

ON THE SPIEGELUNGSSATZ FOR THE 4-RANK

ÉTIENNE FOUVRY AND JÜRGEN KLÜNERS

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

1. INTRODUCTION

1.1. Conventions and notations. Throughout this work, the letter D is reserved to denote 1 or a fundamental discriminant, *i.e* the discriminant of a linear or quadratic extension of $\mathbb{Q}$. Let $K = \mathbb{Q}(\sqrt{D})$. On the set of non zero fractional ideals of the ring of integers of K we say that two fractional ideals $\mathfrak{I}$ and $\mathfrak{J}$ are *equivalent in the narrow sense*, if there is an element $a \in K$, such that $\mathfrak{I} = (a)\mathfrak{J}$ and a has positive norm. By the multiplication of the ideal classes, we obtain the (*narrow*) *class group of K* , that we denote by C_D . This is a finite abelian group.

We extend this definition of C_D in the following way: if d is a non square integer, not necessarily a fundamental discriminant, we also denote by C_d the class group of the quadratic field $\mathbb{Q}(\sqrt{d})$. When d is a non zero perfect square, we define $C_d = C_1$ to be the trivial group.

We reserve the letter p to prime numbers. For positive integers n we denote by $\omega(n)$ the number of distinct prime divisors of n . The Möbius function of a positive integer n is denoted by $\mu(n)$.

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

1.2. Scholz' Theorem. The original *Spiegelungssatz* concerned the 3-rank of C_D and was proved by Scholz [15] in the form of the double inequality

$$(1) \quad \text{rk}_3(C_d) \leq \text{rk}_3(C_{-3d}) \leq \text{rk}_3(C_d) + 1,$$

for any non square $d \geq 1$. With the above convention, it is straightforward to extend (1) to any $d \geq 1$, since the group C_{-3} is trivial.

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

Date: September 21, 2009.

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

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

$$(2) \quad \lim_{X \rightarrow +\infty} \frac{\#\{D; 0 \leq D \leq X, \text{rk}_3(C_D) = r \text{ and } \text{rk}_3(C_{-3D}) = r+1\}}{\#\{D; 0 \leq D \leq X, \text{rk}_3(C_D) = r\}} = 3^{-(r+1)}.$$

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

$$(3) \quad \text{Prob}^+(\mathcal{A}) := \lim_{X \rightarrow +\infty} \left(\sum_{\substack{0 < D \leq X \\ D \in \mathcal{A}}} 1 \right) / \left(\sum_{0 < D \leq X} 1 \right).$$

In an analogous way we define Prob^- to be the natural density within the set $\mathcal{D}^-$ of negative fundamental discriminants. Let us formulate some statement [3, (C 5 and C9) p. 56-57] of the Cohen–Lenstra–heuristics extended by Gerth to $p = 2$ in this notation.

Conjecture 2. *Let p be a prime and $r \geq 0$. Then*

- (i) $\text{Prob}^-(\{D \in \mathcal{D}^-; \text{rk}_p(C_D^2) = r\}) = a_p^-(r) := p^{-r^2} \eta_\infty(p) \eta_r(p)^{-2},$
- (ii) $\text{Prob}^+(\{D \in \mathcal{D}^+; \text{rk}_p(C_D^2) = r\}) = a_p^+(r) := p^{-r^2-r} \eta_\infty(p) \eta_r(p)^{-1} \eta_{r+1}(p)^{-1},$

where the function $\eta_k(t)$ is defined by

$$(4) \quad \eta_k(t) := \prod_{j=1}^k (1 - t^{-j})$$

for all $k \in \mathbb{N} \cup \{\infty\}$ and $t > 1$.

With the above definition, Conjecture 1 is only a statement concerning the existence and the value of a conditional probability. In other words, Dutarte believes that for any $r \geq 0$ we have the equality

$$(5) \quad \text{Prob}^+(\text{rk}_3(C_{-3D}) = r+1 \text{ and } \text{rk}_3(C_D) = r \mid \text{rk}_3(C_D) = r) = 3^{-r-1}.$$

Conjectures 1 & 2 imply that, for every $r \geq 0$, one has the equalities

$$(6) \quad \text{Prob}^+(\text{rk}_3(C_{-3D}) - 1 = \text{rk}_3(C_D) = r) = 3^{-(r+1)} a_3^+(r),$$

and

$$(7) \quad \text{Prob}^+(\text{rk}_3(C_{-3D}) = \text{rk}_3(C_D) = r) = (1 - 3^{-(r+1)}) a_3^+(r).$$

Let $\mathcal{D}^+(X)$ be the cardinality of the set $\mathcal{D}^+ \cap [1, X]$, and let R be a fixed parameter. Then summing (6) & (7) for all $0 \leq r \leq R$, we get the two lower bounds

$$(8) \quad \#\{D \in \mathcal{D}^+; D \leq X, \text{rk}_3(C_{-3D}) = \text{rk}_3(C_D) + 1\} \geq \left(\sum_{r=0}^R 3^{-(r+1)} a_3^+(r) - o_R(1) \right) \cdot \mathcal{D}^+(X)$$

and

$$(9) \quad \#\{D \in \mathcal{D}^+; D \leq X, \text{rk}_3(C_{-3D}) = \text{rk}_3(C_D)\} \geq \left(\sum_{r=0}^R (1 - 3^{-(r+1)}) a_3^+(r) - o_R(1) \right) \cdot \mathcal{D}^+(X),$$

where $X \rightarrow \infty$. However, since the two sets appearing in the left parts of (8) & (9) are a partition of the set $\mathcal{D}^+ \cap [1, X]$, we obtain the double inequality

$$(10) \quad \frac{\sum_{r=0}^R 3^{-(r+1)} a_3^+(r) - o_R(1)}{\mathcal{D}^+(X)} \leq \frac{\#\{D \in \mathcal{D}^+; D \leq X, \text{rk}_3(C_{-3D}) = \text{rk}_3(C_D) + 1\}}{\mathcal{D}^+(X)} \leq 1 - \sum_{r=0}^R (1 - 3^{-(r+1)}) a_3^+(r) + o_R(1).$$

