Cohen–Lenstra heuristics of quadratic number fields

Étienne Fouvry[1] and Jürgen Klüners[2]

[1] Mathématique, Bât. 425, Univ. Paris–Sud, Campus d'Orsay, F–91405 ORSAY Cedex, France, Etienne.Fouvry@math.u-psud.fr
[2] Universität Kassel, Fachbereich Mathematik/Informatik, Heinrich-Plett-Str. 40, 34132 Kassel, Germany, klueners@mathematik.uni-kassel.de

Abstract. We establish a link between some heuristic asymptotic formulas (due to Cohen and Lenstra) concerning the moments of the p–part of the class groups of quadratic fields and formulas giving the frequency of the values of the p–rank of these class groups.
Furthermore we report on new results for 4–ranks of class groups of quadratic number fields.

1 Introduction and Notations

In [1], Cohen and Lenstra have built a probabilistic model to guess the frequency of some algebraic properties of the narrow class group C_D of the ring of integers of the quadratic fields $\mathbb{Q}(\sqrt{D})$, where the letter D is reserved to fundamental discriminants, throughout this paper. Their idea was, roughly speaking, to attach to each abelian group a weight which is the inverse of the number of its automorphisms. These *heuristics*, the proof of which must lie very deep, are strongly supported by numerical evidence and explain why, for instance, the odd part of C_D is a cyclic group with a higher frequency than one could think at first approach. From these heuristics, they deduce several facts and the aim of our work is to show that some of these deductions imply another ones.

To present the results, we shall use the following notations. The letter p is reserved to prime numbers. For A a finitely generated abelian group, the p–rank of A is defined as $\mathrm{rk}_p(A) = \dim_{\mathbb{F}_p}(A/A^p)$. For an integer $k \geq 0$ and $t > 1$, we introduce the functions η_k and η_∞ defined by

$$\eta_k(t) = \prod_{1 \leq j \leq k} \left(1 - t^{-j}\right)$$

and

$$\eta_\infty(t) = \prod_{j \geq 1} \left(1 - t^{-j}\right).$$

If $f(D)$ is a real valued function defined on the set of positive or negative discriminants, we say that $f(D)$ has the *average value* $c_0 (\in \mathbb{R})$, if, as $X \to +\infty$, we have

$$\sum_{0 < \pm D < X} f(D) = (c_0 + o(1)) \sum_{0 < \pm D < X} 1. \tag{1}$$

In the particular case, where $f(D)$ is the characteristic function of the set of discriminants satisfying some indicated property, we say that c_0 is the *density* of this set.

One of the consequences of the Cohen–Lenstra heuristics is to describe the distribution of the values of $\mathrm{rk}_p(C_D)$ as D ranges over the set of positive or negative discriminants, and p a fixed odd prime. These heuristics do not concern the special prime $p = 2$. To circumvent this defect, Gerth [4], [5] had the idea to generalize these heuristics to the group C_D^2. He was led to this generalization by meeting with the densities quoted in Conjectures 2 and 4 (for $p = 2$) below again, when studying the sets of D with a fixed number of prime factors and a fixed value of the 2–rank for C_D^2 (see [4, (1.5) & (1.6)]). From [1], generalized by Gerth, we extract the four conjectures, anyone of which is a consequence of these heuristics.

Conjecture 1. *For every positive integer α, for every prime p, the average value of*

$$\prod_{0 \le i < \alpha} \left(p^{\mathrm{rk}_p(C_D^2)} - p^i \right)$$

is equal to 1*, when D ranges over the set of negative fundamental discriminants.*

Conjecture 2. *For every non-negative integer r, for every prime p, the density of negative fundamental discriminants D such that $\mathrm{rk}_p(C_D^2) = r$ is equal to*

$$p^{-r^2}\, \eta_\infty(p)\, \eta_r(p)^{-2}.$$

Conjecture 3. *For every positive integer α, for every prime p, the average value of*

$$\prod_{0 \le i < \alpha} \left(p^{\mathrm{rk}_p(C_D^2)} - p^i \right)$$

is equal to $p^{-\alpha}$, when D ranges over the set of positive fundamental discriminants.

Conjecture 4. *For every non-negative integer r, for every prime p, the density of positive fundamental discriminant D such that $\mathrm{rk}_p(C_D^2) = r$ is equal to*

$$p^{-r(r+1)} \eta_\infty(p) \eta_r(p)^{-1} \eta_{r+1}(p)^{-1}.$$

For $p \ge 3$, Conjectures 1, 2, 3 and 4 are the conjectures (C.6), (C.5), (C.10) and (C.9) of [1, p. 56 & 57], respectively. Note that for $p \ge 3$, we have the equality $\mathrm{rk}_p(C_D^2) = \mathrm{rk}_p(C_D)$, and, by definition we have $\mathrm{rk}_2(C_D^2) = \mathrm{rk}_4(C_D)$, the 4–rank of C_D.

