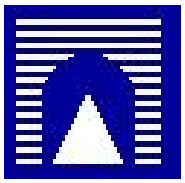
UNIVERSITÀ DEGLI STUDI ROMA TRE
FACOLTÀ DI S.M.F.N.



Sintesi di tesi di Laurea in Matematica
presentata da Manuela Grella

Algebraic, analytic and computational theory of the Class Number

Relatore
Prof. Francesco Pappalardi

Il Candidato
Manuela Grella

Il Relatore
Francesco Pappalardi.

ANNO ACCADEMICO 2005-2006

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

Il protagonista di questa tesi è il Numero di Classe. Tratteremo la sua teoria algebrica, analitica e computazionale.
Il Numero di Classe nel corso della storia ha rivestito un ruolo molto importante sia in Teoria Analitica dei Numeri, dove è stato fondamentale nella dimostrazione del teorema di esistenza di infiniti primi in progressione aritmetica, sia in Teoria Algebrica dei Numeri, poiché esso rappresenta una misura di quanto l'anello degli interi di un campo di numeri si discosta dall'essere un Dominio a Fattorizzazione Unica (UFD). Esso è stato definito inizialmente nell'ambito della Teoria delle Forme Quadratiche Binarie. Rappresenta, infatti, il numero di classi in cui le forme $ax^2+bxy+cy^2$ con a, b, c $\in \mathbb{Z}$, con discriminante $d = b^2 - 4ac$ fissato, si suddividono sotto una definita relazione di equivalenza. Successivamente, nell'ambito della teoria dei campi di numeri, esso è stato definito come la cardinalità di un gruppo quoziente, detto proprio Gruppo delle Classi.
Nel 1832 Jacobi congetturò una formula per esprimere il Numero di Classe. La dimostrazione di tale famosa formula fu trovata nel 1839 da Dirichlet, il quale la utilizzò per terminare la dimostrazione del seguente teorema:

Teorema 1. *(Esistenza di infiniti primi in progressione aritmetica.) Se a, $q \in \mathbb{N}$, $(a,q) = 1$ e P rappresenta l'insieme di tutti i numeri primi, risulta*

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

Il legame tra il Numero di Classe e tale teorema sta nella definizione dei cosiddetti caratteri di Dirichlet e di particolari funzioni, molto simili alla Zeta di Riemann, note come L-serie di Dirichlet. Questi oggetti, strettamente connessi, sono utilizzati moltissimo nella nostra trattazione.
Un carattere di Dirichlet modulo un intero q è una funzione

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

con le seguenti proprietà:

1. χ è periodica di periodo q, cioè tale che $\chi(n+q) = \chi(n)$, $\forall n \in \mathbb{N}$;

2. χ è totalmente moltiplicativa, cioè $\chi(n \cdot m) = \chi(n) \cdot \chi(m)$, $\forall n, m \in \mathbb{N}$;

3. χ è supportata su $U(\mathbb{Z}/q\mathbb{Z})$, cioè tale che $\chi(n) = 0$ se $(q, n) \neq 1$.

Può accadere che un carattere abbia periodo $q_1 < q$, in tal caso esso è detto imprimitivo, altrimenti lo chiamiamo primitivo. Utilizzeremo quasi sempre caratteri primitivi. E' possibile dimostrare che tutti i caratteri primitivi reali sono identificati con i simboli di Jacobi $\left(\frac{d}{n}\right)$ dove d è prodotto di fattori relativamente primi della forma

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

con $p > 2$ primo e il simbolo di Jacobi è un carattere reale di modulo $|d|$. I principali risultati sui caratteri che utilizzeremo sono le leggi di ortogonalità e la disuguaglianza trovata da Polya e Vinogradov nel 1918.

Proposizione 1. *(Leggi di Ortogonalità dei Caratteri)*
Se χ è un carattere modulo q

1.

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

dove

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

è detto carattere principale.

