JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Étienne FOUVRY et Peter KOYMANS

On Dirichlet biquadratic fields

Tome 34, nº 3 (2022), p. 637-646.

https://doi.org/10.5802/jtnb.1220

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **34** (2022), 637–646

On Dirichlet biquadratic fields

par Étienne FOUVRY et Peter KOYMANS

Résumé. Nous prouvons l'existence d'un sous–ensemble, de densité positive, d'entiers $n > 0$ sans facteur carré, tels que le 4–rang du groupe de classes d'idéaux de $\mathbb{Q}(\sqrt{-n}, \sqrt{n})$ vaut $\omega_3(n) - 1$. On a désigné par $\omega_3(n)$ le nombre de diviseurs premiers de l'entier n qui sont congrus à 3 modulo 4. Rappelons que, pour les groupes de classes associés à $\mathbb{Q}(\sqrt{n})$ et $\mathbb{Q}(\sqrt{-n})$, un sous–ensemble analogue d'entiers n n'existe pas.

Abstract. We prove the existence of a subset, with positive natural density, of squarefree integers $n > 0$ such that the 4–rank of the ideal class group of $\mathbb{Q}(\sqrt{-n}, \sqrt{n})$ is $\omega_3(n) - 1$, where $\omega_3(n)$ is the number of prime divisors of n that are 3 modulo 4. Recall that for the class groups associated to $\mathbb{Q}(\sqrt{n})$ or $\mathbb{Q}(\sqrt{-n})$ an analogous subset of n does not exist.

1. Introduction

The Cohen–Lenstra heuristics [2] predict the distribution of the p-parts of class groups for the family of imaginary quadratic and real quadratic fields, where p is an odd prime. These heuristics have been extended to $p = 2$ by Gerth [10], and have recently been proven by Smith [17, Theorem 1.4] in a major breakthrough in the context of imaginary quadratic fields. The last paragraph of the introduction of [13] now explains how to develop Smith's method in the case of real quadratic fields.

The Cohen–Lenstra heuristics have been extended to more general families of fields by Cohen and Martinet [3]. However, their work only deals with the p-part with p coprime to the degree of the number field. In this work we explore some of the interesting features when one considers the 2-part of class groups of biquadratic fields. To the best of our knowledge, there are no heuristics in this setting and it would be an interesting task to develop such heuristics. The odd part of the class group is much better understood, since it is known to be isomorphic to the direct product of the odd parts of the class groups of its quadratic subfields (about this isomorphism, see [14, p. 246] for instance).

Manuscrit reçu le 15 avril 2021, révisé le 31 mai 2021, accepté le 1er octobre 2021.
Mathematics Subject Classification. 11R29, 11R45.
Mots-clefs. Class groups, Dirichlet biquadratic fields.
The second author wishes to thank the Max Planck Institute for Mathematics in Bonn for its financial support, great work conditions and an inspiring atmosphere.

To present our results, we will use the following notations

- if K is a number field, $\mathcal{O}_K$ is the ring of integers of K, $\mathrm{Cl}(K)$ is the ordinary class group of ideals of $\mathcal{O}_K$ and $\mathrm{Cl}^+(K)$ is the corresponding narrow class group,
- throughout this paper, n is a squarefree integer greater than 1 and K_n is the biquadratic field defined by $K_n := \mathbb{Q}(\sqrt{n}, \sqrt{-n})$. The fields K_n were first studied by Dirichlet and are called *Dirichlet biquadratic fields*,
- if G is a finite abelian group and $k \geq 1$ is an integer, the 2^k–rank of G is by definition

$$\mathrm{rk}_{2^k}(G) := \dim_{\mathbb{F}_2}(2^{k-1}G)\Big/(2^kG),$$

- the letters p, $p_1, \ldots, p'$ are reserved to prime numbers. The total number of prime divisors of $n \geq 1$ is denoted by $\Omega(n)$. The number of distinct prime divisors of n is denoted by $\omega(n)$ and the number of distinct prime divisors congruent to 1 and 3 modulo 4 are denoted by $\omega_1(n)$ and $\omega_3(n)$ respectively,
- we denote by $\mathcal{E}$ the following *exceptional set*

$$\mathcal{E} := \{n > 3 : n \text{ squarefree and there exist } c, e \in \mathbb{Z} \text{ with } c^2 - ne^2 = \pm 2\}.$$

