\sum_{D_{\mathbf{u}} \equiv h_{\mathbf{u}} \bmod 4} 2^{-k\omega(D_{\mathbf{u}})}\Big(\frac{2}{D_{\mathbf{u}}}\Big) =$$

$$\sum_{D_{\mathbf{u}} \equiv h_{\mathbf{u}} \bmod 8} 2^{-k\omega(D_{\mathbf{u}})}\Big(\frac{2}{D_{\mathbf{u}}}\Big) + \sum_{D_{\mathbf{u}} \equiv h_{\mathbf{u}}+4 \bmod 8} 2^{-k\omega(D_{\mathbf{u}})}\Big(\frac{2}{D_{\mathbf{u}}}\Big).$$

Since $h_{\mathbf{u}} = \pm 1$ the Jacobi symbol in the first sum is identically 1, whereas the Jacobi symbol in the second sum is identically -1. We see the wanted cancellation by a suitable application of Lemma 19 modified to modulus 8. Since $\mathbf{u} \in \mathscr{U}$, the variable $D_{\mathbf{u}}$ has a large enough domain of variations (see conditions (49)) to consider congruences of $D_{\mathbf{u}}$ mod 8. Therefore we can reject the corresponding term in the error term. This explains the restriction on the summation to the $\mathscr{U}$, such that $\lambda_k \equiv 0$ on $\mathscr{U}$, in the formula (109). □

The first step to pass from Proposition 7 to Theorem 8 is

Lemma 35 *We have*

$$S_1 := \sum_{\mathscr{U}} \gamma(\mathscr{U},1) = 2^{2^k-1}\mathscr{N}(k,2),$$

where the sum is over maximal unlinked subsets of $\mathscr{U} \subset \mathbb{F}_2^{2k}$ *such that* λ_k *is identical to* 0 *on* $\mathscr{U}$.

Proof We first restrict the sum to the $\mathscr{U}$ of the form $\mathbf{c}+\mathscr{U}_0$, where $\mathscr{U}_0$ is good (see Lemma 24). We shall use the following description of the $\mathscr{U}$ appearing in Lemma 35, in terms of the point

$$\rho := (0,1,0,1\ldots,0,1) \in \mathbb{F}_2^{2k}.$$

by the following

Lemma 36 *Let* $\mathscr{U}_0$ *be a good subspace of* $\mathbb{F}_2^{2k}$. *Let* $\mathscr{U}$ *a subspace of the form* $\mathbf{c}+\mathscr{U}_0$. *Then* $\lambda_k(\mathbf{u}) \equiv 0$ *identically on* $\mathscr{U}$, *if and only if* $\mathscr{U}$ *is of the form* $\mathscr{U} = \rho + \mathscr{U}_0$.

Proof Write $\mathbf{c} = (c_1, c_2, \ldots, c_{2k})$. The condition $\lambda_k(\mathbf{u}) \equiv 0$ on $\mathscr{U}$ is equivalent to both conditions $\lambda_k(\mathbf{c}+\mathbf{u}) = \lambda_k(\mathbf{c})$ for all $\mathbf{u} \in \mathscr{U}_0$ and $\lambda_k(\mathbf{c}) = 0$. The first condition is equivalent to

$$(c_2u_1 + c_1u_2 + u_1u_2) + \cdots + (c_{2k}u_{2k-1} + c_{2k-1}u_{2k} + u_{2k-1}u_{2k}) = 0,$$

but, since $\mathscr{U}_0$ is good, this equation simplifies into

$$(c_2+1)u_1 + c_1u_2 + \cdots + (c_{2k}+1)u_{2k-1} + c_{2k-1}u_{2k} = 0.$$

Since $\mathscr{U}_0$ is a vector space of dimension k, the set of $(c_1, c_2+1, \ldots, c_{2k-1}, c_{2k}+1)$ satisfying the above equation for every $\mathbf{u} \in \mathscr{U}_0$ is a vector subspace $\mathscr{V}$ of dimension k. It is easy to see that this vector space contains $\mathscr{U}_0$, since for all $\mathbf{u}$ and $\mathbf{v} \in \mathscr{U}_0$, we have

$$v_2u_1 + v_1u_2 + \cdots + v_{2k}u_{2k-1} + v_{2k-1}u_{2k} = L(\mathbf{u},\mathbf{v}) + L(\mathbf{v},\mathbf{u}) = 0,$$

since $\mathscr{U}_0$ is good. Hence, we have $\mathscr{V} = \mathscr{U}_0$. Finally, we check that $\lambda_k(\rho) = 0$. □

We return to the study of S_1. By Lemma 36, we have

$$S_1 = \sum_{\mathscr{U}_0 \text{ good}} \sum_{\substack{S \subset \rho + \mathscr{U}_0 \\ s \equiv 1 \bmod 2}} (-1)^{e(S)},$$

by Lemma 25, we have

$$S_1 = \sum_{\mathscr{U}_0 \text{ good}} \sum_{\substack{S \subset \rho + \mathscr{U}_0 \\ s \equiv 1 \bmod 2}} 1 = 2^{2^k-1} \sum_{\mathscr{U}_0 \text{ good}} 1.$$

Lemma 26 completes the proof of Lemma 35. □

The second step to pass from Proposition 7 to Theorem 8 is

Lemma 37 *We have*

$$S_0 := \sum_{\mathscr{U}} \gamma(\mathscr{U},0) = 2^{2^k-1}\mathscr{N}(k,2),$$

where the sum is over maximal unlinked subsets of $\mathscr{U} \subset \mathbb{F}_2^{2k}$ *such that* λ_k *is identical to* 0 *on* $\mathscr{U}$.