2.

$$\sum_{\chi(\bmod q)} \chi(n) = \begin{cases} \varphi(q) & \text{se } n \equiv 1 (\bmod q) \\ 0 & \text{altrimenti} \end{cases}.$$

Teorema 2. *(Disuguaglianza di Polya-Vinogradov)*
Sia χ un carattere non principale modulo q. Allora risulta

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

Le L-serie di Dirichlet sono funzioni definite come

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

e sono assolutamente convergenti per $s > 1$. Come per la Zeta di Riemann, è possibile esprimere tali funzioni mediante un prodotto di Eulero cioè

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

Ancora una volta analogamente alla funzione Zeta, le L-serie verificano un'equazione funzionale che utilizzeremo per molti dei nostri risultati.
Questa equazione assume diverse forme a seconda che $\chi(-1) = 1$ o $\chi(-1) = -1$, dove χ è un carattere reale primitivo di modulo q. Se $\chi(-1) = 1$, abbiamo

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

dove $\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt$ è la funzione Gamma e $|\tau(\chi)| = q^{1/2}$ per un carattere primitivo; nel caso $\chi(-1) = -1$ l' equazione diventa

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

Dirichlet capì che la chiave per dimostrare il Teorema 1 era dimostrare che se $\chi \neq \chi_0$, χ carattere primitivo, risulta $L(1,\chi) \neq 0$. La dimostrazione di ciò avviene oggi tramite strumenti di analisi complessa che Dirichlet non possedeva. Egli utilizzò quindi solo l'analisi reale ed, in particolare, si avvalse della stretta connessione tra i caratteri reali primitivi e la teoria delle forme quadratiche binarie o quella equivalente dei campi quadratici. E' facile, infatti, dimostrare che i moduli d dei caratteri primitivi reali descritti sopra rappresentano proprio particolari discriminanti, detti fondamentali, nella teoria delle forme quadratiche binarie, e i discriminanti dei campi quadratici nella teoria dei campi di numeri.
Dirichlet, nel suo lavoro, riuscì a mettere in relazione il Numero di Classe di

forme quadratiche aventi un dato discriminante d con il valore della L-serie $L(1,\chi)$, dove χ è un carattere reale primitivo $\left(\frac{d}{n}\right)$ e questo è il simbolo di Kronecker, cioè l'estensione ai reali del simbolo di Jacobi. Tale relazione gli permise di dimostrare che $L(1,\chi)$ risulta essere strettamente positiva, e di trovare, inoltre, un'espressione di tale L-serie come somma finita.
In questa tesi seguiamo inizialmente un percorso simile a quello di Dirichlet, studiando in breve la teoria delle forme quadratiche binarie per ottenere la Formula del Numero di Classe; quindi studiamo il Numero di Classe dal punto di vista della teoria algebrica dei numeri, le sue proprietà analitiche e nell'ultima parte ci concentriamo sul problema computazionale, cioè analizziamo gli algoritmi trovati finora per calcolare in modo più o meno efficiente il Numero di Classe e la struttura del Gruppo delle Classi.
Il nostro lavoro è organizzato nel modo seguente.

Nel primo capitolo definiamo una relazione di equivalenza nell'insieme delle forme quadratiche binarie di discriminante fissato d in questo modo: diciamo che due forme F e G sono equivalenti se lo sono sotto una trasformazione unimodulare, cioè se esistono r, s, t e $u \in \mathbb{Z}$ tali che $ru - st = 1$ e risulta

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

Definiamo, quindi, fissato un discriminante d, il Numero di Classe $h(d)$ come il numero di classi di equivalenza di forme di discriminante d. Un primo importante risultato è la finitezza di $h(d)$ che riusciamo a dimostrare utilizzando il fatto, dimostrato per la prima volta da Lagrange, che ogni classe di equivalenza contiene una forma $F(x,y) = ax^2 + bxy + cy^2$, detta ridotta, tale che $|b| \leq |a| \leq |c|$. Ci concentriamo, quindi, sul problema di trovare una formula che rappresenti $h(d)$ e per fare ciò lavoriamo sulla natura delle trasformazioni tra forme e sul problema della rappresentabilità di un intero tramite particolari forme. Un risultato interessante riguarda il numero di trasformazioni unimodulari di una forma F in se stessa (i cosiddetti automorfi). Se la forma ha discriminante d negativo si può dimostrare che il

numero di tali trasformazioni è

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

mentre se d è positivo la situazione risulta più complicata in quanto tutte le trasformazioni di F in se stessa sono determinate dalle infinite soluzioni dell'equazione di Pell $t^2 - du^2 = 4$.

