UNIVERSITÀ DEGLI STUDI ROMA TRE
FACOLTÀ DI S.M.F.N.

Tesi di Laurea in Matematica
presentata da Manuela Grella

Algebraic, analytic and computional theory of the Class Number

Relatore
Prof. Francesco Pappalardi

Il Candidato | Il Relatore

ANNO ACCADEMICO 2005-2006

Classificazione: 11R20 (11M41, 11Y40)
Parole chiave: Class Number, Class Number Formula, Dirichlet L-series, Multiplicative Number Theory, Algebraic Number Theory.

Contents

Introduction

This thesis is about the Class Number. We will deal with its algebraic, analytic and computational theory.
The Class Number has a very important role either in Analytic Number Theory, where it has been used in the proof of the Theorem of the existence of infinitely many primes in a given arithmetic progression, or in Algebraic Number Theory, since it measures how far the ring of integers of a number field is from being a Unique Factorization Domain (UFD). At first the Class Number has been defined in the theory of binary quadratic forms. It represents, in fact, the number of the classes of a defined equivalence relation in which the forms $ax^2 + bxy + cy^2$ with $a,\ b,\ c \in \mathbb{Z}$ and a fixed discriminant $d = b^2 - 4ac$, split. Then, in the theory of number fields, it has been defined as the order of a quotient group, said Class Group.
In 1832 Jacobi conjectured a Class Number formula. In 1839 Dirichlet proved this famous formula and used it to complete the proof of the following theorem [17]:

Theorem 0.1. *(Existence of infinitely many primes in a given artihmetic progression.) If $a,\ q \in \mathbb{N}$, $(a, q) = 1$ and if P is the set of all the primes , then*

$$\#\{a, a+q, a+2q, \dots\} \cap P = \infty.$$

The connection between the Class Number and the Theorem 0.1 is given by the definition of the so-called Dirichlet's characters and of particular functions, similar to the Riemann Zeta function, said Dirichlet's L-functions. These objects, which are related, will be used often in our work.

A Dirichlet's character modulo an integer q is a function

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C}$$

with the following properties :

1. χ is periodic with period q, i.e. $\chi(n+q) = \chi(n)$, $\forall n \in \mathbb{N}$;
2. χ is multiplicative, i.e. $\chi(n \cdot m) = \chi(n) \cdot \chi(m)$, $\forall n, m \in \mathbb{N}$;
3. χ is supported on $U(\mathbb{Z}/q\mathbb{Z})$, i.e. $\chi(n) = 0$ when $(q, n) \neq 1$.

It is possible that for values of n such that $(n, q) = 1$ the function $\chi(n)$ may have a period less than q, in this case the character is said imprimitive and otherwise primitive. We are interested in primitive characters. It is possible to prove that all the real primitive characters are identical with the Jacobi symbols $\left(\frac{d}{n}\right)$ where d is a product of relatively prime factors of the form

$$-4,\ 8,\ -8,\ (-1)^{(p-1)/2}p$$

where $p > 2$, p prime. Moreover the Jacobi symbol is a real primitive character modulo $|d|$. A useful result about the characters which we are going to use are the Ortogonality Laws and the inequality found in 1918 by Polya and Vinogradov. [18, 19]

Proposition 0.1. *(Ortogonality Laws of characters)*
If χ is a character modulo q

1.

$$\sum_{n \in (\mathbb{Z}/q\mathbb{Z})} \chi(n) = \begin{cases} \varphi(q) & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0 \end{cases}$$

where

$$\chi_0 = \begin{cases} 0 & \text{if } (n, q) \neq 1 \\ 1 & \text{if } (n, q) = 1 \end{cases}$$

is said the principal character modulo q.

2.

$$\sum_{\chi(\bmod q)} \chi(n) = \begin{cases} \varphi(q) & \textit{if } n \equiv 1(\mathrm{mod} q) \\ 0 & \textit{otherwise} \end{cases}.$$

Theorem 0.2. *(Polya-Vinogradov Inequality)*
If χ is a nonprincipal character modulus q, then

$$\sum_{n=M+1}^{M+N} \chi(n) \ll q^{1/2} \log q.$$

Dirichlet's L-functions are defined as

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

and they are absolutely convergent for $\mathrm{Re}\, s > 1$. As for the Riemann Zeta function, it is possible to write this function as an Euler product that is

$$L(s,\chi) = \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Moreover, again as the Zeta function, the L-series satisfy a functional equation which we are going to use a lot in our results. This equation takes different forms according as $\chi(-1) = 1$ or $\chi(-1) = -1$, where χ is a primitive character modulo q. If $\chi(-1) = 1$, we have

$$\begin{cases} \pi^{-\frac{1}{2}(1-s)} q^{\frac{1}{2}(1-s)} \Gamma\left[\frac{1}{2}(1-s)\right] L(1-s,\overline{\chi}) \\ = \frac{q^{\frac{1}{2}}}{\tau(\chi)} \pi^{-\frac{1}{2}s} q^{\frac{1}{2}s} \Gamma(\frac{1}{2}s) L(s,\chi), \end{cases}$$

where $\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt$ is the Gamma function and $|\tau(\chi)| = q^{1/2}$ for a primitive character; in the case $\chi(-1) = -1$ the equation becomes

$$\begin{cases} \pi^{-\frac{1}{2}(2-s)} q^{\frac{1}{2}(2-s)} \Gamma\left[\frac{1}{2}(2-s)\right] L(1-s,\overline{\chi}) \\ = \frac{iq^{\frac{1}{2}}}{\tau(\chi)} \pi^{-\frac{1}{2}(s+1)} q^{\frac{1}{2}(s+1)} \Gamma\left[\frac{1}{2}(s+1)\right] L(s,\chi). \end{cases}$$

Dirichlet realized that, in order to prove Theorem 0.1, it needs to prove that if $\chi \neq \chi_0$, χ primitive character, then $L(1,\chi) \neq 0$. Nowadays this can be proved by the complex analysis methods but Dirichlet did not know it. So he used only real analysis and particularly the connection between real primitive characters and the theory of binary quadratic forms or the equivalent theory of quadratic fields. In fact it is simple to prove that the numbers d described above are identical with particular discriminants, said fundamental, in the theory of binary quadratic forms, and the discriminants of the quadratic fields in the theory of number fields. In his work, Dirichlet found a connection between the Class Number of quadratic forms with a given discriminant d and the L-function $L(1, \chi)$, where χ is a real primitive character $\left(\frac{d}{n}\right)$ and this is the Kronecker symbol, that is the real extension of the Jacobi symbol. This connection allowed him to prove that $L(1, \chi)$ is strictly positive, and moreover to find an expression of such an L-function as a finite sum.

In this thesis at first, like in Dirichlet's work, we study briefly the theory of binary quadratic forms to obtain the Class Number Formula, then we study Class Numbers from the point of view of the algebraic number theory and its analytic properties and, in the last chapter, we deal with the computational problem, that is we analise the algorithm found until now to compute efficiently the Class Number and the structure of the Class Group.

Our work is organized in the following way.

In Chapter 1 we define an equivalence relation in the set of the binary quadratic forms of a fixed discriminant d in the following way: two forms F and G are said to be equivalent if they are under a unimodular transformation. That is if there exist r, s, t and $u \in \mathbb{Z}$ such that $ru - st = 1$, such that

$$F(rX + sY, tX + uY) = G(X, Y).$$

So, we define, given a discriminant d, the Class Number $h(d)$ as the number of equivalence classes of forms with discriminant d. We prove the finiteness of $h(d)$ [28] using the result, proved by Langrange, that in every equivalence class there is a unique reduced form. That is a form $F(x, y) = ax^2 + bxy + cy^2$ such that $|b| \leq |a| \leq |c|$. Then we try to find a formula for $h(d)$ studing the transformations between forms and the problem of the representability of an integer by particular forms. An interesting result is about the number of unimodular transformations of a form F into itself (the so called *automorphs*). If the form has a negative discriminant d we can prove that the number of these transformations is

$$w = \begin{cases} 2 & \text{if } d < -4 \\ 4 & \text{if } d = -4 \\ 6 & \text{if } d = -3 \end{cases},$$

while, if d is positive, we have a different situation because all the transformations of F into itself are related to the infinity solutions of the Pell's equation $t^2 - du^2 = 4$. [29]

The question of the representability of a number by a form can be expressed in the following way: given a system of representatives, that is a set of forms (one for each class), how many are the representations of a positive integer k (i.e. the pairs (x, y) such that $F(x, y) = k$), by forms belonging to a such system? Since, when d is positive, every representation by a form F gives rise to an infinity of others by the applications of the automorphs of such a form, we consider particular representations, said primary, which are in every case of finite number. A representation of a positive integer k by a form of coefficients a, b, c is said primary if $d < 0$ in every case, while, if $d > 0$, when the following conditions are verified

1. $2ax + (b - \sqrt{d})y > 0$,

2. $1 \leq \frac{2ax+(b+\sqrt{d})y}{2ax+(b-\sqrt{d})y} < \epsilon^2$

where $\epsilon = \frac{t_0+u_0\sqrt{d}}{2}$ and (u_0, t_0) is the smallest positive solutions of the Pell's equation (i.e. the solution for which t_0 has the smallest possible positive value and for which $x_0 > 0$).

One of the main results of the theory of quadratic forms, which allow us to obtain a relation between $h(d)$ and $L(1, \chi)$, where $\chi(n) = \left(\frac{d}{n}\right)$ is a character modulo d, is that the number $\Psi(k)$ of primary representations of a positive integer k, where $(k,d)=1$, by forms belonging to a system of representatives is finite and is expressed by the formula:

$$\Psi(k)=w\sum_{n|k}\left(\frac{d}{n}\right).$$

The proof of such a result is based on the fact that the number of solutions of the congruence $x^2\equiv d(\mathrm{mod}4k)$, when $0\le x<2k$, is $\sum_{f|k}\left(\frac{d}{f}\right)$. Here the sum is extendedon square-free values of f.

The second step of our work is to determine the average value of $\Psi(k)$ as k varies; in order to do it we use the properties of Dirichlet's characters (in particular way the Ortogonality Laws). We obtain the following result

$$\lim_{\tau\to\infty}\frac{H(\tau)}{\tau}=w\frac{\varphi(|d|)}{|d|}L(1,\chi),$$

where

$$H(\tau)=\sum_{\substack{1\le k\le\tau\\(k,d)=1}}\Psi(k).$$

Moreover, using elementary results of Number Theory, we have that, if we set

$$H(\tau,F)=\sum_{\substack{1\le k\le\tau\\(k,d)=1}}\Psi(k,F),$$

where $\Psi(k,F)$ is the number of primary representations of k by a form F of the representative system, it follows

$$\lim_{\tau\to\infty}\frac{H(\tau,F)}{\tau}=\begin{cases}\frac{2\pi}{\sqrt{|d|}}\frac{\varphi(|d|)}{|d|} & \text{if } d<0\\ \frac{\log\epsilon}{\sqrt{d}}\frac{\varphi(d)}{d} & \text{if } d>0.\end{cases}$$

From the defintion of the Class Number and the above results, we obtain the goal of the chapter that is Dirichlet's formula:

$$h(d)=\begin{cases}\frac{w\sqrt{|d|}}{2\pi}L(1,\chi) & \text{if } d<0\\ \frac{\sqrt{d}}{\log\epsilon}L(1,\chi) & \text{if } d>0.\end{cases}$$

In a similar way, using also results from the classical theory of Fourier series, we are able to write $L(1, \chi)$ as a finite sum:

$$L(1,\chi) = \begin{cases} -\frac{1}{\sqrt{d}} \sum_{r=1}^{d-1} \left(\frac{d}{r}\right) \log\sin\left(\frac{\pi r}{d}\right) & d > 0 \\ -\frac{\pi}{|d|^{3/2}} \sum_{r=1}^{|d|-1} \left(\frac{d}{r}\right) r & d < 0. \end{cases}$$

In Chapter 2 at first we recall some fundamental facts about algebraic number theory. We are particularly interested in the number fields, and in particular in the quadratic fields, that are the subfields of $\mathbb{C}$ with dimension 2 as $\mathbb{Q}$ vector spaces and so expressed in the form $\mathbb{Q}(\sqrt{d})$, where d is a square-free integer, $d \neq 1$. We also recall the definitions of discriminant, trace and norm. In order to give a new definition of the Class Number we use the ring of integers $\mathcal{O}_K$ of a number field K (and in particular its ideals) that is the set of the elements of K which are roots of a monic polynomial with integral coefficients. An important question is to know when the ring of integers of a quadratic field is a UFD as d varies. This problem was studied for the first time by Gauss in its *Disquisitiones Arithmeticae* and it has been solved only in the case $d < 0$. In 1967, in fact, Baker and Stark [2, 33] proved that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a UFD only for nine values of d, precisely

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

In the case $d > 0$ Gauss conjectured that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a UFD for infinitely many values of d. Today this problem is still unsolved but we know several positive values of d for which the unique factorization occurs.
In the central part of this chapter we define the Class Group of a number field K using the ideals of $\mathcal{O}_K$ and in particular the so-called fractional ideals, that are $\mathcal{O}_K$-submodules F of K which can be written as $F = d^{-1}I$ where d is an element of $\mathcal{O}_K$ different from zero and $I \subseteq \mathcal{O}_K$ an ideal.

Fractional ideals form a group under the multiplication. So, the Class Group is the quotient of the group of fractional ideals of $\mathcal{O}_K$ by the normal subgroup of principal fractional ideals, that is $\mathbf{Cl}(\mathcal{O}_K) = \frac{\mathbf{F}(\mathcal{O}_K)}{\mathbf{P}(\mathcal{O}_K)}$ where

$\mathbf{F}(\mathcal{O}_K) = \{F|F$ fractional ideal of $\mathcal{O}_K$ $\}$ and $\mathbf{P}(\mathcal{O}_K) = \{z\mathcal{O}_K|z \in K, z \neq 0\}$. The order of the Class Group is also said Class Number. Now the proof of the finiteness of the Class Number comes from a fundamental result in the geometry of numbers, the Minkowsky's Theorem of 1896, and from the concept of the norm of an ideal, defined as the order of the quotient of $\mathcal{O}_K$ by the ideal. We have outlined the connection between the Class Number and the factorization in the ring of integers of a number field, this connection is evident from the definition of the Class Group stated above; in fact, since the ring of integers of a number field is a Dedekind domain, it is a UFD if and only if all the ideals are principal, also the fractional ideals, and this means that the Class Group has order 1 and so the Class Number is equal to 1.
In the last part of the chapter we connect all these results with those of the previous chapter, that is we analise the connections between the theory of quadratic forms and the theory of the ideals in the ring of integers of quadratic fields. We describe, using two lemmas, the existence of a correspondence between ideals and forms and we state the so-called Correspondence Theorem [16] according to which equivalent forms corresponds to equivalent ideals and conversely, where we have to use the definition of the narrow equivalence between ideals (two ideals I and J are said to be strictly equivalent if there exists two principal ideals $\langle a\rangle$, $\langle b\rangle$ such that $I\langle a\rangle = J\langle b\rangle$ and $N(ab) > 0$.) This correspondence allow us to talk, in the case of fundamental discriminant, in the same way, about the Class Number of forms of discriminant d or about the Class Number of a quadratic field $\mathbb{Q}(\sqrt{d})$, and to obtain again, working with the ideals, Dirichlet's Class Number Formula.

In Chapter 3 we deal with some questions about the Class Number which have interested mathematicians also in recent years. A famous problem, called Gauss's Class Number Problem is that to determine, given an integer m, all the negative fundamental discriminants having the Class Number equal to m. Such a problem in the case $m = 1$ is equivalent to find all the values of $-d$ such that the quadratic imaginary field $\mathbb{Q}(\sqrt{-d})$ is a UFD; it has been solved, as we said in the second chapter, finding only nine values of $-d$. In the case $m \neq 1$, until now the question has been solved only in particular cases, for example for $5 \leq m \leq 23$ when m is odd.

The main question in this chapter is to study the behavior of the Class Number as d varies, finding asymptotic estimates for $h(d)$ and for its mean value. Also in this case Gauss stated some conjectures. He said that $h(d) \to \infty$ as $d \to -\infty$ and this, after the attempts of Hecke and Heilbronn, was proved in 1935 by Siegel by his famous ineffective theorem [22] about the L-series. The Theorem of Siegel gives an estimate of $L(1, \chi)$ from which, using the Class Number Formula , follows an inequality for the Class Number; in particular we obtain $h(d) > C_2(\epsilon)|d|^{\frac{1}{2}-\epsilon}$, if d is negative, and $h(d) \log \eta > C_2(\epsilon) d^{\frac{1}{2}-\epsilon}$ if d is positive, where η is the fundamental unity of the field $\mathbb{Q}(\sqrt{d})$ and $C_2(\epsilon)$ is an ineffective constant.

Using again the Polya-Vinogradov inequality and the expression of $L(1, \chi)$ as a finite sum, found in the first chapter, we have some estimates of $h(d)$, i.e. $\log(h(d)) \sim \log(\sqrt{|d|})$ if $d \to -\infty$, and $\log(h(d) \log(\eta)) \sim \log(\sqrt{d})$ if $d \to \infty$.

In order to estimate the mean value of $h(d)$, that is the average number of quadratic forms of a fixed discriminant d, we prove a result found by Siegel in 1944 according to which, if d is a square-free integer such that $d \equiv 0, 1(\text{mod} 4)$, it follows

$$\sum_{0<-d<N} h^+(d) = \frac{\pi}{18\zeta(3)} N^{3/2} + O(N \log N)$$

and

$$\sum_{0<d<N} h^+(d) \log \eta^+ = \frac{\pi^2}{18\zeta(3)} N^{3/2} + O(N \log N)$$

where $h^+(d)$ is the Class Number obtained from the narrow equivalence of ideals, $\zeta(s)$ is the Riemann Zeta function and $\eta^+ = \frac{t+u\sqrt{d}}{2}$ where (t, u) is the smallest positive solution of the Pell's equation $t^2 - du^2 = 4$. To prove these estimates we use a lot the properties of the Jacobi symbol $\left(\frac{d}{n}\right)$ and the fact that it represents a primitive character modulo $|d|$. From this result, by the definition of fundamental discriminant and the expansion of the Riemann

Zeta function as a Euler product, we obtain that, if $d < 0$,

$$\sum_{0<-d\leq N} \frac{h(d)}{\sqrt{|d|}} = \frac{N}{2\pi}C + O(N^{3/4}\log N),$$

and, if $d > 0$,

$$\sum_{0<d\leq N} \frac{h(d)\log\eta^+}{\sqrt{d}} = \frac{N}{4}C + O(N^{3/4}\log N)$$

where

$$C = \prod_p \left(1 - \frac{1}{p^2(p+1)}\right)$$

and the sums are over fundamental discriminants.
In the last part of the Chapter we state a list of conjectures about the behavior of the Class Number and the Class Group which are called "Cohen and Lenstra Heuristics" [9], from the names of the mathematics which proposed them. These conjectures are very important because until now we know very few theorems about this argument. Moreover many results have been confirmed by a large number of experimental observations. Some of these conjectures are about the frequency with which odd primes p divide the Class Number, the probability that the odd part of the Class Group is non-cyclic, and the number of non-cyclic factors of the p-Sylow subgroups. An interesting hypothesis is that the probability that the subgroup of all the elements of the Class Group of an imaginary quadratic field with odd order is cyclic is 97%.

In Chapter 4 we deal with the problem to build an efficient algorithm which, given a discriminant D as input, finds the Class Number $h(D)$ and the structure of the Class Group $\mathbf{Cl}(D)$. We studied with more details the algorithm found by Shanks in 1968 because it was the first efficient method found and a lot of the subsequent work is based on similar ideas or they are its improvements. At first we explain that we can describe the structure of an abelian finite group G, by an algorithm, using the so-called invariants, that is integers $d_1, \dots d_n$ such that d_i divides d_{i+1} for $i = 1, \dots, n$ and G is isomorphic to the group $\mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \dots \mathbb{Z}/d_n\mathbb{Z}$, from the fundamental classification theorem of finitely generated abelian groups.

The first algorithm which we study is very immediate but not much efficient. It is based on the definition of the Class Number given in the first chapter, that is it count, given a discriminant D, the number of the classes of quadratic forms with such a discriminant counting the number of reduced forms. We show that the complexity of this algorithm is $O(|D|)$, this means that for large discriminants the algorithm is very slow.

The second method which we analise is based on the analythic formulas of $h(D)$ and, although it is not very efficient, we study it because it represents an interesting use of the functional equation of the L-series $L(1, \chi)$. Using such equation we find, in fact, the following formula for $h(D)$, when $D < -4$ is a fundamental discriminant,

$$h(D) = \sum_{n \geq 1} \left(\frac{D}{n} \right) \left(\operatorname{erfc} \left(n \sqrt{\frac{\pi}{|D|}} \right) + \frac{|D|}{n\pi} e^{-\frac{\pi n^2}{|D|}} \right)$$

where

$$\operatorname{erfc} = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2} dt$$

is the called *Error Complementary Function.* Using this formula we can build an algorithm with running time $O\left(|D|^{1/2+\epsilon}\right)$ $\forall \epsilon > 0$.

We remark that these methods compute only the Class Number and do not give information about the Class Group. So the main part of the chapter is about the study of Shanks's algorithm, called Baby Steps Giant Steps, which firstly is a method to compute the order of an element g in an abelian finite group G. Furthermore it can be modified to obtain the order of a group and its invariants and can be used to find the Class Number and the invariants of the Class Group.

At first we give a description and a pesudocode for the original Shanks's algorithm which computes the order of an element g, when we know at least an upper bound B of it. The idea is the following. Set $q = \left\lceil \sqrt{B} \right\rceil$, we compute powers of the element g, in particular g^r with $0 \leq r < q$ (baby steps) and

g^{-aq} with $0 \leq a < q$ (giant steps), to obtain a multiple (precisely $aq + r$) of the order of g; then the order is obtained by factorization. We find that the computational cost of this method, using an efficient sorting algorithm, is $O\left(q \log q\right)$.

Then we describe the theory used to represent the group G in order to modify the previous algorithm to obtain the order of G, given an upper bound of it, and its invariants. All is based on a representation of the group via generators and relations. So the problem becomes that of finding, at every steps of the algorithm, a relation between the elements $g_1, \ldots, g_r$ of the group, chosen in a random way, and this is equivalent to find integers $(\rho_1, \ldots, \rho_r)$ such that $\prod_{i=1}^{r} g_i^{\rho_i} = 1$; in this way we obtain, at every steps, the columns of a matrix, called relation matrix. The invariants are obtained computing the Smith Normal Form of the relation matrix, that is applyng to this matrix an efficient algorithm which transform it in a diagonal matrix $\mathrm{diag}(d_1, \ldots, d_n)$ such that for $i = 1, \ldots, n$, $d_i | d_{i+1}$ and the invariants of G are the d_i's. So we explain how obtain the relations between the elements by the Baby Steps Giant Steps method described above and we remark the importance of knowing an upper bound of the order of the group to give a criterion to stop the algorithm.

Also in this case we give a pesudocode of the algorithm and a description of the tecnique used to obtain the columns of the relation matrix, storing the exponents of the elements found at every steps in particular lists of lists.

Then we explain how use this algorithm for the Class Group. The main questions are how to compute in $\mathbf{Cl}(D)$ and how obtain an upper bound for $h(D)$.

The first probem is solved using an operation between reduced forms, said composition, which was introduced by Gauss in 1798. In particular we give the pseudocode of the algorithm which, given a form, computes the reduced equivalent form and the pseudocode of one which computes the composition of two given forms.