Very little is known about these conjectures : Conjectures 1 and 3 are trivially true for any p and $\alpha = 0$. These conjectures are also proved for $p = 3$ and $\alpha = 1$, this is the famous work of Davenport and Heilbronn [2]. Both authors of this paper recently proved that Conjectures 1 and 3 are true for $p = 2$ and any $\alpha \ge 0$ (see [3, Theorem 1]) and that they remain true if the narrow class group C_D is replaced by the ordinary class group Cl_D.

The aim of this paper, roughly speaking, is to prove that if for some p, Conjecture 1 is true for every α, then Conjecture 3 is also true for this p and every r. The same implication holds between Conjecture 2 and Conjecture 4. More precisely, we shall prove

Theorem 1. *Let p a prime and assume that for every integer $\alpha \geq 0$ the average value of*

$$\prod_{0 \leq i < \alpha} \left(p^{\mathrm{rk}_p(C_D^2)} - p^i \right)$$

is equal to 1, when D ranges over the set of negative fundamental discriminants. Then for every integer $r \geq 0$ the density of the set of negative fundamental discriminants D such that $\mathrm{rk}_p(C_D^2) = r$ is equal to

$$p^{-r^2} \eta_\infty(p) \eta_r(p)^{-2}.$$

and

Theorem 2. *Let p a prime and assume that for every integer $\alpha \geq 0$ the average value of*

$$\prod_{0 \leq i < \alpha} \left(p^{\mathrm{rk}_p(C_D^2)} - p^i \right)$$

is equal to $p^{-\alpha}$, when D ranges over the set of positive fundamental discriminants. Then, for every integer $r \geq 0$, the density of the set of positive fundamental discriminants D such that $\mathrm{rk}_p(C_D^2) = r$ is equal to

$$p^{-r(r+1)} \eta_\infty(p) \eta_r(p)^{-1} \eta_{r+1}(p)^{-1}.$$

Since Conjectures 1 and 3 are proved in the particular case $p = 2$ and for every α, see Theorem 5 and [3, Theorem 1], we now state the following corollary.

Corollary 1. *For ever integer $r \geq 0$ the density of the set of negative fundamental discriminants such that $\mathrm{rk}_4(C_D) = r$ is equal to*

$$2^{-r^2} \eta_\infty(2) \eta_r(2)^{-2}.$$

and for positive discriminants, this density is equal to

$$2^{-r(r+1)} \eta_\infty(2) \eta_r(2)^{-1} \eta_{r+1}(2)^{-1}.$$

We remark that this corollary implies that the probability for a discriminant D to satisfy $\mathrm{rk}_4(C_D) = 0$ is twice larger when it is positive than when it is negative. It would be interesting to have a direct proof of that phenomenon.

Reciprocally, it seems difficult to deduce Conjecture 1 from Conjecture 2 or Conjecture 3 from Conjecture 4 in the form they are written above. Such implications may require a more precise statement for Conjectures 2 and 4 (for instance, with a control of the term $o(1)$ in the formulas (1), corresponding to the densities in question).

In Section 3 we report on results obtained in [3]. We show that Conjectures 1 and 3 are true for all $\alpha \geq 0$ in the case $p = 2$.

1.1 Acknowledgments.

The first author thanks P. Gérard for interesting conversations about §4.2.

2 A transition to moments

In [3] an equivalent form of Conjectures 1 and 3 is proved in terms of the function $\mathcal{N}(\alpha,p)$ which denotes the total number of vector subspaces of $\mathbb{F}_p^\alpha$. This equivalent form was an important step in our proof of Conjectures 1 and 3, for $p=2$ and appears to be more natural in terms of analytic methods : to study the values of an arithmetic function f. These methods are more adapted to deal with the moments f^α of this function f rather than with expressions of the form $\prod_{0\le i<\alpha}\big(f-p^i\big)$ even if these expressions have been introduced to seize the algebraic properties of an abelian group (see [1, p.50], for the particular case $f(D)=p^{\mathrm{rk}_p(C_D)}$).

We have

Proposition 1. *[3, Prop.1] Let p be a fixed prime and α_0 be a fixed positive integer. Then the average value of*

$$\prod_{0\le i<\alpha}\Big(p^{\mathrm{rk}_p(C_D^2)}-p^i\Big)$$

is equal to 1, for every $0\le\alpha\le\alpha_0$, when D ranges over the set of negative fundamental discriminants, if and only if, under the same conditions, the average value of

$$p^{\alpha\,\mathrm{rk}_p(C_D^2)}$$

is equal to $\mathcal{N}(\alpha,p)$, for every $0\le\alpha\le\alpha_0$.

The same holds for positive discriminants if the above average values 1 and $\mathcal{N}(\alpha,p)$ are replaced by $p^{-\alpha}$ and $p^{-\alpha}\big(\mathcal{N}(\alpha+1,p)-\mathcal{N}(\alpha,p)\big)$, respectively.