The relation

$$\sum_{r=0}^{\infty} a_p^+(r) = 1,$$

implies the equality

$$\sum_{r=0}^{\infty} 3^{-(r+1)} a_3^+(r) = 1 - \sum_{r=0}^{\infty} (1 - 3^{-(r+1)}) a_3^+(r).$$

Hence, letting $R \rightarrow \infty$ in (10), we obtain the equality

$$(11) \quad \begin{aligned} \text{Prob}^+(\text{rk}_3(C_{-3D}) = \text{rk}_3(C_D) + 1) &= \lim_{R \rightarrow \infty} \sum_{r=0}^R 3^{-(r+1)} a_3^+(r) \\ &= \eta_{\infty}(3) \sum_{r=0}^{\infty} 3^{-(r+1)^2} \eta_r^{-2}(3) (1 - 3^{-(r+1)})^{-1} \\ &= 0.29765117 \dots \end{aligned}$$

But the equality (11) is conjectural for the moment. We remark that it has been tested on a computer (see [6, §4.2]). We did some similar experiments on a computer and the constants are close, but not too close. We remark that similar problems occur in experiments when we check proven results for the 4-rank in this way or one wishes to test one of the Cohen–Lenstra heuristics. E.g. similar problems for experiments occur in [12, p. 336] or in [16]. Usually, the problem is that the second expected main term in the asymptotic expansion is close to the main term, see [13] for the case $p = 3$.

As far as we know, the only result concerning the conjectural value (11) is due to Belabas [1, Theorem 2.1] & [2], who proved the following equality

$$(12) \quad \frac{\sum_{\substack{0 < D \leq X \\ \text{rk}_3(C_{-3D}) = \text{rk}_3(C_D) + 1}} 3^{\text{rk}_3(C_D)}}{\sum_{0 < D \leq X} 3^{\text{rk}_3(C_D)}} = \frac{1}{4} + O\left(\exp\left(-\frac{1}{5}(\log X \log \log X)^{\frac{1}{2}}\right)\right),$$

as X tends to $+\infty$. The equality (12) can be seen as a weighted version of (11). These weights are chosen in order to easily apply the seminal work of Davenport & Heilbronn [4] concerning the average behavior of the 3-part of C_D .

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

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

$$(13) \quad \text{rk}_4(C_d) \leq \text{rk}_4(C_{-d}) \leq \text{rk}_4(C_d) + 1.$$

Note the equality $\mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(\sqrt{-4d})$. We shall say that the fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-d})$ are *reflected*. Note that $\mathbb{Q}$ is reflected to $\mathbb{Q}(\sqrt{-1})$ by definition.

As for the 3-rank, the natural question is to evaluate the frequency of each of the events “ $\text{rk}_4(C_{-d}) = \text{rk}_4(C_d)$ ” and “ $\text{rk}_4(C_{-d}) = \text{rk}_4(C_d) + 1$ ”. The only paper concerning this question is due to Gerth [11]. In order to present his results we introduce several notations. For $x \geq 1$ and $r, t \geq 0$ integers we introduce the two sets

$$A_{t;x} := \{m; 1 \leq m \leq x, m \text{ squarefree, exactly } t \text{ primes ramify in } \mathbb{Q}(\sqrt{-m})/\mathbb{Q}\},$$

and

$$A_{t,r;x}^\pm := \{m; m \in A_{t;x}, \text{rk}_4(C_{-m}) = \text{rk}_4(C_m) = r\}.$$

With these conventions, Gerth proved

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

$$(14) \quad \lim_{t \rightarrow \infty} \lim_{x \rightarrow \infty} \frac{\# A_{t,r;x}^\pm}{\# A_{t;x}} = 2^{-r} 2^{-r^2} \eta_\infty(2) \eta_r(2)^{-2} = 2^{-r} a_2^-(r).$$

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

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

Theorem C. *For every integer $r \geq 0$ we have*

$$\lim_{t \rightarrow \infty} \lim_{X \rightarrow \infty} \frac{\#\{D; 0 < -D \leq X, \omega(|D|) = t, \text{rk}_4(C_D) = \text{rk}_4(C_{-D}) = r\}}{\#\{D; 0 < -D \leq X, \omega(|D|) = t\}} = 2^{-r} a_2^-(r)$$

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

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

$$\lim_{t \rightarrow \infty} \lim_{X \rightarrow \infty} \frac{\#\{D; 0 < -D \leq X, \omega(|D|) = t, \text{rk}_4(C_D) = \text{rk}_4(C_{-D}) = r\}}{\#\{D; 0 < -D \leq X, \omega(|D|) = t, \text{rk}_4(C_D) = r\}} = 2^{-r}.$$

This corollary, roughly speaking, asserts that for an imaginary quadratic field with 4-rank equal to r , the probability (in the special sense introduced by Gerth) that its reflected field has the same 4-rank is equal to 2^{-r} .