Un upper bound for $h(D)$ is found using again Analytic Number Theory; in particular the Euler products and the properties of Dirichlet's Characters. Such upper bound, under the assumption of the Generalized Riemann Hypothesis (i.e. the Riemann Hypothesis for the functions $L(s,\chi)$), is given, when $P \to \infty$, by

$$h(D) - \widetilde{h} = O(\widetilde{h} P^{-1/2} \log(P|D|)),$$

where

$$\widetilde{h} = \left\lfloor \frac{\sqrt{|D|}}{\pi} \prod_{l \leq P} \left(1 - \frac{\left(\frac{D}{l}\right)}{l} \right)^{-1} \right\rfloor .$$

At this point , having all the information, we give the pseudocode of Shanks's algorithm applied to the Class Group and we estimate its running time by $O\left(|D|^{1/4} \log^2(|D|^{1/4})\right)$.

The last part of the chapter is about the description of other algorithms more efficient and to a rapid discussion of some of the most important results obtained until now. We describe the so-called sub-exponential algorithm of Mc Curley and Atkin, which uses a strategy similar to that of Shanks's method but, at every iterations, computes multiples of the Class Number instead of divisors. Its running time is $O\left(L(|D|)^{\sqrt{9/8}}\right)$ where $L(x)$ is the function defined as

$$L(x) = e^{\sqrt{\log x \log \log x}}.$$

Then we deal with the last improvements of the discussed algorithm; in particular we discuss a recent paper by M. J. Jacobson, Jr., S. Ramachandran and H. C. Williams [26], 2006. This work has been sent us, by e-mail, by Williams and will be discussed in the Proceedings of the 7th Algorithm Number Theory Symposium (ANTS VII) at the end of July. In it the authors describe the tecniques used to compute, by a $O(|d|^{1/4})$ algorithm, the Class Number and the Class Group Structure of all imaginary quadratic fields with discriminant d for $0 < |d| < 10^{11}$.

Chapter 1

Quadratic forms and Class Number

In this chapter we are going to analize in short the theory of binary quadratic forms, that are expressions of the form $ax^2 + bxy + cy^2$, where a, b, $c \in \mathbb{Z}$.
In particular we are going to define **the discriminant** of a form and to deal with the problem of determining the so-called **Class Number** for quadratic forms with fixed discriminant d and its connection with Dirichlet L-series $L(s, \chi)$ (in particular with $L(1, \chi)$), where χ stands for a primitive real character.
In 1832 **Jacobi** conjectured a **Class Number formula** and lately, in 1839, **Dirichlet** the same proved it and used it to finish the proof of the existence of infinitely many primes in a given arithmetic progression.

1.1 Forms and discriminants

Definition 1.1. *Given a,b, $c \in \mathbb{Z}$ then $F(x, y) = ax^2 + bxy + cy^2$ is said a binary quadratic form. We will denote it as $F = \{a, b, c\}$.*

The **discriminant** of the form $ax^2+bxy+cy^2$ is the number $d=b^2-4ac$ where d is not a perfect square, since in this case the form has rational linear factors. We always have $d \equiv 0$ or $1(\mathrm{mod} 4)$.
Given d is always possible to find at least one form with such discriminant:

$$F=\begin{cases} \{1,0,-\frac{d}{4}\} & \text{if } d \equiv 0(\mathrm{mod}4) \\ \{1,1,-\frac{d-1}{4}\} & \text{if } d \equiv 1(\mathrm{mod}4) \end{cases}.$$

This form is called the **principal form**.
Moreover we always have $4aF=(2ax+by)^2-dy^2$.

If we have $F(x,y)=k$ for a form F and an integer k, we say that F represents k. Now we will ask with the following question: can we establish the sign of the integers represented by a form F with discriminant d?
We have the following theorem:

Theorem 1.1. *If $d>0$, for suitable (x,y), F represents both positive and negative numbers (indefinite form); if $d<0$ and $a>0$, F represents no negative numbers and $0 \iff x=y=0$ (positive definite form); if $d<0$ and $a<0$, F represents no positive numbers and $0 \iff x=y=0$ (negative definite form).*

Remark 1.1. *That theorem has the following geometric interpretation : if $d>0$ and $k>0$ or $k<0$, $F=k$ is an hyperbola; if $d>0$, $F=0$ represents a pair of straight lines, precisely the pair of asymptotes belonging to all hyperbolas $F=k$ for $k \neq 0$; if $d<0$, $F=k$ is an ellipse when $ka>0$, a so-called imaginary pair of lines when $k=0$, an imaginary ellipse when $ka<0$.*

Proof. 1) Let F be a form with $d>0$. We have $F(1,0)=a$, $F(b,-2a)=ab^2-2b^2a+c4a^2=a(4ac-b^2)=-da$ and of these two numbers, one is positive and the other is negative;
2) if $d<0$, since $4aF=(2ax+by)^2-dy^2$, we have $aF>0$ except when

$x = y = 0$. So F has the same sign as a because, if $aF \leq 0$, we have that $2ax + by = 0$, $y = 0$ and finally $x = 0$.

□

1.2 Equivalence of forms and Class Number

In the set of all quadratic forms we can define a relation as follows:

Definition 1.2. *A form $F = \{a, b, c\}$ is said to be equivalent to $G = \{a_1, b_1, c_1\}$, $F \sim G$, if there are r, s, t and $u \in \mathbb{Z}$, for which $ru - st = 1$, such that*

$$x = rX + sY, \quad y = tX + uY$$

and $F(X, Y) = G(x, y)$.
We say that F goes into G under the transformation

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}.$$

Remark 1.2. *We remark that if F has discriminant d, then G also has this discriminant and equivalent forms represents the same numbers. Moreover we can obtain the following relations:*

$$a_1 = ar^2 + brt + ct^2;$$

$$b_1 = 2ars + b(ru + st) + 2ctu;$$

$$c_1 = as^2 + bsu + cu^2.$$

The previous defined relation is an equivalence one, that means it is reflexive, symmetric and transitive; so it is possible to split the set of all quadratic forms into equivalence classes. Now, given a discriminant d, we will ask about the number of equivalence classes of forms with such discriminant; this number is said **Class Number**.

1.3 Finiteness of the Class Number

A first result concerns the finiteness of the Class Number. It derives from the following theorem proved by Lagrange. More details can be found in the book of E. Landau [28].

Theorem 1.2. *Every class contains a form $F = \{a, b, c\}$ for which $|b| \leq |a| \leq |c|$. This form is called* **reduced form**.

Proof. Let $\{a_0, b_0, c_0\}$ be a form belonging to a fixed class and let a be the smallest number in absolute value, $a \neq 0$, which is representable by such form. So we have, for suitable r and t, $a = a_0r^2 + b_0rt + c_0t^2$ where $(r, t) = 1$, otherwise $\frac{a}{(r,t)^2}$ would already be representable by the form $\{a_0, b_0, c_0\}$ but it would be smaller in absolute value than a.
Then, since the previous remark, we can find two numbers s and u such that $ru - st = 1$ and the transformation $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ takes $\{a_0, b_0, c_0\}$ into $\left\{a, b^{'}, c^{'}\right\}$.
The transformation $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ (where h is arbitrary) takes $\left\{a, b^{'}, c^{'}\right\}$ into $\{a, b, c\}$ where $b = 2ah + b^{'}$ and, for suitable h , it follows that $|b| \leq |a|$.
Finally, since $c \neq 0$ and since it can be represented by $\{a, b, c\}$ (with $x = 0$ and $y = 1$), we have, from previous remark and the minimality of $|a|$, $|a| \leq |c|$. □

From Theorem 1.2, we deduce:

Theorem 1.3. *For every fixed d, the Class Number is finite.*

Proof. 1)If $d > 0$, from the previous theorem, we have that in every class we can select a form, $\{a, b, c\}$, such that $|ac| \geq b^2 = d + 4ac > 4ac$; then $ac < 0$ and $4a^2 \leq 4|ac| = -4ac = d - b^2 \leq d \Rightarrow |a| \leq \sqrt{d}/2 \Rightarrow |b| \leq |a| \leq \sqrt{d}/2$.
It follows that the possible values of a and b are finite and therefore so those of $c = \frac{b^2-d}{4a}$.

2)if $d < 0$, since $a > 0$ and $c > 0$, we have $|b| \leq a \leq c$; then $4a^2 \leq 4ac = -d + b^2 \leq |d| + a^2 \Rightarrow |b| \leq a \leq \sqrt{|d|/3}$.
Even in this case the possible values of c are finite . □

1.4 Primitive forms and proper representations

Now let us give some definitions about some particular quadratic forms and representations:

Definition 1.3. *A form $F = \{a, b, c\}$ is called* **primitive** *if the Greatest Common Divisor $(a, b, c) = 1$; otherwise it is called imprimitive.*

We can state the following theorem about imprimitive forms without proof [27]:

Theorem 1.4. *If F is imprimitive, so that $(a, b, c) = g > 1$, then g^2 divides d and $\left\{\frac{a}{g}, \frac{b}{g}, \frac{c}{g}\right\}$ is a primitive form of discriminant $\frac{d}{g^2}$ and conversely.*

So we realize that we can obtain all the classes with discriminant d from all the primitives one with a discriminant of the form $\frac{d}{g^2}$, where $g > 0$ and g^2 divides d, multiplying every class by g.

Definition 1.4. *Let $k \neq 0$. $F(x, y) = k$ is said to be a* **proper representation** *of k by F if $(x, y) = 1$. If $(x, y) > 1$, F is said to be an improper representation.*

An important result on proprer representations is that we can choose some positive number represented properly by the form and any such number occurs as the first coefficients of equivalent forms. So we have the following theorem:

Theorem 1.5. *Let $k > 0$ and let $F(x, y) = k$ be a proper representation. We can choose in exactly one way r, s and l such that $xs - ry = 1$, with $l^2 \equiv d(\mathrm{mod} 4k)$ and $0 \leq l < 2k$; moreover F goes into $\{k, l, m\}$ by the transformation $\begin{pmatrix} x & r \\ y & s \end{pmatrix}$ where m is obtained by $l^2 - 4km = d$.*

Remark 1.3. *It is important to notice the fact that a fixed number l, belonging to $[0, 2k)$, is associated to every proper representation .*

Proof. A solution of $xs - ry = 1$ is of the form $r = r_0 + hx$, $s = s_0 + hy$.
If $F = \{a, b, c\}$ and, $\{k, l, m\}$ represents the new form, it follows, from Remark 1.2, that $l = 2axr + b(xs + yr) + 2cys = l_0 + 2hk$; hence, for suitable h, we have $0 \leq l < 2k$.
From $l^2 - 4km = d$ comes out $l^2 \equiv d(\mathrm{mod} 4k)$.

□

Now we determine the number and the nature of the transformations which take a form $F = \{a, b, c\}$ into itself:

Theorem 1.6. *All transformations of $F = \{a, b, c\}$ into itself are given by $\begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix}$ where (t, u) is a solution of* **Pell's equation**[1]

$$t^2 - du^2 = 4 \tag{1.1}$$

[1] If (x_0, y_0) is that solution for which y_0 has the smallest positive value and $x_0 > 0$, if $\epsilon = \frac{x_0+y_0\sqrt{d}}{2}$, then the general solution (x, y) is given by the formulas $\pm\epsilon^n = \frac{x+y\sqrt{d}}{2}$ where $n \in \mathbb{Z}$.

Remark 1.4. *The trivial transformations*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

are given by the trivial solutions of equation (1.1): $(\pm 2, 0)$.

Proof. 1) In order to prove that every transformation defined in the theorem takes F into itself, it suffices to show that it leaves the first two coefficients of F unaltered. We have, in fact,

$$\begin{aligned} a_1 &= a\left(\frac{t-bu}{2}\right)^2 + b\left(\frac{t-bu}{2}\right)au + ca^2u^2 \\ &= a\frac{t^2}{4} - ab\frac{tu}{2} + ab^2\frac{u^2}{4} + ab\frac{tu}{2} - ab^2\frac{u^2}{2} + a^2cu^2 \\ &= \frac{a}{4}\left(t^2 - (b^2-4ac)u^2\right) = a, \end{aligned} \tag{1.2}$$

$$\begin{aligned} b_1 &= -2a\frac{t-bu}{2}cu + b\left(1-2acu^2\right) + 2cau\frac{t+bu}{2} \\ &= -actu + abcu^2 + b - 2abcu^2 + actu + abcu^2 = b. \end{aligned} \tag{1.3}$$

2)In order to show that every transformation $\begin{pmatrix} r & s \\ m & n \end{pmatrix}$ such that $rn - sm = 1$ and which takes F into itself is of the form of Theorem 1.6, we remark at first that

$$a = ar^2 + brm + cm^2 \tag{1.4}$$

$$b = 2ars + b(1+2sm) + 2cmn \tag{1.5}$$

and, from (1.5), it follows that

$$0 = ars + bsm + cmn. \tag{1.6}$$

By multiplying (1.4) by s and by replacing (1.6) into it, we have

$$as = cm(sm - rn) = -cm \tag{1.7}$$

and , by multiplying (1.4) by n, we have

$$a(n - r) = bm. \tag{1.8}$$

From these equations it follows that: a divides cm and a divides bm; but $(a, b, c) = 1$, then we have also a divides m. It means that exists u such that $m = au$.
From (1.7) and (1.8), we obtain $s = -cu$ and $n - r = bu$; so we can write:

$$\begin{aligned} (n + r)^2 = (n - r)^2 + 4nr = b^2u^2 + 4(1 + sm) \\ = b^2u^2 + 4(1 - acu^2) = du^2 + 4. \end{aligned} \tag{1.9}$$

If we choose $n + r = t$, it follows that

$$t^2 - du^2 = 4$$

and

$$r = \frac{t - bu}{2} \ , \ n = \frac{t + bu}{2}.$$

□

Let us introduce another fundamental concept, the one of **primary representation**:

Definition 1.5. *A representation of $k > 0$ by a form $F = \{a, b, c\}$ where $a > 0$ is said primary if one of the two following conditions is verified :*

1. $d < 0$;
2. $d > 0$, *provided that* $2ax + (b - \sqrt{d})y > 0$, *and* $1 \leq \frac{2ax+(b+\sqrt{d})y}{2ax+(b-\sqrt{d})y} < \epsilon^2$

($\epsilon = \frac{t_0+u_0\sqrt{d}}{2}$; $\epsilon > 1$ where (t_0, u_0) is the smallest positive solution of Pell's equation, as defined in the footnote 1).

Remark 1.5.

1. *If we set $2ax + (b+\sqrt{d})y = L$ and $2ax + (b-\sqrt{d})y = \overline{L}$, in the point 2 of the definition 1.5, then we can write $\overline{L} > 0, 1 \leq \frac{L}{\overline{L}} < \epsilon^2$ and we have $L \geq \overline{L} > 0$.*

2. *if a representation of k by a form $\{a, b, c\}$ is primary and improper , and if $(x, y) = g$, it follows that $\frac{k}{g^2}$ has a proper primary representation by $\{a, b, c\}$ where $\frac{x}{g}$ and $\frac{y}{g}$ are used in place of x and y, and conversely.*

Given a number k, how many are its primary representations?
The following theorem will have as a consequence that the number of the primary representations of k is anyway finite.

Theorem 1.7. *If $k > 0$ has a proper representation by a form $F = \{a, b, c\}$ where $a > 0$, then for every l such that $l^2 \equiv d(\bmod 4k)$, where $0 \leq l < 2k$, as defined in Theorem 1.5, there exist exactly w primary proper representations of k where*

$$w = \begin{cases} 1 & se\ d > 0 \\ 2 & se\ d < -4 \\ 4 & se\ d = -4 \\ 6 & se\ d = -3 \end{cases}$$

Proof. : Since $l^2 \equiv d(\text{mod}4k)$, we have that there is exactly one value m such that $l^2 - 4km = d$ and, from Theorem 1.5, there exists at least one transformation $\begin{pmatrix} x_0 & r_0 \\ y_0 & s_0 \end{pmatrix}$ that takes the form $F = \{a, b, c\}$ into $G = \{k, l, m\}$.

We are interested in all the transformations $\begin{pmatrix} x & r \\ y & s \end{pmatrix}$ and we wish to prove that the first column of this matrix is formed by w pairs of values x and y, in every case if $d < 0$ and, provided the conditions of Defintion 1.5 , if $d > 0$.
Let $\begin{pmatrix} x_1 & r_1 \\ y_1 & s_1 \end{pmatrix}$ be a general transformation that fixes F, we can prove that

$$\begin{pmatrix} x & r \\ y & s \end{pmatrix} = \begin{pmatrix} x_1x_0 + r_1y_0 & x_1r_0 + r_1s_0 \\ y_1x_0 + s_1y_0 & y_1r_0 + s_1s_0 \end{pmatrix}. \tag{1.10}$$

The matrix on the right side takes F into G because of the transitivity of the previous defined relation in the set of quadratic forms; in fact, if we take F into G by means of this matrix, or, if we first transform F by means of $\begin{pmatrix} x_1 & r_1 \\ y_1 & s_1 \end{pmatrix}$ and then the new form by means of $\begin{pmatrix} x_0 & r_0 \\ y_0 & s_0 \end{pmatrix}$, we obtain the same result. Moreover, thanks to the symmetric property, if F goes into G by means of $\begin{pmatrix} x_0 & r_0 \\ y_0 & s_0 \end{pmatrix}$, G goes into F by means of $\begin{pmatrix} s_0 & -r_0 \\ -y_0 & x_0 \end{pmatrix}$.
According to the result above, the transformation $\begin{pmatrix} xs_0 - ry_0 & -xr_0 + rx_0 \\ ys_0 - sy_0 & -yr_0 + sx_0 \end{pmatrix}$ takes F into F.
We can set this transformation equal to $\begin{pmatrix} x_1 & r_1 \\ y_1 & s_1 \end{pmatrix}$ i.e., comparing the elements of the matrices, we obtain

$$x = x_1x_0 + r_1y_0,\ r = x_1r_0 + r_1s_0,$$

$$y = y_1x_0 + s_1y_0,\ s = y_1r_0 + s_1s_0$$

and so the prove of (1.10). From Theorem 1.6, we have that all the transformations which take F into itself are represented by matrices of the form

$$\begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix}$$

where (t, u) solutions of (1.1), so x and y are given by

$$\begin{cases} x = \frac{t-bu}{2}x_0 - cuy_0 \\ \\ y = aux_0 + \frac{t+bu}{2}y_0 \end{cases}$$

where distinct pairs (t, u) correspond to distinct pairs (x, y).
The determinant of the coefficients of t and u is

$$\frac{1}{4}\begin{vmatrix} x_0 & -(bx_0 + 2cy_0) \\ y_0 & 2ax_0 + by_0 \end{vmatrix} = \frac{1}{4}(2ax_0^2 + 2bx_0y_0 + 2cy_0^2) = \frac{k}{2} \neq 0.$$

So, for $d < 0$, since the equation (1.1) has w solutions, the theorem has been proved.
For $d > 0$ we have to show that for every fixed pair (t, u), that is for one sign and one exponent in the formula

$$\frac{t + u\sqrt{d}}{2} = \pm\epsilon^n,$$

we have

$$\overline{L} > 0,\ 1 \leq \frac{L}{\overline{L}} < \epsilon^2, \tag{1.11}$$

where x and y defined above.
From the expressions found for x and y, it follows that :
$4ax+2(b+\sqrt{d})y = 2a(t-bu)x_0 - 4acuy_0 + 2abux_0 + (t+bu)by_0 + \sqrt{d}(2aux_0 + (t + bu)y_0) = t(2ax_0 + by_0) + duy_0 + \sqrt{d}(2aux_0 + buy_0 + ty_0) = (2ax_0 + (b + \sqrt{d})y_0)(t + u\sqrt{d})$;
and so

$$2ax + \left(b + \sqrt{d}\right) y = \left(2ax_0 + (b + \sqrt{d})y_0\right) \frac{t + u\sqrt{d}}{2}.$$

If we set

$$L_0 = 2ax_0 + (b + \sqrt{d})y_0,$$

we obtain

$$L = \pm L_0\epsilon^n.$$

Since $L > 0$, it results

$$L = |L_0|\epsilon^n$$

and so it needs to show that exists exactly one value of n in this equation such that (1.11) holds.
By the definition of discriminant, it follows that

$$4ak = (2ax + (b + \sqrt{d})y)(2ax + (b - \sqrt{d})y) = L\overline{L};$$

and, since $L > 0$, it has to be $\overline{L} = (4ak)/L > 0$.
Moreover

$$\frac{L}{\overline{L}} = \frac{L^2}{4ak} = \frac{|L_0|^2\epsilon^{2n}}{4ak}$$

and so precisely we have

$$1 \leq \frac{|L_0|^2\epsilon^{2n}}{4ak} < \epsilon^2.$$

This is equivalent to

$$\frac{2\sqrt{ak}}{|L_0|} \leq \epsilon^n < \frac{2\sqrt{ak}\epsilon}{|L_0|}$$

and so we have these inequalities for exactly one value of n. □

Remark 1.6. *The finiteness of the number of the primary representations of k comes out the possibility to have just a finite number of l.*

1.5 Representative system of forms and Class Number Formula

The following theorems allow us to proof the Class Number formula. They will be stated for **representative system** of the classes of forms. So let us give the following defintion:

Definition 1.6. *A representive system of the classes of forms with discriminant d (where, if $d < 0$, we take $a > 0$) is a set of representatives, one for each class, having $a > 0$.*

Theorem 1.8. *If $k > 0$ and $(k, d) = 1$, the number $\Psi(k)$ of primary representations of k by all the forms belonging to a representative system is finite and it has this value :*

$$\Psi(k) = w \sum_{n|k} \left(\frac{d}{n} \right) \tag{1.12}$$

Proof. Let us at first consider the case of the proper primary representations. From a theorem of Number Theory [2] follows that the congruence $l^2 \equiv d(\mathrm{mod} 4k)$, with $0 \leq l < 2k$, has exactly $\sum_{f|k}(\frac{f}{n})$ solutions where f is a square-free divisor of k and $(\frac{f}{n})$ is the Jacobi symbol ; for every l we obtain, from Theorem 1.5, a form $\{k, l, m\}$ equivalent to exactly one form of the representative system and, by means of this form, we obtain exactly w proper primary representations of k belonging to l. It follows that the number of proper primary representations of k by forms belonging to the representative system is :

$$\Psi(k) = w \sum_{f|k} \left(\frac{d}{f} \right)$$

By the second point of Remark 1.5, it follows that, if $(d, k) = g$, the number of primary representations of k by forms belonging to the representative system is :

$$\Psi(k) = w \sum_{\substack{g^2|k \\ g>0}} \sum_{f|\frac{k}{g^2}} \left(\frac{d}{f} \right) .$$

[2] Let $k > 0$ and let $(d, k) = 1$. The number of solutions of the congruence $x^2 \equiv d(\mathrm{mod} 4k)$ is $2\sum_{f|k}(\frac{d}{f})$ where f is a square-free positive divisor of k . Remarking that, whenever x_0 satisfies the congruence, so does $x_0 + 2k$, in the interval $[0, 2k)$ there are $\sum_{f|k}(\frac{d}{f})$ solutions.

Since $(d, g^2) = 1$, by another theorem of Number Theory [3], follows that

$$\Psi(k) = w \sum_{\substack{g^2|k \\ g>0}} \sum_{f|\frac{k}{g^2}} \left(\frac{d}{fg^2}\right) = w \sum_{n|k} \left(\frac{d}{n}\right)$$

because every $n > 0$ can be uniquely written in the form fg^2 where f is square-free and $g > 0$; it follows that, if n divides k, then g^2 divides k and f divides $\frac{k}{g^2}$ and conversely. □

Now we are going to consider the mean value of $\Psi(k)$, as k varies, to obtain finally a relation with the L-function $L(1, \chi)$, where χ is a primitive real character. Therefore we have the following theorem:

Theorem 1.9. *If, for $\tau > 1$, we set*

$$H(\tau) = \sum_{\substack{1 \leq k \leq \tau \\ (k,d)=1}} \Psi(k),$$

then

$$\lim_{\tau \to \infty} \frac{H(\tau)}{\tau}$$

exists, and we have

$$\lim_{\tau \to \infty} \frac{H(\tau)}{\tau} = w \frac{\varphi(|d|)}{|d|} \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \left(\frac{1}{n}\right).$$

Remark 1.7. *$H(\tau)$ represents the number of primary representations, by forms belonging to the representative system, of all of the natural numbers up to τ that are relatively prime to d.*

[3] If $m_1 > 0$ e $m_2 > 0$, then $\left(\frac{d}{m_1 m2}\right) = \left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right)$

Proof. Since $(\frac{d}{n})$ is a nonprincipal primitive real character $\bmod|d|$,

$$\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\left(\frac{1}{n}\right)$$

converges.

