ON THE MEAN 3-RANK OF QUADRATIC FIELDS

KARIM BELABAS

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. In the present paper, 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.

1. INTRODUCTION

Through the far-reaching heuristics of Cohen, Lenstra and Martinet [3, 4] and the subsequent results in that direction by Gerth [10], and Datkovsky–Wright [6], a picture is emerging of how 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 [5] 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 [7, 8]. They devised a clever bijection between classes of integral binary cubic forms and isomorphism classes of cubic fields, compatible with the arithmetic structure of the fields. They used it to compute the mean 3-rank of quadratic fields and related densities. In the present 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 $\mathbb{Q}$. Denote by $\Delta^{\pm}(X)$ the intersection of the half-line $\mathbb{R}^{\pm}$ with $\{|\Delta| \leqslant X\}$, and $\Delta^{\pm}_{fund}(X)$ the subset of fundamental discriminants in $\Delta^{\pm}(X)$. Then, setting

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

the main result of this paper, proven in Section 3.a, is as follows.

Date: July 7, 1997.

1991 *Mathematics Subject Classification.* 11R11, 11R29, 11R45.

Key words and phrases. Class groups, Heuristics, 3-Rank, Quadratic fields.

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

$$\frac{N_3^{\pm}(X)}{X} = \frac{\lambda^{\pm}}{4\zeta(3)} + \mathrm{O}_c(L_c(X)) \ , \tag{1}$$

$$\sum_{\Delta\in\Delta^{\pm}_{fund}(X)} 3^{r_3(\Delta)} \Big/ \sum_{\Delta\in\Delta^{\pm}_{fund}(X)} 1 = 1 + \lambda^{\pm} + \mathrm{O}_c(L_c(X)) \ , \tag{2}$$

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

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

$$P(A) = \lim_{X\to+\infty} \sum_{\Delta\in\Delta^+(X)} 1_A(\mathrm{Cl}(\Delta)) \Big/ \sum_{\Delta\in\Delta^+(X)} 1 \ ,$$

P is only finitely additive, but is one's best choice to define 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 [12], implies that $\delta(\Delta)$ belongs to $\{0, 1\}$. We will prove in Section 3.b:

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

$$\sum_{\substack{\Delta\in\Delta^+(X)\\ \delta(\Delta)=0}} 3^{r_3(\Delta)} \Big/ \sum_{\Delta\in\Delta^+(X)} 3^{r_3(\Delta)} = \frac{1}{2} + \mathrm{O}_c(L_c(X)) \ .$$

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

Acknowledgements: We thank Profs. Henri Cohen, Etienne Fouvry and Georges Gras for many helpful discussions, and the Max-Planck-Institut für Mathematik for its hospitality while we were preparing this paper.

2. Cubic forms and congruences

Let F be a class of binary forms modulo $\mathrm{GL}(2,\mathbb{Z})$ (*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 $\Delta^{\pm}_{fund}(X)$, 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 $\mathrm{GL}(2,\mathbb{Z})$ action, which is for instance the case when it depends only on the discriminant of the form. We follow the proof given in [2] in the special case *$\Delta(F)$ is fundamental and q divides* Δ. In the present paper, we will deal with an adelic congruence. If one wants a privileged congruence modulo q, and keep control of q in the error term, the computations become much more involved, and highly dependent on the congruence considered. Such was the point of view of [2], and we refer the reader to this article for an example of these.

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 $\mathrm{GL}(2,\mathbb{Z})$ on the lattice of integral binary cubic forms. We consider a compact truncature $C_{X,\rho}^{\pm}$, whose definition depend on a parameter ρ, and cut it into hypercubes whose width equals the congruence modulus to evaluate the number of those which satisfy the congruence. 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 be a set of classes of forms modulo p^{α_p}, and assume that there exists an integer α such that $\alpha_p \leqslant 4\alpha$ for almost all p. By abuse of notation, we write $F \in E_p$ whenever $F \bmod p \in E_p$. Let

$$E = \bigcap E_p, \quad E_m = \bigcap_{p|m} E_p, \quad s(p) = \frac{|E_p|}{p^{\alpha_p}} \quad \text{and} \quad t(p) = 1 - s(p) \ .$$

Lemma 2.1. *Let $m = \mathrm{o}(X^{1/4})$. For all $\varepsilon > 0$, the number of irreducible classes of cubic forms $F \in \Delta^{\pm}(X) \cap E_m$ is equal to*

$$H^{\pm} \prod_{p|m} s(p) X + \mathrm{O}_{\varepsilon}(m^{1/4} X^{15/16+\varepsilon}) \ ,$$

where we put $H^+ = \frac{\pi^2}{72}$ and $H^- = \frac{\pi^2}{24}$.