Il problema di rappresentabilità che ci interessa può essere espresso invece nel seguente modo: fissato un sistema rappresentativo di forme di discriminante d, cioè un insieme di rappresentanti (uno per ogni classe), quante sono le rappresentazioni di un intero positivo k (cioè gli (x, y) tali che $F(x, y) = k$), tramite forme appartenenti a tale sistema? In particolare, per ovviare al fatto che se d è positivo ogni rappresentazione dà luogo ad infinite rappresentazioni perché ogni forma ha infiniti automorfi, limitiamo la nostra attenzione alle cosiddette rappresentazioni primarie che sono in ogni caso in numero finito. Una rappresentazione di un intero positivo k tramite una forma di coefficienti a, b, c è detta primaria se $d < 0$ in ogni caso, oppure nel caso di $d > 0$ sotto le ulteriori condizioni:

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

dove $\epsilon = \frac{t_0+u_0\sqrt{d}}{2}$ e (u_0, t_0) è la più piccola soluzione dell'equazione di Pell (cioè la soluzione per cui t_0 ha il più piccolo valore positivo possibile e per cui $u_0 > 0$).

Uno dei principali risultati della teoria delle forme quadratiche, che rappresenta il primo passo per ottenere la famosa relazione tra $h(d)$ e $L(1, \chi)$, dove $\chi(n) = \left(\frac{d}{n}\right)$ è un carattere modulo d, è che il numero di rappresentazioni primarie $\Psi(k)$ di un intero positivo k, coprimo con d, tramite forme appartenenti ad un sistema rappresentativo è finito ed è espresso mediante la formula

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

La dimostrazione di tale risultato sfrutta in modo particolare il fatto che il numero di soluzioni della congruenza $x^2 \equiv d(\mathrm{mod} 4k)$ è, quando $0 \leq x < 2k$, $\sum_{f|k} \left(\frac{d}{f}\right)$ con f privo di fattori quadratici.
Il secondo passo fondamentale nella nostra trattazione è riuscire a determinare il valor medio di $\Psi(k)$ al variare di k; per far ciò utilizziamo in modo particolare le proprietà dei caratteri di Dirichlet (soprattutto le Leggi di Ortogonalità). Otteniamo il seguente risultato

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

dove

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

da cui, sfruttando risultati elementari di Teoria dei Numeri, riusciamo a ricavare che, posto

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

dove $\Psi(k, F)$ è il numero di rappresentazioni primarie di k tramite una forma F del sistema rappresentativo, risulta

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

Mettendo insieme la definizione di Numero di Classe con i risultati sopra, otteniamo il risultato centrale del capitolo cioè la formula di Dirichlet

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

Con un procedimento simile a quello descritto finora, utilizzando anche dei risultati della teoria classica sulle serie di Fourier, riusciamo anche ad ottenere una espressione per la L-serie $L(1, \chi)$ come somma finita:

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

Nel secondo capitolo richiamiamo inizialmente alcuni concetti basilari di Teoria algebrica dei Numeri, quali la definizione di campo di numeri, di discriminante, norma e traccia. Per dare una nuova definizione di Numero di Classe lavoriamo sull'anello degli interi $\mathcal{O}_K$ di un campo di numeri K (in particolare sui suoi ideali), cioè sull'insieme degli elementi di K che sono radici di polinomi monici a coefficienti interi. Una delle questioni più importanti su $\mathcal{O}_K$ è stabilire quando, nel caso dei campi quadratici, al variare di d, esso risulta essere un Dominio a Fattorizzazione Unica (UFD). Questo problema fu affrontato già da Gauss nelle sue *Disquisitiones Arithmeticae* ed è stato risolto completamente solo nel caso $d < 0$. Infatti, nel 1967, Baker e Stark hanno dimostrato che $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ è un UFD solo per nove valori negativi di d, precisamente