From Theorem 1.8, since, if n divides k and $n > 0$, we can write

$$\left(\frac{d}{n}\right)\left(\frac{d}{\frac{k}{n}}\right)^2 = \begin{cases} (\frac{d}{n}) & (k,d)=1 \\ 0 & (k,d)>1 \end{cases},$$

it follows that

$$\frac{H(\tau)}{w} = \sum_{\substack{1\le k\le\tau \\ (k,d)=1}}\sum_{n|k}\left(\frac{d}{n}\right) = \sum_{1\le k\le\tau}\sum_{n|k}\left(\frac{d}{n}\right)\left(\frac{d}{\frac{k}{n}}\right)^2.$$

Taking $n \geq 1$ and $m \geq 1$, therefore we have

$$\frac{H(\tau)}{w} = \sum_{nm\le\tau}\left(\frac{d}{n}\right)\left(\frac{d}{m}\right)^2.$$

Now, in order to separate the sum, we also remark that if $nm \leq \tau$, then either $n \leq \sqrt{\tau}$, and so we have $m \leq \frac{\tau}{n}$; or else $n > \sqrt{\tau}$, so that we have $m \leq \sqrt{\tau}$ and $\sqrt{\tau} < n \leq \frac{\tau}{m}$.

We obtain:

$$\frac{H(\tau)}{w} = \sum_{n\le\sqrt{\tau}}\left(\frac{d}{n}\right)\sum_{m\le\frac{\tau}{n}}\left(\frac{d}{m}\right)^2 + \sum_{m\le\sqrt{\tau}}\left(\frac{d}{m}\right)^2\sum_{\sqrt{\tau}<n\le\frac{\tau}{m}}\left(\frac{d}{n}\right). \qquad (1.13)$$

Taking $\xi = \frac{\tau}{n}$,

$$\sum_{m\le\xi}\left(\frac{d}{m}\right)^2$$

represents the number of positive integers up to ξ that are relatively prime to d and results[4] :

$$\left|\sum_{m\leq\xi}\left(\frac{d}{m}\right)^2-\frac{\varphi(|d|)}{|d|}\xi\right|<\varphi(|d|)\leq|d|. \tag{1.14}$$

Moreover, since $\left(\frac{d}{n}\right)$ is a non-principal character mod$(|d|)$, from the ortogonality laws of the characters, it follows that

$$\left|\sum_{\sqrt{\tau}<n\leq\frac{\tau}{m}}\left(\frac{d}{n}\right)\right|\leq\frac{\varphi(|d|)}{2}<|d|. \tag{1.15}$$

We remark also that, once more from the properties of the characters,

$$\sum_{m\leq\sqrt{\tau}}\left(\frac{d}{m}\right)^2\sum_{\sqrt{\tau}<n\leq\frac{\tau}{m}}\left(\frac{d}{n}\right)=O(\sqrt{\tau}).$$

From this remark and by the previous equations , it follows that:

$$\frac{H(\tau)}{w}=\tau\frac{\varphi(|d|)}{|d|}\sum_{n\leq\sqrt{\tau}}\left(\frac{d}{n}\right)\frac{1}{n}+O(\sqrt{\tau})$$

and, as $\tau\rightarrow\infty$, we obtain

$$\lim_{\tau\rightarrow\infty}\frac{H(\tau)}{\tau}=w\frac{\varphi(|d|)}{|d|}\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{d}{n}\right).$$

But $\sum_{n=1}^{\infty}\frac{1}{n}(\frac{d}{n})=L(1,\chi)$, and so:

$$\lim_{\tau\rightarrow\infty}\frac{H(\tau)}{\tau}=w\frac{\varphi(|d|)}{|d|}L(1,\chi).$$

□

Now, let $\tau>1$, we consider :

$$H(\tau,F)=\sum_{\substack{1\leq k\leq\tau\\(k,d)=1}}\Psi(k,F) \tag{1.16}$$

[4] Let $d>0$ and $\xi>0$. Then the number of positive numbers $n\leq\xi$ which belong to any given residue class *mod* d differs from $\frac{\xi}{d}$ by less then 1.

where $\Psi(k, F)$ is the number of primary representations of k by a form F of the representative system. We are going to calculate :

$$\lim_{\tau \to \infty} \frac{H(\tau, F)}{\tau}.$$

In order to do it, we state and proof two theorems.

Theorem 1.10. *If x and y belong to a complete set of residues* $\mod |d|$, *then exactly $|d|\varphi(|d|)$ of the d^2 numbers $F(x, y)$, which result, are relatively prime to d.*

Proof. : at first we consider a prime p such that $p^l|d$ with $l > 0$. In this case it suffices to show that if x and y belong to a complete set of residues mod p^l, then p does not divide $F(x, y)$ exactly $p^l\varphi(p^l)$ times.

Then we consider $|d| = \prod_{p||d|} p^l$ and, since $(F, d) = 1$ is equivalent to $p \not| F$, for all p which divides $|d|$, there are exaclty

$$\prod_{p||d|} p^l\varphi(p^l) = |d|\varphi(|d|)$$

pairs of classes $x \equiv x_0(\text{mod}|d|), y \equiv y_0(\text{mod}|d|)$.

We remark that, since $(a, b, c) = 1$ and $b^2 - 4ac = d$, if $p|d$ we cannot have both $p|a$ and $p|c$. Let, for example, $p \not| a$. We distinguish two cases:

1. let $p > 2$; we have $(p, 4a) = 1$ and, since $p|d$ and $4aF = (2ax+by)^2 - dy^2$, it must be $2ax + by \not\equiv 0(\text{mod}p)$ to have $p \not| F$.

   Since $p \not| 2a$ and, for each of our p^l possibile values for y, all of the x belonging to a certain set of $p-1$ residue classes $(\mod p)$ have the previous property, we have exactly $p^{l-1}(p-1) = \varphi(p^l)$ possible values for x.

2. Let $p = 2$, so that $2|d$ and $2|b$. The condition $p \not| F$ is equivalent to :

$$ax^2 + bxy + cy^2 \equiv 1(\text{mod}2)$$

and this implies:

$$x + cy \equiv 1(\mathrm{mod} 2).$$

For each of our 2^l possible values for y, all of the x belonging to one residue class mod 2 have this property and they have exactly $2^{l-1} = \varphi(2^l)$ possibile values.

□

Theorem 1.11. *Let $m > 0$. We consider an ellipse or a sector of an hyperbola (the curvilinear triangle bounded by an arc of the hyperbola and two rays drawn from its endpoints to the center of the hiperbola); let I denote its area. Instead to consider the original set of points (ξ, η) , we consider that of points $(\xi\sqrt{\tau}, \eta\sqrt{\tau})$.*
Let $U(\tau)$ be the number of points with integral coordinates within the extended figure (which each boundary point counted or not) which satisfy the additional conditions:

$$x \equiv x_0(\mathrm{mod} m), y \equiv y_0(\mathrm{mod} m).$$

Then we have

$$\lim_{\tau\to\infty} \frac{U(\tau)}{\tau} = \frac{I}{m^2}$$

Proof. : in the plane of the original figure, let us lay out two mutually perpendicular systems of parallel lines, spaced $\frac{m}{\sqrt{\tau}}$ units apart, around the point $\xi = \frac{x_0}{\sqrt{\tau}}, \eta = \frac{y_0}{\sqrt{\tau}}$; the equations of these straight lines are:

$$\xi = \frac{x_0 + rm}{\sqrt{\tau}}, \quad \eta = \frac{y_0 + sm}{\sqrt{\tau}}.$$

Let $W(\tau)$ be the number of squares in this net which are contained in the ellipse or in the sector of the hyperbola. We have :

$$U(\tau) = W(\tau).$$

Since $\frac{m^2}{\tau}$ is the area of each square of the net , it follows :

$$I = \int \int d\xi d\eta = \lim_{\tau \to \infty} \left(\frac{m^2}{\tau} W(\tau) \right)$$

and this proves the theorem. □

Now we can state and prove the following result:

Theorem 1.12. *Given $H(\tau, F)$ defined in (1.16), then*

$$\lim_{\tau \to \infty} \frac{H(\tau, F)}{\tau} = \begin{cases} \frac{2\pi}{\sqrt{|d|}} \frac{\varphi(|d|)}{|d|} & \textit{if } d < 0 \\ \frac{\log \epsilon}{\sqrt{d}} \frac{\varphi(d)}{d} & \textit{if } d > 0 \end{cases}$$

where $\epsilon = \frac{t_0 + u_0\sqrt{d}}{2}$, as in Definition 1.5.

Proof. Let us consider two cases.

1. Let $d < 0$. Since in this case all the representations are primary, $H(\tau, F)$ is given by the number of (x, y) such that

   $$0 < ax^2 + bxy + cy^2 \leq \tau, \ (ax^2 + bxy + cy^2, d) = 1.$$

   From Theorem 1.10, the second condition is satisfied by $\varphi(|d|)|d|$ pairs (x, y) of residues mod$|d|$; from the first condition the points (x, y) belong to an ellipse with center in the origin which expands as $\tau \to \infty$. The area of such ellipse is $\frac{2\pi}{|d|^{\frac{1}{2}}}\tau$ and, from Theorem 1.11, when $\tau \to \infty$, the number of points with integral coordinates, within it, is asymptotic to

   $$\frac{1}{|d|^2} \frac{2\pi}{|d|^{\frac{1}{2}}} \tau.$$

   So, in this case, we obtain :

   $$\lim_{\tau \to \infty} \frac{H(\tau, F)}{\tau} = \frac{2\pi}{\sqrt{|d|}} \frac{\varphi(|d|)}{|d|}.$$

2. Let $d > 0$; we take

$$\Lambda = 2ax + (b + \sqrt{d})y,\ \overline{\Lambda} = 2ax + (b - \sqrt{d})y.$$

The pairs (x, y) satisfy the following conditions:

$$0 < ax^2 + bxy + cy^2 \leq \tau, (ax^2 + bxy + cy^2, d) = 1$$
$$\overline{\Lambda} > 0, 1 \leq \frac{\Lambda}{\overline{\Lambda}} < \epsilon^2.$$

So in this case, the points (x, y) with integral coordinates belong to the sector of the hyperbola

$$ax^2 + bxy + cy^2 \leq 1,\ \overline{\Lambda} > 0,\ 1 \leq \frac{\Lambda}{\overline{\Lambda}} < \epsilon^2 \tag{1.17}$$

of which we are going to compute the area.

The area is given by

$$I = \int \int dxdy$$

over the region

$$\Lambda\overline{\Lambda} \leq 4a, \overline{\Lambda} > 0,\ 1 \leq \frac{\Lambda}{\overline{\Lambda}} < \epsilon^2.$$

Let

$$\rho = \frac{\Lambda}{2\sqrt{a}},\ \sigma = \frac{\overline{\Lambda}}{2\sqrt{a}}$$

be chosen as new variables; we have

$$\begin{vmatrix} \frac{\partial\rho}{\partial\xi} & \frac{\partial\rho}{\partial\eta} \\ \frac{\partial\sigma}{\partial\xi} & \frac{\partial\sigma}{\partial\eta} \end{vmatrix} = \frac{1}{2\sqrt{a}} \frac{1}{2\sqrt{a}} \begin{vmatrix} 2a & b + \sqrt{d} \\ 2a & b - \sqrt{d} \end{vmatrix} = -\sqrt{d}.$$

So the integral becomes:

$$I = \frac{1}{\sqrt{d}} \int \int d\rho d\sigma,$$

over the region

$$\rho\sigma \leq 1,\ \sigma \geq 0,\ \sigma \leq \rho \leq \epsilon^2\sigma,$$

that is the sector of the hyperbola having the vertices $(0,0); (\epsilon, \frac{1}{\epsilon}); (1,1)$. It follows

$$\begin{aligned}\sqrt{d}I &= \int_0^\epsilon d\rho \int_{\frac{\rho}{\epsilon^2}}^{Min(\rho,\frac{1}{\rho})} d\sigma = \int_0^1 d\rho \int_{\frac{\rho}{\epsilon^2}}^{\rho} d\sigma + \int_1^\epsilon d\rho \int_{\frac{\rho}{\epsilon^2}}^{\frac{1}{\rho}} d\sigma \\ &= \int_0^1 (\rho - \frac{\rho}{\epsilon^2}) d\rho + \int_1^\epsilon (\frac{1}{\rho} - \frac{\rho}{\epsilon^2}) d\rho = \int_0^1 \rho d\rho + \int_1^\epsilon \frac{d\rho}{\rho} \\ &- \int_0^\epsilon \frac{\rho}{\epsilon^2} d\rho = \log \epsilon.\end{aligned} \tag{1.18}$$

□

The previous result allows us to state the following theorem that gives a clear expression of the class-number and so it represents the fundamental result of this chapter:

Theorem 1.13.

$$h(d) = \begin{cases} \frac{w\sqrt{|d|}}{2\pi} L(1,\chi) & \textit{if } d < 0 \\ \frac{\sqrt{d}}{\log \epsilon} L(1,\chi) & \textit{if } d > 0 \end{cases}$$

Remark 1.8. *If we denote as F_n the forms belonging to a representative system, we have*

$$\sum_{n=1}^{h} H(\tau, F_n) = H(\tau)$$

and, from Theorem 1.9,

$$h(d) \lim_{\tau\to\infty} \frac{H(\tau, F)}{\tau} = w \frac{\varphi(|d|)}{|d|} L(1,\chi).$$

Proof. 1. if $d < 0$, from Theorem 1.12, we have

$$\lim_{\tau\to\infty} \frac{H(\tau, F)}{\tau} = \frac{2\pi}{\sqrt{|d|}} \frac{\varphi(|d|)}{|d|}.$$

So

$$h(d) \frac{2\pi}{\sqrt{|d|}} \frac{\varphi(|d|)}{|d|} = w \frac{\varphi(|d|)}{|d|} L(1,\chi)$$

and

$$h(d) = \frac{L(1,\chi)w\sqrt{|d|}}{2\pi}$$

2. if $d > 0$, we obtain

$$\lim_{\tau\to\infty} \frac{H(\tau, F)}{\tau} = \frac{\log\epsilon}{\sqrt{d}} \frac{\varphi(d)}{d}.$$

So

$$h(d)\frac{\log\epsilon}{\sqrt{d}} \frac{\varphi(d)}{d} = w\frac{\varphi(|d|)}{|d|}L(1,\chi)$$

and, since in this case $w = 1$, we have

$$h(d) = \frac{\sqrt{d}}{\log\epsilon}L(1,\chi).$$

□

We have just obtained the famous **Class Number formula** found by Dirichlet. From it we can deduce that the L-function $L(1,\chi)$ is strictly positive and so different from zero. That allows Dirichlet himself to complete the proof of the theorem of the existence of infinitely many primes in a given arithmetic progression.

1.6 L-functions as a finite sum

Making use of the results proved until now, we will express $L(1,\chi)$ as a finite sum. It needs to use an expression like a Gauss'sum

$$\sum_{m=1}^{|d|} \left(\frac{d}{m}\right) eq(mn) = \left(\frac{d}{n}\right) \epsilon|d|^{\frac{1}{2}}$$

where $eq(x) = e^{2\pi ix/q}$ and

$$\epsilon = \begin{cases} 1 & \text{if } d < 0 \\ i & \text{if } d > 0 \end{cases}$$

and the following result from the classical theory of Fourier series:

if $0 < \varphi < 2\pi$

$$\sum_{n=1}^{\infty} \frac{\sin(n\varphi)}{n} = \frac{\pi}{2} - \frac{\varphi}{2}$$

and

$$\sum_{n=1}^{\infty} \frac{\cos(n\varphi)}{n} = -\lg\left(2\sin\frac{\varphi}{2}\right).$$

Moreover we have to give the definition of **fundamental discriminant**.

Definition 1.7. *A discriminant D is called fundamental discriminant if $D \neq 0, 1$ and*

$$D = \begin{cases} m & \textit{if } m \equiv 1(\mathrm{mod} 4) \\ 4m & \textit{if } m \equiv 2, 3(\mathrm{mod} 4) \end{cases}$$

for some squarefree integer m.

Every discriminant d can be uniquely written as De^2 with D fundamental discriminant and $e \geq 1$.

Remark 1.9. *We remark that a fundamental discriminant has the property that all the forms of that disciminants are primitive.*

So we can state the following theorem:

Theorem 1.14. *If d is a fundamental discriminant:*

$$L(1, \chi) = \begin{cases} -\frac{1}{\sqrt{d}} \sum_{r=1}^{d-1} \left(\frac{d}{r}\right) \log(\sin\frac{\pi r}{d}) & \textit{if } d > 0 \\ -\frac{\pi}{|d|^{\frac{3}{2}}} \sum_{r=1}^{|d|-1} \left(\frac{d}{r}\right) r & \textit{if } d < 0 \end{cases}$$

Proof. Using the above-mentioned Gauss'sum, we can write

$$\begin{aligned}\sqrt{d}L(1,\chi) &= \sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\sqrt{d}\frac{1}{n} \\ &= \sum_{n=1}^{\infty}\frac{1}{n}\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)e^{\frac{2\pi inr}{|d|}} \qquad (1.19) \\ &= \sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)\sum_{n=1}^{\infty}\frac{1}{n}e^{\frac{2\pi inr}{|d|}}.\end{aligned}$$

If $d > 0$ the left-hand side is real, hence we have

$$\begin{aligned}\sqrt{d}L(1,\chi) &= \sum_{r=1}^{d-1}\left(\frac{d}{r}\right)\sum_{n=1}^{\infty}\frac{\cos(\frac{n2\pi r}{d})}{n} \\ &= -\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)\lg\left(2\sin(\frac{\pi r}{d})\right) \qquad (1.20) \\ &= -\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)\lg\sin\left(\frac{\pi r}{d}\right);\end{aligned}$$

if $d < 0$ the left-hand side is pure imaginary and so:

$$\begin{aligned}\sqrt{d}L(1,\chi) &= \sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)\sum_{n=1}^{\infty}\frac{\sin\left(\frac{n2\pi r}{|d|}\right)}{n} \\ &= \sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)\left(\frac{\pi}{2}-\frac{\pi r}{|d|}\right) \qquad (1.21) \\ &= -\frac{\pi}{|d|}\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)r.\end{aligned}$$

□

1.7 A particular case

Let q a prime such that $d = -q$ with $q \equiv 3(\mod 4)$ and suppose $q \geq 3$. From the previous results , as $d < 0$, we have $w = 2$ and so

$$\begin{aligned} h(d) &= \frac{2|d|^{\frac{1}{2}}}{2\pi} L(1, \chi) \\ &= \frac{2|d|^{\frac{1}{2}}}{2\pi} \left(-\frac{\pi}{|d|^{\frac{3}{2}}} \sum_{n=1}^{|d|-1} \left(\frac{d}{n} \right) n \right) \\ &= -\frac{1}{|d|} \sum_{n=1}^{q-1} n \left(\frac{-q}{n} \right) \\ &= -\frac{1}{q} \sum_{n=1}^{q-1} n \left(\frac{n}{q} \right) \end{aligned} \tag{1.22}$$

We notice that the right-hand side, which we will denote by H, is integral because it follows, from Euler's rule, that

$$\sum_{n=1}^{q-1} n \left(\frac{n}{q} \right) \equiv \sum_{n=1}^{q-1} n^{\frac{q}{2}+\frac{1}{2}} \equiv 0(\mathrm{mod} q).$$

H enjoys some important properties that were proved by Jacobi. Particullarly $\forall p \equiv 1(\mod q)$ there is a representation of $p^{|H|}$ in the form $4p^{|H|} = x^2 + qy^2$.

From the theory of quadratic forms we can deduce that $h(-q)$ enjoys the same properties as H and from this specific remark, Jacobi, examining a particular number of cases, formulated the conjecture that $h(-q) = |H|$.

Chapter 2

Class Group and Class Number

In this chapter we are showing the existence of a connection between the theory of binary quadratic forms, which we studied in the previous chapter, and the theory of ideals in quadratic fields. In particular we deal with the problem of determine the **Class Number Formula** using the theory of ideals.

2.1 Algebraic Number Theory background

Let us first recall some fundamental facts about algebraic number theory, useful to define the **Class Number**.The complete theory can be found in the book of Ian Stewart and David Tall [35].

2.1.1 Quadratic fields

A **quadratic field** is a number field of degree 2 over $\mathbb{Q}$, that is to say a subfield K of $\mathbb{C}$ such that $[K : \mathbb{Q}] = 2$. More precisely quadratic fields are fields of the form $\mathbb{Q}(\sqrt{d})$, where d is a squarefree integer. Every element α $\in \mathbb{Q}(\sqrt{d})$ can be expressed in the form $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$.
The **ring of integers** $\mathcal{O}_d$ of $\mathbb{Q}(\sqrt{d})$, for squarefree d, is the set of $\alpha \in \mathbb{Q}(\sqrt{d})$ that are roots of a monic polynomial $z^2 + bz + c$ with $b, c \in \mathbb{Z}$.
In particular it can be proved that the ring of integers of $\mathbb{Q}(\sqrt{d})$ is:

$$\mathcal{O}_d = \begin{cases} \mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\} & \text{if } d \not\equiv 1(\text{mod}4) \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b(\frac{1+\sqrt{d}}{2}) : a, b \in \mathbb{Z}\right\} & \text{if } d \equiv 1(\text{mod}4) \end{cases}$$

If $K = \mathbb{Q}(\theta)$ is a number field of degree n, let $\{\alpha_1, \dots, \alpha_n\}$ be a basis of K as vector space of $\mathbb{Q}$, we define the **discriminant** of this basis to be $\Delta[\alpha_1, \dots, \alpha_n] = \det[\sigma_i(\alpha_j)]^2$, where σ_i are the distinct monomorphisms $\sigma_i : K \longrightarrow \mathbb{C}, (i = 1, \dots, n)$ and $\sigma_i(\alpha)$ are called the conjugates of α. If $\alpha \in K$ we define the **norm** $N_k(\alpha) := \prod_{i=1}^n \sigma_i(\alpha)$ and the **trace** $T_k(\alpha) := \sum_{i=1}^n \sigma_i(\alpha)$. A basis of the ring of integers of a number field K is called an **integral bases** for K. Every number field possesses an integral basis. The discriminant of an integral basis is independent of the integral basis which we choose, so it is called the discriminant of K.

If $K = \mathbb{Q}(\sqrt{d})$ the monomorphisms are given by $\sigma_1(r + s\sqrt{d}) = r + s\sqrt{d}$ and $\sigma_2(r + s\sqrt{d}) = r - s\sqrt{d}$.

So for every $\alpha = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ we can write the norm and the trace:

$N(r + s\sqrt{d}) = r^2 - ds^2$, $T(r + s\sqrt{d}) = 2r$.

If $d \not\equiv 1(\text{mod}4)$ then $\left\{1, \sqrt{d}\right\}$ is an integral basis for $\mathbb{Q}(\sqrt{d})$ (i.e. a basis of the ring of integers) and so the discriminant of $\mathbb{Q}(\sqrt{d})$ is $4d$; if $d \equiv 1(\text{mod}4)$ then $\mathbb{Q}(\sqrt{d})$ has an integral basis of the form $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ and so its discriminant is d.

2.1.2 Rings of integers and factorization into irreducibles.

Now we investigate some important properties of the ring of integers in a number field K. At first we remark that $\mathcal{O}_k$ is a free abelian group of rank n, where $n = [\mathcal{O}_k : \mathbb{Q}]$, that is to say an abelian group with a basis of n elements.