Considerations on the prime divisors of n and classical sieve techniques imply that $\mathcal{E}$ has $O(x(\log x)^{-1/2})$ elements $n \leq x$. We can now state

Theorem 1.1. *Let $n > 3$ be a squarefree integer satisfying the equalities*

$$\mathrm{rk}_4\,\mathrm{Cl}(\mathbb{Q}(\sqrt{n})) = \mathrm{rk}_4\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-n})) = 0. \tag{1.1}$$

We then have the equality

$$\mathrm{rk}_4\,\mathrm{Cl}(K_n) = \omega_3(n) + \delta(n) + \epsilon(n) - 1,$$

where $\epsilon(n) = 1$ if $n \in \mathcal{E}$ and 0 otherwise, and $\delta(n)$ is defined as follows

$$\delta(n) = \begin{cases} 1 & \text{if } \omega_3(n) = 0 \text{ and } \exists\ p \mid n,\ p \equiv 5 \bmod 8, \\ 0 & \text{if } \omega_3(n) = 0 \text{ and } \forall\ p \mid n \Rightarrow p \not\equiv 5 \bmod 8, \\ 0 & \text{if } \omega_3(n) \geq 1 \text{ and } \exists\ p \mid n,\ p \equiv 5 \bmod 8, \\ -1 & \text{if } \omega_3(n) \geq 1 \text{ and } \forall\ p \mid n \Rightarrow p \not\equiv 5 \bmod 8. \end{cases}$$

Let us remark that the set of n satisfying (1.1) represents about 28% of the set of squarefree integers, see Proposition 2.11. Theorem 1.1 shows that $\mathrm{rk}_4\,\mathrm{Cl}(K_n) = \omega_3(n) - 1$ for the set of $n < x$ satisfying equation (1.1) with at most $O(x/(\log x)^{1/4})$ exceptions. This gives a non-trivial constraint that any future heuristic regarding $\mathrm{Cl}(K_n)$ must take into account.

Our results ultimately follow from a class number formula due to Dirichlet. Here the assumption that n satisfies equation (1.1) is vital, since it ensures that the 8-rank of $\mathrm{Cl}(K_n)$ vanishes. Then the class number formula

allows us to express $\mathrm{rk}_4\,\mathrm{Cl}(K_n)$ in terms of the Hasse unit index, $\mathrm{rk}_2\,\mathrm{Cl}(K_n)$, $\mathrm{rk}_2\,\mathrm{Cl}(\mathbb{Q}(\sqrt{n}))$ and $\mathrm{rk}_2\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-n}))$. The latter three quantities are computed using genus theory.

After publication of this work, the authors have shown in joint work with Pagano [9] that the 4-rank of $\mathrm{Cl}(K_n)$ equals $\omega_3(n)-1$ for 100% of the odd, squarefree integers n, which in turn has been extended to even n in [12]. The results in [9, 12] require more advanced analytic techniques than this work, and furthermore do not offer any control over the exceptional set (here exceptional means not satisfying $\mathrm{rk}_4\,\mathrm{Cl}(K_n)=\omega_3(n)-1$) unlike our Theorem 1.1.

Corollary 1.2. *For every squarefree integer $n>3$ satisfying* (1.1) *we have the inequalities*

$$\max(\omega_3(n)-2,0)\le \mathrm{rk}_4\,\mathrm{Cl}(K_n)\le \omega_3(n)+1.$$

Corollary 1.2 gives a rather precise formula for the function $\mathrm{rk}_4(\mathrm{Cl}(K_n))$ provided that n satisfies (1.1). Furthermore, a classical result of analytic number theory asserts that most of the integers n are such that $\omega(n)$ is very close to its average value $\log\log n$. The same concentration phenomenon holds for the function $\omega_3(n)$ around the value $(1/2)\log\log n$ (see Proposition 2.15 below). Combining these facts with Corollary 1.2, we deduce the following.