Proof By Lemmata 24, 25 and 36, we now have the equalities

$$\begin{aligned} S_0 &= \sum_{\mathscr{U}_0 \text{ good}} \sum_{\substack{S\subset\rho+\mathscr{U}_0 \\ s\equiv 0 \mod 2}} (-1)^{L(\sigma,\rho)+\Lambda(\sigma)} \\ &= \sum_{\mathscr{U}_0 \text{ good}} \sum_{\substack{S\subset\rho+\mathscr{U}_0 \\ s\equiv 0 \mod 2}} 1 \\ &= 2^{2^k-1} \sum_{\mathscr{U}_0 \text{ good}} 1, \end{aligned}$$

and the second part of Lemma 26 completes the proof of Lemma 37. □

Gathering Proposition 7, Lemma 35, Lemma 37 and (16), we finish the proof of Theorem 8.

8 Positive discriminants divisible by 8

We are now concerned with fundamental discriminants D satisfying

$$D > 0,\ D \equiv 0 \bmod 8, \tag{110}$$

in other words with the sum

$$S^+(X,k,0,8) = \sum_{\substack{0<D<X \\ D\equiv 0 \bmod 8}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}.$$

We want to prove

Theorem 9 *For every positive integer* k *and every positive* ε*, we have*

$$S^+(X,k,0,8) = \frac{1}{2^k}\big(\mathscr{N}(k+1,2)-\mathscr{N}(k,2)\big)\Big(\sum_{\substack{0<D<X \\ D\equiv 0 \bmod 8}} 1\Big) + O_{\varepsilon,k}\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big),$$

uniformly for $X \geq 2$*. The same expansion remains true if we replace the narrow class group* C_D *by the ordinary class group* Cl_D*, in the definition of* $S^+(X,k,0,8)$.

The strategy is as above. Using Theorem 5 and Lemma 7 again, we see that the analogue of Lemma 16 now is

Lemma 38 *Let D a fundamental discriminant satisfying* (110)*. Then we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2}\#\big\{(a,b) \mid a,\, b \geq 1, D = 8ab,\ -2a \text{ is a square } \bmod b \text{ and } b \text{ is a square } \bmod a\big\} + \frac{1}{2}\#\big\{(a,b) \mid a,\, b \geq 1, D = 8ab,\ -a \text{ is a square } \bmod b \text{ and } 2b \text{ is a square } \bmod a\big\}.$$

The fact that $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ is the sum of two terms generates extra difficulty. Using again Jacobi symbols, we have the equality

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D/8)}} \times \sum_{D=8D_0D_1D_2D_3} \Big(\frac{2}{D_3}\Big)\Big(\frac{D_2}{D_0}\Big)\Big(\frac{D_1}{D_3}\Big)\Big(\frac{D_3}{D_0}\Big)\Big(\frac{D_0}{D_3}\Big)\Big[\Big(\frac{-1}{D_0}\Big)+\Big(\frac{-1}{D_3}\Big)\Big], \tag{111}$$

for any D satisfying (110). Let $\xi_1(\mathbf{u})$ be the polynomial in two variables over $\mathbb{F}_2$ defined by $\xi_1(\mathbf{u}) = (u_1+1)(u_2+1)$. We write (111) in the following way

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D/8)}} \sum_{D=8D_{00}D_{01}D_{10}D_{11}} \Big\{\prod_{\mathbf{u}\in\mathbb{F}_2^2}\Big(\frac{2}{D_{\mathbf{u}}}\Big)^{\lambda_1(\mathbf{u})}\Big\}\Big\{\prod_{(\mathbf{u},\mathbf{v})\in\mathbb{F}_2^4}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_1(\mathbf{u},\mathbf{v})}\Big\} \times \Big[\Big\{\prod_{\mathbf{u}\in\mathbb{F}_2^2}\Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{\lambda_1(\mathbf{u})}\Big\}+\Big\{\prod_{\mathbf{u}\in\mathbb{F}_2^2}\Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{\xi_1(\mathbf{u})}\Big\}\Big]. \tag{112}$$