We now give expressions of the function $\mathcal{N}(\alpha,p)$ in terms of the function η. Since the number of vector subspaces of dimension ℓ of $\mathbb{F}_p^\alpha$ is equal to

$$\prod_{i=0}^{\ell-1}\frac{p^\alpha-p^i}{p^\ell-p^i}=\prod_{i=1}^{\ell}\frac{p^{\alpha-i+1}-1}{p^i-1}=p^{\ell(\alpha-\ell)}\frac{\eta_\alpha(p)}{\eta_\ell(p)\cdot\eta_{\alpha-\ell}(p)},$$

and since, uniformly in $k\ge0$, we have

$$1\ll_p\eta_k(p)\le1,$$

we get

Lemma 1. *For every integer $\alpha\ge0$ and every $p\ge2$, we have the equalities*

$$\mathcal{N}(\alpha,p)=\eta_\alpha(p)\sum_{\ell=0}^{\alpha}\frac{p^{\ell(\alpha-\ell)}}{\eta_\ell(p)\cdot\eta_{\alpha-\ell}(p)},$$

In particular, the function $\mathcal{N}(\alpha,p)$ satisfies

$$\mathcal{N}(\alpha,p)=O_p\big(p^{\frac{\alpha^2}{4}}\big).$$

3 4–ranks of class groups

The aim of this section is to report on results on 4–ranks of the class group obtained in [3]. We do not give proofs in this section and refer the reader to [3].

We remark that the 4–rank of an abelian group A is the same as the 2–rank of A^2. Therefore we like to study $\mathrm{rk}_2(C_D^2)$ and $\mathrm{rk}_2(\mathrm{Cl}_D^2)$, respectively. We remark that the ordinary class group Cl_D and the narrow class group C_D are the same when $D < 0$. For positive discriminants they are the same if and only if the fundamental unit of $\mathbb{Q}(\sqrt{D})$ has norm -1. In order to simplify we will consider 4–ranks of the narrow class group C_D.

In order to present our results we need the following definition.

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

The 4–rank of the narrow class group can be described by the following theorem which is already implicitly contained in [8, p. 56].

Theorem 3.

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

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

Let us further simplify and concentrate on the case of negative discriminants which are congruent to 1 modulo 4. Then $|D|$ is squarefree as well as the numbers a, b occurring in Theorem 3. Furthermore $b < 0$ in this case and therefore $-b > 0$. It is an easy exercise to see that for coprime integers a and b the symbol $(a|b) = 1$ if and only if a is a square mod b and b is a square mod a. Therefore we get.

Lemma 2. *Let $D < 0$ be a fundamental discriminant with $D \equiv 1 \mod 4$. Then we have the equality*

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

$$\text{and } b \text{ is a square } \mod a\big\}.$$

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

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

By Lemma 2, we get

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

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

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

always under the assumption that $D < 0$ is congruent to 1 modulo 4.

In [3] we show how to do the summation over all D_0, D_1, D_2, D_3 such that $-D_0D_1D_2D_3$ is a fundamental discriminant. We show that this sum has linear asymptotics, where the main term can be obtained by choosing ($D_0 = 1$ or $D_2 = 1$) and ($D_1 = 1$ or $D_3 = 1$). This choice implies that all the four symbols are 1 and the summation can be easily done. In all the other cases we get an oscillating sum. By using large sieve techniques and Siegel-Walfisz theorem, respectively, we are able to show that those oscillating sums are bounded by $O_\epsilon(X \log(X)^{-\frac{1}{2}+\epsilon})$ for all $\epsilon > 0$.

For the higher moments, i.e. the average of $2^{\mathrm{rk}_4(C_D)}$ we use many tricks described in [7], where geometry over $\mathbb{F}_2$ plays a crucial role.

Let us state the main results of [3]. For this we introduce the sums:

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

and

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

Theorem 4. *For every positive integer k and every positive ϵ the following equalities are true, where $R(X,\epsilon,k) := X(\log X)^{-2^{-k}+\epsilon}$:*

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

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

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

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

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

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

Now can we apply Proposition 1 and get

Theorem 5. *Conjectures 1 and 3 are true for $p = 2$ and all $\alpha \geq 0$.*

The results remain true when we replace the narrow class group by the ordinary class group in the definition of $S^+(X, k, a, b)$.

4 Proof of Theorem 1.

We consider first the case of negative discriminants and prove Theorem 1. We postpone the proof of Theorem 2 to §5, where we shall omit details. We follow some ideas contained in [7, p. 359–362]. Since $p \geq 2$ is considered as fixed, we shall forget the dependence on this number in several quantities. Under the hypothesis of Theorem 1 and by Proposition 1, we deduce that for each $k \geq 0$, the average value of $p^{k\,\mathrm{rk}_p(C_D^2)}$ is equal to $\mathcal{N}(k, p)$.