Secondly, if we sum the equality contained in Theorem C for all $r \geq 0$ and if appeal to the same trick already used in the proof of the equality (11), we obtain

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

$$\begin{aligned} \lim_{t \rightarrow \infty} \lim_{X \rightarrow \infty} \frac{\# \{D; 0 < -D \leq X, \omega(-D) = t, \text{rk}_4(C_D) = \text{rk}_4(C_{-D})\}}{\# \{D; 0 < -D \leq X, \omega(|D|) = t\}} \\ = \sum_{r=0}^{\infty} 2^{-r} a_2^-(r) = 0.610321 \dots \end{aligned}$$

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

The purpose of this paper is to prove the statements of Theorem C and Corollaries A & B, but in the context of the more natural space of probability, as defined in (3). This is far from being a simple transposition (see also the comments in §1.5 of the original proofs of Gerth, since he writes [11, p.2547]: *However, computing these limits appears to be very difficult.* The limits given in the results above by Gerth are those which will appear in Theorem 1 below.

1.4. Statement of the results. In the next theorem we state the main result for the following natural densities, where Prob is defined in (3):

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

$$\begin{aligned} (15) \quad \text{Prob}^-(\{D \in \mathcal{D}^-; \text{rk}_4(C_D) = \text{rk}_4(C_{-D}) = r\}) &= a_2^-(r) 2^{-r} \\ (16) \quad \text{Prob}^-(\{D \in \mathcal{D}^-; \text{rk}_4(C_D) = \text{rk}_4(C_{-D}) + 1 = r\}) &= a_2^-(r) (1 - 2^{-r}) \\ (17) \quad \text{Prob}^+(\{D \in \mathcal{D}^+; \text{rk}_4(C_D) = \text{rk}_4(C_{-D}) = r\}) &= a_2^+(r) (1 - 2^{-(r+1)}) \\ (18) \quad \text{Prob}^+(\{D \in \mathcal{D}^+; \text{rk}_4(C_D) = \text{rk}_4(C_{-D}) - 1 = r\}) &= a_2^+(r) 2^{-(r+1)}. \end{aligned}$$

The given densities are the same, if we further restrict to the negative (positive) fundamental D congruent to 1 mod 4, 0 mod 8, or 4 mod 8.

These results can be easily stated in conditional probabilities:

Corollary 1. *For $D < 0$ we get the following conditional probabilities:*

$$\text{Prob}^-(\{\text{rk}_4(C_{-D}) = s \mid \text{rk}_4(C_D) = r\}) = \begin{cases} 2^{-r} & \text{if } r = s \\ (1 - 2^{-r}) & \text{if } s + 1 = r \\ 0 & \text{otherwise} \end{cases}$$

For $D > 0$ we get the following conditional probabilities:

$$\text{Prob}^+(\{\text{rk}_4(C_{-D}) = s \mid \text{rk}_4(C_D) = r\}) = \begin{cases} (1 - 2^{-(r+1)}) & \text{if } r = s \\ 2^{-(r+1)} & \text{if } s - 1 = r \\ 0 & \text{otherwise} \end{cases}$$

The proof of this corollary is an obvious by-product of Theorem 1 as soon as one has the central result of [7] at one's disposal. This result is recalled as Theorem F below. It is interesting to remark that the values of these conditional probabilities, in the case of positive D , coincide with the value conjectured by Dutarte in Conjecture 1, with the natural replacement of 2 by 3. In §3.2 we also prove:

Corollary 2. *We have the equalities*

$$\begin{aligned}
 (19) \quad \text{Prob}^-(\{D \in \mathcal{D}^-; \text{rk}_4(C_D) = \text{rk}_4(C_{-D})\}) &= \sum_{r=0}^{\infty} 2^{-r} a_2^-(r) \\
 (20) \quad \text{Prob}^-(\{D \in \mathcal{D}^-; \text{rk}_4(C_D) = \text{rk}_4(C_{-D}) + 1\}) &= \sum_{r=0}^{\infty} (1 - 2^{-r}) a_2^-(r) \\
 (21) \quad \text{Prob}^+(\{D \in \mathcal{D}^+; \text{rk}_4(C_D) = \text{rk}_4(C_{-D})\}) &= \sum_{r=0}^{\infty} (1 - 2^{-(r+1)}) a_2^+(r) \\
 (22) \quad \text{Prob}^+(\{D \in \mathcal{D}^+; \text{rk}_4(C_D) = \text{rk}_4(C_{-D}) - 1\}) &= \sum_{r=0}^{\infty} 2^{-(r+1)} a_2^+(r)
 \end{aligned}$$

The given densities are the same, if we further restrict to the negative (positive) fundamental D congruent to 1 mod 4, 0 mod 8, or 4 mod 8.

It is important to remark that the values appearing on the right sides of the equations (15) and (19) coincide with the values appearing in Theorem C and Corollary B, but the probabilistic models are not the same at all. However, these coincidences confirm an intuition of Gerth (see [11, p.2547]) expressed as: *Although the limits we compute are not guaranteed to equal the above limits, our results do provide some insight into this question.*

1.5. Comparison of our result with Gerth's approach. It is necessary to compare Gerth's approach [11] to our approach, and the same commentaries apply to [7] when compared with [10]. In order to summarize the situation, let $\mathcal{Y}$ be a set of positive integers. We consider two ways of measuring the density of $\mathcal{Y}$:

- the natural one, defined by

$$\text{dens}_{\text{nat}}(\mathcal{Y}) := \lim_{X \rightarrow \infty} \frac{\#\{m \leq X; m \in \mathcal{Y}\}}{\#\{m \leq X\}}$$

- the density introduced by Gerth and defined by

$$\text{dens}_{\text{Gerth}}(\mathcal{Y}) := \lim_{t \rightarrow \infty} \lim_{X \rightarrow \infty} \frac{\#\{m \leq X; m \in \mathcal{Y}, \omega(m) = t\}}{\#\{m \leq X; \omega(m) = t\}}.$$

