



On the Mean 3-Rank of Quadratic Fields

KARIM BELABAS

Université Paris-Sud, Département de Mathématiques (bât. 425), F-91405 Orsay, France
e-mail: karim.belabas@math.u-psud.fr

(Received: 5 March 1997; accepted in revised form: 24 February 1998)

Abstract. The Cohen–Lenstra–Martinet heuristics give precise predictions about the class groups of a ‘random’ number field. The 3-rank of quadratic fields is one of the few instances where these have been proven. We prove that, in this case, the rate of convergence is at least sub-exponential. In addition, we show that the defect appearing in Scholz’s mirror theorem is equidistributed with respect to a twisted Cohen–Lenstra density.

Mathematics Subject Classifications (1991): 11R11, 11R29, 11R45.

Key words: class groups, heuristics, 3-rank, quadratic fields.

1. Introduction

Through the far-reaching heuristics of Cohen, Lenstra and Martinet [4, 5] and the subsequent results in that direction by Gerth [14], and Datkovsky and Wright [7], a picture is emerging of what the class group of a ‘random’ number field should look like, expressed in terms of natural densities. Even conjecturally, much remains to be understood (see [6] for instance). In addition, to our knowledge nobody has so far risked a conjecture about the actual speed of convergence, the available experimental data being rather scarce.

One of the rare proven results on class group densities is due to Davenport and Heilbronn [10, 11]. They devised a clever bijection between isomorphism classes of cubic fields and an explicit set of classes of integral binary cubic forms, compatible with the arithmetic structure of the fields. They used it to compute the mean 3-rank of quadratic fields and related densities. (In an earlier book, Delone and Faddeev [12, Sect. 15] studied the same application in a simpler setting. It then yielded a one-to-one correspondence between orders of cubic fields and classes of integral irreducible binary cubic forms.)

In this paper, we show that, contrary to what computed data could have suggested, these densities converge (at least) at a sub-exponential rate (see Theorem 1.1 for a precise statement), and this suggests that the Cohen–Lenstra–Martinet densities also converge at least that fast.

More precisely, we will call *fundamental discriminants* the discriminants of number fields K of degree at most 2 over \mathbb{Q} . That is the set of integers Δ without odd square factors, such that $\Delta \equiv 1 \pmod{4}$ or $\Delta \equiv 8$ or $12 \pmod{16}$.

Denote by $\Delta^\pm(X)$ the intersection of the half-line \mathbb{R}^\pm with $\{\Delta \in \mathbb{Z}, |\Delta| \leq X\}$, and $\Delta_{\text{fund}}^\pm(X)$ the subset of fundamental discriminants in $\Delta^\pm(X)$. Then, setting

$$L_c(X) = \exp(-c(\log X \log \log X)^{1/2}),$$

the main result of this paper, proven in Section 3(a), is as follows:

THEOREM 1.1. *Let $N_3^\pm(X)$ be the number of cubic fields belonging to $\Delta^\pm(X)$, and set $\lambda^+ = \frac{1}{3}$, $\lambda^- = 1$. For all $c < 24^{-1/2}$, we have*

$$\frac{N_3^\pm(X)}{X} = \frac{\lambda^\pm}{4\zeta(3)} + O_c(L_c(X)), \quad (1)$$

$$\sum_{\Delta \in \Delta_{\text{fund}}^\pm(X)} 3^{r_3(\Delta)} / \sum_{\Delta \in \Delta_{\text{fund}}^\pm(X)} 1 = 1 + \lambda^\pm + O_c(L_c(X)), \quad (2)$$

where $r_3(\Delta)$ denotes the 3-rank of $\mathbb{Q}(\sqrt{\Delta})$.