Corollary 1.3. *Let $\varepsilon>0$ be given. Then, for $x>x_0(\varepsilon)$ we have that*

$$\frac{|\{3\le n\le x : n \text{ squarefree}, |\mathrm{rk}_4\,\mathrm{Cl}(K_n)-(1/2)\log\log n|\le \varepsilon\log\log n\}|}{|\{3\le n\le x : n \text{ squarefree}\}|}$$

is at least 0.28.

This corollary shows that a positive proportion of squarefree n are such that the associated Dirichlet biquadratic field has a large 4–rank. Since the function $\log\log n$ tends to infinity with n, we see that the situation is completely different for the case of the quadratic fields $\mathbb{Q}(\sqrt{n})$ and $\mathbb{Q}(\sqrt{-n})$, where the 4–rank has an average tendency to be much smaller. For a precise statement, see Proposition 2.9 below.

2. Notations, lemmas and propositions

2.1. Notations. We complete the notations given in the introduction by the following

- to shorten notations, we write $\mathrm{Cl}(n)$ and $\mathrm{Cl}^+(n)$ for $\mathrm{Cl}(\mathbb{Q}(\sqrt{n}))$ and $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{n}))$ respectively. Their cardinalities are denoted by $h(n)$ and $h^+(n)$,
- the subset of invertible elements of $\mathcal{O}_K$ is denoted by $\mathcal{O}_K^*$,

- we also introduce the following set
$$\mathcal{D} := \{D : D \text{ fundamental discriminant}\},$$
and its two subsets $\mathcal{D}^+$ and $\mathcal{D}^-$ containing the fundamental $D > 0$ and $D < 0$ respectively, and finally
$$\mathcal{N} := \{n \geq 3 \text{ squarefree} : \mathrm{rk}_4(\mathrm{Cl}^+(n)) = \mathrm{rk}_4(\mathrm{Cl}(-n)) = 0\},$$
- for every integer $r \geq 0$, the function $\eta_r : \mathbb{R}^+ \to \mathbb{R}^+$ is defined by the formula
$$\eta_r(t) := \prod_{j=1}^{r}(1 - t^{-j}).$$

2.2. The 2–rank of class groups in the case of quadratic fields. The first lemma is famous and was proved by Gauss in the context of binary quadratic forms.

Lemma 2.1. *Let D be an element of $\mathcal{D}$. Then we have*
$$\mathrm{rk}_2(\mathrm{Cl}^+(D)) = \omega(|D|) - 1.$$

If D is negative, the two class groups $\mathrm{Cl}^+(D)$ and $\mathrm{Cl}(D)$ coincide. This may be not the case when $D > 0$. However we have

Lemma 2.2. *Let D be an element of $\mathcal{D}^+$. We have*

(i) $\mathrm{Cl}(D)$ *is a factor group of* $\mathrm{Cl}^+(D)$ *with index* $\mathfrak{i}(D) \in \{1, 2\}$*, in particular we have the inequalities*
$$\mathrm{rk}_2(\mathrm{Cl}^+(D)) - 1 \leq \mathrm{rk}_2(\mathrm{Cl}(D)) \leq \mathrm{rk}_2(\mathrm{Cl}^+(D)),$$

(ii) $\mathfrak{i}(D)$ *is equal to* 2 *if and only if the fundamental unit of* $\mathcal{O}^*_{\mathbb{Q}(\sqrt{D})}$ *has norm* 1*,*

(iii) *we have the equality*
$$\mathrm{rk}_2(\mathrm{Cl}(D)) = \mathrm{rk}_2(\mathrm{Cl}^+(D)) - 1$$
if and only if D is divisible by some $p \equiv 3 \bmod 4$.

For comments on this last item, see [7, Lemma 1]. From Lemmas 2.1 and 2.2 we deduce the following statement.