These densities may not exist. There is no reason that, generally speaking, there exists a link between the existence of these two densities or between their values, as it can be seen in the following two examples. Let

$$\mathcal{Y} := \{m \geq 1; \omega(m) \geq (1/2) \log \log(m+1)\}$$

In that particular case, both densities exist and we have the equality

$$\text{dens}_{\text{nat}}(\mathcal{Y}) = 1,$$

(this is a consequence of the well known fact that the function $m \mapsto \log \log(m+1)$ is a normal order of the additive function $m \mapsto \omega(m)$). For this notion, see for

instance [14, Chapter III.3]) and the trivial equality

$$\text{dens}_{\text{Gerth}}(\mathcal{Y}) = 0.$$

The second example consists in now defining $\mathcal{Y}$ as

$$\mathcal{Y} := \{m \geq 1; \omega(m) \equiv 0 \pmod{2}\}$$

By the Prime Number Theorem, we know that $\text{dens}_{\text{nat}}(\mathcal{Y}) = 1/2$ and we trivially see that $\text{dens}_{\text{Gerth}}(\mathcal{Y})$ does not exist.

However, a link could be established between these two densities, if the situation is such that one can ensure some uniformity in the double limit $\lim_{t \rightarrow \infty} \lim_{X \rightarrow \infty}$.

Gerth ([10] & [11]) builds his proofs on the theory of Redei's matrices with dimension t , and it seems quite difficult to introduce the required uniformity in such an approach. In [7] we draw a new way of attacking these questions by replacing the theory of Redei's matrices by the study of oscillations of Jacobi symbols, without any restriction on the number of prime factors of the numerator and the denominator. Note also that our proofs can be adapted to recover Gerth's results.

2. GENERAL RESULTS ON THE 4-RANK

We have already seen that our problem is deeply connected to the Cohen–Lenstra heuristics which was extended by Gerth to the case $p = 2$. In this section we want to collect the necessary statements we need for our proofs.

As usual for quadratic fields, we need to distinguish between positive and negative D , i.e. totally real and totally imaginary quadratic fields. For each case we also need to consider the behavior at 2, i.e. if $D \equiv a \pmod{q}$ for the cases

$$(23) \quad (a, q) \in \{(1, 4), (0, 8), (4, 8)\}.$$

Therefore we introduce the following six counting functions:

$$(24) \quad \mathcal{D}^{\pm}(X, a, q) := \sum_{\substack{0 < \pm D \leq X \\ D \equiv a \pmod{q}}} 1.$$

These are the cardinalities of positive (negative) fundamental discriminants (including 1) up to X which are congruent to $a \pmod{q}$. These cardinalities are well known since we have

$$(25) \quad \mathcal{D}^{-}(X, 1, 4), \ 4 \cdot \mathcal{D}^{-}(X, 0, 8) \ \& \ 4 \cdot \mathcal{D}^{-}(X, 4, 8) = \frac{2}{\pi^2} X + O(\sqrt{X}),$$

$$(26) \quad \mathcal{D}^{+}(X, 1, 4), \ 4 \cdot \mathcal{D}^{+}(X, 0, 8) \ \& \ 4 \cdot \mathcal{D}^{+}(X, 4, 8) = \frac{2}{\pi^2} X + O(\sqrt{X}),$$

uniformly for $X \geq 2$. The equalities (25) and (26) are only variations of the classical formula

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

which counts the number of squarefree numbers up to X .

In [7, Theorem 3] we proved that Conjecture 2 is true for $p = 2$ and all $r \geq 0$. For our main result we need the stronger result that the above densities are the same when we restrict the fundamental discriminants to the cases $D \equiv a \pmod{q}$ for $(a, q) \in \{(1, 4), (0, 8), (4, 8)\}$. This extension could have been easily stated in [7], but unfortunately we did not. In the following we shortly explain how to get

the stronger result. In [7] we introduced the following sums which are moments of order k of the arithmetic function $2^{\text{rk}_4(C_D)}$:

$$(27) \quad S^\pm(X, k, a, q) := \sum_{\substack{0 < \pm D \leq X \\ D \equiv a \pmod{q}}} 2^{k \text{rk}_4(C_D)},$$

where $X \geq 2$ is a real number, $k \geq 0$ is an integer, and (a, q) is chosen in $\{(1, 4), (0, 8), (4, 8)\}$. Then we proved in [7, Theorems 6–11] the following theorem, where $\mathcal{N}(k, 2)$ denotes the number of $\mathbb{F}_2$ -vector subspaces of $\mathbb{F}_2^k$.

Theorem D. *Let $(a, q) \in \{(1, 4), (0, 8), (4, 8)\}$. Then for every positive integer k , and every positive ϵ we have uniformly for $X \geq 2$:*

$$\begin{aligned} S^-(X, k, a, q) &= \mathcal{N}(k, 2) \mathcal{D}^-(X, a, q) + O_{\epsilon, k}(X(\log X)^{-2^{-k}+\epsilon}), \\ S^+(X, k, a, q) &= \frac{1}{2^k}(\mathcal{N}(k+1, 2) - \mathcal{N}(k, 2)) \mathcal{D}^+(X, a, q) + O_{\epsilon, k}(X(\log X)^{-2^{-k}+\epsilon}). \end{aligned}$$

Using the same proof as in [7, Proposition 1] and applying it to Theorem D we get the following result for our six families.