For $X \geq 1$, let

$$N(X, r) := \sharp\big\{D\,;\, 0 < -D < X,\, \mathrm{rk}_p(C_D^2) = r\big\}.$$

For every $X \geq 1$ and every $k \geq 0$, the definition of $N(X, r)$ and the assertion of Theorem 1 implies

$$\sum_{r=0}^{\infty} \frac{N(X,r)}{X} p^{k\,r} = \frac{1}{X} \sum_{0<-D<X} p^{k\,\mathrm{rk}_p(C_D^2)} = \mathcal{N}(k,p) + o_k(1). \tag{2}$$

We apply (2) with k replaced by $2k+1$ and appeal to Lemma 1 to write

$$\frac{N(X,r)}{X} p^{(2k+1)r} \leq \sum_{\ell=0}^{\infty} \frac{N(X,\ell)}{X} p^{(2k+1)\ell} = O_k(1),$$

from which we deduce that $N(X, r)/X$ goes quickly to 0 as $r \to +\infty$ under the form

$$\frac{N(X,r)}{X} \ll_k p^{-(2k+1)r}, \tag{3}$$

uniformly in $X \geq 1$ and $r \geq 0$.

For each r, the sequence $n \mapsto N(n, r)/n$ is a real sequence in the compact set $[0, 1]$. By a diagonal process, there exists real numbers $d_r \in [0, 1]$ ($r \geq 0$) and an infinite subset $\mathcal{M}$ of positive integers such that

$$N(m, r)/m \to d_r \ (m \in \mathcal{M},\, m \to \infty),$$

for each $r \geq 0$. Write (2) in the particular form

$$\sum_{r=0}^{\infty} \frac{N(m,r)}{m} p^{k\,r} = \mathcal{N}(k,p) + o_k(1), \tag{4}$$

for $m \in \mathcal{M}$, note that (3) implies

$$\sum_{r=0}^{\infty} \frac{N(m,r)}{m} p^{k\,r} = O_k(1)$$

uniformly in $m \in \mathcal{M}$, then apply the Lebesgue Dominated Convergence Theorem (see for instance [9, p. 27]) to (4) to finally write, by definition of the d_r, the equality

$$\sum_{r=0}^{\infty} d_r p^{k\,r} = \mathcal{N}(k,p),$$

which is true for every integer k.

Let (S^-) be the infinite linear system

$$(S^-) \qquad \begin{cases} x_0 & +x_1 & +x_2 & +x_3 & +\cdots & +\cdots & =\mathcal{N}(0,p) \\ x_0 & +x_1 p & +x_2 p^2 & +x_3 p^3 & +\cdots & +\cdots & =\mathcal{N}(1,p) \\ x_0 & +x_1 p^2 & +x_2 p^4 & +x_3 p^6 & +\cdots & +\cdots & =\mathcal{N}(2,p) \\ x_0 & +x_1 p^3 & +x_2 p^6 & +x_3 p^9 & +\cdots & +\cdots & =\mathcal{N}(3,p) \\ \cdots & & & & & & \end{cases}$$

in positive unknowns $(x_i)_{i\geq 0}$. Note that each $(d_r)_{r\geq 0}$ obtained by the above diagonal procedure is a solution to (S^-). Hence this system has at least one solution. We shall first give an explicit solution to (S^-): the numbers appearing in Theorem 1 (see Proposition 2), and prove that (S^-) has at most one system of solutions (see Proposition 3). This will imply that for each $r \geq 0$, the sequence $N(X,r)/X$ has only one limit point as X tends to infinty and that this limit point is $p^{-r^2}\eta_\infty(p)\eta_r^{-2}(p)$.

4.1 A special solution of (S^-)

We shall prove

Proposition 2. *The sequence of numbers $(x_r)_{r\geq 0}$ with $x_r = p^{-r^2}\eta_\infty(p)\eta_r^{-2}(p)$ is a solution to (S^-).*

The proof of this is based on formulas around the theory of partitions. Let $p(n)$ be the partition function, then classically for any x with $|x| < 1$ we have the equality

$$\sum_{n\geq 0} p(n)x^n = \frac{1}{(1-x)(1-x^2)(1-x^3)\cdots} = \eta_\infty(1/x)^{-1}.$$

This formula has been extended into

Lemma 3. *[6, Thm 351] For any $|x| < 1$, we have*

$$\frac{1}{(1-x)(1-x^2)(1-x^3)\cdots} = 1 + \frac{x}{(1-x)^2} + \frac{x^4}{(1-x)^2(1-x^2)^2} + \frac{x^9}{(1-x)^2(1-x^2)^2(1-x^3)^2} + \cdots$$

In other words, we have the formula $\eta_\infty(1/x)^{-1} = \sum_{k=0}^{\infty} \frac{x^{k^2}}{\eta_k^2(1/x)}$. By choosing $x = 1/p$, we proved that the sequence (x_r) satisfies the first equation of (S^-). We must continue this checking to the other equations of (S^-).