Lemma 2.3. *Let $n \geq 3$ be a squarefree integer. Then we have*
$$\mathrm{rk}_2(\mathrm{Cl}(n)) = \begin{cases} \omega(n) - 2 & \text{if } n \equiv 1, 2 \bmod 4 \text{ and } \omega_3(n) \geq 1, \\ \omega(n) - 1 & \text{if } n \equiv 1, 2 \bmod 4 \text{ and } \omega_3(n) = 0, \\ \omega(n) - 1 & \text{if } n \equiv 3 \bmod 4, \end{cases} \tag{2.1}$$
and also
$$\mathrm{rk}_2(\mathrm{Cl}(-n)) = \begin{cases} \omega(n) & \text{if } n \equiv 1 \bmod 4, \\ \omega(n) - 1 & \text{if } n \equiv 2, 3 \bmod 4. \end{cases} \tag{2.2}$$

Proof. It is based on the fact that the discriminant of the field $\mathbb{Q}(\sqrt{\pm n})$ is either $\pm n$ or $\pm 4n$ according to the congruence class of $\pm n$ mod 4. □

We gather (2.1) and (2.2) of Lemma 2.3 in the following statement which will be useful in Section 3.

Proposition 2.4. *Let $n \geq 3$ be a squarefree integer. We then have the equality*

$$\mathrm{rk}_2(\mathrm{Cl}(n)) + \mathrm{rk}_2(\mathrm{Cl}(-n)) = \begin{cases} 2\omega(n) - 1 - \mathbf{1}_{n\equiv 2 \bmod 4} & \text{if } \omega_3(n) = 0, \\ 2\omega(n) - 2 - \mathbf{1}_{n\equiv 2 \bmod 4} & \text{if } \omega_3(n) \geq 1. \end{cases}$$

2.3. The 2–rank of class groups in the case of Dirichlet biquadratic fields. We will prove the following

Proposition 2.5. *Let $n \geq 3$ be a squarefree integer. We have the equality*

$$\mathrm{rk}_2\,\mathrm{Cl}(K_n) = \begin{cases} 2\omega_1(n) + \omega_3(n) - 1 + \mathbf{1}_{n\equiv 2 \bmod 4} & \text{if } \forall\, p \mid n \Rightarrow p \not\equiv 5 \bmod 8, \\ 2\omega_1(n) + \omega_3(n) - 2 + \mathbf{1}_{n\equiv 2 \bmod 4} & \text{if } \exists\, p \mid n,\ p \equiv 5 \bmod 8. \end{cases}$$

The following lemma plays a central role.

Lemma 2.6. *For all squarefree integers $n \geq 3$ we have the equality*

$$2^{\mathrm{rk}_2(\mathrm{Cl}(K_n))} = \frac{|\{\beta \in \mathbb{Z}[i] : \beta \mid n, \beta \equiv \pm 1 \bmod 4\}|}{2^{2-\mathbf{1}_{n\equiv 2 \bmod 4}}}. \tag{2.3}$$

Proof. Since $\mathbb{Q}(i)$ is a PID, we see that the action of $\mathrm{Gal}(K_n/\mathbb{Q}(i))$ on $\mathrm{Cl}(K_n)$ is by inversion. In particular, we see that any unramified, abelian extension L of K_n is Galois over $\mathbb{Q}(i)$. Furthermore, the exact sequence

$$1 \to \mathrm{Gal}(L/K_n) \to \mathrm{Gal}(L/\mathbb{Q}(i)) \to \mathrm{Gal}(K_n/\mathbb{Q}(i)) \to 1$$

is split. Indeed, using once more that $\mathbb{Q}(i)$ is a PID, we see that $K_n/\mathbb{Q}(i)$ is ramified at some place, so a splitting is given by inertia. Hence any quadratic unramified extension L of K_n has Galois group $C_2 \times C_2$ over $\mathbb{Q}(i)$ and is therefore of the shape $K_n(\sqrt{\beta})$ with $\beta \in \mathbb{Z}[i]$.