Theorem E. *Let $(a, q) \in \{(1, 4), (0, 8), (4, 8)\}$. Then for every positive integer k we get:*

$$\lim_{X \rightarrow \infty} \frac{\sum_{\substack{0 < -D \leq X \\ D \equiv a \pmod{q}}} \prod_{0 \leq i < k} (2^{\text{rk}_4(C_D)} - 2^i)}{\mathcal{D}^-(X, a, q)} = 1,$$

and

$$\lim_{X \rightarrow \infty} \frac{\sum_{\substack{0 < D \leq X \\ D \equiv a \pmod{q}}} \prod_{0 \leq i < k} (2^{\text{rk}_4(C_D)} - 2^i)}{\mathcal{D}^+(X, a, q)} = 2^{-k}.$$

We remark that the above theorem is a positive answer for [3, (C6) and (C10), p. 56f] for the case $p = 2$. Now we can use the same approach for our six subfamilies as in the proofs of [8, Theorem 1 and 2]. Altogether, we get the following theorem, which extends [7, Theorem 3] to the six families.

Theorem F. *Let (a, q) satisfying (23). For every $r \geq 0$ we have*

$$\begin{aligned} \lim_{X \rightarrow \infty} \frac{\#\{D; 0 < -D \leq X, D \equiv a \pmod{q}, \text{rk}_4(C_D) = r\}}{\mathcal{D}^-(X, a, q)} &= a_2^-(r), \\ \lim_{X \rightarrow \infty} \frac{\#\{D; 0 < D \leq X, D \equiv a \pmod{q}, \text{rk}_4(C_D) = r\}}{\mathcal{D}^+(X, a, q)} &= a_2^+(r). \end{aligned}$$

3. PROOFS OF OUR MAIN RESULTS

3.1. Some formulas. In this section we give some formulas between the densities occurring in the Cohen–Lenstra densities. In this paper we are using them only for $p = 2$ and $p = 3$, but it is easy to give them for every prime p .

Lemma 1. *Let p be a prime and $a_p^\pm(r)$ be defined as in Conjecture 2. Then*

- (i) $a_p^+(r) = \frac{p}{p^{r+1}-1} a_p^-(r)$ for all $r \geq 0$,
- (ii) $a_p^-(r+1) = \frac{p}{(p^{r+1}-1)^2} a_p^-(r)$ for all $r \geq 1$.

Proof. (i) $a_p^+(r) = p^{-r}(1 - \frac{1}{p^{r+1}})^{-1} a_p^-(r) = \frac{p}{p^{r+1}-1} a_p^-(r)$,
(ii) $a_p^-(r) = p^{-2r-1}(1 - \frac{1}{p^{r+1}})^{-2} a_p^-(r) = \frac{p}{(p^{r+1}-1)^2} a_p^-(r)$.

□

Now we define the quantities which for $p = 2$ and $p = 3$ quite naturally appear in the reflection principle.

Definition 1. For $r, s \geq 0$ we recursively define:

- (i) $c_p(0, 0) := a_p^-(0)$ and $c_p(0, 1) := a_p^+(0) - c(0, 0) = a_p^+(0) - a_p^-(0)$.
- (ii) $\forall r \geq 1 : c_p(r, r) := a_p^-(r) - c_p(r-1, r)$ and
 $c_p(r, r+1) := a_p^+(r) - c_p(r, r) = a_p^+(r) - a_p^-(r) + c(r-1, r)$.
- (iii) $c(r, s) = 0$ in all other cases, i.e. $s - r \notin \{0, 1\}$.

We remark that we have the following two easy identities:

$$a_p^-(r) = c_p(r-1, r) + c_p(r, r) \quad \forall r \geq 1$$

and

$$a_p^+(r) = c_p(r, r) + c_p(r, r+1) \quad \forall r \geq 0.$$

Now we are able to prove

Lemma 2. Let p be a prime. Then

- (i) For all $r \geq 0$ we get: $\frac{c_p(r, r)}{a_p^-(r)} = p^{-r}$.
- (ii) For all $r \geq 1$ we get: $\frac{c_p(r-1, r)}{a_p^-(r)} = 1 - p^{-r}$.
- (iii) For all $r \geq 0$ we get: $\frac{c_p(r, r)}{a_p^+(r)} = 1 - p^{-(r+1)}$.
- (iv) For all $r \geq 0$ we get: $\frac{c_p(r, r+1)}{a_p^+(r)} = p^{-(r+1)}$.

Proof. (i) We prove this by induction and $r = 0$ is trivial. Now

$$\frac{c_p(r+1, r+1)}{a_p^-(r+1)} = \frac{a_p^-(r+1) - c_p(r, r+1)}{a_p^-(r+1)} = 1 - \frac{a_p^+(r) - c_p(r, r)}{a_p^-(r+1)}.$$

Now using Lemma 1 twice this is equal to

$$1 - \frac{p/(p^{r+1}-1) a_p^-(r) - c_p(r, r)}{a_p^-(r) p/(p^{r+1}-1)^2} = 1 - (p^{r+1}-1) + \frac{1}{p^r} \frac{(p^{r+1}-1)^2}{p}$$

by induction. The latter expression equals $p^{-(r+1)}$ which proves (i).

(ii) This follows easily from (i) and $c_p(r-1, r) + c_p(r, r) = a_p^-(r)$.

(iii) By Lemma 2 (i) and by Lemma 1 we have

$$\frac{c_p(r, r)}{a_p^+(r)} = \frac{c_p(r, r)}{a_p^-(r) p/(p^{r+1}-1)} = p^{-r} \frac{p^{r+1}-1}{p} = 1 - p^{-(r+1)}.$$

(iv) The last part follows from (iii) and $a_p^+(r) = c(r, r) + c(r, r+1)$.