Raising (112) to the k–th power, we see that the analogue of Lemma 34 is

Lemma 39 *For every positive X we have the equality*

$$S^+(X,k,0,8) = \frac{1}{2^k}\sum_{\Gamma\subset\{1,\dots k\}} S_\Gamma \tag{113}$$

with $S_\Gamma =$

$$\sum_{(D_{\mathbf{u}})\in\mathscr{D}^{\pm}(X/8,k)} \Big(\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big)\Big(\prod_{\mathbf{u}}\Big(\frac{2}{D_{\mathbf{u}}}\Big)^{\lambda_k(\mathbf{u})}\Big)\Big(\prod_{\mathbf{u}}\Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{Q_\Gamma(\mathbf{u})}\Big)\prod_{\mathbf{u},\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u},\mathbf{v})},$$

where Q_Γ is a polynomial over $\mathbb{F}_2^{2k}$ defined by

$$Q_\Gamma(u_1,u_2,\dots,u_{2k}) = \sum_{\ell\in\Gamma} u_{2\ell-1}u_{2\ell} + \sum_{\substack{1\leq\ell\leq k\\ \ell\notin\Gamma}} (u_{2\ell-1}+1)(u_{2\ell}+1)$$
$$= \lambda_k(\mathbf{u}) + \sum_{\ell\notin\Gamma}(u_{2\ell-1}+u_{2\ell}) + k - \#\Gamma.$$

We follow the same arguments as before to arrive at the formula

$$S_\Gamma = \frac{2^{2-2^k}}{\pi^2}\Big\{\sum_{\mathscr{U}}\sum_{S\subset\mathscr{U}}(-1)^{e_\Gamma(S)}\Big\}\cdot\frac{X}{8}+O\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big), \tag{114}$$

where the sum is over maximal unlinked subsets, such that $\lambda_k(\mathbf{u})=0$, for all $\mathbf{u}\in\mathscr{U}$, and where $e_\Gamma(S)$ is defined by the formula

$$e_\Gamma(S)=\sum_{\mathbf{u}\in S}Q_\Gamma(\mathbf{u})+\sum_{\mathbf{u},\mathbf{v}}\Phi_k(\mathbf{u},\mathbf{v}),$$

where the second sum is over unordered pairs $\{\mathbf{u},\mathbf{v}\}\subset S$, without any hypothesis on the parity of s. This equality is the analogue of the formula (109). Actually, using the hypothesis $\lambda_k(\mathbf{u})=0$ concerning $\mathscr{U}$, the function e_Γ is simplified to

$$e_\Gamma(S)=e(S)+s(k-\#\Gamma)+V_\Gamma(\sigma), \tag{115}$$

where $e(S)$ is defined in (57) and where

$$V_\Gamma(\sigma)=\sum_{\ell\notin\Gamma}(\sigma_{2\ell-1}+\sigma_{2\ell})=\sum_{\mathbf{u}\in S}\sum_{\ell\notin\Gamma}(u_{2\ell-1}+u_{2\ell}).$$

As usual s and σ are the cardinality and the sum of elements of S, respectively. Using (115), we see that the coefficient of (114) can be written as

$$\sum_{\mathscr{U}}\sum_{S\subset\mathscr{U}}(-1)^{e_\Gamma(S)}=\sum_{\mathscr{U}}\Big\{\sum_{\substack{S\subset\mathscr{U}\\ s\equiv 0 \bmod 2}}(-1)^{e(S)+V_\Gamma(\sigma)}+(-1)^{k-\#\Gamma}\sum_{\substack{S\subset\mathscr{U}\\ s\equiv 1 \bmod 2}}(-1)^{e(S)+V_\Gamma(\sigma)}\Big\}, \tag{116}$$

where the sum is over maximal unlinked subsets $\mathscr{U}$ of $\mathbb{F}_2^{2k}$, on which the function λ_k is identically equal to zero. We are in a similar position as in §5.6, when we studied the functions $\gamma(\mathscr{U},0)$ and $\gamma(\mathscr{U},1)$. However we have to follow the effect of the coefficient $V_\Gamma(\sigma)$ on that study. It is easy to see that if $\mathscr{U}=\mathbf{c}+\mathscr{U}_0$, with $\mathscr{U}_0$ not good, then both sums

$$\sum_{\substack{S\subset\mathscr{U}\\ s\equiv 0 \bmod 2}}(-1)^{e(S)+V_\Gamma(\sigma)},\quad \sum_{\substack{S\subset\mathscr{U}\\ s\equiv 1 \bmod 2}}(-1)^{e(S)+V_\Gamma(\sigma)}$$

are zero (analogue of Lemma 24).

We are reduced to the cases of $\mathscr{U}=\rho+\mathscr{U}_0$, with $\mathscr{U}_0$ good. By Lemma 25 we have $e(S)=(1+s)\big(L(\sigma,\rho)+\Lambda(\sigma)\big)=0$ for all $S\subset\mathscr{U}$ since $L(\sigma,\rho)=\Lambda(\sigma)$. With these remarks we simplify (116) into

$$\sum_{\mathscr{U}}\sum_{S\subset\mathscr{U}}(-1)^{e_\Gamma(S)}=\sum_{\mathscr{U}_0\text{ good}}\Big\{\sum_{\substack{S\subset\rho+\mathscr{U}_0\\ s\equiv 0 \bmod 2}}(-1)^{V_\Gamma(\sigma)}+(-1)^{k-\#\Gamma}\sum_{\substack{S\subset\rho+\mathscr{U}_0\\ s\equiv 1 \bmod 2}}(-1)^{V_\Gamma(\sigma)}\Big\}.$$