By straightforward ramification considerations we see that $K_n(\sqrt{\beta})/K_n$ is unramified at all odd places if and only if $\beta \mid n$. For now suppose that n is odd and take $\beta \mid n$. Then a local computation at 2 shows that $K_n(\sqrt{\beta})/K_n$ is unramified at all primes above 2 if and only if $\beta \equiv \pm 1 \bmod 4$. For $\alpha \in K_n^*$, let χ_α is the continuous group homomorphism $G_{K_n} \to \{\pm 1\}$ given by

$$\sigma \mapsto \chi_\alpha(\sigma) = \frac{\sigma(\sqrt{\alpha})}{\sqrt{\alpha}}.$$

Call an element $\beta \in \mathbb{Z}[i]$ *odd* if it is coprime to $1 + i$. If I is an ideal of $\mathbb{Z}[i]$ coprime to $1 + i$, then it has a unique generator that is congruent to 1 mod $2+2i$. This allows us to define the gcd of two odd elements $\alpha, \beta \in \mathbb{Z}[i]$

to be the unique generator of the ideal $(\alpha)+(\beta)$ that is congruent to $1 \bmod 2+2i$. Consider the abelian group

$$\{\beta \in \mathbb{Z}[i] : \beta \mid n, \beta \text{ odd}\},$$

where we define the group law $\beta * \beta'$ to be

$$\frac{\beta\beta'}{\gcd(\beta,\beta')^2}.$$

We have now shown that, for n odd, there is a surjective group homomorphism

$$\{\beta \in \mathbb{Z}[i] : \beta \mid n, \beta \equiv \pm 1 \bmod 4\} \to \mathrm{Cl}(K_n)^\vee[2]$$

by sending β to χ_β. Since the kernel is generated by -1 and n, the lemma follows in case n is odd.

Now suppose that n is even and take $\beta \mid n$. In this case $K_n(\sqrt{\beta})/K_n$ is unramified at all primes above 2 if and only if $\beta \equiv 1, 2, 3, 2i \bmod 4$. Therefore the characters χ_β with $\beta \in \mathbb{Z}[i]$, $\beta \mid n$ and $\beta \equiv 1, 2, 3, 2i \bmod 4$ generate the group of characters $\mathrm{Cl}(K_n)^\vee[2]$. Thus we get a surjection

$$\{\beta \in \mathbb{Z}[i] : \beta \mid n, \beta \equiv 1, 2, 3, 2i \bmod 4\} \to \mathrm{Cl}(K_n)^\vee[2].$$

Since $2i = (1+i)^2$, we see that the map is still surjective if we impose that $2 \nmid \beta$. Hence we get a surjective group homomorphism

$$\{\beta \in \mathbb{Z}[i] : \beta \mid n, \beta \equiv \pm 1 \bmod 4\} \to \mathrm{Cl}(K_n)^\vee[2].$$

In this case the kernel is generated by -1, which completes the proof of the lemma also in this case. □

It remains to count the cardinality, denoted by $F(n)$, of the set of divisors β appearing in the right–hand side of (2.3). We have

Lemma 2.7. *Let $n \geq 3$ be a squarefree integer. We then have the equality*

$$F(n) = \begin{cases} 2^{2\omega_1(n)+\omega_3(n)+1} & \text{if } \forall\ p \mid n \Rightarrow p \not\equiv 5 \bmod 8, \\ 2^{2\omega_1(n)+\omega_3(n)} & \text{if } \exists\ p \mid n,\ p \equiv 5 \bmod 8. \end{cases}$$

Proof. Let $\phi_n : \{\beta \in \mathbb{Z}[i] : \beta \mid n, \beta \text{ odd}\} \to (\mathbb{Z}[i]/4\mathbb{Z}[i])^*$ be the homomorphism of abelian groups given by reducing β modulo 4. Then $F(n) = |\phi_n^{-1}(\{1,-1\})|$. Observe that

$$|\{\beta \in \mathbb{Z}[i] : \beta \mid n, \beta \text{ odd}\}| = 2^{2\omega_1(n)+\omega_3(n)+2}.$$

Now the lemma follows immediately if we can prove that

$$\mathrm{im}(\phi_n) = \begin{cases} \{1,-1,i,-i\} & \text{if } \forall\ p \mid n \Rightarrow p \not\equiv 5 \bmod 8, \\ (\mathbb{Z}[i]/4\mathbb{Z}[i])^* & \text{if } \exists\ p \mid n,\ p \equiv 5 \bmod 8. \end{cases}$$

Clearly, $\{1,-1,i,-i\} \subseteq \mathrm{im}(\phi_n)$. Furthermore, simple considerations of congruences modulo 8 imply that

$$\phi_n(\beta) \notin \{1,-1,i,-i\} \Leftrightarrow N_{\mathbb{Q}(i)/\mathbb{Q}}(\beta) \equiv 5 \bmod 8.$$

This concludes the proof. □

2.4. The 4–rank of class groups in the case of quadratic fields. We recall a weaker form of the results of Fouvry and Klüners ([5, 6]) giving strong evidence for the truth of the Cohen–Lenstra–Gerth heuristics (see Section 1).