□

3.2. The main step. Now we are able to prove the main result which gives the natural density of the set of negative D , such that the 4-rank of C_D and C_{-D} have prescribed values. To state this result, for a and q integers, for r and s non negative integers and $X \geq 1$, we introduce the following:

$$B^\pm(X, a, q, r, s) := \sharp\{D; 0 < \pm D \leq X, D \equiv a \pmod{q}, \text{rk}_4(C_{-D}) = r, \text{rk}_4(C_D) = s\}.$$

We state

Theorem 2. *Let $(a, q) \in \{(1, 4), (0, 8), (4, 8)\}$. Then for every r and $s \geq 0$ we have*

$$\lim_{X \rightarrow \infty} \frac{B^-(X, a, q, r, s)}{\mathcal{D}^-(X, a, q)} = c_2(r, s)$$

Proof. We shall fix the case $(a, q) = (1, 4)$, and give indications for the other two cases. A direct application of Theorems A and F leads to the asymptotic behavior for $X \rightarrow \infty$

$$(28) \quad B^-(X, 1, 4, 0, 0) \sim a_2^-(0) \mathcal{D}^-(X, 1, 4),$$

and

$$(29) \quad B^-(X, 1, 4, s, s) + B^-(X, 1, 4, s-1, s) \sim a_2^-(s) \mathcal{D}^-(X, 1, 4) \quad (s \geq 1).$$

Note that when $D < 0$ is congruent to 1 mod 4, the reflected field $\mathbb{Q}(\sqrt{-D})$ has discriminant $-4D$, hence the reflection creates a bijection between the set of negative discriminants $\geq -X$ and congruent to 1 mod 4 and the set of positive discriminants $\leq 4X$ and congruent to 4 mod 8. We use this bijection in the form of the equalities

$$(30) \quad \mathcal{D}^-(X, 1, 4) = \mathcal{D}^+(4X, 4, 8) \quad \& \quad B^-(X, 1, 4, r, s) = B^+(4X, 4, 8, s, r),$$

which is true for any integers r and s . One more time using Theorems A & F we have

$$(31) \quad B^+(4X, 4, 8, s, s) + B^+(4X, 4, 8, s+1, s) \sim a_2^+(s) \mathcal{D}^+(4X, 4, 8),$$

as $X \rightarrow \infty$, for any $s \geq 0$. We reinterpret this relation by appealing to (30) giving

$$(32) \quad B^-(X, 1, 4, s, s) + B^-(X, 1, 4, s, s+1) \sim a_2^+(s) \mathcal{D}^-(X, 1, 4).$$

Let $b^-(X, r, s) := B^-(X, 1, 4, r, s) / \mathcal{D}^-(X, 1, 4)$. The relations (28), (29) & (32) are written as

$$(33) \quad \begin{cases} b^-(X, 0, 0) & \sim a_2^-(0), \\ b^-(X, s, s) + b^-(X, s-1, s) & \sim a_2^-(s) \quad (s \geq 1), \\ b^-(X, s, s) + b^-(X, s, s+1) & \sim a_2^+(s) \quad (s \geq 0), \end{cases}$$

as $X \rightarrow \infty$. Recall that $b^-(X, r, s) = 0$ when $s - r \notin \{0, 1\}$. An easy induction applied to (33), proves that each $b^-(X, r, s)$ has a limit as $X \rightarrow \infty$, which is denoted by $b^-(r, s)$. The relations (33) give the following equalities between these limits

$$(34) \quad \begin{cases} b^-(0, 0) & = a_2^-(0), \\ b^-(s, s) + b^-(s-1, s) & = a_2^-(s) \quad (s \geq 1), \\ b^-(s, s) + b^-(s, s+1) & = a_2^+(s) \quad (s \geq 0), \end{cases}$$

We exactly recognize the identities satisfied by the coefficients $c_2(r, s)$ for all r and s . By an easy induction, we deduce that $b^-(r, s) = c_2(r, s)$. This completes the proof of Theorem 1 when $(a, q) = (1, 4)$. It remains to give some hints on the other cases.

- When $(a, q) = (4, 8)$, the reflection creates a bijection between the set of negative discriminants $\geq -X$ and congruent to 4 mod 8 with the set of positive discriminants (including 1) $\leq X/4$ and congruent to 1 mod 4.
- When $(a, q) = (0, 8)$, the reflection creates a bijection between the set of negative discriminants $\geq -X$ and congruent to 0 mod 8 with the set of positive discriminants $\leq X$ and congruent to 0 mod 8.

With these remarks, the counting process is the same. $\square$

Proof of Theorem 1. By Theorem 2 we see that (15) and (16) are obvious when we use the first two formulas of Lemma 2 for $p = 2$, in the three cases of $D \equiv 1 \pmod{4}$, $D \equiv 4 \pmod{8}$ and $D \equiv 0 \pmod{8}$. For the equalities (17) and (18), we shall restrict ourselves to the case $D \equiv 1 \pmod{4}$ since the other cases are similar. So we are concerned with the limit of the ratio

$$\frac{\#\{D; 0 < D \leq X, \text{rk}_4(C_D) = \text{rk}_4(C_{-D}) = r, D \equiv 1 \pmod{4}\}}{\mathcal{D}^+(X, 1, 4)}.$$

By the reflection map, this ratio is equal to

$$\frac{\#\{D; 0 < -D \leq 4X, \text{rk}_4(C_D) = \text{rk}_4(C_{-D}) = r, D \equiv 4 \pmod{8}\}}{\mathcal{D}^+(4X, 4, 8)}.$$