There are some easy ways of detecting units and irreducibles elements in the ring of integers. Let $x, y \in \mathcal{O}_k$. Then:

1. x is a unit if and only if $N(x) = \pm 1$;

2. if x and y are associated then $N(x) = \pm N(y)$;

3. if $N(x)$ is a prime, then x is irreducible in $\mathcal{O}_k$.

In $\mathcal{O}_k$ the factorization into irreducibles is possible but not necessarily unique. For example in $\mathbb{Z}(\sqrt{-5})$ there are the following factorizations: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. We notice that there are no elements in O_k with norm ± 2 or ± 3 since $x^2 + 5y^2 = \pm 2$ and $x^2 + 5y^2 = \pm 3$ have no solutions; so $2, 3, 1+\sqrt{-5}$ and $1-\sqrt{-5}$ are all irreducible elements as their norms equal $4, 9, 6, 6$ respectively. Moreover 2 is not associated of $1+\sqrt{-5}$ or $1-\sqrt{-5}$, so for 6 the factorization is not unique.
This example shows that sometimes $\mathcal{O}_k$ is not a unique factorization domain. In particular we have that the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{d})$, for negative squarefree d, is a UFD if and only if d takes one of the values:

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

This result was first conjectured by Gauss. In 1934, Heilbronn and Linfoot [25] proved that there are at most ten negative d for which the ring of integers of $\mathbb{Q}(\sqrt{d})$ is a UFD; nine such d were known (those described above) and so the problem was whether there is a tenth such d. It was proved only in 1966 by **Baker** [2] and in 1967 by **Stark** [33] independently that there is no such tenth d.
If $d > 0$ we know that factorization is unique in many more cases, for istance

$$2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41,$$

$$43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97, \ldots$$

and so the situation is different and more complicated than the previous one. In fact, according to a **Conjecture of Gauss**, unique factorization occurs for infinitely many $d > 0$.

2.1.3 Ideals in $\mathcal{O}_k$

$\mathcal{O}_k$ is also a **Dedekind** ring. This means that it has the following properties:

1. it is a domain with field of fractions K;
2. it is **Noetherian** (i.e. every ideal in $\mathcal{O}_k$ is finitely generated);
3. it is integrally closed (i.e. if $\alpha \in K$ satisfies a monic polynomial equation with coefficients in $\mathcal{O}_k$ then $\alpha \in \mathcal{O}_k$);
4. it is 1-dimensional (i.e. every non-zero prime ideal of $\mathcal{O}_k$ is maximal[1]).

An $\mathcal{O}_k$**-submodule** of K is a subgroup N of K such that if $n \in N$, $k \in \mathcal{O}_k$, then $kn \in N$. So an ideal may be described as an $\mathcal{O}_k$-submodule of $\mathcal{O}_k$.
We define a $\mathbb{Z}$-basis as a linearly independent set which generates an abelian group; every ideal I of $\mathcal{O}_K$ with $I \neq 0$ has a $\mathbb{Z}$-basis $[\alpha_1, \dots, \alpha_n]$ where n is the degree of K.
A fractional ideal F of $\mathcal{O}_k$ is a $\mathcal{O}_k$-submodule such that there exists $c \in \mathcal{O}_k, c \neq 0$ with $cF \subseteq \mathcal{O}_k$. In particular an ideal I is also a fractional ideal and, F is a fractional ideal of $\mathcal{O}_k$ if and only if $F = d^{-1}I$, for some $d \neq 0, d \in \mathcal{O}_k$ and I ideal of $\mathcal{O}_k$. Moreover the non-zero fractionals ideals of $\mathcal{O}_k$ form an abelian group under the multiplication.
We have the following fundamental property of the ideals of $\mathcal{O}_k$ which also characterizes Dedekind domains:

Theorem 2.1. *Every non-zero ideal of $\mathcal{O}_k$ can be written as a product of prime ideals, uniquely up to the order of the factors.*

Moreover in $\mathcal{O}_k$, since it is a Dedekind domain, we can define the divisibility of ideals in the following way:

[1] An ideal I of a domain R is maximal if I is a proper ideal of R and there are no ideals of R strictly between I and R

$$I/J \Longleftrightarrow I \supseteq J.$$

Now let us state a result that enable us to define the norm of ideals.

Proposition 2.1. *If I is a non-zero ideal of $\mathcal{O}_k$, then $\#(\mathcal{O}_k/I)$ is finite.*

Proof. Let $\alpha \in I$, $\alpha \neq 0$; we have $\alpha\mathcal{O}_k \subseteq I$. So we can consider the following surjective application:

$$\mathcal{O}_k/\alpha\mathcal{O}_k \longrightarrow \mathcal{O}_k/I,$$

where

$$x + \alpha\mathcal{O}_k \longrightarrow x + I$$

We will prove that $\#(\mathcal{O}_k/\alpha\mathcal{O}_k)$ is finite; this implies $\#(\mathcal{O}_k/I)$ finite.
Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis of $\mathcal{O}_k$, so we can write:

$$\mathcal{O}_k = \omega_1\mathbb{Z} + \ldots \omega_n\mathbb{Z}$$

and

$$\alpha\mathcal{O}_k = \alpha\omega_1\mathbb{Z} + ...\alpha\omega_n\mathbb{Z}.$$

By properties of abelian free groups[2] and of discriminants[3] we have

$$\#(\mathcal{O}_k/\alpha\mathcal{O}_k) = \sqrt{\Delta(\alpha\omega_1, \ldots, \alpha\omega_n)/\Delta(\omega_1, \ldots, \omega_n)} = |N(\alpha)|$$

and this is finite.

□

[2] Let G a free abelian group of rank n and H a subgroup of G of equal rank; if G and H have $\mathbb{Z}$-bases $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ with $y_i = \sum_j a_{ij}x_j$, then

$$\#(G/H) = |det(a_{ij}|.$$

[3] If $K = \mathbb{Q}(\theta)$ and $\{\alpha_1, \ldots, \alpha_n\}$, $\{\beta_1, \ldots, \beta_n\}$ are bases of K with

$$\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i$$

then

$$\Delta\left[\beta_1, \ldots, \beta_n\right] = \left[det(c_{ij})\right]^2 \Delta\left[\alpha_1, \ldots, \alpha_n\right]$$

We define the **norm** of I to be: $N(I) = \#(\mathcal{O}_k/I)$.
Properties of the norm of an ideal:

1. if $\{\alpha_1, ..., \alpha_n\}$ is a $\mathbb{Z}$-basis for I we have $N(I) = \sqrt{\frac{\Delta(\alpha_1,...,\alpha_n)}{\Delta}}$ where Δ is the discriminant of K;
2. if $I = \langle a \rangle$ is a principal ideal then $N(I) = |N(a)|$;
3. if I and J are non-zero ideals of $\mathcal{O}_k$, then $N(IJ) = N(I)N(J)$;
4. if $N(I)$ is a prime number, then $I \subseteq \mathcal{O}_k$ is a prime ideal;
5. for any m, there are only finitely many ideals of $\mathcal{O}_k$ with norm m.

2.2 The Class Group

In this section we will define the **Class Number** of a number field .
Let $\mathbf{F}(\mathcal{O}_k) = \{F | F$ fractional ideals of $\mathcal{O}_k\}$ be the free group generated by the fractional ideals of $\mathcal{O}_k$ and let $\mathbf{P}(\mathcal{O}_k) = \{z\mathcal{O}_k | z \in K, z \neq 0\}$ be the subgroup of $\mathbf{F}(\mathcal{O}_k)$ generated by principal fractional ideals. We define the **Class Group** of $\mathcal{O}_k$ to be the quotient group $\mathbf{Cl}(\mathcal{O}_k) = \frac{\mathbf{F}(\mathcal{O}_k)}{\mathbf{P}(\mathcal{O}_k)}$ and the **Class Number** to be its order. The Class Group measures the extent to which ideals can be non principal, or how far $\mathcal{O}_k$ is from being a UFD.
In fact if D is a domain, then D is a PID if and only if D is a UFD and every non-zero prime ideal of D is maximal. Since $\mathcal{O}_k$ is a Dedekind ring, $\mathcal{O}_k$ is a UFD if and only if it is a PID.
Moreover, according to the definition, $\mathcal{O}_k$ is a PID if and only if every ideal of $\mathcal{O}_k$ is principal, that means $\mathbf{F}(\mathcal{O}_k) = \mathbf{P}(\mathcal{O}_k)$; this happens if and only if $|\mathbf{Cl}(\mathcal{O}_k)| = 1$. So we have that $\mathcal{O}_k$ is a UFD if and only if the class-group has order 1, or equivalently the class number h is equal to 1.

2.2.1 Equivalence of ideals

Let Γ be the set of the ideals of $\mathcal{O}_k$. We define on Γ this equivalence relation: $\mathbf{x}, \mathbf{y} \in \Gamma, \mathbf{x} \sim \mathbf{y} \iff \exists \langle a \rangle, \langle b \rangle$ principal ideals and $\mathbf{x}\langle a \rangle = \mathbf{y}\langle b \rangle$. If $N(ab) > 0$ the ideals are said **strictly** equivalent and we also say that $\mathbf{x}$ and $\mathbf{y}$ are in the same narrow ideal class.
Now let I, J be two fractional ideals, they are equivalent if $I = \alpha J$ for some nonzero element α of $\mathcal{O}_K$. We can define multiplication of equivalence classes of fractional ideals by setting $[I][J] = [IJ]$; with this definition the set of equivalence classes of fractional ideals forms an abelian multiplicative group that is just $\mathbf{Cl}(\mathcal{O}_k)$. For this reason it is called the **Class Group**.

2.2.2 Finiteness of the Class Number

The proof of the finiteness of the Class Number h is an application of a very important theorem of 1896, due to **Minkowski**. Let us state Minkowski's theorem and its applications [36].

Minkowski's Theorem

At first we define some geometric objects .

Definition 2.1. *Let $e_1, \ldots, e_m$ be a linearly indipendent set of vectors in $\mathbb{R}^n$.The additive subgroup of $(\mathbb{R}^n, +)$ generated by $e_1, \ldots, e_m$ is called a* **lattice** *of dimension m, generated by $e_1, \ldots, e_m$.*

Definition 2.2. *If L is a lattice generated by $\{e_1, \ldots, e_n\}$ the* **fundamental domain** *of L consists of all elements $\sum a_i e_i$ $(a_i \in \mathbb{R})$ for which $0 \leq a_i < 1$.*

Definition 2.3. *Let* $\mathbf{S}$ *denote the set of all complex numbers of modulus 1. The direct product of n copies of* $\mathbf{S}$ *is denoted by* $\mathbf{T}^n$ *and is called the* **n-dimensional torus**.[4]

[4] If L is an n-dimensional lattice in $\mathbb{R}^n$ then $\mathbb{R}^n/L$ is isomorphic to the n-dimensional torus $\mathbf{T}^n$.

Theorem 2.2. *(Minkowski's theorem) Let L be an n-dimensional lattice in $\mathbb{R}^n$ with fundamental domain T, and let X be a bounded symmetric convex*[5] *subset of $\mathbb{R}^n$. If*

$$v(X)^6 > 2^n v(T)$$

then X contains a non-zero point of L.

The finiteness theorem

The following applications of Minkowski's theorem enable us to prove the finiteness of the class-number. We are going to prove only the results in which we are more interested .

Lemma 2.1. *If M is a lattice in L^{st} of dimension $s+2t$ having fundamental domain of volume V, and if $c_1, \dots, c_{s+t}$ are positive real numbers whose product*

$$c_1 \dots c_{s+t} > (4/\pi)^t V$$

then there exists in M a non-zero element

$$x = (x_1, \dots, x_{s+t})$$

such that

$$|x_1| < c_1, \dots, |x_s| < c_s;$$

$$|x_{s+1}|^2 < c_{s+1}, \dots, |x_{s+t}|^2 < c_{s+t}.$$

Theorem 2.3. *Let K be a number field of degree $n = s+2t$ with ring of integers $\mathcal{O}_k$, and let $0 \neq I$ be an ideal of $\mathcal{O}_k$. Then the volume of a*

[5] A subset $X \subseteq \mathbb{R}^n$ is **convex** if whenever $x, y \in X$ then all points on the straight line segment joining x to y also lie in X.

[6] The **volume** $v(X)$ of a subset $X \subseteq \mathbb{R}^n$ is defined as:

$$\int_X dx_1 \dots dx_n$$

where $(x_1, \dots, x_n)$ are coordinates. The volume exists only when the integral does.

fundamental domain for $\sigma(I)$[7] in $\subseteq L^{st} := \mathbb{R}^s \times \mathbb{C}^t$ is equal to

$$2^{-t}N(I)\sqrt{|\Delta|}$$

where Δ is the discriminant of K.

Corollary 2.1. *If $I \neq 0$ is an ideal of $\mathcal{O}_k$ then I contains an integer α with*

$$|N(\alpha)| \leq (2/\pi)^t N(I)\sqrt{|\Delta|}$$

where Δ is the discriminant of K.

Proof. We consider an arbitrary $\epsilon > 0$, let $c_1, \ldots, c_{s+t}$ be positive real numbers with

$$c_1 \ldots c_{s+t} = (2/\pi)^t N(I)\sqrt{|\Delta|} + \epsilon.$$

By Lemma 2.1 and Theorem 2.3 we obtain that exists $\alpha \neq 0$ such that

$$|\sigma_1(\alpha)| < c_1, \ldots, |\sigma_s(\alpha)| < c_s,$$

$$|\sigma_{s+1}(\alpha)|^2 < c_{s+1}, \ldots, |\sigma_{s+t}(\alpha)|^2 < c_{s+t}.$$

By multiplication of all these inequalities and by the multiplicative property of the norm of elements, we have:

$$|N(\alpha)| < c_1 \ldots c_s c_{s+1} \ldots c_{s+t} = (2/\pi)^t N(I)\sqrt{|\Delta|} + \epsilon.$$

Now we call A_ϵ the set of such α. Since a lattice is discrete, A_ϵ is finite and also $A_\epsilon \neq \emptyset$. So $A = \bigcap_\epsilon A_\epsilon \neq \emptyset$. If $\alpha \in A$, then we have

$$|N(\alpha)| \leq (2/\pi)^t N(I)\sqrt{|\Delta|}$$

□

[7] If $\alpha \in K = \mathbb{Q}(\theta)$, we can define a ring homomorphism $\sigma : K \longrightarrow L^{st}$ by $\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha); \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha))$, $\forall \alpha, \beta \in K$ where $\sigma_i(\alpha)$ for $i = 1, \ldots, s+t$ are the monomorphisms $K \longrightarrow \mathbb{C}$

Corollary 2.2. *Every non-zero ideal I of $\mathcal{O}_k$ is equivalent to an ideal with norm* $\leq (2/\pi)^t\sqrt{|\Delta|}$.

Proof. If we consider I^{-1} we have that the class of fractional ideals equivalent to I^{-1} contains an ideal J and IJ is equivalent to $\mathcal{O}_k$. By the previous corollary we can find an integer $\gamma \in J$ such that

$$|N(\gamma)| \leq (2/\pi)^t N(J)\sqrt{|\Delta|}.$$

By properties of ideals, since J divides γ, we have

$$\langle\gamma\rangle = JH$$

for some ideal H. Since $N(H)N(J) = N(HJ) = N(\langle\gamma\rangle) = |N(\gamma)|$ it follows that

$$N(H) \leq (2/\pi)^t\sqrt{|\Delta|}$$

and H is equivalent to I because J is equivalent to I^{-1} and H is equivalent to J^{-1}.

□

Finally we state and prove the fundamental result of this section:

Theorem 2.4. *The Class Group of a number field is a finite abelian group. The Class Number h is finite.*

Proof. Let K be a number field of discriminant Δ and degree $n = s + 2t$. $\mathbf{Cl}(\mathcal{O}_k)$ is an abelian group and it is finite if and only if the number of distinct classes of fractional ideals is finite. An equivalence class contains an ideal J with $N(J) \leq (2/\pi)^t\sqrt{|\Delta|}$. Since only finitely many ideals have a given norm, there are only finitely many choises for J and there are only finitely many equivalence classes $[x]$. It follows that $\mathbf{Cl}(\mathcal{O}_k)$ is a finite group.

□

2.3 Quadratic forms and ideals of O_k

Now we will show how the previous concepts are connected to the theory of binary quadratic forms. More details can be found in the book of Harvey Cohn [16].

Let $f(x,y) = ax^2 + bxy + cy^2$ be a primitive binary quadratic form, we recall that its discriminant is $\delta_f = b^2 - 4ac$.

An integer d is a discriminant for some form f if and only if $d \equiv 0, 1 (\bmod 4)$.

We also recall that in Definition 1.7 of Chapter 1 we have defined the notion of fundamental discriminants.

We can prove that the fundamental discriminants are just the discriminants of quadratic fields. So, if we use the notation of Definition 1.7, we have $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{D})$. In this case we will denote the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ as $\mathcal{O}_m$ and $\mathcal{O}_m = \mathbb{Z} + \mathbb{Z}\frac{(D+\sqrt{D})}{2}$.

We defined, in the previous chapter, an equivalence relation in the set of the primitive binary quadratic forms and the Class Number as the number of classes of primitive forms with a fixed discriminant; if this discriminant is a fundamental discriminant D, we denote this number as $h(D)$.

Now we will set up a precise correspondence between forms and ideals. At first we say that an ideal is **primitive** when it is not divisible by any rational ideal except $\langle 1 \rangle$. The definition of primitive form has been given in the previous chapter in Definition 1.3.

Moreover in order to state the following result we need to give the definition of **ordered basis** of an ideal.

Definition 2.4. *A basis $[\alpha, \beta]$ of an ideal I is said to be ordered if*

$$\frac{\Delta}{\sqrt{d}} = \frac{1}{\sqrt{d}} \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix} = \frac{\alpha\beta' - \beta\alpha'}{\sqrt{d}} > 0$$

where α' and β' are the conjugates of α and β.

We remark that, according to the properties of the norm of an ideal (see pag. 31), we have $\pm\frac{\Delta}{\sqrt{d}} = N(I) > 0$.

Lemma 2.2. *If we denote by $I = [\alpha, \beta]$ an ideal of $\mathcal{O}_m$ with a basis $[\alpha, \beta]$, the form*

$$F(x, y) = N(\alpha x + \beta y)/N(I) = ax^2 + bxy + cy^2$$

has integral coefficients and it is a primitive form of discriminant D.

Proof. We have $N(\alpha x + \beta y) = (\alpha x + \beta y)(\alpha^{'} x + \beta^{'} y) = Ax^2 + Bxy + cy^2$, where $\alpha^{'}, \beta'$ are the conjugates of α and β.
So $N(\alpha x + \beta y)$ is a quadratic form. The coefficients of that form belong to $II^{'}$, where $I^{'} = \left[\alpha^{'}, \beta^{'}\right]$. So we can write:

$$\begin{cases} A = \alpha\alpha^{'} = aN(I), \\ B = \alpha\beta^{'} + \alpha^{'}\beta = bN(I) \\ C = \beta\beta^{'} = cN(I) \end{cases} .$$

$\langle N(I)\rangle$ contains (hence divides) A, B, C; so the coefficients of $F(x, y)$ are integers and it is simple to prove that F is primitive.
Moreover, we obtain that

$$b^2 - 4ac = (B^2 - 4AC)/(N(I))^2 = (\alpha\beta^{'} - \beta\alpha^{'})/(N(I))^2 = D.$$

□

We can say that the form F *belongs* to the ideal I, writing

$$\begin{cases} F = F\left[\alpha, \beta\right] = F(I), \\ I = [\alpha, \beta] \to F \end{cases} ,$$

we also say that I *leads* to F.

Lemma 2.3. *Let $F(x, y) = Ax^2 + Bxy + Cy^2 = t(ax^2 + bxy + cy^2)$ be a quadratic form, where $\pm t$ is the greatest common divisor of A, B, C. We let $t > 0$ if $B^2 - 4AC > 0$ and we choose t so that $a > 0$ if $B^2 - 4AC < 0$. We suppose that $D = b^2 - 4ac$ is the discriminant for the field $\mathbb{Q}(\sqrt{D})$.*

Then the ideal I, given by the formulas:

$$I = [\alpha, \beta] = \begin{cases} \left[a, (b - \sqrt{D})/2\right], & a > 0, \forall D \\ \left[a, (b - \sqrt{D})/2\right] \sqrt{D}, & a < 0,\ D > 0 \end{cases}$$

is integral (i.e. the basis elements are integer) and has an ordered basis. I is primitive when $a > 0$, whereas $I/\sqrt{D}$ is primitive when $a < 0$.

Proof. If $D \equiv 1(\mathrm{mod}4)$ we have that the basis elements of I are integers because b is odd; the same is true if $D \equiv 0(\mathrm{mod}4)$ because, in this case, b is even. Moreover, assuming $d > 0$, we have $\Delta = a\sqrt{d}$, if $a > 0$, and $\Delta = a(-d)\sqrt{d}$, if $a < 0$. So, since $\Delta/\sqrt{d} > 0$, the basis of I is ordered.
The ideal I is primitive, otherwise an integer $u > 1$ exists such that u divides a and u divides $(b - \sqrt{D})/2$. So we have that u divides $(\beta - \beta')$ or u^2 divides D; by the definition of the field discriminant, this is possible only when $D \equiv 0(\mathrm{mod}4)$, and limits u to the value 2. But, if $D \equiv 0(\mathrm{mod}4)$, a and b are even, so 2 divides β and 2 divides $\sqrt{D}/2$ and this is not possible as 4 does not divide $\sqrt{D}$ ($D/4$ is square-free by nature of the field discriminant). □

If F is a form satisfying the properties of the Lemma 2.3 and I is the ideal determined by this form, we write:

$$\begin{cases} [\alpha, \beta] = I = I(A, B, C) = I(F), \\ F \to I \end{cases}$$

and say that F *leads* to I. By Lemma 2.2 and Lemma 2.3 we can describe the correspondence procedure and then state the **Correspondence Theorem**.
Starting with a primitive form $F = ax^2 + bxy + cy^2$ with $a > 0$, we can construct the ideal $I(a, b, c)$ as described in Lemma 2.3; from this ideal, according to Lemma 2.2, we can costruct a quadratic form $F^*(\alpha, \beta)$. We obtain $F^* = F$.
Starting with a primitive ideal $I = [\alpha, \beta]$ we can construct, by Lemma 2.2, a

quadratic form $F[\alpha, \beta]$; from this form we obtain, using Lemma 2.3, an ideal I^*, generally different from I, which is strictly equivalent to I.
Then the situation is the following:

$$F \to I \to F^* \Rightarrow F = F^*;$$

$$I \to F \to I^* \Rightarrow I \sim I^*$$

where the equivalence of ideals is in the narrow sense.
So we have this important theorem:

Theorem 2.5. *(Correspondence Theorem) If we have two equivalent forms*

$$F_1 \sim F_2$$

and $F_1 \to I_1$, $F_2 \to I_2$, then

$$I_1 \sim I_2$$

where the equivalence ideal is always narrow.
Conversely, if two ideals I_1,I_2 are strictly equivalent and $I_1 \to F_1$, $I_2 \to F_2$, then

$$F_1 \sim F_2.$$

Then we can say that there is a one-to-one correspondence between a representative set of forms of discriminant D and a representative set of ideals strictly equivalent; in other words the abelian group of classes of primitive binary quadratic forms of discriminant D (where the operation between forms is the Gaussian Composition[8]) isomorphic to the narrow class group $\mathbf{Cl}(\mathcal{O}_m)^+$ (where the relationship between m and D was described earlier).

2.3.1 Class Number Formula

Now, by the Correspondence Theorem and by the results of the first chapter, we are going to find again a Class Number formula.