Let $\text{Cl}(\Delta)$ denote the class group of $\mathbb{Q}(\sqrt{\Delta})$, Ω be the set of all $\text{Cl}(\Delta)$, $\Delta > 0$, and $A \subseteq \Omega$. Following Cohen and Lenstra, we consider, when the limit exists,

$$P(A) = \lim_{X \rightarrow +\infty} \sum_{\Delta \in \Delta_{\text{fund}}^+(X)} 1_A(\text{Cl}(\Delta)) / \sum_{\Delta \in \Delta_{\text{fund}}^+(X)} 1,$$

P is only finitely additive, but is one's best choice for defining a 'probability' on Ω . If Δ is a positive fundamental discriminant, we define the *defect* $\delta(\Delta)$ by $r_3(-3\Delta) = r_3(\Delta) + 1 - \delta(\Delta)$. A classical mirror theorem, due in this case to Scholz [16], implies that $\delta(\Delta)$ belongs to $\{0, 1\}$. In Section 3(b), we will prove

THEOREM 1.2. *When X tends to $+\infty$, we have*

$$\sum_{\substack{\Delta \in \Delta_{\text{fund}}^+(X) \\ \delta(\Delta)=0}} 3^{r_3(\Delta)} / \sum_{\Delta \in \Delta_{\text{fund}}^+(X)} 3^{r_3(\Delta)} = \frac{1}{2} + O_c(L_c(X)).$$

In other words, $\delta(\Delta)$ is equidistributed with respect to a twisted Cohen–Lenstra density.

2. Cubic Forms and Congruences

Let F be a class of binary forms modulo $\text{GL}(2, \mathbb{Z})$ (not the modular group), or a number field. In both cases, the discriminant will be denoted by $\Delta(F)$. By abuse of notation, we say that F belongs to $\Delta^\pm(X)$, or $\Delta_{\text{fund}}^\pm(X)$, whenever $\Delta(F)$ does.

We first need to count the classes of integral cubic forms satisfying a given congruence. This congruence needs to be compatible with the $\text{GL}(2, \mathbb{Z})$ action,

which is, for instance, the case when it depends only on the discriminant of the form. We follow the proof given in [1] in the special case $\Delta(F)$ is fundamental and q divides Δ . In this paper, we will deal with an adelic congruence. If one wants a privileged congruence modulo q , and needs to keep control of q in the error term (as in [1] or [3]), the computations become much more involved, and highly dependent on the congruence considered.

In essence, we count integral points in a volume C_X^\pm (depending on the discriminants being positive or negative), which is a fundamental domain for the action of $GL(2, \mathbb{Z})$ on the lattice of integral binary cubic forms of discriminant bounded by X . We consider a compact truncature $C_{X,\rho}^\pm$, whose definition depend on a free parameter ρ . To evaluate the number of points which satisfy the congruence, we cut $C_{X,\rho}^\pm$ into hypercubes whose width equals the congruence modulus. Should the congruence include the Davenport–Heilbronn local conditions, these points are now in one-to-one correspondence with isomorphism classes of cubic fields, having the same discriminant.

Here and in the sequel, the letter p will always denote a prime number. For every prime p , let $E_{p^{\alpha p}}$ be a set of forms modulo $p^{\alpha p}$ and, for any integer m , let

$$E_m = \bigcap_{p^{\alpha p} | m} E_{p^{\alpha p}}, \quad E = \bigcap_p E_{p^{\alpha p}}.$$

By abuse of notation, if F is an integral form or is defined modulo a multiple of m , we will write $F \in E_m$ whenever its reduction $F \bmod m$ belongs to E_m . Thus, by the Chinese remainder theorem, E_m can be thought as containing forms defined modulo m , the total number of which is m^4 . Define local densities by

$$s(p) = \frac{|E_{p^{\alpha p}}|}{p^{4\alpha p}}, \quad t(p) = 1 - s(p).$$

Assume, moreover, that the family $(E_{p^{\alpha p}})_p$ satisfies the following two conditions:

- if $F \in E_{p^{\alpha p}}$ is an integral form, then $F \circ \gamma \in E_{p^{\alpha p}}$, for all $\gamma \in GL(2, \mathbb{Z})$;
- there exists an integer α such that $\alpha_p \leq 4\alpha$ for almost all p .