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

Nel caso $d > 0$ Gauss congetturò che $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ fosse un UFD per infiniti valori di d. Oggi tale problema è ancora aperto, sebbene siano stati trovati moltissimi valori positivi di d per cui la fattorizzazione risulta unica.
Nella parte centrale del capitolo definiamo il Gruppo delle Classi di un campo di numeri K a partire dagli ideali di $\mathcal{O}_K$ ed in particolare dai cosiddetti ideali frazionari, cioè quegli $\mathcal{O}_K$-sottomoduli F di K che possono essere espressi come $F = d^{-1}I$ dove d è un elemento non nullo di $\mathcal{O}_K$ e I un suo ideale. Gli ideali frazionari formano un gruppo sotto la moltiplicazione. Il Gruppo delle Classi $\mathbf{Cl}(\mathcal{O}_K)$ è quindi il gruppo quoziente del gruppo degli ideali frazionari di $\mathcal{O}_K$, $\mathbf{F}(\mathcal{O}_K)$, modulo il suo sottogruppo normale degli ideali frazionari principali, $\mathbf{P}(\mathcal{O}_K)$. La cardinalità del Gruppo delle Classi è detta Numero di Classe. La dimostrazione che il Numero di Classe è finito questa volta avviene utilizzando un importante teorema di natura geometrica, il Teorema di Minkowski del 1896, e il concetto di norma di un ideale, definita come la cardinalità del gruppo quoziente di $\mathcal{O}_K$ modulo l'ideale. Abbiamo sottolineato, all'inizio, il legame tra il Numero di Classe e l'unicità della fat-

torizzazione nell'anello degli interi di un campo di numeri; questo legame è evidente dalla definizione di Gruppo delle Classi data sopra: infatti, poiché l'anello degli interi di un campo di numeri è un dominio di Dedekind, dire che esso è un UFD equivale a dire che tutti i suoi ideali sono principali, cioè che il Gruppo delle Classi è il gruppo banale e quindi che il Numero di Classe è 1.
Nell'ultima parte del capitolo colleghiamo tutto ciò con quanto visto nel primo capitolo, cioè analizziamo i legami esistenti tra la teoria delle forme quadratiche e quella degli ideali dell'anello degli interi dei campi quadratici di numeri. Descriviamo tramite due lemmi la possibilità di costruire una corrispondenza tra ideali e forme, ed enunciamo proprio il cosiddetto Teorema di Corrispondenza il quale afferma che a forme equivalenti corrispondono ideali equivalenti e viceversa, stando attenti a considerare l'equivalenza stretta tra ideali (due ideali I e J sono equivalenti in senso stretto se esistono due ideali principali $\langle a\rangle$, $\langle b\rangle$ tali che $I\langle a\rangle = J\langle b\rangle$ e $N(ab) > 0$). Tale corrispondenza ci consente di parlare, nel caso di discriminanti fondamentali, indistintamente di Numero di Classe di forme di discriminante d o di Numero di Classe di un campo quadratico $\mathbb{Q}(\sqrt{d})$, e di ottenere nuovamente, lavorando con gli ideali, la formula del Numero di Classe di Dirichlet.

Nel terzo capitolo presentiamo alcune delle questioni sul Numero di Classe che hanno interessato i matematici nel corso degli anni. Uno dei problemi più famosi è noto come Problema di Gauss: esso consiste nel trovare, dato un intero m, tutti i discriminanti fondamentali negativi il cui Numero di Classe è uguale a m. Tale problema nel caso $m = 1$ è equivalente a trovare tutti i valori di $-d$ per cui il campo quadratico immaginario $\mathbb{Q}(\sqrt{-d})$ è un UFD, ed fu risolto, come abbiamo spiegato nel secondo capitolo, trovando solo nove valori di $-d$. Per valori di m diversi da 1 la questione fino ad oggi è stata risolta solo in alcuni casi ad esempio per tutti gli m dispari tra 5 e 23.
Ma il problema a cui ci dedichiamo maggiormente in questo capitolo è studiare il comportamento del Numero di Classe al variare di d trovando delle

stime asintotiche su $h(d)$ e sul suo valor medio. Anche in questo caso il primo a fare delle congetture è stato Gauss: egli ipotizzò che $h(d) \to \infty$ quando $d \to -\infty$ e ciò, dopo vari tentativi da parte di matematici come Hecke e Heilbronn, è stato dimostrato da Siegel tramite il suo famoso teorema sulle L-serie del 1935