[8] see Definition 4.2

At first we notice that if $m < 0$ (and so D) there is no distinction between equivalence in the narrow sense and in the ordinary sense because every element has a strictly positive norm. Also if $m > 0$ and there is a unit in K of norm -1, there is no distinction because, if necessary, we can have an element of positive norm by multiplying it by this unit. If $m > 0$ and there is no unit of norm -1, each ideal class in the ordinary sense contains two ideal class in the narrow sense. So if denote by $h(m)$ the number of ideal classes in K in the ordinary sense and by $h^+(m)$ that of classes of equivalence in the narrow sense, we have:

$$\begin{cases} h^+(m) = h(m) & \text{if } m < 0 \text{ or } \exists \epsilon \in U(O_m) \text{ s.t. } N(\epsilon) = -1 \\ h^+(m) = 2h(m) & \text{if } m > 0 \text{ and there is no unit of norm } -1 \text{ .} \end{cases}$$

If $m > 0$ we can combine these results by using the **fundamental unit** of K that is a unit $\epsilon_1 > 1$ such that every other unit can be written as $\pm\epsilon_1^n$, $n \in \mathbb{Z}$.
In fact the unit ϵ with norm -1 is

$$\epsilon = \begin{cases} \epsilon_1 & \text{if } N(\epsilon_1) = 1 \\ \epsilon_1^2 & \text{if } N(\epsilon_1) = -1 \end{cases},$$

so if $m > 0$, we have:

$$h^+(m)\log(\epsilon) = 2h(m)\log(\epsilon_1).$$

By using this formula we obtain the final expressions for the class number of a quadratic field :

$$h(m) = -\frac{w}{2|m|}\sum_{k=1}^{|m|} k\left(\frac{m}{k}\right) \qquad \text{if } m < 0 \tag{2.1}$$

$$h(m)\log(\epsilon_1) = -\frac{1}{2}\sum_{k=1}^{|m|}\left(\frac{m}{k}\right)\log\sin\left(\frac{m\pi}{d}\right) \qquad \text{if } m > 0. \tag{2.2}$$

Chapter 3

Analytic properties of the Class Number

Many problems about the class-number h_d have attracted mathematicians also in recent years. In this chapter we are going to deal with some of these. In particular now we will touch on the so-called Gauss's Class Number Problem and we will analyse some important analytic properties of h_d and some conjectures about it; in the next chapter we will turn our attention to the question of searching an efficient computation of it.

3.1 Gauss's Class Number Problem.

In the previous chapter we said that the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{d})$, when d is negative, is a UFD if and only if d takes one of the values $\{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$; this means that we know all the values of the integer $-d$ such that $h(-d) = 1$. For a given m, the problem to determine a list of fundamental discriminants $-d$ such that $h(-d) = m$ is called Gauss's Class Number Problem because Gauss was the first to deal with it; the above-mentioned numbers solve this problem for $m = 1$.

Baker, in 1971, and **Stark**, in 1975, independently found the values of d such that $h(-d) = 2$; successively the cases $h(-d) = 3$ and $h(-d) = 4$ were solved by **Oesterlé** in 1985 and **Arno** in 1992.
Arno himself, in 1993, solved $h(-d) = m$ where m is odd and $5 \leq m \leq 23$ and **Watkins** solved this problem for all $m \leq 16$.

3.1.1 Class Number for particular d

The behavior of the class-number is well-known only when the number d has a particular form. Now we will show some examples.
When $d = p$, where $p \equiv 3 \mod 4$, and $h_p = 1$, we have this important result due to **Hirzebruch** [23]:

$$h_{-p} = \frac{1}{3}\sum_{i=1}^{l}(-1)^{l-i}k_i;$$

where $k_1, ..., k_l$ is the sequence of denominators in one period of the continued fraction expansion[1] of the number $\sqrt{p} - \lfloor\sqrt{p}\rfloor$.
Particular are also the situations when the discriminant is $d_j = j^2 + 4$, where j is a positive integer, or $d_k = 4k^2 + 1$; in fact in these cases we have the two inequalities

$$h_j = h(j^2 + 4) > 1, \text{if } j \text{ is odd and } j > 17;$$

$$h_k = h(4k^2 + 1) > 1, \text{if } k > 13$$

conjectured respectively by **Yokoi** and **Chowla**, and proved by **Birò** in 2003. Precisely, in his work, Birò [3, 4] uses the Siegel's Theorem (which we will state in the next section) and the fact that $h_j = 1$ if and only if the Legendre symbol $\left(\frac{d_j}{r}\right) = -1$ for all the primes r such that $2 \leq r < j$ (the same occurs for h_k), to prove that

$$h_j = 1 \Longleftrightarrow j \in \{1, 3, 5, 7, 13, 17\}$$

[1] The continued fraction expansion of a number is an expression $x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3 + \frac{1}{\ddots}}}}$ which can be periodic; the numbers $x_1, x_2, x_3, \ldots$ are said the denominators of the fraction.

and

$$h_k = 1 \Longleftrightarrow k \in \{1, 2, 3, 5, 7, 13\}\,.$$

3.2 Properties of the Class Number

3.2.1 Estimates of $h(d)$

A first important property of the Class-number was conjectured by Gauss in his *Disquisitiones Arithmeticae.*

He said that $h(d) \to \infty$ as $d \to -\infty$, but a proof of that conjecture has been given only in modern times.

In 1918 **Hecke** proved that if every real zero β of $L(s, \chi)$, where χ is a real primitive character to the modulus q, satisfies the inequality

$$\beta < 1 - c_1 / \log q,$$

then

$$h(d) > c_2 |d|^{\frac{1}{2}} / \log(|d|),$$

where c_1 and c_2 are constants; but the proof given by Hecke came out from the generalized Riemann hypothesis[2].

In 1934 **Heilbronn** proved that $h(d) \to \infty$ as $d \to -\infty$ under the assumption of the falsity of the generalized Riemann hypothesis.

Helibronn's result with the one of Hecke, gave a proof of the conjecture of Gauss unconditionally.

The fundamental result of those years about L-functions and class-number was **Siegel**'s theorem (1935); we will state it in one of its two forms:

[2] This is the hypothesis that all the functions $L(s, \chi)$ have their zeros, $\sigma + it$, in the critical strip on the line $\sigma = \frac{1}{2}$; this hypothesis was formulated in 1884 by Piltz.

Theorem 3.1. *For any $\epsilon > 0$ there exists a positive number $C_1(\epsilon)$ such that, if χ is a real primitive character to the modulus q, then*

$$L(1, \chi) > C_1(\epsilon) q^{-\epsilon}.$$

By Class Number Formula, obtained in the previous chapters

$$h(d) = \frac{w|d|^{\frac{1}{2}}}{2\pi} L(1, \chi) \qquad \text{for } d < 0 \tag{3.1}$$

$$h(d) = \frac{d^{\frac{1}{2}}}{\log \eta} L(1, \chi) \qquad \text{for } d > 0, \tag{3.2}$$

where η is the fundamental unit, we have that Siegel's theorem implies the following inequalities:

$$h(d) > C_2(\epsilon)|d|^{\frac{1}{2}-\epsilon} \qquad \text{for } d < 0 \tag{3.3}$$

and

$$h(d) \log \eta > C_2(\epsilon) d^{\frac{1}{2}-\epsilon} \qquad \text{for } d > 0. \tag{3.4}$$

There are many applications of those results to study class-number properties. First of all we remark that Siegel's Theorem gives an immediate proof of the above-stated conjecture of Gauss.
Moreover it implies the following estimates:

Proposition 3.1. *If d is a fundamental discriminant and η the fundamental unit, then*

$$\log(h(d)) \sim \log(\sqrt{|d|}) \qquad \textit{as } d \to -\infty \tag{3.5}$$

and

$$\log(h(d) \log(\eta)) \sim \log(\sqrt{d}) \qquad \textit{as } d \to \infty. \tag{3.6}$$

In order to prove Proposition 3.1, we need to state another fundamental result known as **Polya-Vinogradov inequality**:

Lemma 3.1. *(Polya-Vinogradov Inequality) Let χ be a nonprincipal character* $(\mathrm{mod} q)$*, then*

$$\sum_{n=M+1}^{M+N} \chi(n) = O(q^{1/2} \log q) \tag{3.7}$$

Proof. (of Proposition 3.1) We consider the case $d < 0$ and give a proof of (3.5); (3.6) is obtained using exactly the same method.
From (3.3) we obtain

$$\log(h(d)) > \log(C_2(\epsilon)|d|^{1/2-\epsilon})$$

and this implies

$$\frac{\log(h(d))}{\log(|d|^{\frac{1}{2}})} > \frac{\log(C_2(\epsilon)|d|^{1/2-\epsilon})}{\log(|d|^{\frac{1}{2}})} = \frac{\log(C_2(\epsilon))}{\log(|d|^{\frac{1}{2}})} + \frac{\log(|d|^{1/2-\epsilon})}{\log(|d|^{\frac{1}{2}})}.$$

As $d \to -\infty$, we have

$$\frac{\log(h(d))}{\log(|d|^{\frac{1}{2}})} > 1 - \epsilon. \tag{3.8}$$

Moreover, in the first chapter we proved that, if $d < 0$,

$$L(1, \chi) = -\frac{\pi}{|d|^{\frac{3}{2}}} \sum_{m=1}^{|d|} m \left(\frac{d}{m}\right)$$

and now we recall that the Jacobi symbol $\left(\frac{d}{m}\right)$ is a nonprincipal character modulo $|d|$, whenever $d \equiv 0$ or $1(\mathrm{mod} 4)$ and not a square number.
So we have

$$L(1, \chi) = -\frac{\pi}{|d|^{\frac{3}{2}}} \sum_{m=1}^{|d|} m \left(\frac{d}{m}\right) = -\frac{\pi}{|d|^{\frac{3}{2}}} \sum_{m=1}^{|d|} m\chi(m)$$

and, using partial summation formula of Abel,

$$\sum_{m=1}^{|d|} m\chi(m) = |d| \sum_{m=1}^{|d|} \chi(m) - 1\chi(1) - \int_1^{|d|} \sum_{m=1}^{t} \chi(m) dt.$$

Since $\sum_{m=1}^{|d|} \chi(m) = 0$ and $\sum_{m=1}^{t} \chi(m) = O(\sqrt{|d|}\log(|d|))$, from Lemma 3.1, it follows that $L(1,\chi) = O(\log|d|)$.

From this result we obtain

$$h(d) < c\frac{w|d|^{\frac{1}{2}}}{2\pi}\log(|d|),$$

where c is an absolute constant, and so

$$\log(h(d)) < \log\left(\frac{cw}{2\pi}\right) + \log(|d|^{1/2}) + \log(\log(|d|));$$

$$\frac{\log(h(d))}{\log(|d|^{1/2})} < \frac{\log(\frac{cw}{2\pi})}{\log(|d|^{1/2})} + 1 + \frac{\log(\log(|d|))}{\log(|d|^{1/2})}$$

As $d \to -\infty$ we have

$$\frac{\log(h(d))}{\log(|d|^{1/2})} < 1 + \epsilon. \tag{3.9}$$

From (3.8) and (3.9) it follows that $\log(h(d)) \sim \log(\sqrt{|d|})$, as $d \to -\infty$. □

3.2.2 The mean value of $h(d)$

Other important results are about the mean value of $h(d)$. A first conjecture for the average number of properly primitive classes of a fixed discriminant was given by Gauss in Sects. 302 and 304 of the Disquisitiones.

If $h^+(d)$ denotes, as in the previous chapter, the class-number obtained from the narrow definition of equivalence (of quadratic forms or of ideals), Gauss stated that as $N \to \infty$

$$\sum_{\substack{0<-d<4N \\ 4|d}} h^+(d) \sim \frac{4\pi}{21\zeta(3)} N^{3/2}, \tag{3.10}$$

and

$$\sum_{\substack{0<d<4N\\4|d}} h^+(d)\log\eta^+ \sim \frac{4\pi^2}{21\zeta(3)}N^{3/2}, \tag{3.11}$$

where $\eta^+ = \frac{t+u\sqrt{d}}{2}$, with t,u the smallest positive solutions of $t^2 - du^2 = 4$, and $\zeta(s)$ is the Riemann Zeta Function.

In 1944, Siegel proved more general results [32] which implied the conjectures of Gauss:

Theorem 3.2. *If* $d \equiv 0, 1(\text{mod}4)$ *no square*

$$\sum_{0<-d<N} h^+(d) = \frac{\pi}{18\zeta(3)}N^{3/2} + O(N\log N) \tag{3.12}$$

and

$$\sum_{0<d<N} h^+(d)\log\eta^+ = \frac{\pi^2}{18\zeta(3)}N^{3/2} + O(N\log N) \tag{3.13}$$

Proof. At first we will prove (3.13). Since $d > 0$, from the definition, we can write

$$d^{-\frac{1}{2}}h^+(d)\log\eta^+ = \sum_{n=1}^{\infty}\left(\frac{d}{n}\right)n^{-1}$$

and we can introduce these notations

$$d^{-\frac{1}{2}}h^+(d)\log\eta^+ = f_d \qquad\qquad \sum_{n=1}^{N}\left(\frac{d}{n}\right)n^{-1} = \sigma_d. \tag{3.14}$$

If we also denote $s_n = \sum_{k=1}^{n}\chi(k)$, we will obtain

$$\sum_{n=N+1}^{\infty}\chi(n)n^{-1} = \sum_{n=N+1}^{\infty}(s_n - s_{n-1})n^{-1} = \sum_{n=N}^{\infty}s_n\left(\frac{1}{n} - \frac{1}{n+1}\right) - s_nN^{-1}$$

and so, from Lemma 3.1,

$$\left|\sum_{n=N+1}^{\infty}\chi(n)n^{-1}\right| < 2cN^{-1}d^{1/2}\log d. \tag{3.15}$$

From (3.15) we have

$$|f_d - \sigma_d| < 2cN^{-1}d^{\frac{1}{2}}\log d \tag{3.16}$$

and, when d is a square,

$$|\sigma_d| \leq \sum_{n=1}^{N} n^{-1} < 1 + \log N. \tag{3.17}$$

Let r be either 0 or 1 and let t be such that $1 \leq t \leq N$ and $t \equiv r(\mathrm{mod}4)$, so we can consider d belonging to the set of all those t which are no square numbers.

We have

$$\sum_d f_d = \sum_d \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-1} = \sum_{n=1}^{N} n^{-1} \sum_t \left(\frac{t}{n}\right) + \sum_{n=N+1}^{\infty} n^{-1} \sum_t \left(\frac{t}{n}\right),$$

where the sums are all over non-square t, and so, from (3.16) and (3.17), as $N \to \infty$, we obtain

$$\sum_d f_d = \sum_{n=1}^{N} n^{-1} \sum_t \left(\frac{t}{n}\right) + O(N^{\frac{1}{2}}\log N) \tag{3.18}$$

Now we define

$$P_r(n) = \sum_t \left(\frac{t}{n}\right) \qquad (n = 1, 2, ..., N). \tag{3.19}$$

At first we consider the case when n is not a square. If n is even, from the properties of Jacobi Symbol, we obtain $P_r(n) = 0$. Instead, if n is odd, since $\chi_1(k) = \left(\frac{k}{n}\right)$ is a nonprincipal character modulo n, from Lemma 3.1, it follows that

$$P_0(n) = \sum_{4k \leq N} \chi_1(k) = n^{\frac{1}{2}} \log n O(1).$$

Let $l = 2^\alpha$ such that $l|n$ but $2l \not| n$, then $s = n/l$ is odd and, whenever t is odd, $\left(\frac{t}{n}\right) = \left(\frac{t}{ls}\right) = \left(\frac{t}{l}\right)\left(\frac{t}{s}\right) = \left(\frac{l}{t}\right)\left(\frac{t}{s}\right)$.

If we consider $\chi_2(k) = \left(\frac{4l}{k}\right)\left(\frac{k}{s}\right)$ and $\chi_3(k) = \left(\frac{-4l}{k}\right)\left(\frac{k}{s}\right)$, these are nonprincipal characters modulo $4n$; then, again from Lemma 3.1, we obtain

$$P_1(n) = \frac{1}{2} \sum_{k \leq N} (\chi_2(k) + \chi_3(k)) = n^{\frac{1}{2}} \log n O(1)$$

and so, when $r = 0, 1$ and $1 \leq n \leq N$, n no square,

$$P_r(n) = n^{\frac{1}{2}} \log n O(1). \tag{3.20}$$

Now we consider the case $n = u^2$.

We recall that the Jacobi symbol $\left(\frac{t}{u^2}\right) = 1$, then $P_r(n)$ is equal to the number of integers t such that $1 \leq t \leq N$, $(t, u) = 1$ and $t \equiv r(\text{mod}4)$. Since $\#\{t \equiv 0(\text{mod}4)\} = \#\{t \equiv 1(\text{mod}4)\} = \frac{N}{4}$, we have

$$P_r(u_1^2) = \frac{\varphi(u_1)}{4u_1}N + u_1 O(1) \qquad (u_1 \text{ odd},) \tag{3.21}$$

because the number of t such that $(t, u_1^2) = 1$ is equal to $\frac{\varphi(u_1)}{u_1} + u_1 O(1)$.

Instead, if we consider an even integer $u_2 = 2k$, whenever $t \equiv 0(\text{mod}4)$, we have $(t, u_2) \geq 2$, and so $P_0(u_2^2) = 0$. When $t \equiv 1(\text{mod}4)$ we have $(2k, t) = (k, t)$, then

$$P_1(u_2^2) = P_1(k^2) = \frac{N}{4}\frac{\varphi(k)}{k} = \frac{N}{2}\frac{\varphi(u)}{u},$$

because of $\varphi(u) = \varphi(2k) = \varphi(2)\varphi(k) = \varphi(k)$. So we can write:

$$P_r(u_2^2) = r\frac{\varphi(u_2)}{2u_2}N + u_2 O(1) \qquad (u_2 \text{ even.}) \tag{3.22}$$

Those results allow us to write the following expression:

$$\begin{aligned} \sum_{u^2 \leq N} u^{-2} P_r(u^2) &= \frac{N}{4} \sum_{\substack{u_1^2 \leq N \\ u_1 \text{ odd}}} u_1^{-3}\varphi(u_1) + \frac{rN}{2} \sum_{\substack{u_2^2 \leq N \\ u_2 \text{ even}}} u_2^{-3}\varphi(u_2) + O(\log N) \\ &= \frac{N}{4}\frac{\zeta(2)}{\zeta(3)}\left(1 + \frac{2r-1}{7}\right) + O(\sqrt{n}), \end{aligned} \tag{3.23}$$

where $\zeta(s) = \frac{1}{n^s}$ is the Riemann zeta-function, because of

$$\sum_{\substack{u_2 \leq \sqrt{N} \\ u_2 \text{ even}}} \frac{\varphi(u_2)}{u_2^s} = \frac{1}{2^s - 1}\frac{\zeta(s-1)}{\zeta(s)} + O\left(\frac{1}{N^{\frac{s-2}{2}}}\right);$$

$$\sum_{\substack{u_1 \leq \sqrt{N} \\ u_1 \text{odd}}} \frac{\varphi(u_1)}{u_1^s} = \frac{2^s - 2}{2^s - 1}\frac{\zeta(s-1)}{\zeta(s)} + O\left(\frac{1}{N^{\frac{s-2}{2}}}\right).$$

From (3.18), (3.19), (3.20), (3.23), recalling that $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, it follows

$$\begin{aligned} \sum_d f_d &= \sum_{n=1}^{N} n^{-1} P_r(n) + O(N^{\frac{1}{2}} \log N) \\ &= \frac{\pi^2 N}{24\zeta(3)} \left(1 + \frac{2r-1}{7}\right) + O(N^{\frac{1}{2}} \log N). \end{aligned} \tag{3.24}$$

Now we apply the partial summation formula to obtain

$$\sum_d d^{\frac{1}{2}} f_d = \frac{\pi^2 N^{\frac{3}{2}}}{36\zeta(3)} \left(1 + \frac{2r-1}{7}\right) + O(N \log N), \tag{3.25}$$

where d are integers belonging to $1 \leq t \leq N$,$d \equiv r(\text{mod}4)$ and they are not squares.
Recalling that $h^+(d) \log \eta^+ = f_d d^{\frac{1}{2}}$, we have from (3.25)

$$\sum_d h^+(d) \log \eta^+ = \frac{\pi^2 N^{\frac{3}{2}}}{42\zeta(3)} + \frac{2\pi^2 N^{\frac{3}{2}}}{63\zeta(3)} + O(N \log N) = \frac{\pi^2}{18\zeta(3)} N^{3/2} + O(N \log N).$$

So we have proved (3.13).
The proof of (3.12) is similar. In fact, using the formula

$$|d|^{-\frac{1}{2}} h^+(d) \frac{2\pi}{w} = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-1}$$

where w has been defined in the previous chapter, we obtain

$$\sum_{\substack{d \leq N \\ -d \equiv r(mod4)}} d^{-\frac{1}{2}} h^+(-d) = \frac{\pi N}{24\zeta(3)} \left(1 + \frac{2r-1}{7}\right) + O(N^{\frac{1}{2}} \log N)$$

and so

$$\sum_{0 < -d < N} h^+(d) = \frac{\pi}{18\zeta(3)} N^{3/2} + O(N \log N).$$

□

Remark 3.1. *We remark that we obtain similar results for the wide definition of equivalence, using the relationship* $h^+(d) \log \eta^+ = 2h(d) \log \eta$.

Another fundamental result about the mean value of $h(d)$ is given by the following theorem [1]:

Theorem 3.3. *If $d < 0$,*

$$\sum_{0<-d\leq N}{}^{'} \frac{h(d)}{\sqrt{|d|}} = \frac{N}{2\pi}C + O(N^{3/4}\log N),$$

and

if $d > 0$

$$\sum_{0<d\leq N}{}^{'} \frac{h(d)\log\epsilon}{\sqrt{d}} = \frac{N}{4}C + O(N^{3/4}\log N)$$

where

$$C = \prod_p \left(1 - \frac{1}{p^2(p+1)}\right)$$

and $\sum'$ means that the summation is over the fundamental discriminants.