By Theorem 2 as $X \rightarrow \infty$, this ratio tends to

$$c_2(r, r) = a_2^+(r)(1 - 2^{-(r+1)}),$$

by Lemma 2 (iii). $\square$

Proof of Corollary 2. Heuristically, we want to sum up the results of Theorem 1. But this is an infinite summation of all the probabilities corresponding to $0 \leq r < \infty$. Following the technique used in the proof of (11), we can perform this infinite series. Hence we can pass from each of the four equalities of Theorem 1 to each of the four equalities of Corollary 2. $\square$

3.3. The case $p = 3$. Analyzing the proof of Theorem 1, we see that everything works for $p = 3$ as soon as we have a suitable proven version of Conjecture 2. For $p = 2$ we used Theorem F which gives the corresponding densities for the cases $D \equiv a \pmod{q}$ and (a, q) as in (23). It is important for our argument in the proof of Theorem 2 that the reflection from $\mathbb{Q}(\sqrt{d})$ to $\mathbb{Q}(\sqrt{-d})$ is order preserving and is a permutation of the set consisting of the three congruence classes defined in (23).

The latter is true for $p = 3$ when we restrict to the above when we distinguish the cases $D \equiv 0 \pmod{3}$ and $D \equiv 1, 2 \pmod{3}$. Indeed, if $D > 0$ is a fundamental discriminant, then $-3D$ is a fundamental discriminant, when $D \not\equiv 0 \pmod{3}$. In case that $D \equiv 0 \pmod{3}$, the reflected field has discriminant $-D/3$. Since $-3 \equiv 1 \pmod{4}$ we have no problems with ramification at 2 in this case.

Here also, we recognize a permutation of the set consisting of the two subsets $\{D \equiv 0 \pmod{3}\}$ and $\{D \not\equiv 0 \pmod{3}\}$. Denote by

$$\mathcal{A}_0^\pm := \{D \in \mathcal{D}^\pm; D \equiv 0 \pmod{3}\} \text{ and } \mathcal{A}_{\neq 0}^\pm := \{D \in \mathcal{D}^\pm; D \not\equiv 0 \pmod{3}\}$$

four different sets. The proof of the following theorem is now obvious using the above remarks.

Theorem 3. *Assume that the following four equations are true, where $*$ $\in \{+, -\}$ and b can be 0 or $\neq 0$:*

$$\lim_{X \rightarrow \infty} \frac{\#\{D \in \mathcal{A}_b^*; 0 < |D| \leq X, \text{rk}_3(C_D) = r\}}{\#\{D \in \mathcal{A}_b^*; 0 < |D| \leq X\}} = a_3^*(r).$$

Then the corresponding result of Theorem 1 is true. Especially, Conjecture 1 is true.

The four statements assumed in the hypotheses of Theorem 3 are only extensions of some Cohen-Lenstra heuristics (see conjecture 2 above, with $p = 3$) to congruence classes modulo 3.

3.4. A weighted version. We already said in (12) that in [1, 2] a weaker result for $p = 3$ is proved. Here the density is considered with some weight which makes it possible to deduce this result by only knowing the following averages for $p = 3$:

$$\lim_{X \rightarrow \infty} \frac{\sum_{0 < D \leq X} p^{\text{rk}_p(C_D^2)}}{\sum_{0 < D \leq X} 1} = 1 + 1/p \quad \text{and} \quad \lim_{X \rightarrow \infty} \frac{\sum_{0 < -D \leq X} p^{\text{rk}_p(C_D^2)}}{\sum_{0 < -D \leq X} 1} = 2.$$

Knowing these averages (and some proven error term) for all discriminants divisible by 3, and not divisible by 3, respectively, for $p = 3$, equation (12) can be deduced.

We mention this type of result for two reasons. First, it can be proven for $p = 3$ and second we get rational constants for this weighted density. On the other hand, this weighted density is not the one, we want to get. As in Theorem 1 we have four different points of view to express this result. It is clear that in [1, 2] all of these four viewpoints could have been proved. For $p = 2$, i.e. the reflection principle for 4-ranks we can easily prove similar statements. Let us define the following weighted densities (if they exist) for $p \in \{2, 3\}, a \in \{0, 1\}$:

$$(35) \quad d_{3,a,\pm} := \lim_{X \rightarrow \infty} \frac{\sum_{\substack{0 < \pm D \leq X \\ \text{rk}_3(C_{-3D}^2) = \text{rk}_3(C_D^2) \mp a}} 3^{\text{rk}_3(C_D^2)}}{\sum_{0 < \pm D \leq X} 3^{\text{rk}_3(C_D^2)}}$$

$$(36) \quad d_{2,a,\pm} := \lim_{X \rightarrow \infty} \frac{\sum_{\substack{0 < \pm D \leq X \\ \text{rk}_2(C_{-D}^2) = \text{rk}_2(C_D^2) \mp a}} 2^{\text{rk}_2(C_D^2)}}{\sum_{0 < \pm D \leq X} 2^{\text{rk}_2(C_D^2)}}.$$

Theorem 4. *Let $p = 2$ or 3 . Then the weighted densities exist and have the following values:*

$$d_{p,1,+} = \frac{1}{p+1} \quad \text{and} \quad d_{p,0,+} = \frac{p}{p+1}$$

$$d_{p,1,-} = \frac{1}{2} \quad \text{and} \quad d_{p,0,-} = \frac{1}{2}.$$

Proof. Let us start with $d_{2,0,-}$. We multiply (15) in Theorem 1 by 2^r and using the same arguments as in the proof of Corollary 2 we have to do the summation:

$$\sum_{r=0}^{\infty} a_2^-(r) 2^{-r} 2^r = \sum_{r=0}^{\infty} a_2^-(r) = 1.$$

We know that the denominator of (36) has average 2 by Theorem D and therefore we get $1/2$ as the weighted density. The result $d_{2,1,-} = 1 - 1/2 = 1/2$ is now obvious.