LEMMA 2.1. *Let $m = o(X^{1/4})$. For all $\varepsilon > 0$, the number of irreducible classes of cubic forms $F \in \Delta^\pm(X) \cap E_m$ is equal to $H^\pm \prod_{p|m} s(p)X + O_\varepsilon(m^{1/4} X^{15/16+\varepsilon})$, where we put $H^+ = \pi^2/72$ and $H^- = \pi^2/24$.*

Proof. We use the results and notations of [1]: the irreducible classes of forms in E_m correspond, discarding a $O_\varepsilon(X^{3/4+\varepsilon})$, to half the number of integral points in C_X^\pm , satisfying the same congruence (Theorems 3.3 and 3.5). If $m = o(X^{1/4})$, the number of integral points in the truncature $C_{X,\rho}^\pm$ of C_X^\pm belonging to E_m is

$$2H^\pm \prod_{p|m} s(p)X + O_\varepsilon(X^{1-\rho+\varepsilon} + mX^{3/4+3\rho+\varepsilon})$$

(Theorem 3.12 and Proposition 4.4) and the number of those points in C_X^\pm not belonging to $C_{X,\rho}^\pm$ is dominated by $X^{1-\rho+\varepsilon}$ (Lemma 3.11). Choose $X^\rho = X^{1/16}m^{-1/4}$ and the lemma is proven. \square

Note that, by taking $m = 1$ in the lemma, $|\Delta^\pm(X)|$ is asymptotic to $H^\pm X$. (This result is originally due to Davenport [8, 9], and was refined by Shintani [17].) Hence, we do not need to check the condition $m = o(X^{1/4})$ since, otherwise, the error term dominates the total number of classes of forms. Thus, Lemma 2.1 is also true (albeit empty) in this case.

COROLLARY 2.2. *Let $Y > 0$, and denote by $f^\pm(r)$ the number of irreducible $F \in \Delta^\pm(X)$ such that, for all primes p , we have*

- $p \mid r$ implies $F \bmod p^{\alpha_p} \notin E_{p^{\alpha_p}}$;
- $p \leq Y$ implies $F \bmod p^{\alpha_p} \in E_{p^{\alpha_p}}$.

Let P_Y be the product of all primes less than Y . Then, for all $\varepsilon > 0$, all r and Y such that $(r, P_Y) = 1$, we have

$$f^\pm(r) = H^\pm \prod_{p \leq Y} s(p) \prod_{p \mid r} t(p) \cdot X + O_\varepsilon(X^{15/16+\varepsilon} e^{(\alpha+\varepsilon)Y} r^\alpha).$$

Proof. Applying the lemma, we obtain

$$f^\pm(r) = H^\pm \prod_{p \leq Y} s(p) \prod_{p \mid r} t(p) X + O_\varepsilon \left(X^{15/16+\varepsilon} \prod_{p \mid r P_Y} p^{\alpha_p/4} \right),$$

and the conclusion follows from the prime number theorem. \square

THEOREM 2.3. *Suppose there exists $C > 0$ and $u > 1$ such that*

- (H1) $t(p) \leq Cp^{-u}$,
- (H2) *the forms in $E_{p^{\alpha_p}}$ are nonzero modulo p ,*
- (H3) *the number of classes belonging to $\Delta^\pm(X)$, but not to $E_{p^{\alpha_p}}$, is $O(Xp^{-u})$.*

Then, for all $c < c_0 = (u - 1)/4(\alpha + 1)^{1/2}$, the number of irreducible primitive classes of binary cubic forms in $\Delta^\pm(X) \cap E$ is equal to $H^\pm \prod_p s(p)X + O_c(XL_c(X))$.

Proof. We want to count the classes belonging to $E_{p^{\alpha_p}}$ for all p , thus primitive because of hypothesis (H2). Using the notation from our previous corollary, this is equal to

$$f(1) - \sum_{k \geq 1} \sum_{\substack{p_1 < \dots < p_k \\ Y < p_i < Z}} (-1)^{k-1} f(p_1 \dots p_k) - O \left(\sum_{p \geq Z} f(p) \right), \quad (3)$$

by the inclusion–exclusion principle, for any parameter Z . The remainder term is dominated by XZ^{1-u} , thanks to (H3). We now introduce another parameter K and decompose the main term in the form

$$f(1) - \sum_{1 \leq k < K} \sum_{\substack{p_1 < \dots < p_k \\ Y < p_i < Z}} (-1)^{k-1} f(p_1 \dots p_k) + O\left(\sum_{\substack{p_1 < \dots < p_K \\ Y < p_i < Z}} f(p_1 \dots p_K)\right).$$