Summing over the S with the same $\sigma\in\mathscr{U}_0$ (s even) or the same $\sigma\in\rho+\mathscr{U}_0$ (s odd), we also have

$$\begin{aligned}\sum_{\mathscr{U}}\sum_{S\subset\mathscr{U}}(-1)^{e_\Gamma(S)}&=2^{2k-k-1}\sum_{\mathscr{U}_0\text{ good}}\Big\{\sum_{\mathbf{u}\in\mathscr{U}_0}(-1)^{V_\Gamma(\mathbf{u})}+(-1)^{k-\#\Gamma}\sum_{\mathbf{u}\in\mathscr{U}_0}(-1)^{V_\Gamma(\rho+\mathbf{u})}\Big\}\\&=2^{2k-k}\sum_{\mathscr{U}_0\text{ good}}\sum_{\mathbf{u}\in\mathscr{U}_0}(-1)^{V_\Gamma(\mathbf{u})},\end{aligned} \tag{117}$$

since $V_\Gamma(\rho) = k - \#\Gamma$. Assume $\Gamma = \{1,\dots,k\}$. Then $V_\Gamma \equiv 0$ and we get

$$\sum_{\mathscr{U}} \sum_{S\subset\mathscr{U}} (-1)^{e_\Gamma(S)} = 2^{2^k}\mathscr{N}(k,2),$$

by the second part of Lemma 26. For $\Gamma \neq \{1,\dots,k\}$, (117) leads to

$$\sum_{\mathscr{U}} \sum_{S\subset\mathscr{U}} (-1)^{e_\Gamma(S)} = 2^{2^k}\#\{\mathscr{U}_0 \text{ good } ;\ \mathbf{u}\in\mathscr{U}_0 \Rightarrow V_\Gamma(\mathbf{u}) = 0\} = 2^{2^k}\mathscr{N}(k-1,2),$$

by the third part of Lemma 26. Putting these last two equations in (114) and in (113), and then summing over $\Gamma \subset \{1,\dots,k\}$ we get the following main term for $S^+(X,k,0,8)$:

$$\frac{1}{2^k}\cdot\frac{4}{\pi^2}\Big(\mathscr{N}(k,2) + (2^k-1)\mathscr{N}(k-1,2)\Big)\cdot\frac{X}{8}.$$

By (16) and (10), we see that this main term coincides with the main term announced in Theorem 9. To pass from the function C_D to Cl_D, we use Corollary 1.

9 Negative discriminants $D \equiv 4 \bmod 8$

We are now concerned with fundamental discriminants D satisfying

$$D < 0,\ D \equiv 4 \bmod 8, \tag{118}$$

in other words with the sum

$$S^-(X,k,4,8) = \sum_{\substack{0<-D<X\\ D\equiv 4 \bmod 8}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}.$$

We want to prove

Theorem 10 *For every positive integer k and every positive ε, we have*

$$S^-(X,k,4,8) = \mathscr{N}(k,2)\Big(\sum_{\substack{0<-D<X\\ D\equiv 4 \bmod 8}} 1\Big) + O_{\varepsilon,k}\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big),$$

uniformly for $X \geq 2$.

The strategy is as above. Using Theorem 5 and Lemma 7 again, we see that the analogue of Lemma 16 now is

Lemma 40 *Let D a fundamental discriminant satisfying* (118)*. Then we have the equality*

$$\begin{aligned} 2^{\mathrm{rk}_4(\mathrm{C}_D)} = {} & \frac{1}{2}\#\big\{(a,b)\mid a,b\geq 1, -D = 4ab, \textit{ a is a square } \bmod b \\ & \qquad\qquad \textit{and } b \textit{ is a square } \bmod a\big\} \\ & + \frac{1}{2}\#\big\{(a,b)\mid a,b\geq 1, -D = 4ab, \textit{ } 2a \textit{ is a square } \bmod b \\ & \qquad\qquad \textit{and } 2b \textit{ is a square } \bmod a\big\}. \end{aligned}$$

With this lemma, the analogue of (111) is

$$2^{\mathrm{rk}_4(\mathrm{C}_D)}=\frac{1}{2\cdot 2^{\omega(-D/4)}}\sum_{-D=4D_0D_1D_2D_3}\Big(\frac{D_2}{D_0}\Big)\Big(\frac{D_1}{D_3}\Big)\Big(\frac{D_3}{D_0}\Big)\Big(\frac{D_0}{D_3}\Big)\Big[1+\Big(\frac{2}{D_0}\Big)\Big(\frac{2}{D_3}\Big)\Big],\tag{119}$$

and, using the polynomial $(\lambda_1+\xi_1)(\mathbf{u})=u_1+u_2+1$, we get

$$2^{\mathrm{rk}_4(\mathrm{C}_D)}=\frac{1}{2\cdot 2^{\omega(-D/4)}}\sum_{-D=4D_{00}D_{01}D_{10}D_{11}}\Big\{\prod_{(\mathbf{u},\mathbf{v})\in\mathbb{F}_2^4}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_1(\mathbf{u},\mathbf{v})}\Big\}\\ \times\Big[1+\Big\{\prod_{\mathbf{u}\in\mathbb{F}_2^2}\Big(\frac{2}{D_{\mathbf{u}}}\Big)^{(\lambda_1+\xi_1)(\mathbf{u})}\Big\}\Big].\tag{120}$$