We shall first generalize Lemma 3 in

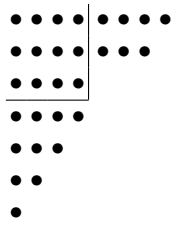
Lemma 4. *Let $t \geq 0$ be an integer. Then for any $|x| < 1$, we have*

$$\frac{1}{(1-x)(1-x^2)(1-x^3)\cdots}$$
$$= \sum_{r=t}^{\infty} \frac{x^{r(r-t)}}{(1-x)^2\cdots(1-x^{r-t})^2(1-x^{r-t+1})\cdots(1-x^r)}.$$

In other words, we have the formula

$$\eta_\infty(1/x)^{-1} = \sum_{r=t}^{\infty} \frac{x^{r(r-t)}}{\eta_{r-t}(1/x)\eta_r(1/x)}.$$

Proof. This formula for instance is in [1, Cor. 6.7,p.51], where the authors say that a proof can be given directly or as a consequence of combination of theorems of their work. For sake of completeness, we give a proof which follows the proof of [6, Thm 351]. The integer $t \geq 0$ is now fixed, and we define the Durfee rectangle with defect $-t$ of a partition of an integer n as the largest rectangle of size $(r, r-t)$ that can be inserted in the northwest corner of this partition. For instance, choose $t = 1$ and $n = 29$, and consider



The above drawing explains for the partition

$$29 = 8 + 7 + 4 + 4 + 3 + 2 + 1,$$

what is the Durfee rectangle of defect -1. It has size $(4, 3)$. Note that there are $\ell = 10$ points out of this Durfee rectangle, southwards, and this ℓ appears as decomposed in partition with summands $\leq r = 4$ $(10 = 4+3+2+1)$. Similarly, eastwards, it remains $m = 7$ points, written in partition with summands $\leq r - 1 = 3$ $(7 = 2 + 2 + 2 + 1)$.

More generally, given a partition of n, with a Durfee rectangle of defect $-t$, with dimension $(r, r-t)$, we write $n = r(r-t) + \ell + m$ and the number of partitions of ℓ in parts $\leq r$ is the coefficient of x^ℓ in

$$\frac{1}{(1-x)(1-x^2)\cdots(1-x^r)}.$$

Similarly, the number of partitions of m in parts $\leq r-t$ is the coefficient of x^m in

$$\frac{1}{(1-x)(1-x^2)\cdots(1-x^{r-t})}.$$

Hence the number of partitions of n, with Durfee rectangle of size $(r, r-t)$ is the coefficient of $x^{n-r(r-t)}$ in the fraction

$$\frac{1}{(1-x)^2(1-x^2)^2\cdots(1-x^{r-t})^2(1-x^{r-t+1})\cdots(1-x^r)}.$$

Summing over all the possible of $r \geq t$, we obtain the expected expression of the function $\sum p(n)x^n$. □

We shall also prove

Lemma 5. *Let $r \geq k \geq 0$ be integers. Then for every $|x| < 1$ we have the equality*

$$\frac{x^{r(r-k)}}{(1-x)^2\cdots(1-x^r)^2} = \sum_{\ell=0}^{k} \frac{\mathfrak{n}(k,\ell,1/x)x^{r(r-\ell)}}{(1-x)^2\cdots(1-x^{r-\ell})^2(1-x^{r-(\ell-1)})\cdots(1-x^r)},$$

where

$$\mathfrak{n}(k,\ell,1/x) = \begin{cases} \displaystyle\prod_{i=1}^{\ell} \frac{(1/x)^{k-i+1}-1}{(1/x)^i-1}, & \text{for } 0 \leq \ell \leq k \\ \\ 0, & \text{for } \ell > k. \end{cases}$$

Proof. Remark first that $\mathfrak{n}(k,\ell,p)$ is equal to the number of vector subspaces of $\mathbb{F}_p^k$ with dimension ℓ, and that this function satisfies the recursive formula (see [3, Lemma 1]):

$$\mathfrak{n}(k+1,\ell,1/x) = \mathfrak{n}(k,\ell-1,1/x) + \frac{1}{x^\ell}\mathfrak{n}(k,\ell,1/x). \tag{5}$$

By multiplication, we see that Lemma 5 is proved if and only if we proved

$$x^{r(r-k)} = \sum_{\ell=0}^{k} \mathfrak{n}(k,\ell,1/x)x^{r(r-\ell)}(1-x^{r-(\ell-1)})\cdots(1-x^r),$$

or equivalently

$$\sum_{\ell=0}^{k} \mathfrak{n}(k,\ell,1/x)x^{r(k-\ell)}(1-x^{r-(\ell-1)})\cdots(1-x^r) = 1. \tag{6}$$

Actually, the fact that r is an integer is useless in the proof of (6), and defining $y = x^r$, we shall prove

$$\sum_{\ell=0}^{k} \mathfrak{n}(k,\ell,1/x)y^{k-\ell}\big(1-\frac{y}{x^{\ell-1}}\big)\cdots\big(1-\frac{y}{x}\big)(1-y) = 1, \tag{7}$$

for every real positive numbers x and y and any positive integer $k \geq 0$. The proof of (7) works by induction on k.