Lemma 2.8. *For every integer $r \geq 0$, there exist two constants $\alpha_r^+ > 0$ and $\alpha_r^- > 0$, satisfying the equalities*

$$\sum_{r\geq 0} \alpha_r^{\pm} = 1,$$

and such that, as $X \to +\infty$, one has

$$|\{D \in \mathcal{D}^{\pm} : 0 < \pm D < X,\ \mathrm{rk}_4(\mathrm{Cl}(D)) = r\}| \sim \alpha_r^{\pm} |\{D \in \mathcal{D}^{\pm} : 0 < \pm D < X\}|.$$

Similar statements hold with the following three congruence restrictions on the fundamental D :

$$D \equiv 1 \bmod 4,\ D \equiv 4 \bmod 8,\ D \equiv 0 \bmod 8.$$

The constants $\alpha_r^{\pm}$ do not depend on the three congruences above and they can be expressed in terms of the η_r–function. From the remark that a squarefree integer $n \geq 3$ is either a fundamental discriminant (when $n \equiv 1 \bmod 4$) or one quarter of a fundamental discriminant (when $n \equiv 2, 3 \bmod 4$) we deduce from Lemma 2.8 the following

Proposition 2.9. *Let $\psi : \mathbb{R}^+ \to \mathbb{R}^+$ be an increasing function tending to infinity. Then as X tends to infinity, we have*

$$|\{n : 1 \leq n \leq X,\ n \text{ squarefree},\ \mathrm{rk}_4(\mathrm{Cl}(n)) \geq \psi(n)\}| = o(X).$$

A similar statement holds for negative n.

We will appeal to another result of Fouvry and Klüners concerning the values of the pair $(\mathrm{rk}_4(\mathrm{Cl}(n)), \mathrm{rk}_4(\mathrm{Cl}(-n)))$. We have

Lemma 2.10. [8, Theorem 1.8] *For any integer $r \geq 0$ we have*

$$\lim_{X\to\infty} \frac{|\{D \in \mathcal{D}^+ : D \equiv 1 \bmod 4, D \leq X, \mathrm{rk}_4 \mathrm{Cl}^+(D) = \mathrm{rk}_4 \mathrm{Cl}(-D) = r\}|}{|\{D \in \mathcal{D}^+ : D \equiv 1 \bmod 4, D \leq X\}|} = 2^{-r^2-r}(1-2^{-(r+1)})\eta_\infty(2)\eta_r(2)^{-1}\eta_{r+1}(2)^{-1}.$$

A similar statement holds true when the congruence $D \equiv 1 \bmod 4$ is replaced by $D \equiv 4 \bmod 8$ or $D \equiv 0 \bmod 8$.

Apply this lemma with $r = 0$. Since n or $4n$ is a fundamental discriminant and computing numerically the value of $\eta_\infty(2)$, we deduce

Proposition 2.11. *We have*

$$\lim_{X\to\infty} \frac{|\{1 \leq n \leq X : n \in \mathcal{N}\}|}{|\{1 \leq n \leq X : n \text{ squarefree}\}|} = \eta_\infty(2) = .28878\,80950\ldots$$

2.5. The 8–rank of some Dirichlet biquadratic fields.

Proposition 2.12. *For all $n \in \mathcal{N}$ we have*

$$\mathrm{rk}_8(\mathrm{Cl}(K_n)) = 0.$$

Proof. This is a particular case of Lemma 3.2 of [1]. □

2.6. A formula due to Dirichlet.

Proposition 2.13. *Let $n \geq 3$ be a squarefree integer. Then we have the equality*

$$\frac{1}{2}h(n)h(-n)Q(n) = \big|\mathrm{Cl}(K_n)\big|, \tag{2.4}$$

where $Q(n)$ takes the values 1 or 2. More precisely $Q(n)$ is the Hasse unit index

$$Q(n) := \left[\mathcal{O}_{K_n}^* : \mathcal{O}_{\mathbb{Q}(\sqrt{n})}^* \mathbb{Z}[i]^*\right].$$