Raising (120) to the k–th power, we see that the analogue of Lemma 39 is

Lemma 41 *For every positive X we have the equality*

$$S^-(X,k,4,8)=\frac{1}{2^k}\sum_{\Gamma\subset\{1,\dots k\}}T_\Gamma\tag{121}$$

with

$$T_\Gamma=\sum_{(D_{\mathbf{u}})\in\mathscr{D}^+(X/4,k)}\Big\{\prod_{\mathbf{u}}2^{-k\,\omega(D_{\mathbf{u}})}\Big\}\ \Big\{\prod_{\mathbf{u}}\Big(\frac{2}{D_{\mathbf{u}}}\Big)^{V_\Gamma(\mathbf{u})+(k-\#\Gamma)}\Big\}\Big\{\prod_{\mathbf{u},\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u},\mathbf{v})}\Big\},$$

where V_Γ is the polynomial over $\mathbb{F}_2^{2k}$ defined by

$$V_\Gamma(u_1,u_2,\dots,u_{2k})=\sum_{\ell\notin\Gamma}(u_{2\ell-1}+u_{2\ell}).$$

By the same transformations as before, we arrive at

$$T_\Gamma=\frac{2^{2-2^k}}{\pi^2}\Big\{\sum_{\mathscr{U}}\sum_{\substack{S\subset\mathscr{U}\\ s\equiv 0 \bmod 2}}(-1)^{e(S)}\Big\}\cdot\frac{X}{4}+O\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big),\tag{122}$$

where the sum is over maximal unlinked subsets $\mathscr{U}$, such that $V_\Gamma(\mathbf{u})+(k-\#\Gamma)=0$, for all $\mathbf{u}\in\mathscr{U}$, and where the function $e(S)$ was defined in (57).

As before, we restrict the sum over the $\mathscr{U}=\mathbf{c}+\mathscr{U}_0$ such that $\mathscr{U}_0$ is good. Then Lemma 25 gives for such $S\subset\mathscr{U}$ with even cardinality, the equality $e(S)=L(\sigma,\mathbf{c})+\Lambda(\sigma)$. From this, we gather all the $S\subset\mathscr{U}$ with even cardinality, with the same value of $\sigma\in\mathscr{U}_0$. We deduce that the coefficient of (122) satisfies the equality

$$\Big\{\sum_{\mathscr{U}}\sum_{\substack{S\subset\mathscr{U}\\ s\equiv 0 \bmod 2}}(-1)^{e(S)}\Big\}=2^{2^k-k-1}\sum_{\mathscr{U}}\sum_{\mathbf{u}\in\mathscr{U}_0}(-1)^{L(\mathbf{u},\mathbf{c})+\Lambda(\mathbf{u})},$$

where the sum is over the maximal unlinked $\mathscr{U}$ such that $V_\Gamma(\mathscr{U}) = \{k - \#\Gamma\}$ and such that the associated $\mathscr{U}_0$ is good. Writing $\mathscr{U} = \mathbf{c} + \mathscr{U}_0$, summing over all the $\mathbf{c}$ instead of summing over the $\mathscr{U}$, we get

$$\Big\{ \sum_{\mathscr{U}} \sum_{\substack{S \subset \mathscr{U} \\ s \equiv 0 \bmod 2}} (-1)^{e(S)} \Big\} = 2^{2^k - k - 1} \sum_{\mathbf{c}} \sum_{\mathscr{U}_0 \text{ good}} 1,$$

where $\mathbf{c}$ and $\mathscr{U}_0$ also satisfy the conditions

$$\begin{cases} L(\mathbf{u}, \mathbf{c}) + \Lambda(\mathbf{u}) = 0 & \forall \mathbf{u} \in \mathscr{U}_0, \\ V_\Gamma(\mathbf{c} + \mathbf{u}) = k - \#\Gamma & \forall \mathbf{u} \in \mathscr{U}_0. \end{cases}$$

These conditions are equivalent to

$$\begin{cases} L(\mathbf{u}, \mathbf{c}) + \Lambda(\mathbf{u}) = 0 \ \forall \mathbf{u} \in \mathscr{U}_0, \\ V_\Gamma(\mathbf{u}) = 0 \ \forall \mathbf{u} \in \mathscr{U}_0, \\ V_\Gamma(\mathbf{c}) = k - \#\Gamma. \end{cases} \tag{123}$$