Using Corollary 2.2, this is equal to

$$H^\pm \prod_{p \leq Y} s(p)X \left[1 - \sum_{k=1}^{K-1} \sum_{\substack{p_1 < \dots < p_k \\ Y < p_i < Z}} (-1)^{k-1} t(p_1 \dots p_k) \right] + O_\varepsilon \left(X^{15/16+\varepsilon} e^{(\alpha+\varepsilon)Y} K \sum_{p_1 < \dots < p_K < Z} (p_1 \dots p_K)^\alpha + \sum_{\substack{p_1 < \dots < p_K \\ Y < p_i < Z}} t(p_1 \dots p_K)X \right),$$

where t has been extended by multiplicativity to all integers. Using (H1), we obtain

$$H^\pm \prod_{p \leq Y} s(p)X \left[1 + \sum_{k \geq 1} \sum_{\substack{p_1 < \dots < p_k \\ Y < p_i < Z}} (-1)^k t(p_1 \dots p_k) \right] + O_\varepsilon \left(X^{15/16+\varepsilon} e^{(\alpha+\varepsilon)Y} K \left(\sum_{p < Z} p^\alpha \right)^K + X \left(C \sum_{p > Y} p^{-u} \right)^K \right).$$

That is, factoring back the Euler product,

$$H^\pm \prod_{p < Z} s(p)X + O_\varepsilon(X^{15/16+\varepsilon} e^{(\alpha+\varepsilon)Y} K Z^{K(1+\alpha)} + X(CY^{1-u} / \log Y)^K).$$

Finally, using (H1) again to evaluate the product of the $s(p)$, we find that (3) is equal to

$$H^\pm \prod s(p)X + O_\varepsilon(X^{15/16+\varepsilon} e^{(\alpha+\varepsilon)Y} K Z^{K(1+\alpha)} + XY^{K(1-u)} + XZ^{1-u}).$$

We choose $Y = \log X / \log \log \log X$ and assume $K = o(X^\varepsilon)$. The remainder term, divided by X , is dominated by

$$\begin{aligned} X^{-1/16+\varepsilon} Z^{K(1+\alpha)} + (\log X)^{K(1-u)} + Z^{1-u} \\ = e^{(-1/16+\varepsilon) \log X + K(1+\alpha) \log Z} + e^{K(1-u) \log \log X} + e^{(1-u) \log Z}. \end{aligned} \tag{4}$$

To equalize the first two terms, we set

$$K = \frac{(1/16 - \varepsilon) \log X}{(\alpha + 1) \log Z + (u - 1) \log \log X}.$$

We now choose $\log Z = \lambda(\log X \log \log X)^{1/2}$, where $\lambda = (16(\alpha + 1))^{-1/2}$. A simple computation yields

$$K \sim \lambda(1 - 16\varepsilon) \left(\frac{\log X}{\log \log X} \right)^{1/2} = o(X^\varepsilon),$$

and the result is proven, with $c = \lambda(u - 1) - \varepsilon$. \square

For ‘sensible’ $E_{p^{\alpha_p}}$, exponential sum techniques may improve on Lemma 2.1, thus increasing c_0 . This is the case for all our subsequent applications, where we could take $c_0 = (17/3)^{-1/2} \approx 0.420$, most of the corresponding estimates being done in [1]. We nonetheless keep the value given by Theorem 2.3 in the sequel.

3. Applications

3.1. DAVENPORT–HEILBRONN DENSITIES

THEOREM 3.1. *Set $\alpha_2 = 4$, $\alpha_p = 2$ for p odd, and let n be an integer such that $p|n$ implies $p^{\alpha_p}|n$. Let E_n be any set of classes of forms modulo n , whose discriminants are congruent to fundamental discriminants modulo n , and let $\Delta(E_n)$ be the set of discriminants of all forms belonging to E_n . For all $c < 24^{-1/2}$, we have*

$$\sum_{\substack{\Delta \in \Delta_{\text{fund}}^\pm(X) \\ \Delta \in \Delta(E_n)}} \frac{3^{r_3(\Delta)} - 1}{2} = \frac{H^\pm X}{\xi^2(2)} \prod_{p|n} \frac{s(p)}{(1 - p^{-2})^2} + O_{n,c}(XL_c(X)).$$

Proof. In the case $n = 1$, it follows from a remark of Hasse [15, Satz 8] that the left-hand side counts isomorphism classes of cubic fields having fundamental discriminants. Now, take for $E_{p^{\alpha_p}}$ the classes modulo p^{α_p} whose discriminants are fundamental modulo p^{α_p} , with the additional constraint that they belong to E_n if $p|n$ (after this choice, the notation E_n is compatible with the one given before Lemma 2.1).