Proof. We will prove only the case $d > 0$ because the prove of the case $d < 0$ is similar. Since $h(d) = \frac{d^{1/2}}{\log\eta}L(1,\chi)$ and from Lemma 3.1, we have

$$h(d)\log\eta = \sum_{n=1}^{N} \frac{\chi(n)}{n} + O\left(\frac{|d|^{1/2}\log|d|}{N}\right). \tag{3.26}$$

We sum (3.26) over all fundamental discriminants; so we obtain

$$\sum_{\substack{0<d\leq N;\\ d \text{ fund.}}} \log\eta h(d) = \sum_{\substack{0<d\leq N;\\ d \text{ fund.}}} \sum_{n=1}^{N} \frac{\chi(n)}{n} + O\left(\sum_{0<d\leq N} \frac{|d|^{1/2}\log|d|}{N}\right), \tag{3.27}$$

and so

$$\sum_{\substack{0<d\leq N;\\ d \text{ fund.}}} \log\eta h(d) = \sum_{n=1}^{N} \frac{1}{n} \sum_{\substack{0<d\leq N;\\ d \text{ fund.}}} \left(\frac{d}{n}\right) + O\left(N^{1/2}\log N\right). \tag{3.28}$$

Now we denote

$$S(n) = \sum_{\substack{0<d\leq N;\\ d \text{ fund.}}} \left(\frac{d}{n}\right). \tag{3.29}$$

We recall that d is a fundamental discriminant if $d \neq 0, 1$ and

$$d = \begin{cases} \text{m} & \text{if } m \equiv 1(\mod 4) \\ \text{4m} & \text{if } m \equiv 2, 3(\mod 4) \end{cases},$$

for some squarefree integer m. So we have

$$\begin{aligned} S(n) = & \sum_{\substack{0<d\leq N; \\ d\equiv 1(\mod 4); \\ d \text{ fund.}}} \left(\frac{d}{n}\right) + \sum_{\substack{0<d\leq N; \\ d/4\equiv 2(\mod 4); \\ d \text{ fund.}}} \left(\frac{d}{n}\right) \\ & + \sum_{\substack{0<d\leq N; \\ d/4\equiv 3(\mod 4); \\ \text{d fund.}}} \left(\frac{d}{n}\right) \\ & = S_1(n) + S_2(n) + S_3(n). \end{aligned} \tag{3.30}$$

Since d is square-free, we have

$$\sum_{\substack{0<d\leq N; \\ d\equiv 1(\mod 4)}} \left(\frac{d}{n}\right) \mu^2(d),$$

where $\mu(d)$ is the Mӧbius function. Moreover we can write

$$\mu^2(d) = \sum_{l^2|d} \mu(l)$$

and so, if we put $d = l^2 k$,

$$S_1(n) = \sum_{\substack{0<l^2k\leq N; \\ l^2k\equiv 1(\mod 4)}} \left(\frac{l^2 k}{n}\right) \mu(l). \tag{3.31}$$

Now we observe that the condition $l^2 k \equiv 1(\text{mod}4)$ forces l to be odd, that means $l^2 \equiv 1(\text{mod}4)$, and so we have

$$\begin{aligned} S_1(n) = & \sum_{\substack{0<l^2k\leq N; \\ k\equiv 1(\mod 4); \\ (l,n)=(l,2)=1}} \left(\frac{k}{n}\right) \mu(l) \\ = & \sum_{\substack{0<l\leq\sqrt{N}; \\ (l,2n)=1}} \mu(l) \sum_{\substack{0<k\leq N/l^2; \\ k\equiv 1(\mod 4)}} \left(\frac{k}{n}\right). \end{aligned} \tag{3.32}$$

Using the same method, we have

$$S_2(n) = \left(\frac{4}{n}\right) \sum_{\substack{0<l\leq\sqrt{N}/2; \\ (l,2n)=1}} \mu(l) \sum_{\substack{0<k\leq N/4l^2; \\ k\equiv 2(\bmod 4)}} \left(\frac{k}{n}\right); \tag{3.33}$$

$$S_3(n) = \left(\frac{4}{n}\right) \sum_{\substack{0<l\leq\sqrt{N}/2; \\ (l,2n)=1}} \mu(l) \sum_{\substack{0<k\leq N/4l^2; \\ k\equiv 3(\bmod 4)}} \left(\frac{k}{n}\right). \tag{3.34}$$

Let

$$P(r,n,M) = \sum_{\substack{0<k\leq M; \\ k\equiv r(\bmod 4)}} \left(\frac{k}{n}\right).$$

We remark that when n is even, then $S_2(n) = S_3(n) = 0$. Now let us consider two cases: n square or not-square.

If n is not a square, from the properties of the Jacobi symbol, used also in the proof of Theorem 3.2, and also from Lemma 3.1, we obtain

$$P(r,n,M) = O(\min(n^{1/2}\log n, M)) \tag{3.35}$$

and

$$S(n) = O(N^{1/2}n^{1/4}\log^{1/2} n). \tag{3.36}$$

If n is a square $n = m^2$, we have

$$P(r,m^2,M) = \frac{\varphi(4m)M}{4m} + O(m),$$

when m is odd and

$$P(1,m^2,M) = \frac{\varphi(m)M}{2m} + O(m),$$

when m is even.

So, when n is odd, we can write

$$\begin{aligned} S(n) &= S_1(n) + S_2(n) + S_3(n) \\ &= \frac{\varphi(m)N}{8m} \sum_{\substack{0<l\leq\sqrt{N}/2; \\ (l,2n)=1}} \frac{\mu(l)}{l^2} + \frac{\varphi(m)N}{4m} \sum_{\substack{0<l\leq\sqrt{N}; \\ (l,2n)=1}} \frac{\mu(l)}{l^2} + O(m\sqrt{N}) \\ &= \frac{3\varphi(m)N}{8m} \sum_{\substack{l=1; \\ (l,2n)=1}}^{\infty} \frac{\mu(l)}{l^2} + O\left(\frac{\varphi(m)N}{m} \sum_{l>N} \frac{1}{l^2}\right) + O(m\sqrt{N}) \qquad (3.37) \\ &= \frac{3\varphi(m)N}{8m} \sum_{\substack{l=1; \\ (l,2m)=1}}^{\infty} \frac{\mu(l)}{l^2} + O(\sqrt{N}) + O(m\sqrt{N}), \end{aligned}$$

and, when n is even,

$$S(n) = \frac{\varphi(m)N}{2m} \sum_{\substack{l=1; \\ (l,m)=1}}^{\infty} \frac{\mu(l)}{l^2} + O(\sqrt{N}) + O(m\sqrt{N}). \qquad (3.38)$$

Using the properties of the Mӧbius function and recalling also that $\varphi(m) = m\prod_{p|m}(1-1/p)$, the sum in ??3.37) is

$$\begin{aligned} \sum_{\substack{l=1; \\ (l,2m)=1}}^{\infty} \frac{\mu(l)}{l^2} &= \prod_{p\nmid 2m}\left(1+\frac{\mu(p)}{p^2}\right) = \prod_{p}\left(1-\frac{1}{p^2}\right)\prod_{p|2m}\left(1-\frac{1}{p^2}\right)^{-1} \\ &= \frac{1}{\zeta(2)}\frac{4}{3}\prod_{p|m}\left(1-\frac{1}{p}\right)^{-1}\left(1+\frac{1}{p}\right)^{-1} \qquad (3.39) \\ &= \frac{4m}{3\zeta(2)\varphi(m)}g(m), \end{aligned}$$

where $g(m) = \prod_{p|m}(1+1/p)^{-1}$.

Moreover, by the same argument, we obtain

$$\sum_{\substack{l=1; \\ (l,m)=1}}^{\infty} \frac{\mu(l)}{l^2} = \frac{m}{\zeta(2)\varphi(m)}g(m). \qquad (3.40)$$

Therefore, from (3.37), (3.38), (3.39), it follows

$$S(n) = \frac{N}{2\zeta(2)}g(m) + O(\sqrt{N}) + O(m\sqrt{N}), \qquad (3.41)$$

where n is a square, $n = m^2$. Now, using (3.28), (3.41), (3.36), we can write

$$\begin{aligned}\sum_{\substack{0<d\le N;\\ d \text{ fund.}}} \log \eta h(d) &= \sum_{n=1}^{N} \frac{S(n)}{n} + O(N^{1/2}\log N)\\ &= \frac{N}{2\zeta(2)} \sum_{1\le m\le\sqrt{N}} \frac{g(m)}{m^2} + O(N^{3/4}\log N)\end{aligned} \tag{3.42}$$

Moreover we observe that

$$g(m) = \prod_{p|m}\left(1+\frac{1}{p}\right)^{-1} = \prod_{p|m}\left(1-\frac{1}{p+1}\right)$$

and that $g(m)$ is a multiplicative function.
Therefore

$$\begin{aligned}\frac{1}{\zeta(2)}\sum_{m=1}\frac{g(m)}{m^2} &= \frac{1}{\zeta(2)}\prod_p\left(1+\sum_{r=1}^{\infty}\frac{g(p^r)}{p^{2r}}\right)\\ &= \frac{1}{\zeta(2)}\prod_p\left(1+\left(1-\frac{p}{p+1}\right)\sum_{r=1}^{\infty}\frac{1}{p^{2r}}\right)\\ &= \prod_p\left(1-\frac{1}{p^2(p+1)}\right)\end{aligned} \tag{3.43}$$

and we can conclude that

$$\sum_{\substack{0<d\le N;\\ d \text{ fund.}}} \log \eta h(d) = \frac{N}{2}\prod_p\left(1-\frac{1}{p^2(p+1)}\right) + O(N^{3/4}\log N).$$

□

From Theorem 3.3, since $\sum'_{0<-d<N} 1 \sim (3\pi^2)N \sim \sum'_{0<d<N} 1$, where $\sum'$, as defined before, is the sum over the fundamental discriminants, we have the following mean value results:

$$\lim_{N\to\infty}\frac{\sum'_{0<-d<N}(h(d)/\sqrt{-d})}{\#\{0<-d<N\}} = \frac{\pi c}{6},$$

$$\lim_{N\to\infty}\frac{\sum'_{0<d<N}((h(d)\log\eta)/\sqrt{d})}{\#\{0<d<N\}} = \frac{\pi^2 c}{12}$$

where

$$c = \prod_p\left(1-\frac{1}{p^2(p+1)}\right).$$

3.2.3 Estimates of $L(1, \chi_d)$

The problem to determine the distribution of values of $L(1, \chi_d)$ as d varies over all fundamental discriminants with $|d| \leq N$ has also interested mathematicians for a long time.

Under the generalized Riemann hypotesis, in 1928, **Littlewood** showed that

$$\left(\frac{1}{2} + o(1)\right) \frac{\zeta(2)}{e^{\gamma} \log \log d} \leq L(1, \chi_d) \leq (2 + o(1))\, e^{\gamma} \log \log d,$$

where γ is Euler's constant. In 1949, **Chowla** proved the following inequalities:

$$L(1, \chi_d) \leq (1 + o(1))\, \frac{\zeta(2)}{e^{\gamma} \log \log d}$$
$$L(1, \chi_d) \geq (1 + o(1))\, e^{\gamma} \log \log d.$$

Thus, those results showed a discrepancy between the extreme values taken by $L(1, \chi_d)$ and the conditional bounds on these extreme values. To study this question, **Montgomery** and **Vaughan** [30], in 1999, introduced a probabilistic model to predict precisely the frequencies by which some extreme values of $L(1, \chi_d)$ occur.

In 2003 **Granville** and **Soundararajan** [24] proved a part of the conjectures of Montgomery and Vaughan and obtained that the behavior of the extreme values of $L(1, \chi_d)$ is just that described by the results of Chowla. Granville and Soundararajan used a simple probabilistic model. They considered, for primes p, the independent random variables $X(p)$ taking the following values:

$$\begin{cases} 1 & \text{with probability } p/(2(p+1)) \\ 0 & \text{with probability } 1/(p+1) \\ \text{-1} & \text{with probability } p/(2(p+1)) \end{cases}$$

and they extended X to all integers n as $X(n) = \prod_{p^{\alpha} || n} X^{\alpha}(p)$. So they compared the distribution of values of $L(1, \chi_d)$ to the distribution of the "random Euler products" $L(1, X) = \prod_p (1 - X(p)/p)^{-1}$. The fundamental unconditional result which they obtained was the existence of infinitely many

d such that $L(1, \chi_d)$ is as large as

$$e^{\gamma}(\log\log d + \log\log\log d + c^{'} + o(1)),$$

where $c^{'}$ is a calculable constant.

3.2.4 Cohen-Lenstra Heuristics

In 1984, **H. Cohen** and **H. W. Lenstra** [9] devepoled some conjectures about the behavior of the class-number and the class-group that are very important because of the existence of very few theorems about them. Those conjectures were based on a large number of observations and on solid heuristic grounds. Many results have been confirmed by numerical evidence and some of them have been proved in recent years by other means.

At first we consider the case of imaginary quadratic fields.
We denote by $\widetilde{H}_d$ the odd part of the class-group, which is the subgroup of all elements in the class group H_d with odd order.

Conjecture 3.1. *Let d be a negative fundamental discriminant. For any odd prime p let $\eta(p) = \prod_{k=1}^{\infty}\left(1 - \frac{1}{p^k}\right)$ and let $C = \prod_{j=2}^{\infty}\zeta(j)$.*

1. *The probability that $\widetilde{H}_d$ is cyclic is equal to*

$$\frac{\pi^2\zeta(3)}{18\zeta(6)C\eta(2)} = 0.9775748102...$$

2. *If p is an odd prime, the probability that p divides h_d is equal to*

$$f(p) = 1 - \eta(p);$$

for example $f(3) \approx 0.439873$, $f(5) \approx 0.239667$ and $f(7) \approx 0.163204$.

3. *If p is an odd prime, the probability that the p-Sylow[3] subgroup of H_d is isomorphic to a given finite Abelian p-group G is equal to $\eta(p)/|Aut(G)|$, where $Aut(G)$ is the group of automorphism of G.*

[3] The p-Sylow subgroup of a finite abelian group G is a p-subgroup with the property that its order is the maximal power that divides |G|.

4. *If p is an odd prime, the probability that the p-Sylow subgroup of H_d has rank r (i.e. is isomorphic to a product of r cyclic groups) is equal to $p^{-r^2}\eta(p)/((p)_r)^2$, where $(p)_r := \prod_{k=1}^{r}\left(1 - \frac{1}{p^k}\right)$.*

The situation for real quadratic fields is more complicated because we know even less about them than about imaginary quadratic fields. However we can state the following:

Conjecture 3.2. *Let d a positive fundamental discriminant.*

1. *If p is an odd prime, the probability that p divides h_d is equal to*

$$1 - \frac{\eta(p)}{1 - 1/p}.$$

2. *The probability that $\widetilde{H}_d$ is isomorphic to a given finite abelian group G of odd order g is equal to*

$$1/(2g\eta(2)C|Aut(G)|).$$

3. *If p is an odd prime, the probability that the p-Sylow subgroup of H_d has rank r is equal to*

$$p^{-r(r+1)}\eta(p)/((p)_r(p)_{r+1}).$$

4.
$$\sum_{\substack{p \leq x \\ p \equiv 1 (mod 4)}} h(p) \sim \frac{x}{8}.$$

We notice that those conjectures explain the experimental observation that 3/4 of real quadratic fields have a class- number equal to one.

Chapter 4

Computing the Class Number and the structure of the Class Group

In the previous chapters we gave the definition of the Class Number, we found an analytic formula for computing it and we studied its main properties using the theory of binary quadratic forms and the theory of ideals in quadratic fields.

Now we turn our attention to the computational problem. It means that we are going to study the algorithms which allows us to compute efficiently the Class Number and the structure of the Class Group. It is important to recall that, by the Correspondence Theorem stated in the second chapter, computing on binary quadratic forms or computing on ideals is the same thing. However we are going to use usually ideals to state theory before the construction of the algorithms and quadratic forms for pratical computation. We are going to study in details only the case of class numbers of imaginary quadratic fields. In particular we are going to describe Shanks' baby-step giant-step method, since it was the first efficient method found, and we are going to talk about its the improvements until the last results. For every algorithm we will propose a pseudocode and the analysis of its complexity.

4.1 Computing Class Number counting reduced forms.

In the first chapter we defined (Definition 1.2) an equivalence relation on the set of all quadratic forms and the Class Number as the number of corresponding equivalence classes of forms with a fixed discriminant D.
Two forms F and G are said to be equivalent if there are r, s, t and $u \in \mathbb{Z}$, for which $ru - st = 1$, such that

$$x = rX + sY, y = tX + uY$$

and $F(X, Y) = G(x, y)$.
Let's also recall the definition of reduced form.

Definition 4.1. *A positive definite quadratic form $\{a, b, c\}$ of discriminant D is said to be reduced if $|b| \leq a \leq c$ and if, either $|b| = a$ or $a = c$, then $b \geq 0$.*

From Theorem 1.2 of Chapter 1, we have that every class of positive defined quadratic forms of discriminant $D < 0$ contains exactly one reduced form. Moreover $h(D)$ is equal to the number of primitive reduced forms of discriminant D, where we recall that a form $\{a, b, c\}$ is said to be primitive if $(a, b, c) = 1$.
The following lemma allows us to count the number of reduced positive defined forms with a fixed negative discriminant D:

Lemma 4.1. *Let $F = \{a, b, c\}$ a positive defined quadratic form of discriminant $D < 0$.*

1. *if F is reduced, we have*

$$a \leq \sqrt{|D|/3};$$

2. *if*

$$a < \sqrt{|D|/4} \textit{ and } -a < b \leq a$$

then F is reduced.

The proof of this lemma follows from the proof of Theorem 1.3 of the first chapter.
A consequence of this result is that we can compute the Class Number of an imaginary quadratic field by counting reduced forms of discriminant D, using the inequalities $|b| \leq a \leq \sqrt{|D|/3}$.
Using these results, we can build an algorithm to compute Class Number of an imaginary quadratic field of discriminant D. We remark that the following algorithm computes the Class Number when D is a fundamental discriminant, but it can be extended to non-fundamental discriminants because we can write every discriminant D as $D = D_0 f^2$, where D_0 is a fundamental discriminant [10].

REDUCED-FORMS(D)
Input: a fundamental negative discriminant D.
Output: the Class Number $h(D)$.

```
if D $\equiv 0 (\mathrm{mod} 4)$;
    set $b = 0$;
else;
    set $b = 1$;
set $B = \sqrt{|D|/3}$;
set $k = 1$;
do ;
```

```
        set h=COUNT($b$, $D$, $k$);
        $b=b+2$;
        $k=h$;
while $b \leq B$;
 $j=k$;
 return $j$.
```

Let's now describe the subalgorithm COUNT.

COUNT(b, D, k)

```
set $h=k$;
set $q=(b^2-D)/4$;
set $a=b$;
if $a>1$;
    do;
        if $q$ divides $a$;
            if $a=b$ or $b=0$ or $a^2=q$;
                set $h=h+1$;
            else;
                set $h=h+2$ ;
            $a=a+1$;
        else;
            set $a=a+1$;
    while $a^2 \leq q$;
else;
    set $a = 2$;
    while $a^2 \leq q$;
        if $q$ divides $a$;
            if $a = b$ or $b = 0$ or $a^2 = q$;
                set $h = h + 1$;
            else;
                set $h = h + 2$ ;
            $a = a + 1$;
        else;
            set $a = a + 1$;
return $h$.
```

4.1.1 The complexity of the algorithm REDUCED-FORMS.

The complexity of REDUCED-FORMS equals the complexity of the subalgorithm COUNT times the number of its iterations .

In COUNT we have a loop on a which is executed only when $a^2 \leq q$ and $b \leq B$, so its complexity is

$$O\left(\left\lfloor\sqrt{(b^2 - D)/4}\right\rfloor\right) = O\left(\left\lfloor\sqrt{|D|}\right\rfloor\right).$$

COUNT is executed when $b \leq B$ and at every step b becomes $b + 2$; so the complexity of REDUCED-FORMS is

$$O\left(\left\lfloor\sqrt{|D|}\right\rfloor \left\lfloor\sqrt{|D|}\right\rfloor\right) = O\left(|D|\right).$$

This method is useful for making tables of Class Number of imaginary quadratic fields up to a fixed discriminant bound, but it becomes very slow for large discriminants. Moreover it does not give information about the structure of the Class Group.

4.2 Analytic Formulas to compute Class Number

Another method to compute Class Number is based on the analytic formula proved in the first chapter and on the functional equation of the L functions which is proved in the book of H. Davenport [21].
We recall that, when D is a negative discriminant and $D < -4$,

$$h(D) = \frac{\sqrt{|D|}L_D(1)}{\pi}, \tag{4.1}$$

where

$$L_D(1) = \sum_{n \geq 1} \frac{1}{n} \left(\frac{D}{n} \right).$$

Moreover, since the Kronecker Symbol $\left(\frac{D}{n}\right)$ is a character modulo D and $\left(\frac{D}{-1}\right) = -1$, we have the following functional equation of $L_D(1)$

$$\begin{aligned} \pi^{-1}|D|L(1) &= \frac{1}{2}\int_1^\infty \sum_{-\infty}^{\infty} n \left(\frac{D}{n}\right) e^{-\frac{n^2\pi x}{D}} dx \\ &+ \frac{1}{2}\int_1^\infty \sum_{-\infty}^{\infty} n \left(\frac{D}{n}\right) e^{-\frac{n^2\pi x}{D}} x^{-1/2} dx. \end{aligned} \tag{4.2}$$

Using this equation we can obtain an efficient formula to compute Class Number [15].

Proposition 4.1. *Let $D < -4$ be a fundamental discriminant. Then*

$$h(D) = \sum_{n \geq 1} \left(\frac{D}{n}\right) \left(\operatorname{erfc}\left(n\sqrt{\frac{\pi}{|D|}} \right) + \frac{|D|}{n\pi} e^{\frac{-\pi n^2}{|D|}} \right)$$

where

$$\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2} dt$$

is the **Error Complementary Function.**

Proof. From the equation (4.2) we have

$$\begin{aligned} L_D(1) = \frac{\pi}{2|D|} \int_1^\infty \sum_{-\infty}^{\infty} n \left(\frac{D}{n}\right) e^{\frac{-n^2\pi x}{D}} dx \\ + \frac{1}{2} \int_1^\infty \sum_{-\infty}^{\infty} n \left(\frac{D}{n}\right) e^{\frac{-n^2\pi x}{D}} x^{-\frac{1}{2}} dx. \end{aligned} \tag{4.3}$$

Since we have the uniform convergence of the series $\sum_{-\infty}^{\infty} n \left(\frac{D}{n}\right) e^{\frac{-n^2\pi x}{D}}$, we can exchange the series and the integral and so we obtain

$$\begin{aligned} L_D(1) &= \frac{\pi}{2|D|} \sum_{-\infty}^{\infty} n \left(\frac{D}{n}\right) \int_1^\infty e^{\frac{-n^2\pi x}{D}} dx \\ &+ \frac{1}{2} \sum_{-\infty}^{\infty} n \left(\frac{D}{n}\right) \int_1^\infty e^{\frac{-n^2\pi x}{D}} x^{-\frac{1}{2}} dx \\ &= \frac{\pi}{2|D|} \sum_{-\infty}^{\infty} n \left(\frac{D}{n}\right) \frac{D}{n^2\pi} e^{-\frac{n^2\pi}{D}} \\ &+ \frac{\pi}{2|D|} \sum_{-\infty}^{\infty} n \left(\frac{D}{n}\right) 2 \int_{n\sqrt{\frac{\pi}{|D|}}}^\infty e^{-t^2} \sqrt{\frac{|D|}{\pi}} \frac{1}{n} dt \\ &= \sum_{n\geq 1} \frac{1}{n} \left(\frac{D}{n}\right) e^{-\frac{n^2\pi x}{D}} + 2\sqrt{\frac{\pi}{|D|}} \sum_{n\geq 1} \left(\frac{D}{n}\right) \int_{n\sqrt{\frac{\pi}{|D|}}}^\infty e^{-t^2} dt, \end{aligned} \tag{4.4}$$

where we have used the substitution $\frac{n^2\pi x}{D} = t^2$, in the integral, and the fact that $\sum_{-\infty}^{\infty} \frac{1}{n} \left(\frac{D}{n}\right) = 2\sum_{n\geq 1}^{\infty} \frac{1}{n} \left(\frac{D}{n}\right)$. So from (4.1) and (4.4) we obtain

$$h(D) = \sum_{n\geq 1} \left(\frac{D}{n}\right) \left(\operatorname{erfc}\left(n\sqrt{\frac{\pi}{|D|}}\right) + \frac{|D|}{n\pi} e^{\frac{-\pi n^2}{|D|}}\right).$$

□

In order to compute the function erfc(x) we can use this proposition.

Proposition 4.2. *We have*

$$\operatorname{erfc}(x) = 1 - \frac{2}{\sqrt{\pi}} \sum_{k \geq 0} (-1)^k \frac{x^{2k+1}}{k!(2k+1)}$$

when $x \leq 2$ and

$$\operatorname{erfc}(x) = \frac{e^{-x^2}}{x\sqrt{\pi}} \left(1 - \cfrac{1/2}{2 + X - \cfrac{1 \cdot 3/2}{4 + X - \cfrac{2 \cdot 5/2}{6 + X - \ddots}}} \right),$$

where $X = x^2 - 1/2$, when $x \geq 2$.

So we can compute Class Number using the series of Proposition 4.1 as shows the following result.

Corollary 4.1. *$h(D)$ is the closest integer to the n-th partial sum of the series of Proposition 4.1 where*

$$n = \left\lfloor \sqrt{|D| \log |D| / (2\pi)} \right\rfloor .$$

The running time of this method is $O\left(|D|^{1/2+\epsilon}\right)$ $\forall \epsilon > 0$, however with a large constant O.