• When $\Gamma = \{1, \ldots, k\}$, we have $V_\Gamma \equiv 0$ and we separate the case : $c_{2j-1} + c_{2j} + 1 = 0$ for all $1 \leq j \leq k$, to find that the number of $(\mathbf{c}, \mathscr{U}_0)$ verifying (123) is equal to

$$2^k \mathscr{N}(k, 2) + (2^{2k} - 2^k) \mathscr{N}(k - 1, 2) \tag{124}$$

by the second and fourth part of Lemma 26.
• When $\Gamma \neq \{1, \ldots, k\}$ and when $c_{2j-1} + c_{2j} + 1 = 0$ for all $1 \leq j \leq k$, then we have $V_\Gamma(\mathbf{c}) = k - \#\Gamma$, and the corresponding number of $(\mathbf{c}, \mathscr{U}_0)$ verifying (123) and the just above condition is equal to

$$2^k \mathscr{N}(k - 1, 2). \tag{125}$$

by the third part of Lemma 26.
• Now suppose $\Gamma \neq \{1, \ldots, k\}$ and $c_{2j-1} + c_{2j} + 1 \neq 0$ for at least one $1 \leq j \leq k$. The second condition of (123) gives us by using the proof of the third part of Lemma 26 that the vector

$$\sum_{\ell \notin \Gamma} (e_{2\ell-1} + e_{2\ell})$$

belongs to $\mathscr{U}_0$, where $\{e_1, \ldots, e_{2\ell}\}$ is the canonical basis. We need to check, if this vector satisfies the first equation of (123):

$$\sum_{\ell \notin \Gamma} (c_{2\ell-1} + c_{2\ell} + 1) = 0 \Leftrightarrow \sum_{\ell \notin \Gamma} (c_{2\ell-1} + c_{2\ell}) = -(k - \#\Gamma).$$

Therefore our vector belongs to $\mathscr{U}_0$, if the last condition of (123) is satisfied. Using the (proof of the) fourth part of Lemma 26, the $\mathscr{U}_0$ satisfying the first condition of (123) are parametrized by all vector subspaces of a vector space of dimension $k - 1$. In order to satisfy the second equation we only need to count those subspaces, which contain the above mentioned vector. Therefore using Lemma 2 we have $\mathscr{N}(k - 2, 2)$ possibilities for $\mathscr{U}_0$. For $\Gamma \neq \{1, \ldots, k\}$ the last condition is satisfied for 2^{2k-1} choices of $\mathbf{c}$ by choosing the remaining coordinate in a way such

that the last condition of (123) is satisfied. Since we already consider 2^k of those possibilities in the case $\Gamma = \{1,\dots,k\}$ we have

$$(2^{2k-1}-2^k)\mathscr{N}(k-2,2) = 2^k(2^{k-1}-1)\mathscr{N}(k-2,2)$$

different $(\mathbf{c},\mathscr{U}_0)$ satisfying (123).

Gathering with (125), we see that when $\Gamma \neq \{1,\dots,k\}$, the total number of solutions to (123) is equal to

$$2^k\big(\mathscr{N}(k-1,2)+(2^{k-1}-1)\mathscr{N}(k-2,2)\big) = 2^k\big(\mathscr{N}(k,2)-\mathscr{N}(k-1,2)\big), \quad (126)$$

by (10). We now incorporate the values (124) and (126) of the coefficient of the main term of T_Γ (see (122)) to see that the main term of $S^-(X,k,4,8)$ is, by (121), after summation over Γ, equal to

$$\begin{aligned}&\frac{1}{2^k}\cdot\frac{2^{2-2^k}}{\pi^2}\cdot 2^{2^k-k-1}\cdot 2^k\Big(\mathscr{N}(k,2)+(2^k-1)\mathscr{N}(k-1,2)\\ &\qquad\qquad +(2^k-1)\big(\mathscr{N}(k,2)-\mathscr{N}(k-1,2)\big)\Big)\cdot\frac{X}{4}\\ &=\frac{2}{\pi^2}\cdot\mathscr{N}(k,2)\cdot\frac{X}{4}.\end{aligned}$$

By (16), we complete the proof of Theorem 10.

10 Positive discriminants $D \equiv 4 \bmod 8$

Finally, we are now concerned with fundamental discriminants D satisfying

$$D>0,\ D\equiv 4 \bmod 8, \quad (127)$$

in other words with the sum

$$S^+(X,k,4,8) = \sum_{\substack{0<D<X\\ D\equiv 4 \bmod 8}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}.$$

We want to prove

Theorem 11 *For every positive integer k and every positive ε, we have*

$$S^+(X,k,4,8) = \frac{1}{2^k}\big(\mathscr{N}(k+1,2)-\mathscr{N}(k,2)\big)\Big(\sum_{\substack{0<D<X\\ D\equiv 4 \bmod 8}} 1\Big) + O_{\varepsilon,k}\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big),$$

uniformly for $X \geq 2$. The same expansion remains true if we replace the narrow class group C_D by the ordinary class group Cl_D, in the definition of $S^+(X,k,4,8)$.

The strategy is as above. Using Theorem 5 and Lemma 7 again, we see that the analogue of Lemma 16 now is

Lemma 42 *Let D a fundamental discriminant satisfying* (127)*. Then we have the equality*

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2}\#\big\{(a,b) \mid a,b \geq 1, D = 4ab,\ -a \text{ is a square } \bmod b \text{ and } b \text{ is a square } \bmod a\big\} + \frac{1}{2}\#\big\{(a,b) \mid a,b \geq 1, D = 4ab,\ -2a \text{ is a square } \bmod b \text{ and } 2b \text{ is a square } \bmod a\big\}.$$