Teorema 3. *Dato $\epsilon > 0$ esiste una costante positiva $C_1(\epsilon)$ tale che, se χ è un carattere reale primitivo di modulo q, allora*

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

Tale teorema fornisce una stima su $L(1, \chi)$ da cui, usando la formula di Dirichlet, seguono immediatamente delle disuguaglianze sul Numero di Classe; precisamente risulta

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

se d è negativo, e

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

se d è positivo, dove η è l'unità fondamentale del campo $\mathbb{Q}(\sqrt{d})$ e $C_2(\epsilon)$ è una costante.
Utilizzando ancora una volta la disuguaglianza di Polya-Vinogradov sui caratteri ed, in particolare, la scrittura di $L(1, \chi)$ come serie finita ricavata nel primo capitolo, otteniamo delle stime asintotiche su $h(d)$, cioè

$$\log(h(d)) \sim \log(\sqrt{|d|}),$$

se $d \to -\infty$, e

$$\log(h(d) \log(\eta)) \sim \log(\sqrt{d}),$$

se $d \to \infty$.
Per stimare il valor medio di $h(d)$, cioè il numero medio di classi di forme quadratiche di discriminante fissato d, dimostriamo inizialmente un risultato provato da Siegel nel 1944 che afferma che se d è un intero privo di fattori quadratici tale che $d \equiv 0, 1 (\mathrm{mod} 4)$ risulta

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

e

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

dove $h^+(d)$ rappresenta il Numero di Classe ottenuto considerando l'equivalenza stretta tra ideali, $\zeta(s)$ è la funzione Zeta di Riemann e $\eta^+ = \frac{t+u\sqrt{d}}{2}$, dove (t,u) è la più piccola soluzione positiva dell'equazione di Pell $t^2 - du^2 = 4$. Per dimostrare queste stime, oltre ad usare ancora la disuguaglainza di Polya-Vinogradov, sfruttiamo molto le proprietà del simbolo di Jacobi $\left(\frac{d}{n}\right)$ e il fatto che esso rappresenta un carattere primitivo modulo $|d|$. Da questo risultato, tramite la definizione di discriminante fondamentale e la scrittura della funzione Zeta di Riemann come prodotto di Eulero, ricaviamo che risulta

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

se $d<0$, e

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

se $d>0$, dove

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

e le somme sono effettuate solo sui discriminanti fondamentali.

L'ultima parte del capitolo la dedichiamo ad una serie di congetture sul comportamento del Numero di Classe e del Gruppo delle Classi che vanno sotto il nome di Euristiche di Cohen e Lenstra, dai due matematici che le hanno elaborate. La loro importanza sta nel fatto che fino ad oggi sull'argomento sono pochi i risultati effettivamente dimostrati. Tali congetture, inoltre, sono confermate da un grandissimo numero di osservazioni sperimentali. Alcune di esse riguardano, ad esempio, la frequenza con cui un primo dispari divide il Numero di Classe, la probabilità che la parte dispari del Gruppo delle Classi non sia ciclica, e il numero di fattori non ciclici del p-sottogruppo di Sylow di $\mathrm{Cl}(d)$. Uno dei risultati più interessanti è che la probabilità che il sottogruppo costituito da tutti gli elementi di ordine dispari del Gruppo delle Classi di un campo quadratico immaginario sia ciclico è pari a circa il 97%.