4.3 Shanks's Baby Step Giant Step Algorithm

In 1968, Shanks [11] found a method to compute the order of an element g of an abelian finite group G. This method can be modified to obtain the order of the group G and its structure and so it can be used to compute the Class Number of a quadratic field and the structure of the Class Group.
It is based on the representation of a finite abelian group G via generators and relations.
Such description allows us to obtain the structure of G by manipuling particular matrices. In the sections first we describe the method applied to a general finite abelian group and then we use it in the case of the Class Group.

4.3.1 Computing the order of an element

Let us describe Shanks's algorithm to compute the order n of an element g of the group, when an upper bound B for such a order is known [34]. We can proceed in the following way.

We denote $q = \left\lceil \sqrt{B} \right\rceil$. We compute g^r where $0 \leq r < q$ (these are called **baby steps**) and we record these elements in a sorted list. We set $g_1 = g^{-q}$; we compute g_1^a for all $0 \leq a < q$ (these are called **giant steps**) and we search for it in the previous list; if it is found we have $g^{aq+r} = 1$. This means that $aq + r$ is a multiple of n; so by the factorization of $aq + r$ (we suppose this number is of factorable size) and, by using basic properties, we obtain the order of g.

We can improve this algorithm if we know also a lower bound C of n. In this case, in fact, we can reduce the number of the giant steps by starting the list with g^C instead of g^0 and we can set $q = \left\lceil \sqrt{B - C} \right\rceil$.

A pseudocode for the algorithm is the following.

BABY-STEP GIANT-STEP$(g,\ B,\ C)$

Input: B and C such that $B/2 < C \leq n \leq B$.

Output: the order n.

```
Set $q = \lceil \sqrt{B - C} \rceil$;
for $0 \leq r < q$;
    compute baby step $g^r$;
    store $(g^r, r)$ in a sorted list;
for $0 \leq a \leq q$;
    compute giant step $g^{-C-aq}$;
    search for this element in the list $(g^r, r)$;
    if $g^{-C-aq} = g^r$;
    set $n = C + aq + r$;
factorize $n$;
while $p$ is a prime which divides $n$;
    compute $g^{n/p}$;
    if $g^{n/p} = 1$;
        $n = n/p$;
return $n$.
```

Let us now discuss the computational cost of this method.
We need to execute the following computations : q baby steps, $\lfloor (n-C)/q \rfloor + 1$ giant steps. Moreover we need to precompute g^{-C} and we need to store q pairs (g^j, j). So, if we sort the list with a $O(q \log q)$ sorting method, the search in the sorted list takes only $O(\log q)$ operations and so the total computational time is $O(q \log q)$.

4.3.2 Computing order and structure of the group

Before explaining the algorithm to compute the order and the structure of the group G, let briefly present the theory used to describe the group structure. More details can be found in the papers by [31] and [8].

Generators and relations

At first we recall that every finite abelian group G is said to be finitely generated if there exist finitely many elements $g_1, \dots, g_k$ such that $g \in G$ can be written in the form $g = \prod_{i=1}^{k} g_i^{\alpha_i}$ with integers $\alpha_1, \dots, \alpha_k$.
$\{g_1, \dots, g_k\}$ is said a **generating set** of G.
Moreover let also recall **the fundamental theorem of finitely generated abelian groups**.

Theorem 4.1. *Every finitely generated abelian group G is isomorphic to a direct sum of primary cyclic groups and infinite cyclic groups; where a primary cyclic group is one whose order is a power of a prime. Hence every such a group is isomorphic to one of the form*

$$\mathbb{Z}^n \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$$

where $n \geq 0$ and the numbers $m_1, \ldots, m_t$ are (not necessarily distinct) powers of prime numbers.The values of n, $m_1, \ldots, m_t$ are (up to their order) uniquely determined by G. In particular, G is finite if and only if $n = 0$.

We remark that, since $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to the direct product of $\mathbb{Z}/j\mathbb{Z}$ and $\mathbb{Z}/k\mathbb{Z}$ if and only if j and k are coprime and $m = jk$, we can also write any abelian group G as a direct product of the form

$$\mathbb{Z}^n \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}$$

where $d_i | d_{i+1}$ for all $i = 1 \ldots, s-1$. The numbers n and $d_1, \ldots, d_s$ are uniquely determined by G and they are called the **invariants** of G.
So the problem of the determining the group structure is equivalent to compute the invariants $d_1, \ldots, d_s$ of G.
In order to solve this problem, we use the existence of relations among the elements of a generating system and we suppose that G is finite so that $n = 0$. Let $g_1, \ldots, g_r$ be a generating system of G. Since a finite abelian group is a $\mathbb{Z}$-module, we can consider a surjective $\mathbb{Z}$-module homomorphism

$$\varphi : \mathbb{Z}^r \longrightarrow G$$

such that

$$(\rho_1, \ldots \rho_r) \longrightarrow \prod_{i=1}^{r} g_i^{\rho_i}.$$

Let K be the kernel of φ. We have, from the fundamental theorem on homomorphisms, that $G \cong \mathbb{Z}^r/K$.
If $(\rho_1, \ldots \rho_r)$ is an element of K we have $\prod_{i=1}^{r} g_i^{\rho_i} = 1$; this means that an element of K allows us to write a relation among the generators $g_1, \ldots, g_r$.

So K is called **the relation submodule** of $\mathbb{Z}^r$ relative to the generators $g_1, \ldots, g_r$. Since K is finitely generated (being a submodule of $\mathbb{Z}_n$), it admits a generating system. So every element of this system can be seen as a column of a matrix which we denote as $A = (a_{ij})$. This matrix has coefficients in $\mathbb{Z}$ and is called **the relation matrix** for G. It depends on the generating sets for G and K and also on the order of the elements in these sets.
Generating sets of the group G and of the relation submodule K are not uniquely defined. Elementary row and column operations on A correspond to changes of the set of generators.
The construction of the matrix A allows us to find the structure of G as shows the following proposition:

Proposition 4.3. *Let A be a relation matrix for a finite abelian group G. If there are invertible matrices P and Q for which*

$$PAQ = \begin{pmatrix} a_1 & 0 & \ldots & & \\ 0 & a_2 & 0 & \ldots \\ \vdots & & \ddots & \\ & & & a_n \\ 0 & \ldots & & \end{pmatrix}$$

is a diagonal matrix and $a_1, \ldots, a_n \in \mathbb{Z}$, then $G \cong \mathbb{Z}/\langle a_1 \rangle \oplus \cdots \oplus \mathbb{Z}/\langle a_n \rangle$.

However in our algorithm we will obtain the structure of the group by computing the **Smith Normal Form** of the matrix A.
We recall that a matrix A is in Smith Normal Form if there are nonzero integers $a_1, \ldots, a_n$ such that a_i divides a_{i+1} for each $i < m$, and for which

$$A = \begin{pmatrix} a_1 & & & & & \\ & \ddots & & & & \\ & & a_m & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

An important result is that every matrix with integer coefficients has a Smith normal form and it is possible to write an algorithm to compute it. This algorithm can be found in the book of H.Cohen [12].
A consequence is the following proposition which we are going to use in our algorithm.

Proposition 4.4. *Let A be a relation matrix for a finite abelian group. Let D be the Smith normal form of A, with $D = \operatorname{diag}(d_1, \ldots, d_k, 1, \ldots, 1)$. Let $D = PAQ$ with P, Q invertible matrices. Then the following are true.*

1. *The order of G is $|\det A|$.*
2. *The invariants of G are $d_1, \ldots, d_k$.*

In our algorithm we proceed as follows: at every step we find a minimal relation among some given elements $g_1, g_2, \ldots, g_r$ of the group. At the end of the process this allows us to obtain the order of the group and a relation matrix. Then we compute the Smith normal form of that matrix and so we obtain also the structure of the group.

Description of the algorithm

Let us now describe the modification of Shanks's algorithm to compute the order of the group and its structure.
Suppose that we know an upper bound B of the order h of G. The idea is to find relations $\prod_i g_i^{a_i}$ with $0 \leq a_i < B_i$ between given elements of the group $g_1, \ldots, g_r$. The bounds $B_1, \ldots, B_r$ are a subproduct of the algorithm and they verify $B = B_1 \geq \cdots \geq B_r \geq h$.
The sequence of bounds is constructed inductively as follows.
At first set $B_1 = B$ and choose one element g_1 at random.
At step 1 we compute the order of g_1 which we denote as n_1. Then, at step 2, we consider an other element g_2 and we work with g_1, g_2 and with the quotient group $G_2 = G/\langle g_1 \rangle$. The new bound is $B_2 = B_1/n_1$ and, at the end

of this step, we compute the order n_2 of $g_2\langle g_1\rangle$ in G_2. This is equivalent to a relation between g_1 and g_2.

At the step i we work with the elements $g_1,\dots,g_i$, with the group $G_i = G/\langle g_1,\dots,g_{i-1}\rangle$ and we will set $B_i = B_1/(\prod_{k=1}^{i-1} n_k)$; in this case we obtain the order of g_i in G_i and therefore a relation between the elements $g_1,\dots g_i$.

At the end of the algorithm (where the criterion on where to stop will be describe below) we obtain the order h of the group G as $h = \prod_i n_i$ and relations which we use to compute the structure of the group.

We are going to describe how it is possible to determine at every step minimal relations between given elements of the group.

Suppose, for example, that at step i of the algorithm we want to determine a minimal relation for the elements $g_1,\dots,g_{i-1},g_i$. We know, from the previous steps, that $B_i = B_1/(\prod_{j=1}^{i-1} n_j)$.

1. For each baby-step g_i^k with $1 \leq k \leq \left\lceil\sqrt{B_{i-1}}\right\rceil$, we compute every element
$$\prod_{j=1}^{i} g_j^{-a_j} g_i^k$$
with $0 \leq a_j \leq \left\lceil\sqrt{n_j}\right\rceil$ and we check if it is equal to 1_G; if it is , we have found the minimal relation $(a_1,\dots,a_{i-1},k)$. If not, we sort these elements in a list.

2. For each giant-step $g_i^{l\left\lceil\sqrt{B_{i-1}}\right\rceil}$ with $2 \leq l \leq \left\lfloor\sqrt{B_{i-1}}\right\rfloor + 1$ we compute every element
$$g_i^{l\left\lceil\sqrt{B_{i-1}}\right\rceil}\prod_{j=1}^{i} {g_j}^{q_j\left\lceil\sqrt{n_j}\right\rceil}$$
with $1 \leq\ q_j \leq \left\lceil\sqrt{n_j}\right\rceil + 1$ and we check if it is equal to 1_G (in this case we have found the minimal relation). If not, we search for it in the above list; if it is found, the minimal relation is
$$\left(q_1\cdot\lceil\sqrt{n_1}\rceil - a_1,\dots,q_{i-1}\cdot\lceil\sqrt{n_{i-1}}\rceil - a_{i-1}, l\cdot\left\lceil\sqrt{B_{i-1}}\right\rceil - k\right).$$

By this algorithm we can compute also the structure of G by computing the Smith Normal Form of the matrix whose columns are the relations above obtained.

As we have remarked about the computation of the order of an element g, if we know also a lower bound on the order of the group G we can improve the algorithm.

Moreover the correctness of the result depends on the correctness of the bounds which we know. That means that we have a probabilistic algorithm. If, for example, we know that $B/2 < C \leq h \leq B$, we can give an easy criterion on where to stop.

That is $h \geq C$. In fact, if we have a multiple of h larger than h, i.e. αh with $\alpha \geq 2$, it would be $h/\alpha \geq C > B/2$, that is $h > B$.

Pseudocode of the algorithm

Now let us give the pseudocode of the discussed above algorithm.

We will call it `STRUCTURE-ORDER`.

Let us suppose to be able to compute in the group G and we denote by $\cdot$ the operation in G and by 1 the identity element of G.

In order to obtain the columns of the relation matrix, we must keep track of all the exponents of the elements obtained during every step of the computation. So we will use the two subsets S and L (respectively for the baby steps and for the giant steps) of the group G which are constructed, at every step, as a list of lists.

The elements of L and S, in fact, are composed of four fields; two fields "info" in which we store the found element and its exponent, so those fields will be denoted as "element" and "exponent"; and two fields "next", i.e. two pointers, one at the next element and one at another list constructed at the next step. For example we explain as we act for the list S.

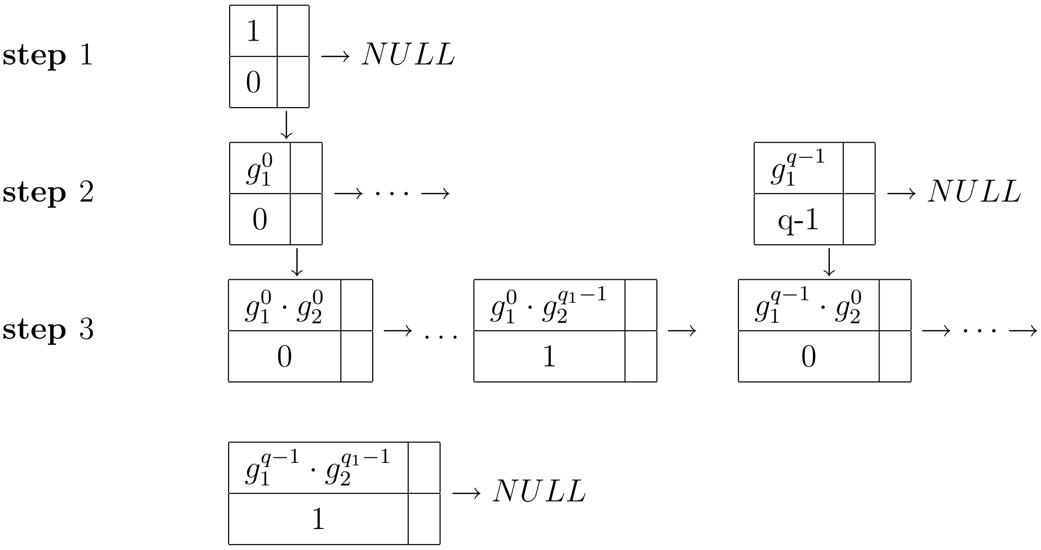
At first this list is composed of only one element with 1 in the field "element", 0 in the field "exponent" and two pointers at NULL.

During the step 1, we compute, for the chosen element g_1, g_1^r for each $0 \leq r \leq q-1$ with $q = \lceil\sqrt{B-C}\rceil$, and we construct a new list whose elements have $1 \cdot g^r$ in the field "element" and r in the field "exponent". So we modify the list S by the construction of a pointer from its element to the new list .

In the next step, for a new element g_2, we compute g_2^s for each $0 \leq s < q_1$ with $q_1 = \lceil\sqrt{n_1}\rceil$ and we modify again S by the construction of a pointer from each element g_1^r to a new list whose elements have $g_2^s \cdot g_1^r$ in the field "element" and s in the field "exponent".

So, when in our algorithm a relation is found, we can obtain its elements, going up again to the fields "exponent" of the lists S and L.

Moreover, at every step i of the algorithm, $S \cdot L$ represents the subgroup $\langle g_1, \ldots, g_{i-1}\rangle$.



STRUCTURE-ORDER$(B,\ C)$

Input: B and C such that $B/2 < C \leq h \leq B$.

Output: the order h of the group and the invariants.

```
1. set $h = 1$, $C_1 = C$, $B_1 = B$, $S = \{1\}$, $L = \{1\}$, $n = 0$, $i = 1$;

2. choose a random $g$ in $G$;
```

```
set $A$ as a matrix of order $\log_2 B$ with zero-elements;
while $h < C$;
    SHANKS( $B_1$, $C_1$, $S$, $L$, $h$, $A$);
    set $h = hn$;
    $i++$;
    set $B_1 = \lfloor B_1/n \rfloor$, $C_1 = \lceil C_1/n \rceil$, $q = \lceil \sqrt{n} \rceil$, $S = \bigcup_{0 \le r < q} g^r \cdot S$,
     $y = g^q$, $L = \bigcup_{0 \le a \le q} y^a \cdot L$;
SMITH NORMAL FORM(A);
print A;
return $h$.
```

The main part of that algorithm is the sub-algorithm called SHANKS.

SHANKS(B_1, C_1, S, L, h, A, i)

```
set $q = \lceil \sqrt{B_1 - C_1} \rceil$;
set $x_0 = 1$, $x_1 = g^h$;
if $x_1 = 1$;
    set $n = 1$;
    set $n = hn$;
    set the $i$-th element of the $i$-th column of the matrix $A$
    equal to $n$;
    FACTOR($n$, $S$, $L$, $g$, $i$);
    return;
```

```
else;
    for $2 \leq r \leq q-1$;
        set $x_r = x_1 \cdot x_{r-1}$;
        compute the list of lists $S_{1,r} = x_r{\cdot}S$ in which we also
         store the exponents of all the elements used until now;
    for $0 \leq r < q$ compute the list $S_1 = \bigcup_{0 \leq r < q} S_{1,r}$ and sort
    $S_1$;
    if we find $1 \in S_{1,r}$ and $r > 0$ ;
        set $n = r$;
        go up again, from the element $1$, to the fields "exponent"
         of the list $S_{1,r}$ and set the found values in the i-th
         column of the matrix $A$;
        FACTOR($n$, $S$, $L$, $g$,$i$);
        return;
    else;
        $y = x_1 \cdot x_{q-1}$, $z = x_1^{C_1}$, $n = C_1$;
        GIANT-STEPS($L$, $S_1$, $n$, $z$);
            set $n = hn$;
            FACTOR($n$, $S$, $L$, $g$);
            return.
```

The sub-algorithm GIANT-STEPS can be constructed as follows.

GIANT-STEPS(L, S_1,n ,z, i)

```
for each element $w$ in the list $L$;
    set $z_1 = z \cdot w$;
    search for $z_1$ in the list $S_1$;
    if we find $z_1$ in $S_{1,r}$;
        set $n = n - r$;
        set $n = hn$;
        set the exponent of $z$ equal to $l$; go up again to the fields "exponent" of $L$ from $w$ and set the found values equal to $r_j$; go up again to the fields "exponent" of $S_{1,r}$ from $z_1$ and set the found values equal to $s_j$; set the elements of the $i$-th column of the matrix $A$ equal to $lr_j - s_j$
        return;
    else;
        $z = y \cdot z$;
        $n = n + q$;
        GIANT-STEPS($L$, $z$, $S_1$, $n$, $i$).
```

The subalgorithm FACTOR allows us to obtain the order of the element g module the subgroup $S \cdot L$.

FACTOR(n, S, L, g, i)

```
factorize $n$;
while $p$ divides $n$;
    compute $S_1 = g^{n/p} \cdot S$;
```

```
if exists $z$ such that $z$ is in $L$ and $z$ is in $S_1$;
    replace the elements of the $i$-th column of the matrix
   $A$ with the differences between the values obtained going
   up again to the fields "exponent" from $z_1$ in $L$ and those
   obtained going up to the fields "exponent" from $z_1$ in
   $S_1$.
    set $n = n/p$;
     FACTOR($n$, $S$, $L$, $g$, $i$);
else;
     return.
```

Let us now study the complexity of our algorithm.
We remark that in SHANKS the total number of group operations (baby steps, giant steps) is

$$O\left(\prod_{j=1}^{m}(\sqrt{n_j})q_m\right) = \left(\prod_{j=1}^{m}(\sqrt{n_j})\frac{q}{\sqrt{\prod_{j=1}^{m} n_j}}\right) = O\left(q\right)$$

where q_m is the value of q at step m, and the total number of arithmetical operations (sorting, searching, etc...) is $O\left(q \log q\right)$. Moreover the complexity of FACTOR is $O\left(q \log q\right)$; so the complexity of SHANKS is also $O\left(q \log q\right)$. This subalgorithm is performed for every new chosen element; so, since the worst situation happens when all the elements of G have order equal to a power of 2 and so the number of the used elements in the algorithm is $\log_2 h$, we have that the complexity of STRUCTURE-ORDER is $O\left(q \log^2(q)\right)$.

4.3.3 Shanks's method to compute Class Number

Let us now show to apply Shanks's method to the class group.
To apply the method is necessary to use bounds for the class number.
From the Theorem of Correspondence, stated in Chapter 2, we know that

the set of classes of quadratic forms is in a natural bijection with the class group; so we can give a group structure to classes of quadratic forms.
In order to work with classes of forms we will consider reduced forms and we are going to give an algorithm to find, given any quadratic form, the unique reduced form in its class. An operation between classes of forms, called **composition**, was introduced by Gauss in 1798.
The following definition of composition between two forms (representative of two classes) is deduced from the product of ideals, using the isomorphism of the Theorem of Correspondence.

Definition 4.2. *Let $f_1 = \{a_1, b_1, c_1\}$ and $f_2 = \{a_2, b_2, c_2\}$ be two quadratic forms with discrimininat D. Set $s = (b_1 + b_2)/2$, $n = (b_1 - b_2)/2$ and let u, v, w and d be such that*

$$ua_1 + va_2 + ws = d = (a_1, a_2, s),$$

and let $d_0 = (d, c_1, c_2, n)$. The composite of f_1 and f_2 is the form

$$\{a_3, b_3, c_3\} = \left(d_0 \frac{a_1 a_2}{d^2}, b_2 + \frac{2a_2}{d}(v(s - b_2) - wc_2), \frac{b_3^2 - D}{4a_3} \right).$$

It is possible to give an algorithm to find the composition of two given forms and so by this algorithm we are able to compute in the class group.

Algorithms for computation and reduction of positive definite forms

In Shanks's method to compute class number we are going to use the algorithms for reduction and composition of forms.
Let us now describe them.

REDUCTION`(f)`
Input: a positive definite form $f = \{a, b, c\}$ of negative discriminant D.
Output: the unique reduced form in the equivalence class of f.

1. if $-a < b \leq a$;

```
    while $a > c$;
        set $b = -b$;
        exchange $a$ and $c$;
        EUCLIDE($b$, $a$, $c$);
    if $a = c$ and $b < 0$;
        $b = -b$;
        return $\{a, b, c\}$;
else;
    EUCLIDE($b$, $a$, $c$);
    while $a > c$;
        set $b = -b$;
        exchange $a$ and $c$;
        EUCLIDE($b$, $a$, $c$);
  if $a = c$ and $b < 0$;
        $b = -b$;
        return $\{a, b, c\}$.
```

EUCLIDE(b, a, c)

```
find $q$ and $r$ such that $b = 2aq + r$ with $0 \leq r < 2a$;
if $r > a$;
    set $r = r - 2a$ and $q = q + 1$;
set $c = c - \frac{1}{2}(b + r)$ and $b = r$;
return.
```

COMPOSITION(f_1, f_2)
Input: two primitive positive defined quadratic forms $f_1 = \{a_1, b_1, c_1\}$ and $f_2 = \{a_2, b_2, c_2\}$ with discriminant D.
Output: the composite form $f_3 = \{a_3, b_3, c_3\}$.

```
if $a_1 > a_2$;
    exchange $f_1$ and $f_2$;
set $s = \frac{1}{2}(b_1 + b_2)$ and $n = b_2 - s$;
if $a_1$ divides $a_2$;
    set $y_1 = 0$ and $d = a_1$;
else;
    compute $u$ ,$v$ and $d$ such that $ua_2 + va_1 = d = gcd(a_2, a_1)$;
    set $y_1 = u$;
if $d$ divides $s$;
    set $y_2 = -1$, $x_2 = 0$ and $d_1 = d$;
else;
    compute $u$ ,$v$ and $d_1$ such that $us + vd = d_1 = gcd(s, d)$;
    set $x_2 = u$ and $y_2 = -v$;
set $v_1 = a_1/d_1$, $v_2 = a_2/d_1$, $r = (y_1 y_2 n - x_2 c_2 \bmod v_1)$;
set $b_3 = b_2 + 2v_2r$, $a_3 = v_1v_2$, $c_3 = (c_2d_1 + r(b_2 + v_2r))/v_1$;
reduce $f = \{a_3, b_3, c_3\}$;
return $f$.
```

Bounds for Class Numbers

Let us now deal with the question to give bounds for the Class Number. In order to obtain a faster performance, we can use the Euler product expansion of the L-function $L_D(1)$.
In fact we have the following result.