With this lemma, we obtain an analogue of (119) as

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D/4)}} \times \sum_{D=4D_0D_1D_2D_3} \Big(\frac{-1}{D_3}\Big)\Big(\frac{D_2}{D_0}\Big)\Big(\frac{D_1}{D_3}\Big)\Big(\frac{D_3}{D_0}\Big)\Big(\frac{D_0}{D_3}\Big)\Big[1+\Big(\frac{2}{D_0}\Big)\Big(\frac{2}{D_3}\Big)\Big], \tag{128}$$

and, using the polynomials λ_1 and ξ_1 we get the equality

$$2^{\mathrm{rk}_4(\mathrm{C}_D)} = \frac{1}{2\cdot 2^{\omega(D/4)}} \sum_{D=4D_{00}D_{01}D_{10}D_{11}} \Big\{\prod_{(\mathbf{u},\mathbf{v})\in\mathbb{F}_2^4}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_1(\mathbf{u},\mathbf{v})}\Big\}\Big\{\prod_{\mathbf{u}\in\mathbb{F}_2^2}\Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{\lambda_1(\mathbf{u})}\Big\} \times\Big[1+\Big\{\prod_{\mathbf{u}\in\mathbb{F}_2^2}\Big(\frac{2}{D_{\mathbf{u}}}\Big)^{(\lambda_1+\xi_1)(\mathbf{u})}\Big\}\Big]. \tag{129}$$

Raising (129) to the k–th power, we see that the analogue of Lemma 41 is

Lemma 43 *For every positive X we have the equality*

$$S^+(X,k,4,8) = \frac{1}{2^k}\sum_{\Gamma\subset\{1,\dots k\}} R_\Gamma \tag{130}$$

with

$$R_\Gamma = \sum_{(D_{\mathbf{u}})\in\mathscr{D}^-(X/4,k)} \Big\{\prod_{\mathbf{u}} 2^{-k\,\omega(D_{\mathbf{u}})}\Big\}\ \Big\{\prod_{\mathbf{u}\in\mathbb{F}_2^2}\Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{\lambda_k(\mathbf{u})}\Big\} \times\Big\{\prod_{\mathbf{u}}\Big(\frac{2}{D_{\mathbf{u}}}\Big)^{V_\Gamma(\mathbf{u})+(k-\#\Gamma)}\Big\}\Big\{\prod_{\mathbf{u},\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_k(\mathbf{u},\mathbf{v})}\Big\},$$

where V_Γ is defined in Lemma 41.

By the same transformations as before, we arrive at

$$R_\Gamma = \frac{2^{2-2^k}}{\pi^2}\Big\{\sum_{\mathscr{U}}\sum_{\substack{S\subset\mathscr{U}\\ s\equiv 1 \bmod 2}} (-1)^{e^+(S)}\Big\}\cdot\frac{X}{4} + O\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big), \tag{131}$$

where the sum is over maximal unlinked subsets, such that $V_\Gamma(\mathbf{u})+(k-\#\Gamma)=0$, for all $\mathbf{u}\in\mathscr{U}$, and where $e^+(S)$ is defined in (86). As before, by Lemma 31, we restrict the sum over the $\mathbf{c}+\mathscr{U}$ such that $\mathscr{U}_0$ is good. Since s is odd, Lemma 32 gives the equality $e^+(S)=\lambda_k(\sigma)$.

As usual we gather all the $S\subset\mathscr{U}$ with an odd cardinality with the same value of $\sigma\in\mathbf{c}+\mathscr{U}_0$ to write that the coefficient of (131) satisfies the equality

$$\Big\{\sum_{\mathscr{U}}\sum_{\substack{S\subset\mathscr{U}\\ s\equiv 1 \bmod 2}}(-1)^{e^+(S)}\Big\}=2^{2^k-k-1}\sum_{\mathscr{U}_0 \text{ good}}\sum_{\mathbf{u}\in\mathscr{U}}(-1)^{\lambda_k(\mathbf{u})},$$

where the sum is over all the $\mathscr{U}$ cosets of $\mathscr{U}_0$ such that $V_\Gamma(\mathbf{u})\equiv k-\#\Gamma$ on $\mathscr{U}$. We now sum over all the $\mathbf{c}$ such that $\mathscr{U}=\mathbf{c}+\mathscr{U}_0$, to write the equality

$$\Big\{\sum_{\mathscr{U}}\sum_{\substack{S\subset\mathscr{U}\\ s\equiv 1 \bmod 2}}(-1)^{e^+(S)}\Big\}=2^{2^k-2k-1}\sum_{\mathscr{U}_0 \text{ good}}\sum_{\mathbf{c}}\sum_{\mathbf{u}\in\mathscr{U}_0}(-1)^{\lambda_k(\mathbf{c}+\mathbf{u})},$$

where the sum is over the $\mathbf{c}$ and $\mathscr{U}_0$ such that $V_\Gamma(\mathbf{c})=k-\#\Gamma$ and $V_\Gamma(\mathbf{u})\equiv 0$ on $\mathscr{U}_0$. Since $\mathscr{U}_0$ is good, we use the equality

$$\lambda_k(\mathbf{c}+\mathbf{u})=(c_2+1)u_1+c_1u_2+\cdots+(c_{2k}+1)u_{2k-1}+c_{2k-1}u_{2k}+\lambda_k(\mathbf{c}).$$