This formula is true for $k = 0$ and $k = 1$, since $\mathfrak{n}(0, 0, 1/x) = \mathfrak{n}(1, 0, 1/x) = \mathfrak{n}(1, 1, 1/x) = 1$. It is also true for $k = 2$, since $\mathfrak{n}(2, 0, 1/x) = \mathfrak{n}(2, 2, 1/x) = 1$ and $\mathfrak{n}(2, 1, 1/x) = 1 + 1/x$. Suppose now that (7) is true for some value $k \geq 3$. So we now study

$$\sum_{\ell=0}^{k+1} \mathfrak{n}(k+1, \ell, 1/x) y^{k+1-\ell} \big(1 - \frac{y}{x^{\ell-1}}\big) \cdots \big(1 - \frac{y}{x}\big)(1-y), \tag{8}$$

and replace the term $\mathfrak{n}(k+1, \ell, 1/x)$ by the recursive formula (5). The contribution of the second term on the right–hand side of (5) is equal to

$$\begin{aligned}
&\sum_{\ell=0}^{k} \mathfrak{n}(k, \ell, 1/x) \frac{y^{k+1-\ell}}{x^\ell} \big(1 - \frac{y}{x^{\ell-1}}\big) \cdots \big(1 - \frac{y}{x}\big)(1-y) \\
&\quad = -\sum_{\ell=0}^{k} \mathfrak{n}(k, \ell, 1/x) y^{k-\ell} \big(1 - \frac{y}{x^{\ell}}\big) \cdots \big(1 - \frac{y}{x}\big)(1-y) \\
&\qquad + \sum_{\ell=0}^{k} \mathfrak{n}(k, \ell, 1/x) y^{k-\ell} \big(1 - \frac{y}{x^{\ell-1}}\big) \cdots \big(1 - \frac{y}{x}\big)(1-y).
\end{aligned}$$

By hypothesis, the last sum of the above equation is equal to 1, and the first sum annihilates with the contribution to (8) of the first term $\mathfrak{n}(k, \ell-1, 1/x)$ coming from the right–hand side of (5) (make the change of variable $\ell \mapsto \ell - 1$). Hence (7) is proved, and subsequently (6). The proof of Lemma 5 is complete. □

We now turn to the proof of Proposition 2. To check that the equation of order $k+1$ of (S^-) is satisfied by the values of (x_r) given in Proposition 2, we have to compute, for $x = 1/p$ the quantity

$$S_k := \sum_{r=0}^{\infty} x_r p^{k\,r} = \eta_\infty(p) \sum_{r=0}^{\infty} \frac{x^{r(r-k)}}{(1-x)^2 \cdots (1-x^r)^2}. \tag{9}$$

By Lemma 5, this is equal to $S_k =$

$$\eta_\infty(p) \sum_{\ell=0}^{k} \mathfrak{n}(k, \ell, 1/x) \sum_{r=0}^{\infty} \frac{x^{r(r-\ell)}}{(1-x)^2 \cdots (1-x^{r-\ell})^2 (1-x^{r-(\ell-1)}) \cdots (1-x^r)},$$

and finally, by Lemma 4, we obtain the equality (still having $x = 1/p$)

$$S_k = \eta_\infty(p) \sum_{\ell=0}^{k} \frac{\mathfrak{n}(k, \ell, 1/x)}{\eta_\infty(1/x)} = \mathcal{N}(k, p). \tag{10}$$

This completes the proof of Proposition 2.

4.2 Unicity of solutions of an infinite linear system.

Let a be a real integer > 1, and $(C_k)_{k\geq 0}$ an infinite sequence of positive real numbers. We are searching for growth conditions on (C_k) to ensure that the linear system with infinitely many equations

$$\sum_{s=0}^{\infty} x_s a^{sk} = C_k \quad (k = 0, 1, \dots) \tag{11}$$

has at most one solution $(x_i)_{i\geq 0}$ with $x_i \geq 0$. Such a system was considered by Heath–Brown [7, Lemmas 17&18] in the particular case $a = 4$, with an appeal to the properties of Vandermonde determinants. We shall rather use Jensen's formula (see Lemma 6 below).

A condition on the growth of C_k is obligatory to ensure the unicity of solutions of (11) in non-negative x_s as can be seen in the following example.

Example 1. Let a be a positive integer and $C_k = \sinh(\pi a^k)$. Then define the coefficients x_s and x'_s by the Taylor expansions $\sinh(\pi t) = \sum x_s t^s$, and $\sin(\pi t) + \sinh(\pi t) = \sum x'_s t^s$. Both sequences (x_s) and (x'_s) consist of non-negative numbers and are solutions of (11).

However the particular coefficients C_k chosen before do not satisfy (13) below.