Proposition 4.5. *Assuming the Generalized Riemann Hypothesis (GRH), when $P \to \infty$,*

$$h(D) - \widetilde{h} = O(\widetilde{h}P^{-1/2}\log(P|D|))$$

where

$$\widetilde{h} = \left\lfloor \frac{\sqrt{|D|}}{\pi} \prod_{l \leq P} \left(1 - \frac{\left(\frac{D}{l}\right)}{l}\right)^{-1} \right\rfloor .$$

For example Shanks showed experimentally that the error is very small when P is equal to 2^{17}.
In order to prove this proposition we use the following lemmas.

Lemma 4.2. *If $u \to 0$,*

$$-\log(1-u) = u + O(u^2).$$

Lemma 4.3. *If $u \to 0$,*

$$e^u = 1 + O(u).$$

Lemma 4.4. *[20] Under GRH, if χ is a real non principal character* mod D *and D a discriminant of an imaginary quadratic field,*

$$\sum_{l<T} \chi(l)\log(l) \ll \sqrt{T}\log^2(|D|T).$$

Lemma 4.5. *If χ is a real non principal character and P is a large number,*

$$\prod_{\substack{l>P\\ l\ prime}} \left(1-\frac{\chi(l)}{l}\right)^{-1} - 1 \ll \sum_{\substack{l>P\\ l\ prime}} \frac{\chi(l)}{l} + O\left(\frac{1}{p}\right).$$

Proof. If we set $k=\frac{\chi(l)}{l}$, we can write

$$\prod_{\substack{l>P\\ l\text{ prime}}} (1-k)^{-1} - 1 = \exp\left(\sum_{\substack{l>P\\ l\text{ prime}}} -\log(1-k)\right) - 1.$$

From Lemma 4.2 we have

$$\exp(\sum_{\substack{l>P\\ l\text{ prime}}} -\log(1-k)) - 1 = \exp\left(\sum_{\substack{l>P\\ l\text{ prime}}} k + O\left(\sum_{\substack{l>P\\ l\text{ prime}}} \frac{1}{l^2}\right)\right) - 1$$

and, from Lemma 4.3,

$$\exp\left(\sum_{\substack{l>P\\ l\text{ prime}}} k + O\left(\sum_{\substack{l>P\\ l\text{ prime}}} \frac{1}{l^2}\right)\right) -1 = \left(1+O\left(\frac{1}{P}\right)\right)\left(1+O\left(\sum_{\substack{l>P\\ l\text{ prime}}} k\right)\right) -1$$

$$= O\left(\sum_{\substack{l>P\\ l\text{ prime}}} k\right) + O\left(\frac{1}{P}\right) + O\left(\frac{1}{P}\sum_{\substack{l>P\\ l\text{ prime}}} k\right) \ll \sum_{\substack{l>P\\ l\text{ prime}}} \frac{\chi(l)}{l} + O\left(\frac{1}{P}\right).$$

□

Proof. (of Proposition 4.5)
We have

$$|h(D)-\widetilde{h}| = \left|\widetilde{h}\left(\prod_{l>P}\left(1-\frac{\chi(l)}{l}\right)^{-1} - 1\right)\right|,$$

so our thesis is equivalent to

$$\prod_{l>P}\left(1-\frac{\chi(l)}{l}\right)^{-1} - 1 \ll \frac{\log(P|D|)}{\sqrt{P}}.$$

From Lemma 4.5 we have that

$$\prod_{l>P}\left(1-\frac{\chi(l)}{l}\right)^{-1} - 1 \ll \sum_{l>P}\frac{\chi(l)}{l} + O\left(\frac{1}{P}\right)$$

so we can use partial summation to obtain

$$\sum_{l>P}\frac{\chi(l)}{l}+O\left(\frac{1}{P}\right)\ll-\int_P^\infty\sum_{P<l\le t}\chi(l)\log(l)d\left(\frac{1}{t\log t}\right)+O\left(\frac{1}{P}\right).$$

Since

$$d\left(\frac{1}{t\log t}\right)=\frac{-\log t+1}{t^2\log^2 t}\ll\frac{1}{t^2\log t}$$

and from Lemma 4.4, we have

$$-\int_P^\infty\sum_{P<l\le t}\chi(l)\log(l)d\left(\frac{1}{t\log t}\right)+O\left(\frac{1}{P}\right)\ll$$

$$\int_P^\infty\left(\frac{\sqrt{t}\log^2(|D|t)-\sqrt{P}\log^2(|D|P)}{t^2\log t}\right)dt+O\left(\frac{1}{P}\right)\ll\frac{\log(P|D|)}{\sqrt{P}}.$$

□

Description and pseudocode of the algorithm

Now we have the information to apply Shanks's method to the Class Group. We remark that we can improve the computation by noticing that the inverse of a form $\{a,b,c\}$ is $\{a,-b,c\}$, so in our algorithm we can double the number of giant steps and set $q=\sqrt{(B-C)/2}$.

Moreover, as in the above algorithm STRUCTURE-ORDER, at every step we need to choose a random element of the group to start the computation; in our case we will act in the following way: we consider, in the computation of the Euler product, the first primes p such that $\left(\frac{D}{p}\right)=1$ and we compute b_p such that $b_p^2\equiv D(\bmod 4p)$, then, at every new step of the algorithm, we take as a new element the form $\{p,b_p,c_p\}$ where $c_p=\left(b_p^2-D\right)/(4p)$. So we can also say that the algorithm fails to give an answer when the number of the made steps, denoted as c, becomes larger than the number of the chosen random elements.

We note that the following one is an heuristic algorithm because, as we have outlined for STRUCTURE-ORDER, the result depends on the correctness of the known bounds in Proposition 4.5 and in this case we have found our bounds under the assumption of the GRH. So our output may be false and we should use other methods to verify its correctness .

CLASS-NUMBER(D)

Input: D.

Output: $h(D)$.

```
set $P = \max(2^{18}, |D|^{1/4})$;
compute
    $$Q = \left\lfloor \frac{\sqrt{|D|}}{\pi} \prod_{p \leq P} \left(1 - \frac{\left(\frac{D}{p}\right)}{p}\right)^{-1} \right\rfloor;$$
set $B = \left\lfloor Q(1 + 1/(2\sqrt{P})) \right\rfloor$ and $C = \left\lceil Q(1 - 1/(2\sqrt{P})) \right\rceil$;
for the first $b$ values of the primes $p$ such that $\left(\frac{D}{p}\right) = 1$
  compute $b_p$ such that $b_p^2 \equiv D(\mathrm{mod} 4p)$;
set $f_p = \left\{p, b_p, (b_p^2 - D)/(4p)\right\}$;
set $e = 1$, $c = 0$, $B_1 = B$, $C_1 = C$, $Q_1 = Q$;
while $e \leq B - C$;
set $g = f_p$;
set $c = c + 1$ and $q = \left\lceil \sqrt{(B_1 - C_1)/2} \right\rceil$;
    $x_0 = 1$ and $x_1 = g^e$;
    for $2 \leq r \leq q - 1$;
        $x_r = x_1 \cdot x_{r-1}$;
        if $x_r = 1$;
```

```
14.             set $n = r$;
15.             $n =$ORDER($g$, $n$);
16.             set $e = en$;
17.         else;
18.             sort the $x_r$ in a list $S$;
19.             set $y = x_1 \cdot x_{q-1}$, $y = y^2$, $z = x_1^{Q_1}$ and $n = Q_1$;
20.             $n =$GIANT-STEP2($z$, $S$, $n$);
21.             set $e = en$;
22.             if $c \geq b$;
23.                 output a message saying that the algorithm fails
                    to find $h(D)$;
24.             else;
25.                 set $B_1 = \lfloor B_1/n \rfloor$ and $C_1 = \lceil C_1/n \rceil$;
26. set $h = e\lfloor B/e \rfloor$;
27. return $h$.
```

```
ORDER($g$, $n$)
1. factorize $n$;
2. while $p$ divides $n$;
3.     if $x_1^{n/p} = 1$;
```

```
        set $n = n/p$;
return $n$.
```

```
GIANT-STEP2($z$, $S$, $n$, $y$)
for $0 \leq r < q$
    search for $z$ or $z^{-1}$ in the list $S$;
if we find $z = x_r$;
    set $n = n - r$;
    return $n$;
if we find $z^{-1} = x_r$;
    set $n = n + r$;
    return $n$;
else;
    set $z = y \cdot z$ and $n = n + 2q$;
    GIANT-STEP2($z$, $S$, $n$, $y$).
```

We remark that we can modify this algorithm to obtain the structure of the Class Group as we have seen in STRUCTURE-ORDER.
Even the complexity of this method is obtained from that of STRUCTURE-ORDER,

recalling that, from the Theorem of Siegel, when D is negative, $h(D)$ grows as $|D|^{1/2}$. So the algorithm CLASS-NUMBER allows us to compute $h(D)$ in time $O\left(|D|^{1/4}\log^2(|D|^{1/4})\right)$.

4.4 Sub-exponential Algorithms

4.4.1 Mc Curley's Algorithm

Let us now describe other faster algorithms to compute Class Numbers .
In particular we will deal with the sub-exponential algorithm by **Mc Curley** in 1988 and the variant of this method found by **Atkins**.
The idea of these methods , as in Shanks's, is that of finding relations between the elements of the class group, i.e. between reduced forms, but, unlike the previous method, at every step of this algorithm we are going to find multiples of the class number instead of divisors. Let us explain the theory used to obtain this result.
As in the above algorithm, let us consider a set P of primes such that $\left(\frac{D}{p}\right) = 1$ and, for each $p \in P$, we find reduced forms $f_p = \{p, b_p, c_p\}$, called **prime forms**. Then we use a very important result, depending on the Generalized Riemann Hypothesis (GRH).

Lemma 4.6. *Under the assumption of the GRH, there exists a "computable" constant c such that if*

$$\mathrm{P} = \left\{ p \textit{ prime such that } \left(\frac{D}{p}\right) = 1 \textit{ and } p \leq c\log^2|D| \right\}$$

then the class group is generated by the forms f_p where $p \in \mathrm{P}$.

So, if we denote by n the order of P, we can consider the following surjective group homomorphism :

$$\varphi : \mathbb{Z}^n \longrightarrow \mathrm{Cl}(D)$$

$$(\alpha_p)_{p\in P} \longrightarrow \prod_{p\in P} f_p^{\alpha_p}.$$

Let Λ denote the kernel of φ, we have that Λ is a submodule of $\mathbb{Z}^n$ and it is just the submodule of the relations among the f_p's. Moreover, from the fundamental Theorem of homomorphisms, it follows that

$$\mathbb{Z}^n/\Lambda \cong \mathrm{Cl(D)}$$

and, from the properties of the $\mathbb{Z}$-modules,

$$h(D) = |\det(\Lambda)|.$$

So, whenever we find a system of n independent elements of Λ, we find a multiple of $|\det(\Lambda)|$, hence a multiple of $h(d)$.
Now the question is how to determine the relations among the f_p.
Again from the Theorem of Correspondence of Chapter 2, we have the following lemma.

Lemma 4.7. *Let $\{a, b, c\}$ a primitive positive defined quadratic form of negative discriminant D. Let's consider the prime decomposition of a, that is $a = \prod_p p^{v_p}$. If f_p is the prime form corresponding to p we have the following equivalence*

$$\{a, b, c\} = \prod_p f_p^{\epsilon_p v_p}$$

where $\epsilon_p = \pm 1$ is defined by the congruence

$$b \equiv \epsilon_p b_p (\mathrm{mod} 2p).$$

Using this result, in order to generate relations in Λ, we act in the following way:

- choose random integers e_p;
- compute the reduced form $\{a, b, c\}$ equivalent to $\prod_{p\in P} f_p^{e_p}$;
- compute all the factors of a;

- if they are in P, a relation is found;
- otherwise we choose other exponents e_p;
- when the form is kept we obtain the relation

$$\prod_{p \in P} f_p^{e_p - \epsilon_p v_p} = 1.$$

If the set P is chosen in an appropriate way, by this method we "hope" to obtain Λ.
Mc Curley showed that, if we set $P = \left\{ p \leq P, \left(\frac{D}{p}\right) \neq -1 \right\}$, to optimize the algorithm we could choose

$$P = \max\left(6 \log^2 |D|, L(|D|)^{1/\sqrt{8}}\right)$$

where $L(x)$ is a function defined as

$$L(x) = e^{\sqrt{\log x \log \log x}}.$$

Let us now give the pseudocode of the algorithm without explaining the tecniques to reduce the size of the relation matrix and to compute its determinant.

Mc-Curley(D)
Input: a fundamental negative discriminant D.
Output: the Class Number $h(D)$ and the invariants of the Class Group $Cl(D)$.

```
1. Set $m = 6\log^2(|D|)$ and $M = L(|D|)^{1/\sqrt{8}}$;
2.  set $P = \lfloor \max(m, M) \rfloor$;
3.  set $P = \left\{ p$ prime such that $p \leq P, \left(\frac{D}{p}\right) \neq -1$ and $p$ not divides $D \right\}$;
```

```
4. compute the product
       $B = \left\lfloor \frac{\sqrt{|D|}}{\pi} \prod_{p \leq P} \left( 1 - \frac{\left(\frac{D}{p}\right)}{p} \right)^{-1} \right\rfloor$;
5. set $n$ equal to the number of $p \leq P$;
6. set $k = 0$;
7.  for the primes $p$ in $P$;
8.     do;
9.     compute the forms $f_p$ as in Shanks' method;
10.    choose random integers exponents $e_p$;
11.    compute the reduced form $\{a, b, c\}$ equivalent to $\prod_{p \in P} f_p^{e_p}$;
12.    factorize $a$;
13.    if a prime factor of $a$ is larger than $P$;
14.         choose other exponents and repeat the steps 9-10;
15.    else, i.e.  if $a = \prod_{p \leq P} p^{v_p}$;
16.        $k = k + 1$;
17.        set the elements of the found relation in the k-th
   column of a matrix $A$;
18.     calculate the determinant of the matrix $A$;
19.    set $h = \det(A)$;
20.    if $h \geq B\sqrt{2}$;
21.        return to step 10 ;
```

```
    else;
        return $h$;
        compute the Smith Normal Form $B$ of the matrix $A$;
        return the diagonal elements of $B$ which are the invariants
         of $Cl(D)$.
```

As already mentioned, this method is much faster than the previous one over large discriminants; in fact we can prove that, if we use appropriate tecniques to compute the determinant of A and its Smith Normal Form, the expected asymptotic average running time is

$$O\left(L\left(|D|\right)^{\sqrt{9/8}}\right).$$

4.4.2 Atkin's Algorithm

An improvement of the above method has been given by Atkin. It is faster over all prime discriminants but it does not always gives the class group.
The idea of this method is similar to that of the previous one, i.e. it is based on finding relations among prime forms, but in this case we work with a single form denoted as f.
In order to obtain the order of the group, we find the order of the form f in the class group. Let's denote as n the number of prime forms in the factor base P; we compute the reduced forms equivalent to $f, f^2, f^3, \dots$ and then we try to find relations, as in the previous algorithm, until $n+1$ of them have been found.
We denote as $e_1, e_2, \dots, e_{n+1}$ the exponents of the form f for which we have found a relation. So we have a matrix $n \times (n+1)$ by which, computing its kernel (by a simple linear algebra method), we are able to obtain minimal relations. As soon as we find a non-trivial relation, i.e. when we have $f^N = 1$

where $N = \sum_{1 \le i \le n+1} x_i e_i$ and N is not zero, we can compute the order of f using a method similar to the subalgorithm FACTOR in Shanks's algorithm. Let us denote as e the order of f; so e is a divisor of the class number h. Now we can give a stopping criterion, using Euler product, in the following way: assuming GRH, we check if e statisfies the inequalitity:

$$e > \frac{1}{\sqrt{2}} \frac{\sqrt{|D|}}{\pi} \prod_{p \le P} \left(1 - \frac{\left(\frac{D}{p}\right)}{p} \right)^{-1} ;$$

if it does, we have $e = h(D)$ and f is a generator of the class-group which is cyclic. If e does not statisfies the above inequality we must choose another form and we must repeat the algorithm.
We remark that this method is faster than Mc Curley's when the class group is cyclic. So we ask when this happens. We know that if D is a prime the class number is odd and, according to Cohen-Lenstra Heuristics, stated in the previous chapter, the probability that the odd part of the class group is cyclic is greater than 97%. So, when D is a prime, the class group is often cyclic and so our algorithm is very efficient. Moreover we know that the number of generators of a cyclic group of order h is $\varphi(h)$; since this number is quite large, we have a good chance that the chosen form f is a generator of the group.

4.5 Recent Results

In the last years many authors have given variants of the algorithm described above and have enabled the computation of Class Number of discriminants with more than 100 decimal digits. In 1997 Buchmann, Jacobson and Teske [6] improved and implemented Shanks's method; their algorithms have the advantage that no upper bound on the group order is needed. However all of these results are given under the assumption of the Generalized Riemann Hypothesis, in the sense that the result are not known to be correct without it. On March 21, 2006, Andrew Booker [5] published an article in which he combined Buchmann's algorithm for Class Number of quadratic fields, with analytic methods to give an unconditional algorithm whose running time is $O(|d|^{1/2+\epsilon})$, and $O(|d|^{1/4+\epsilon})$, if GRH is true. He used this method to show that $h(d) = 43$ for $d = 10^{31} + 33$; this computation required 95 hours using a 500 Mhz UltrasparеII.

The most recent work we refer is the paper of M.J. Jacobson, S. Ramachandran and H.C. Williams [26], which will be discussed in the Proceedings of the 7th Algorithm Number Theory Symposium (ANTS VII) at the end of July. In this work, the authors, using an improvement of Shanks's method, compute the Class Number and the Class Group structure of all imaginary quadratic fields with discriminant d for $0 < |d| < 10^{11}$. The correctness of their algorithm is again conditional on GRH, but they verify the obtained results unconditionally using a new verification algorithm which is very efficient. The total running time of this method is $O(|d|^{1/4})$ steps for discriminant. The computations required about 6 days and the verification 8 days. The importance of this work is also given by the fact that the obtained data provides evidence for the Cohen-Lenstra heuristics and Littlewood's bounds on $L(1, \chi)$, stated in Chapter 3.

4.6 Numerical Results

TABLE 1. Class Number of forms with discriminant $-d$ for $1 \leq d \leq 34$.

d	h(d)	d	h(d)
163	1	48427	18
427	2	38707	19
907	3	58507	20
1555	4	61483	21
2683	5	85507	22
3763	6	90787	23
5923	7	111763	24
6307	8	93307	25
10627	9	103027	26
13843	10	103387	27
15667	11	126043	28
17803	12	166147	29
20563	13	134467	30
30067	14	133387	31
34483	15	164803	32
31243	16	222643	33
37123	17	189883	34

TABLE 2. Invariants of Class Groups of some imaginary quadratic fields with discriminant D.

D	$4 \times (2^{2^7} + 1)(40)$
$h(D)$	17787144930223461408
$Cl(D)$	[2 8893572465111730704]
D	$-(4 \times 10^{54} + 4)(55)$
$h(D)$	1056175002108254379317829632
$Cl(D)$	[2 2 2 2 2 33005468815882949353682176]
D	−56759029509462061499204078404947821190422701840487390196283(59)
$h(D)$	34708563502858399116135176220
$Cl(D)$	[34708563502858399116135176220]
D	$-(4 \times 10^{64} + 4)(65)$
$h(D)$	178397819605839608466892693850112
$Cl(D)$	[4 4 11149863725364975529180793365632]

Bibliography

[1] R.Ayoub. *An introduction to the Analytic Theory of Numbers.* Amer. Math. Soc., 1963, pp.320-327.

[2] A.Baker. *Linear forms in the logarithms of algebraic numbers.* Mathematika 13, (1966) 204-216.

[3] A.Birò. *Chowla's conjecture.* Acta Arith. 107 (2003), no.2, pp.179-194.

[4] A.Birò. *Yokoi's conjecture.* Acta Arith. 106 (2003), no.1, pp.85-104.

[5] A.Booker *Quadratic Class Numbers and Character Sums* Math. Comp. 75 (2006) no.255, 1481-1492.

[6] J.Buchmann, M.J.Jacobson,Jr., and E.Teske. *On some computations problems in finite abelian groups.* Math.Comp.66 (1997) no.220, 1663-1687.

[7] Johannes Buchmann, Sachar Paulus. *Algorithms for finite abelian groups.* 1993

[8] Johannes Buchmann, Arthur Schmidt. *Computing the structure of a finite abelian group.* Mathematics of computation Vol. 74, No.252, pp. 2017-2026, 2005.

[9] Henri Cohen. *A course in Computational Algebraic Number Theory.* Springer, 1996, pp.295-297.

[10] Henri Cohen. *A course in Computational Algebraic Number Theory.* Springer, 1996, pag.233.

[11] Henri Cohen. *A course in Computational Algebraic Number Theory.* Springer, 1996, pp.240-241.

[12] Henri Cohen. *A course in Computational Algebraic Number Theory.* Springer, 1996, pag.77.

[13] Henri Cohen. *A course in Computational Algebraic Number Theory.* Springer, 1996, pag.250.

[14] Henri Cohen. *A course in Computational Algebraic Number Theory.* Springer, 1996, pag. 252-261.

[15] Henri Cohen. *A course in Computational Algebraic Number Theory.* Springer, 1996, pp.238-240.

[16] Harvey Cohn. *Advanced Number Theory.* Dover Publications, Inc. New York, pp. 198-204.

[17] H.Davenport *Multiplicative Number Theory.* Springer, pp.27-34.

[18] H.Davenport *Multiplicative Number Theory.* Springer, pag.30.

[19] H.Davenport *Multiplicative Number Theory.* Springer, pp.135-136.

[20] H.Davenport *Multiplicative Number Theory.* Springer, pp.124-125.

[21] H.Davenport. *Multiplicative Number Theory.* Springer, pag.70.

[22] H.Davenport *Multiplicative Number Theory.* Springer, pag.126.

[23] Steven Finch. *Class Number Theory.* May 26, 2005.

[24] A. Granville, K. Soundararajan. *The distribution of values of* $L(1, \chi_d)$. Geom. Funct. Anal. 13 (2003), no.5, pp. 992-1028.

[25] H. Heilbronn, E.H. Linfoot. *On the imaginary quadratic corpora of class-number one.* Quartery Journal of Mathematics (Oxford)(1934) 5, 293-301.

[26] M.J.Jacobson, Jr., S.Ramachandran, H.C.Williams. *Numerical Results on Class Groups of Imaginary Quadratic Fields.* Department of Computer Science, University of Calgary.

[27] Edmund Landau. *Elementary Number Theory.* Chelsea Publishing Company, pag.178.

[28] Edmund Landau. *Elementary Number Theory.* Chelsea Publishing Company, pag.176.

[29] Edmund Landau. *Elementary Number Theory.* Chelsea Publishing Company, pag.76.

[30] H.L.Montgomery, R.C.Vaughan. *Number theory in progress.* Vol. 2, de Gruyter, Berlin, 1999 pp.1039-1052.

[31] Patrick J. Morandi. *The Smith Normal Form of a Matrix.* 2005.

[32] Carl Ludwig Siegel. *The average measure of quadratic forms with given determinant and signature.* Annals of Mathematics. Vol.45, No.4, October, 1944.

[33] Stark. *A complete determination of the complex quadratic fields of class-number one.* Michigan Mathematical Journal 14, (1967) 1-27.

[34] Andreas Stein, Edlyn Teske. *Optimized Baby Step-Giant Step Methods.* J.Ramanujan Math.Soc. 20, No.1 (2005) 1-32.

[35] Ian Stewart, David Tall. *Algebraic Number Theory.* Mathematics Institute University of Warwick Coventry, pp. 66-69.

[36] Ian Stewart, David Tall. *Algebraic Number Theory.* Mathematics Institute University of Warwick Coventry, pp. 151-156.