Hence the associated sum $\sum_{\mathbf{u}\in\mathscr{U}_0}(-1)^{\lambda_k(\mathbf{c}+\mathbf{u})}$ is non zero if and only if we have

$$(c_2+1)u_1+c_1u_2+\cdots+(c_{2k}+1)u_{2k-1}+c_{2k-1}u_{2k}\equiv 0$$

on $\mathscr{U}_0$, which is equivalent to $\mathbf{c}\in\rho+\mathscr{U}_0$ (see the proof of Lemma 36). Noticing also that $\lambda_k(\rho)=V_\Gamma(\rho)-(k-\#\Gamma)=0$, we finally get the equality

$$\Big\{\sum_{\mathscr{U}}\sum_{\substack{S\subset\mathscr{U}\\ s\equiv 1 \bmod 2}}(-1)^{e^+(S)}\Big\}=2^{2^k-1}\#\big\{\mathscr{U}_0 \text{ good } ;\ V_\Gamma\equiv 0 \text{ on } \mathscr{U}_0\big\}. \tag{132}$$

• When $\Gamma=\{1,\dots,k\}$, the cardinality of such $\mathscr{U}_0$ is $\mathscr{N}(k,2)$ since $V_\Gamma\equiv 0$.
• When $\Gamma\neq\{1,\dots,k\}$, the cardinality of such $\mathscr{U}_0$ is $\mathscr{N}(k-1,2)$ by the third part of Lemma 26.

We insert these values in (132) and in (131). Then we sum over all $\Gamma\subset\{1,\dots,k\}$ in (130) in order to obtain the equality

$$S^+(X,k,4,8)=\frac{1}{2^k}\cdot\frac{2}{\pi^2}\Big(\mathscr{N}(k,2)+(2^k-1)\mathscr{N}(k,2)\Big)\frac{X}{4}+O\Big(X(\log X)^{-2^{-k}+\varepsilon}\Big),$$

which gives Theorem 11 by appealing to formulas (16) and (10). In this case the 4–ranks of the ordinary class group and the narrow class group always coincide since there is at least one prime divisor of D which is congruent to 3 mod 4 (see Lemma 10).

Acknowledgements Part of this work was done when the second author was visiting Centre Emile Borel (Paris) to participate in the trimester *Explicit Methods in Number Theory* (Fall 2004). He thanks this institution for this invitation. Both authors are very grateful to Karim Belabas. The authors also benefited from the generous advices of E. Kowalski and E. Royer and express their gratitude to these colleagues.

References

1. Brüdern, J.: Einführung in die analytische Zahlentheorie, Springer (1995)
2. Cohen, H., Lenstra, H.W.: Heuristics on class groups of number fields. In: Number theory, Noordwijkerhout 1983, volume 1068 of Lecture Notes in Math., pages 33–62. Springer, Berlin (1984)
3. Davenport, H.,Heilbronn, H: On the density of discriminants of cubic fields II. Proc. Roy. Soc. London Ser. A **322**(1551),405–420 (1971)
4. Dieudonné, J.: La Géométrie des Groupes Classiques. (Troisième édition). Springer (1971)
5. Fouvry, E., Klüners, J.: Cohen–Lenstra heuristics of quadratic number fields. In: F. Hess, S. Pauli, and M. Pohst (ed.) ANTS 2006, LNCS 4076, 40-55 (2006)
6. Gerth III, F.: The 4-class ranks of quadratic fields. Invent. Math. **77**(3),489–515 (1984)
7. Gerth III, F.: Extension of conjectures of Cohen and Lenstra. Exposition. Math. **5**(2),181–184 (1987)
8. Hardy, G.H. and Ramanujan, S.: The normal number of prime factors of a number *n*. Quart. J. of Math. **48**,76–92 (1920)
9. Heath–Brown, D.R.: The size of Selmer groups for the congruent number problem. Inv. Math. **111**, 171–195 (1993)
10. Heath–Brown, D.R.: The size of Selmer groups for the congruent number problem, II. Inv. Math., **118**, 331–370, (1994)
11. Heath–Brown, D.R.: A mean value estimate for real characters sums. Acta. Arith. **72**, 235–275 (1995)
12. Heilbronn, H.: On the averages of some arithmetic functions of two variables. Mathematika, **5**, 1–7, (1958)
13. Herz, C.S.: Construction of class fields. In: Seminar on Complex Multiplication, vol. 21 of Lecture Notes in Math., chap. VII. Springer, Berlin (1966)
14. Iwaniec, H., Kowalski, E.: Analytic Number Theory. Colloquium Publications **53**, AMS (2004)
15. Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers. Springer (1989)
16. Redei, L.: Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. J. Reine Angew. Math. **171**, 55–60 (1934)
17. Redei, L.: Eine obere Schranke der Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. J. Reine Angew. Math. **171**, 61–64 (1934)
18. Serre, J.P.: A Course in Arithmetic. Graduate Texts in Math. **7**, Springer, New York (1973)
19. Shiu, P.: A Brun–Titchmarsh theorem for multiplicative functions. J. Reine Angew. Math. **313**, 161–170 (1980)