Proof. We use the results and notations of [2]: the irreducible classes of forms in E_m correspond, discarding a $\mathrm{O}_{\varepsilon}(X^{3/4+\varepsilon})$, to half the number of integral points in $C_X^{\pm}$, satisfying the same congruence (Theorems 3.3 and 3.5). If $m = \mathrm{o}(X^{1/4})$, the number of integral points in the truncature $C_{X,\rho}^{\pm}$ of $C_X^{\pm}$ belonging to E_m is

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

(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. ☐

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 $F \bmod p \notin E_p$,*
- *$p \leqslant Y$ implies $F \bmod p \in E_p$.*

Then, for all $\varepsilon > 0$, we have

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

Proof. Let P_Y be the product of all primes less than Y. Applying the lemma,

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

and the conclusion follows from the prime number theorem. □

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

H1. $t(p) \leqslant C p^{-u}$,
H2. *the forms in E_p are non-zero modulo p,*
H3. *the number of classes belonging to $\Delta^{\pm}(X)$, but not to E_p, is $\mathrm{O}(X p^{-u})$.*

Then, for 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:

$$H^{\pm} \prod_{p} s(p) X + \mathrm{O}_c(X L_c(X)) \ .$$

Proof. We want to count the classes belonging to E_p for all p, thus primitive because of hypothesis (H2). Using the notation from our previous corollary, this is equal to

$$f(1) - \sum_{k \geqslant 1} \sum_{\substack{p_1 < \cdots < \mathfrak{p}_k \\ Y < p_i < Z}} (-1)^{k-1} f(p_1 \ldots p_k) - \mathrm{O}\left(\sum_{p \geqslant Z} f(p)\right) \ , \tag{3}$$

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

$$f(1) - \sum_{1 \leqslant k < K} \sum_{\substack{p_1 < \cdots < \mathfrak{p}_k \\ Y < p_i < Z}} (-1)^{k-1} f(p_1 \ldots p_k) + \mathrm{O}\left(\sum_{\substack{p_1 < \cdots < p_K \\ Y < p_i < Z}} f(p_1 \ldots p_K)\right) \ .$$

Using Corollary 2.2, this is equal to

$$\begin{aligned} &H^{\pm} \prod_{p \leqslant Y} s(p) X \left[1 - \sum_{k=1}^{K-1} \sum_{\substack{p_1 < \cdots < \mathfrak{p}_k \\ Y < p_i < Z}} (-1)^{k-1} t(p_1 \ldots p_k)\right] \\ &\quad + \mathrm{O}_{\varepsilon}\left(X^{15/16+\varepsilon} e^{\alpha Y} K \sum_{p_1 < \cdots < p_K < Z} (p_1 \ldots p_K)^{\alpha} + \sum_{p_1 < \cdots < p_K < Z} t(p_1 \ldots p_K) X\right) \ . \end{aligned}$$

Using (H1), we obtain

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

That is, factoring back the Euler product,

$$H^{\pm}\prod_{p<Z}s(p)X+\mathrm{O}_\varepsilon\left(X^{15/16+\varepsilon}e^{\alpha Y}KZ^{K(1+\alpha)}+X\big(CY^{1-u}/\log Y\big)^K\right)\ .$$

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

$$H^{\pm}\prod s(p)X+\mathrm{O}_\varepsilon\left(X^{15/16+\varepsilon}e^{\alpha Y}KZ^{K(1+\alpha)}+XY^{K(1-u)}+XZ^{1-u}\right)\ .$$

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

$$\text{(4)}\quad X^{-1/16+\varepsilon}Z^{K(1+\alpha)}+(\log X)^{K(1-u)}+Z^{1-u}$$
$$=e^{(-1/16+\varepsilon)\log X+K(1+\alpha)\log Z}+e^{K(1-u)\log\log X}+e^{(1-u)\log Z}\ .$$

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

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

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

For "sensible" E_p, exponential sums 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 [2]. We nonetheless keep the value given by Theorem 2.3 in the sequel.