By definition, E contains exactly the classes whose discriminant is fundamental and belong to E_n . Since the discriminant is preserved by the Davenport–Heilbronn bijection, the number of classes of forms belonging to E yields exactly the left-hand side of the formula.

We now check that E satisfies the three hypotheses in Theorem 2.3: this is easy for (H2) since $p|F$ would imply that $p^4|\Delta(F)$, and Δ would not be fundamental. The other two are trivially satisfied for any given finite number of primes so,

excluding the primes $p|n$, we are reduced to the case $n = 1$, i.e. to the original computations of Davenport and Heilbronn [11].

They define their local densities with respect to *primitive* forms. Once translated into our notations, their Lemma 4 yields $s(p) = (1 - p^{-2})^2$ (recall that we assume here that $p \nmid n$). Hence, (H1) is satisfied with $u = 2$.

Proposition 1 in the same paper proves that (H3) is also valid with $u = 2$. This is the technical heart of their work, and uses the language of binary quadratic forms, genera, etc. Datskovski and Wright [7, Sect. 6] have given a more general proof in terms of class field theory.

Hence, we can apply Theorem 2.3 with $s(p) = (1 - p^{-2})^2$ if $p \nmid n$, and $4\alpha = u = 2$. We now notice that $\prod(1 - p^{-2})^2 = \zeta(2)^{-2}$ and the result follows. \square

Proof of Theorem 1.1. Equality (2) is an easy consequence of Theorem 3.1, and the classical density of fundamental discriminants. Using again the results of [11], the hypotheses of Theorem 2.3 are satisfied with $s(p) = (1 - p^{-3})(1 - p^{-2})$ and $4\alpha = u = 2$. Equality (1) follows. \square

The densities in Theorem 1.1 were computed by Davenport and Heilbronn in [11], without any remainder term for lack of uniformity in the congruence modulus (corresponding to our Lemma 2.1). A remainder term in $o(1/\log^2(X))$ was then obtained by the author in [1]. The sub-exponential convergence rates that we have proven are surprisingly fast when matched with numerical data. To give an example, $N_3^+(10^{11}) = 6, 715, 824, 025$, which gives an experimental density of 0.0672 for real cubic fields up to 10^{11} , to compare with $1/12\zeta(3) \approx 0.0693$. In the case of complex cubic fields, we find $N_3^-(10^{11}) = 20, 422, 230, 540$, hence an experimental density of 0.2042, while $1/4\zeta(3) \approx 0.2080$ (see the tables in [2]). A linear regression on this experimental data, suggests one could take c between 0.6 and 0.7 (whereas $24^{-1/2} \approx 0.2$). Of course, there is no real reason to believe that the true speed of convergence is given by a function $L_c(X)$.

3.2. ON THE MIRROR INEQUALITY

Recall that we denote by $\delta(\Delta)$ the defect in Scholz's equality. Under the Cohen–Lenstra model and modulo some reasonable but unproven independence assumptions, Dutarte [13] obtained the following conjecture

CONJECTURE 3.2. *Let P be as in the introduction. For all $a \geq 0$, we have $P(\{\text{Cl}(\Delta) : \delta(\Delta) = 0, r_3(\Delta) = a\}) = 3^{-(a+1)}$.*

Whence $P(\{\text{Cl}(\Delta) : \delta(\Delta) = 0, r_3(\Delta) \leq a\})$ would tend to $\frac{1}{2}$ as $a \rightarrow +\infty$. We now prove this unconditionally for a twisted density

Proof of Theorem 1.2. We write

$$\sum_{\Delta \in \Delta_{\text{fund}}^+(X)} 3^{r_3(-3\Delta)} = \sum_{\substack{\Delta \in \Delta_{\text{fund}}^-(3X) \\ 3|\Delta}} 3^{r_3(\Delta)} + \sum_{\substack{\Delta \in \Delta_{\text{fund}}^-(X/3) \\ 3 \nmid \Delta}} 3^{r_3(\Delta)}.$$