Now we look at $d_{2,1,+}$ and we are led to the sum:

$$\sum_{r=0}^{\infty} a_2^+(r) 2^{-(r+1)} 2^r = 1/2 \sum_{r=0}^{\infty} a_2^+(r) = 1/2.$$

The denominator has average $3/2$ by Theorem D and we get $\frac{1/2}{3/2} = 1/3$ as the weighted density.

The result for $p = 3$ is proven in [1, 2] for $d_{3,1,+}$. Then $d_{3,0,+} = 1 - d_{3,1,+}$ and the other two densities can be proved analogously to the proof in [1, 2]. $\square$

4. SOME REMARKS

In a prior version of this paper we gave a much more complicated proof of Theorem 1. We defined for (a, q) in (23):

$$(37) \quad S_{\text{mix}}^-(X, k, a, q) := \sum_{\substack{0 < -D \leq X \\ D \equiv a \pmod{q}}} 2^{k \text{rk}_4(C_D)} \cdot 2^{\text{rk}_4(C-D)}.$$

Then we proved with similar techniques as in [7] the following theorem.

Theorem 5. *Let (a, q) satisfying (23). Then for any integer $k \geq 0$ and for any $\epsilon > 0$ we have the equality*

$$S_{\text{mix}}^-(X, k, a, q) = \frac{\mathcal{N}(k+1, 2) + \mathcal{N}(k, 2)}{2} \cdot \mathcal{D}^-(X, a, q) + O_{k,\epsilon} \left(X (\log X)^{-2^{-k}+\epsilon} \right)$$

uniformly for $X \geq 2$.

After this it was possible to deduce Theorem 1 from this theorem and the main result in [7].

Our new proof is simply a corollary of Theorem F, which is a slight extension of [7, Theorem 3]. Unfortunately, we did not know about this possibility when we wrote the paper [7]. We already mentioned the results of Gerth [10, 11] which prove these things by considering the number of prime factors. In the second paper he also starts by reproving all the things in a similar way as he did in [10]. It is possible to use the same procedure to derive the results in [11] from the earlier paper [10], provided that it has been generalized to each of the congruence classes appearing in (23).

In [6] Dutarte is checking the compatibility of different principles leading to the Cohen–Lenstra heuristics and to the probabilities occurring in the reflection principle. Theorem 3 shows that the corresponding probabilities in the reflection principle can be deduced when we know that Cohen–Lenstra heuristics are true for $p = 3$ in congruence classes modulo 3. This was not seen in [6]. Nevertheless, he produces a heuristics for the other direction.

REFERENCES

- [1] K. Belabas, On the mean 3–rank of quadratic fields. *Comp. Math.*, 118: 1–9, 1999.
- [2] K. Belabas, Corrigendum: On the mean 3–rank of quadratic fields. *Comp. Math.*, 140: 1221, 2004.
- [3] H. Cohen and H.W. Lenstra, Heuristics on class groups of number fields. in *Number Theory, Noordwijkerhout 1983. Lecture Notes in Math.*, vol. 1068: 33–62, Springer, Berlin, 1984.
- [4] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields (ii). *Proc. Roy. Soc. London A*, 322: 405–420, 1971.

- [5] P. Damey and J.-J. Payan, Existence et construction des extensions galoisiennes et non-abéliennes de degré 8 d'un corps de caractéristique différente de 2. *J. für reine Angew. Math.*, 244 : 37–54, 1970.
- [6] P. Dutarte, Compatibilité avec le Spiegelungssatz de propabilités conjecturales sur le p -rang du groupe de classes. *Théorie des Nombres (Besançon)*, 1983 – 1984, Exp. No. 4, 11 pp., Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1984.
- [7] E. Fouvry and J. Klüners, On the 4-rank of quadratic number fields. *Inv. math.*, 167 : 455–516, 2007.
- [8] E. Fouvry and J. Klüners, Cohen-Lenstra heuristics of quadratic number fields. *Algorithmic number theory, Lecture Notes in Comput. Sci.*, 4076 : 40–55, Springer, Berlin, 2006.
- [9] E. Fouvry and J. Klüners, On the negative Pell equation. *to appear in Annals of Math.*, 2009.
- [10] F. Gerth III, The 4-class ranks of quadratic fields. *Inv. math.*, 77 : 489–515, 1984.
- [11] F. Gerth III, Comparison of 4-class ranks of certain quadratic fields. *Proc. Amer. Math. Soc.*, 129 (n. 9) : 2547–2552, 2001.
- [12] D.R. Heath-Brown, The size of Selmer groups for the congruent number problem.II. *Inv. Math.*, 118 : 331–370, 1994.
- [13] D. Roberts, Density of cubic field discriminants, *Math. Comp.*, 70: 1699–1705, 2001.
- [14] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Collection Échelles, Éditions Belin (2008).
- [15] A. Scholz, Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. *J. für reine Angew. Math.*, 166 : 201–203, 1932.
- [16] P. Stevenhagen, The number of real quadratic fields with units of negative norms. *Experiment. Math.*, 2: 121–136, 1993.

UNIV. PARIS-SUD, LABORATOIRE DE MATHÉMATIQUES D'ORSAY, CNRS, F-91405 ORSAY CEDEX, FRANCE

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

UNIVERSITÄT PADERBORN, INSTITUT FÜR MATHEMATIK, D-33095 PADERBORN, GERMANY

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