This formula, in the context of quadratic forms, was first discovered by Dirichlet, who derived it from his class number formula, see [4]. It can for instance be found in the famous Zahlbericht of Hilbert [11, Theorem 115 p. 153].

2.7. Study of the Hasse unit index.

Proposition 2.14. *Let $n > 3$ be a squarefree integer. Then we have $Q(n) = 2$ if and only if $n \in \mathcal{E}$.*

Proof. We apply [15, Theorem 1 (ii)] with $m = 2$, $K = \mathbb{Q}(\sqrt{n})$ and $L = \mathbb{Q}(i, \sqrt{n})$. It follows that $Q(n) = 2$ if and only if 2 ramifies in $\mathbb{Q}(\sqrt{n})$ and the unique prime $\mathfrak{t}$ above 2 is principal. Hence it suffices to show that the latter condition is equivalent to $n \in \mathcal{E}$.

First suppose that 2 ramifies in $\mathbb{Q}(\sqrt{n})$ and that $\mathfrak{t}$ is principal. Choose a generator $c + e\sqrt{n}$ of $\mathfrak{t}$. Computing the norm of $c + e\sqrt{n}$, we see that $n \in \mathcal{E}$. Conversely, suppose $n \in \mathcal{E}$. Looking at the equation

$$c^2 - ne^2 = \pm 2$$

modulo 4, we deduce that $n \equiv 2, 3 \bmod 4$, so 2 ramifies in $\mathbb{Q}(\sqrt{n})$. Furthermore, the unique prime $\mathfrak{t}$ above 2 is generated by $c + e\sqrt{n}$, and therefore principal. □

2.8. Distribution of the function $\omega_3(n)$. It is well known that the function $\Omega(n)$ concentrates around its average value $\log\log n$, see for instance [16, Theorem 7.20]. The extension of this result to the function $\omega(n)$ is easy. The case of the function $\omega_3(n)$ is straightforward, since we have a good knowledge of the set of primes congruent to 3 mod 4. We have

Proposition 2.15. *For every $\varepsilon > 0$ there exists $c(\varepsilon) > 0$ such that, uniformly for $x \geq 2$, one has the inequalities*

$$|\{n \leq x : \omega_3(n) \leq (1/2 - \varepsilon)\log\log x\}| \ll x(\log x)^{-c(\varepsilon)},$$

and

$$|\{n \leq x : \omega_3(n) \geq (1/2 + \varepsilon)\log\log x\}| \ll x(\log x)^{-c(\varepsilon)},$$

We could even be more precise in the description of $\omega_3(n)$ around its average value by adapting the Erdős–Kac Theorem, see for instance [16, Theorem 7.21].

3. The proof of Theorem 1.1

The proof is a straightforward application of the propositions contained in Section 2. We start from (2.4). Taking the 2–parts of both sides of this equality, and taking the logarithm in basis 2, we deduce the following equality

$$\log_2 Q(n) - 1 + \sum_{k=1}^{\infty}\Big(\mathrm{rk}_{2^k}\big(\mathrm{Cl}(n)\big) + \mathrm{rk}_{2^k}\big(\mathrm{Cl}(-n)\big)\Big) = \sum_{k=1}^{\infty}\mathrm{rk}_{2^k}\big(\mathrm{Cl}(K_n)\big), \tag{3.1}$$

which is true for any squarefree integer $n > 3$. If n is such that

$$\mathrm{rk}_4\big(\mathrm{Cl}(n)\big) = \mathrm{rk}_4\big(\mathrm{Cl}(-n)\big) = 0,$$

then trivially, we have

$$\mathrm{rk}_{2^k}\big(\mathrm{Cl}(n)\big) = \mathrm{rk}_{2^k}\big(\mathrm{Cl}(-n)\big) = 0 \quad (k \geq 3)$$