3. Applications

a. **Davenport-Heilbronn densities.**

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

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

Proof. It was remarked by Hasse [11], in the case $n = 1$ and with a different formulation, that the left-hand side counted isomorphism classes of cubic fields with fundamental discriminants. The discriminant is functorial with respect to the Davenport–Heilbronn bijection. Thus, if we take as E_p the classes modulo p^{α_p} whose discriminants are fundamental modulo p^{α_p} (*i.e.* E contains exactly the classes whose discriminant is fundamental), belonging to E_n if $p \mid n$, we get the left-hand side of the formula. The computations made by Davenport and Heilbronn in [8] show that, for $n = 1$, all three hypotheses in Theorem 2.3 are satisfied, with $s(p) = (1-p^{-2})^2$, and $4\alpha = u = 2$. The result follows. ☐

Proof of Theorem 1.1. Equality (2) is an easy consequence of Theorem 3.1, and the classical density of fundamental discriminants. Using the results of [8], 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. ☐

The densities in Theorem 1.1 were computed by Davenport and Heilbronn in [8], without any remainder term for lack of uniformity in the congruence modulus (corresponding to our Lemma 2.1). A remainder term in $\mathrm{o}(1/\log^2(X))$ was then obtained by the author in [2]. 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 [1]). A linear regression on this experimental data, suggests one could take c between 0.6 et 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 $L_c(X)$.

b. **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 [9] obtained the following conjecture:

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

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

PROOF OF THEOREM 1.2. We write

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

Using Theorem 3.1, and the density computed in [2, Theorem 1.2], we compute

$$\sum_{\substack{\Delta \in \Delta^-(X) \\ 3 \mid \Delta}} \frac{3^{r_3(\Delta)} - 1}{2} = \frac{H^- X}{4\zeta^2(2)} + \mathrm{O}_c(X.L_c(X)) .$$

An easy computation then yields

$$\sum_{\Delta \in \Delta^+(X)} \frac{3^{r_3(-3\Delta)} - 3^{r_3(\Delta)}}{2} = \frac{(H^- - H^+)X}{\zeta^2(2)} + \mathrm{O}_c(X.L_c(X)) .$$

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

$$\sum_{\Delta \in \Delta^+(X)} 3^{r_3(\Delta)} \frac{3^{1-\delta(\Delta)} - 1}{2} \Big/ \sum_{\Delta \in \Delta^+(X)} 3^{r_3(\Delta)} = \frac{1}{2} + \mathrm{O}_c(L_c(X)) .$$

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

REFERENCES

[1] K. BELABAS, A fast algorithm to compute cubic fields, *Math. Comp.*, to appear.

[2] K. BELABAS, Crible et 3-rang des corps quadratiques, *Ann. de l'Inst. Fourier* **46** (1996), pp. 909–949.

[3] H. COHEN & H. W. LENSTRA JR, Heuristics on class groups of number fields, in *Number Theory, Noordwijkerhout 1983*, Lect. Notes in Math., no. 1068, Springer-Verlag, 1984, pp. 33–62.

[4] H. COHEN & J. MARTINET, Études heuristiques des groupes de classes des corps de nombres, *J. reine angew. Math.* **404** (1990), pp. 39–76.

[5] H. COHEN & J. MARTINET, Heuristics on class groups: some good primes are not too good, *Math. Comp.* **207** (1994), pp. 329–334.

[6] B. DATSKOVSKY & D. J. WRIGHT, Density of discriminants of cubic extensions, *J. reine. angew. Math.* **386** (1988), pp. 116–138.

[7] H. DAVENPORT & H. HEILBRONN, On the density of discriminants of cubic fields (i), *Bull. Lond. Math. Soc.* **1** (1969), pp. 345–348.

[8] H. DAVENPORT & H. HEILBRONN, On the density of discriminants of cubic fields (ii), *Proc. Roy. Soc. Lond. A* **322** (1971), pp. 405–420.

[9] P. DUTARTE, Compatibilité avec le Spiegelungsatz de propriétés conjecturales sur le p-rang du groupe des classes, mémoire DEA, Besançon, 1984.

[10] F. GERTH III, The 4-class ranks of quadratic fields, *Invent. Math.* **77** (1984), pp. 489–515.

[11] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Zeitschrift.* **31** (1930), pp. 565–582.

[12] A. Scholz, Über die Beziehung der Klassenzahlen quadratisher Körper zueinander, *J. reine angew. Math.* **166** (1932), pp. 201–203.

Max Planck Institut für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn (Allemagne)
karim@mpim-bonn.mpg.de

Université Bordeaux I
Département de mathématiques (A2X)
351, cours de la Libération
33405 Talence (France)