So let $(x_i)_{i\geq 0}$ be a positive solution to (11). By positivity we deduce the inequality

$$x_s \leq a^{-sk} C_k, \tag{12}$$

for any $s \geq 0$ and $k \geq 0$. To push further the computations, we suppose that there exists an absolute c_0 such that

$$C_k \leq c_0 a^{\frac{k^2}{2}} \quad (k = 0,\, 1, \dots). \tag{13}$$

By choosing $k = s$ in (12), we get

$$0 \leq x_s \leq c_0 a^{-\frac{s^2}{2}}. \tag{14}$$

Now let (x_s) and (x'_s) be two solutions of (11) and consider

$$f(z) = \sum_{s=0}^{\infty} (x_s - x'_s) z^s, \tag{15}$$

considered as a function of the complex variable z. The radius of convergence of this power series is $+\infty$, by (14). It is an entire function, which is zero at each a^k $(k = 0, 1, \dots)$. It also satisfies the inequality

$$|f(z)| \leq 2c_0 \sum_{s=0}^{\infty} a^{-\frac{s^2}{2}} |z|^s.$$

In particular, if $|z| = a^k$, for some absolute c_0', we get

$$|f(z)| \le 2c_0 \sum_{s=0}^{\infty} a^{-\frac{s^2}{2}} a^{ks} \le c_0' a^{\frac{k^2}{2}}. \tag{16}$$

We shall first prove

Lemma 6. *Let $\ell \ge 0$ be an integer and $a \in \mathbb{C}$ such that $|a| > 1$. Furthermore let $g(z)$ be an entire function which has a zero of order ℓ at $z = 0$ and satisfying $g(a^k) = 0$ for any $k \ge 0$. Then for every $k \ge 0$ the function g satisfies the inequality*

$$\sup_{|z|=|a|^k} |g(z)| \ge \frac{|g^{(\ell)}(0)|}{\ell!} |a|^{\frac{k(k+1)}{2}+k\ell}.$$

Proof. This is an application of Jensen's formula (see for instance [9, Thm 15.18]), applied to the function $h(z) = z^{-\ell} g(z)$. With ρ denoting any zero of h, we have the relations

$$|h(0)||a|^{\frac{k(k+1)}{2}} = |h(0)| \prod_{0\le\ell\le k} \frac{|a|^k}{|a^\ell|} \le |h(0)| \prod_{\rho,\, |\rho|\le|a|^k} \frac{|a|^k}{|\rho|}$$
$$= \exp\Big\{ \frac{1}{2\pi} \int_{-\pi}^{\pi} \log\big|h(|a|^k \mathrm{e}^{i\theta})\big| \, \mathrm{d}\theta \Big\} \le \sup_{|z|=|a|^k} |h(z)| = |a|^{-k\ell} \sup_{|z|=|a|^k} |g(z)|,$$

which gives the result. □

Now suppose that we have two distinct solutions (x_s) and (x_s') to (11). Let ℓ be the least index s such that $x_s \ne x_s'$. Hence the function defined in (15) is not identically equal to 0. Then we apply Lemma 6 to $f(z)$, and by comparing with (16), we are led to the lower bound $a^{\frac{k^2}{2}} \gg a^{\frac{k(k+1+2\ell)}{2}}$. This is impossible for k sufficiently large. Hence $f \equiv 0$. In conclusion we proved

Proposition 3. *If the coefficients (C_k) satisfy the conditions* (13)*, then the infinite linear system* (11) *has at most one solution in positive $(x_s)_{s\ge0}$.*

To prove Theorem 1, it remains to combine Proposition 1, 2, 3, and Lemma 1 in order to deduce that, under the hypothesis of this theorem, for each $r \ge 0$, for $X \to +\infty$, the function $N(X, r)/X$ has only one limit point which is equal to $p^{-r^2} \eta_\infty(p) \eta_r(p)^{-2}$.

5 The case of positive discriminants

The strategy is the same. We study the limit points of the sequence $N(X, r)/X$, where $N(X, r)$ is now defined by

$$N(X, r) := \sharp\big\{ D \,;\, 0 < D < X,\, \mathrm{rk}_p(C_D^2) = r \big\}.$$

These limit points are solutions to (S^+) where S^+ the infinite linear system

$$(S^+) \qquad \begin{cases} x_0 & +x_1 & +x_2 & +x_3 & +\cdots & +\cdots & =\mathcal{M}_0(p) \\ x_0 & +x_1 p & +x_2 p^2 & +x_3 p^3 & +\cdots & +\cdots & =\mathcal{M}_1(p) \\ x_0 & +x_1 p^2 & +x_2 p^4 & +x_3 p^6 & +\cdots & +\cdots & =\mathcal{M}_2(p) \\ x_0 & +x_1 p^3 & +x_2 p^6 & +x_3 p^9 & +\cdots & +\cdots & =\mathcal{M}_3(p) \\ \cdots & & & & & & \end{cases}$$

where we defined

$$\mathcal{M}_k(p) = \frac{1}{p^k}\big(\mathcal{N}(k+1,p) - \mathcal{N}(k,p)\big).$$

We first notice

Lemma 7. *For every $k \geq 1$, we have*

$$\mathcal{M}_k(p) = \frac{\mathcal{M}_{k-1}(p)}{p} + \mathcal{N}(k-1,p).$$

Proof. This is an easy consequence of the equality

$$\mathcal{N}(k+1,p) = 2\mathcal{N}(k,p) + (p^k - 1)\mathcal{N}(k-1,p) \ (k \geq 1).$$

which is proved in [3, Lemma 3]. □

We are now in position to prove

Proposition 4. *The sequence of numbers $(x_r)_{r\geq 0}$ with*

$$x_r = p^{-r(r+1)}\eta_\infty(p)\eta_r(p)^{-1}\eta_{r+1}(p)^{-1}$$

is a solution of (S^+).