and also thanks to Proposition 2.12, the equalities $\mathrm{rk}_{2^k}(\mathrm{Cl}(K_n)) = 0$ $(k \geq 3)$. These remarks simplify (3.1) into

$$\begin{aligned}\mathrm{rk}_4(\mathrm{Cl}(K_n)) &\\ = \Big(\mathrm{rk}_2\big(\mathrm{Cl}(n)\big) + \mathrm{rk}_2\big(\mathrm{Cl}(-n)\big)\Big) &- \mathrm{rk}_2(\mathrm{Cl}(K_n)) + \log_2 Q(n) - 1.\end{aligned} \tag{3.2}$$

Propositions 2.4 and 2.5 give the values of each of the two first terms on the right–hand side of the equality (3.2) in terms of the number of prime divisors of n satisfying some congruence conditions. Proposition 2.14 gives the value of $Q(n)$. Then a simple case distinction completes the proof of Theorem 1.1.

References

[1] S. Chan & D. Milovic, "Kuroda's formula and arithmetic statistics", *Math. Z.* **300** (2022), no. 2, p. 1509-1527.

[2] H. Cohen & H. W. Lenstra, "Heuristics on class groups of number fields", in *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, Lecture Notes in Mathematics, vol. 1068, Springer, 1984, p. 33-62.

[3] H. Cohen & J. Martinet, "Étude heuristique des groupes de classes des corps de nombres", *J. Reine Angew. Math.* **404** (1990), p. 39-76.

[4] G. L. Dirichlet, "Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes", *J. Reine Angew. Math.* **24** (1842), p. 291-371.

[5] É. Fouvry & J. Klüners, "Cohen-Lenstra heuristics of quadratic number fields", in *Algorithmic number theory*, Lecture Notes in Computer Science, vol. 4076, Springer, 2006, p. 40-55.

[6] ———, "On the 4-rank of class groups of quadratic number fields", *Invent. Math.* **167** (2007), no. 3, p. 455-513.

[7] ———, "On the negative Pell equation", *Ann. Math.* **172** (2010), no. 3, p. 2035-2104.

[8] ———, "On the Spiegelungssatz for the 4-rank", *Algebra Number Theory* **4** (2010), no. 5, p. 493-508.

[9] É. Fouvry, P. Koymans & C. Pagano, "On the 4-rank of class groups of Dirichlet biquadratic fields", *J. Inst. Math. Jussieu* **21** (2020), no. 5, p. 1543-1570.

[10] F. Gerth, "The 4-class ranks of quadratic fields", *Invent. Math.* **77** (1984), p. 489-515.

[11] D. Hilbert, *The theory of algebraic number fields*, Springer, 1998, translated from the German and with a preface by I. T. Adamson, with an introduction by F. Lemmermeyer and N. Schappacher.

[12] P. Koymans, A. Morgan & H. Smit, "The 4-rank of class groups of $K(\sqrt{n})$", `https://arxiv.org/abs/2101.03407`, 2021.

[13] P. Koymans & C. Pagano, "On the distribution of $\mathrm{Cl}(K)[\ell^\infty]$ for degree ℓ cyclic fields", *J. Eur. Math. Soc.* **24** (2022), no. 4, p. 1189-1283.

[14] F. Lemmermeyer, "Kuroda's class number formula", *Acta Arith.* **66** (1994), no. 3, p. 245-260.

[15] ———, "Ideal class groups of cyclotomic number fields I", *Acta Arith.* **72** (1995), no. 4, p. 347-359.

[16] H. L. Montgomery & R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, 2007.

[17] A. Smith, "2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture", `https://arxiv.org/abs/1702.02325`, 2017.

Étienne Fouvry
Université Paris–Saclay, CNRS,
Laboratoire de mathématiques d'Orsay,
91405 Orsay, France
E-mail: `etienne.fouvry@universite-paris-saclay.fr`

Peter Koymans
Max Planck Institute for Mathematics,
Vivatsgasse 7,
53111 Bonn, Germany
E-mail: `koymans@umich.edu`