Using Theorem 3.1, and the density computed in [1, Thm. 1.2], we compute

$$\sum_{\substack{\Delta \in \Delta_{\text{fund}}^-(X) \\ 3|\Delta}} \frac{3^{r_3(\Delta)} - 1}{2} = \frac{H^- X}{4\zeta^2(2)} + O_c(X.L_c(X)).$$

An easy computation then yields

$$\sum_{\Delta \in \Delta_{\text{fund}}^+(X)} \frac{3^{r_3(-3\Delta)} - 3^{r_3(\Delta)}}{2} = \frac{(H^- - H^+)X}{\zeta^2(2)} + O_c(X.L_c(X)).$$

Whence, by definition of $\delta(\Delta)$, using (2) and the classical density of fundamental discriminants

$$\sum_{\Delta \in \Delta_{\text{fund}}^+(X)} 3^{r_3(\Delta)} \frac{3^{1-\delta(\Delta)} - 1}{2} / \sum_{\Delta \in \Delta_{\text{fund}}^+(X)} 3^{r_3(\Delta)} = \frac{1}{2} + O_c(L_c(X)).$$

We conclude by remarking that $(3^{1-\delta(\Delta)} - 1)/2$ is the characteristic function of the property $\delta(\Delta) = 0$.

Acknowledgements

We thank Henri Cohen and Etienne Fouvry for many helpful and stimulating discussions, and Georges Gras for communicating to us the work of Dutarte which prompted our Section 3.2. We are also grateful to the referee for his comments. Finally, we are indebted to the Max-Planck-Institut für Mathematik (Bonn) for its financial support and for being the wonderful working place it is.

References

1. Belabas, K.: Crible et 3-rang des corps quadratiques, *Ann. de l'Inst. Fourier* **46** (1996), 909–949.
2. Belabas, K.: A fast algorithm to compute cubic fields, *Math. Comp.* **66** (1997), 1213–1237.
3. Belabas, K. and Fouvry, E.: Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier, *Duke Math. J.*, to appear.
4. Cohen, H. and Lenstra Jr., H. W.: Heuristics on class groups of number fields, in: *Number Theory, (Noordwijkerhout 1983)*, Lecture Notes in Math. 1068, Springer-Verlag, New York, 33–62.
5. Cohen, H. and Martinet, J.: Études heuristiques des groupes de classes des corps de nombres, *J. reine angew. Math.* **404** (1990), 39–76.

6. Cohen, H. and Martinet, J.: Heuristics on class groups: some good primes are not too good, *Math. Comp.* **207** (1994), 329–334.
7. Datskovsky, B. and Wright, D. J.: Density of discriminants of cubic extensions, *J. reine. angew. Math.* **386** (1988), 116–138.
8. Davenport, H.: On the class number of binary cubic forms (i), *J. London Math. Soc.* **26** (1951), 183–192, errata *ibid* **27** (1951), 512.
9. Davenport, H.: On the class number of binary cubic forms (ii), *J. London Math. Soc.* **26** (1951), 192–198.
10. Davenport, H. and Heilbronn, H.: On the density of discriminants of cubic fields (i), *Bull. London Math. Soc.* **1** (1969), 345–348.
11. Davenport, H. and Heilbronn, H.: On the density of discriminants of cubic fields (ii), *Proc. Roy. Soc. London A* **322** (1971), 405–420.
12. Delone, B. N. and Faddeev, D. K.: *The Theory of Irrationalities of the Third Degree*, Trans. Math. Monogr. 10, Amer. Math. Soc., Providence, 1964.
13. Dutarte, P.: Compatibilité avec le Spiegelungssatz de propriétés conjecturales sur le p -rang du groupe des classes, mémoire DEA, Besançon, 1984.
14. Gerth III, F.: The 4-class ranks of quadratic fields, *Invent. Math.* **77** (1984), 489–515.
15. Hasse, H.: Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Z.* **31** (1930), 565–582.
16. Scholz, A.: Über die Beziehung der Klassenzahlen quadratischer Körper zueinander, *J. reine angew. Math.* **166** (1932), 201–203.
17. Shintani, T.: On zeta-functions associated with the vector space of quadratic forms, *J. Fac. Sci. Univ. Tokyo, Sec. Ia* **22** (1975), 25–66.