Proof. By linear combination and by Lemma 7, we see that (S^+) is equivalent to the system (Σ^+) defined by

$$(\Sigma^+) \qquad \begin{cases} x_0 & +x_1 & +x_2 & +\cdots = \mathcal{M}_0(p) \\ x_0(1-p^{-1}) & +x_1(p-p^{-1}) & +x_2(p^2-p^{-1}) & +\cdots = \mathcal{N}(0,p) \\ x_0(1-p^{-1}) & +x_1(p^2-1) & +x_2(p^4-p) & +\cdots = \mathcal{N}(1,p) \\ x_0(1-p^{-1}) & +x_1(p^3-p) & +x_2(p^6-p^3) & +\cdots = \mathcal{N}(2,p) \\ \cdots & & & \end{cases}$$

where the line of order $k+1$ $(k \geq 1)$ is given by

$$\sum_{r=0}^{\infty} x_r\big(p^{kr} - p^{(k-1)r-1}\big) = \mathcal{N}(k-1,p). \tag{17}$$

The first line is satisfied with the above choice of the (x_r), since we have the equality

$$\sum_{r=0}^{\infty} x_r = \eta_\infty(p) \sum_{r=0}^{\infty} \frac{(1/p)^{r(r+1)}}{\eta_r(p)\eta_{r+1}(p)} = \eta_\infty(p) \sum_{r=1}^{\infty} \frac{(1/p)^{r(r-1)}}{\eta_{r-1}(p)\eta_r(p)}$$

$$= \eta_\infty(p)\eta_\infty(p)^{-1} = 1 = \mathcal{M}_0(p)$$

by Lemma 4.

To study the line of order $k+1$ $(k \geq 1)$ of (Σ^+), we write the equalities

$$\sum_{r=0}^{\infty} x_r \big(p^{kr} - p^{(k-1)r-1}\big)$$

$$= \eta_\infty(p) \sum_{r=0}^{\infty} \frac{(1/p)^{r(r+1)} \cdot (1/p)^{-k\,r}(1-(1/p)^{r+1})}{(1-(1/p))^2 \cdots (1-(1/p^r))^2(1-(1/p^{r+1}))}$$

$$= S_{k-1},$$

where S_{k-1} is the expression introduced in (9) to study the linear system (S^-). By (10), we know that this is equal to $\mathcal{N}(k-1,p)$. This ends the proof of (17) for all the values of k, hence (Σ^+) and (S^+) are satisfied with the chosen values of x_r. The proof of Proposition 4 is now complete.

□

5.1 Unicity of solutions.

By definition of $\mathcal{M}_k(p)$ and by Lemma 1, we get the relation

$$\mathcal{M}_k(p) = O(p^{\frac{k^2}{4}-\frac{k}{2}}).$$

Hence $\mathcal{M}_k(p)$ satisfy the conditions (13). By Proposition 3, the infinite linear (S^+) system has at most one solution. As for the case of negative discriminants, we deduce that, for any $r \geq 0$, the function $N(X,r)/X$ has only one limit point as $X \to +\infty$. By Proposition 4, these limit points have the values announced in Theorem 2. The proof of this theorem is complete.

References

1. Cohen, H., Lenstra, H.W.: Heuristics on class groups of number fields. In: Number theory, Noordwijkerhout 1983, volume 1068 of Lecture Notes in Math., pages 33–62. Springer, Berlin (1984)
2. Davenport, H.,Heilbronn, H: On the density of discriminants of cubic fields II. Proc. Roy. Soc. London Ser. A **322**(1551),405–420 (1971)
3. Fouvry, E., Klüners, J.: On the 4–rank of class groups of quadratic number fields. Preprint, (2006)
4. Gerth III, F.: The 4-class ranks of quadratic fields. Invent. Math. **77**(3),489–515 (1984)

5. Gerth III, F.: Extension of conjectures of Cohen and Lenstra. Exposition. Math. **5**(2),181–184 (1987)
6. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press (1975)
7. Heath–Brown, D.R.: The size of Selmer groups for the congruent number problem II. Inv. Math., **118**, 331–370, (1994)
8. Redei, L.: Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. J. Reine Angew. Math. **171**, 55–60 (1934)
9. Rudin, W.: Real and Complex Analysis, second edition. McGraw–Hill Book Company, (1974)