Nel quarto capitolo affrontiamo il problema, ancora aperto, di riuscire ad implementare un algoritmo efficiente che, dato in input un discriminante D, restituisca il Numero di Classe $h(D)$ e la struttura del Gruppo delle Classi Cl(D). Studiamo in dettaglio soprattutto l'algoritmo elaborato da Shanks nel 1968 perché è stato il primo algoritmo efficiente trovato e perché molti dei lavori successivi si basano su idee simili o sono suoi miglioramenti. Innanzitutto spieghiamo che ottenere la struttura di un gruppo abeliano finito G tramite un algoritmo vuol dire trovare i cosiddetti invarianti, cioè una successione di interi $d_1, \dots d_n$ tali che d_i divide d_{i+1} per $i = 1, \dots, n$ e tali che G risulta isomorfo al gruppo $\mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \dots \mathbb{Z}/d_n\mathbb{Z}$, in virtù del Teorema Fondamentale sui gruppi abeliani finitamente generati.
Il primo algoritmo che proponiamo è quello più immediato, ma anche quello meno efficiente. Esso sfrutta direttamente la definizione del Numero di Classe data nel primo capitolo cioè conta, dato un discriminante D, il numero di classi di forme quadratiche aventi tale discriminante contando il numero di forme ridotte. Calcoliamo il tempo di esecuzione di tale algoritmo e troviamo che è pari a $O(|D|)$, il che vuol dire che l'algoritmo comincia ad essere molto lento per discriminanti grandi.
Il secondo metodo che analizziamo si basa su un'implementazione delle formule analitiche che esprimono $h(D)$ e, più che per la sua efficienza, lo studiamo perché rappresenta un'applicazione interessante dell'equazione funzionale della L-serie $L(1, \chi)$. Applicando tale equazione troviamo, infatti, la seguente formula per $h(D)$, quando $D < -4$ è un discriminante fondamentale,

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

dove

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

Usando questa formula si può costruire un algoritmo con tempo di esecuzione $O\left(|D|^{1/2+\epsilon}\right)\ \forall \epsilon > 0$, dove la costante, però, è piuttosto grande.

Questi due metodi oltre ad avere tempi di esecuzione non molto rapidi calcolano soltanto il Numero di Classe non fornendo alcuna informazione sul Gruppo delle Classi. La parte centrale del capitolo è perciò interamente dedicata all'algoritmo di Shanks, denominato Baby Steps Giant Steps, che nasce come metodo per calcolare l'ordine di un elemento g in un gruppo abeliano finito G, viene poi modificato in modo da restituire la cardinalità del gruppo e i suoi invarianti e, con diversi accorgimenti, può essere utilizzato per trovare il Numero di Classe e gli invarianti del Gruppo delle Classi.
Per prima cosa forniamo, quindi, una descrizione e una pseudocodifica dell'algoritmo base, cioè quello che calcola l'ordine di un elemento g quando conosciamo almeno un suo limite superiore B. L'idea è quella di calcolare, posto $q = \left\lceil \sqrt{B} \right\rceil$, potenze di g, in particolare g^r con $0 \leq r < q$ (baby steps) e g^{-aq} con $0 \leq a < q$ (giant steps), fino ad ottenere un multiplo (precisamente $aq + r$) dell'ordine di g; quest'ultimo viene poi calcolato mediante fattorizzazione. Troviamo che il tempo computazionale di questo metodo, usando al suo interno un opportuno algoritmo di ordinamento, è pari a $O(q \log q)$.
Descriviamo quindi la teoria che usiamo per rappresentare il gruppo G in modo da modificare l'algoritmo precedente per ottenere la cardinalità di G, dato almeno un suo limite superiore, e i suoi invarianti. Basiamo tutto su una rappresentazione del gruppo tramite generatori e relazioni. Il problema diventa quello di trovare ad ogni passo del nostro algoritmo, una relazione tra elementi $g_1, \ldots, g_r$ del gruppo scelti in modo casuale: questo equivale a trovare interi $(\rho_1, \ldots, \rho_r)$ tali che risulti $\prod_{i=1}^{r} g_i^{\rho_i} = 1$; così riusciamo a costruire ad ogni passo le colonne di una matrice, detta proprio matrice di relazione, il cui determinante ci fornisce la cardinalità del gruppo. Gli invarianti sono ottenuti calcolando la Forma Normale di Smith della matrice di relazione, cioè applicando a tale matrice un algoritmo che la trasforma in una matrice diagonale $\mathrm{diag}(d_1, \ldots, d_n)$ tale che, per $i = 1, \ldots, n$, risulta $d_i | d_{i+1}$ e gli invarianti di G sono proprio i d_i. Spieghiamo, dunque, come le relazioni tra gli elementi si trovano proprio con il metodo Baby Steps Giant Steps descritto in precedenza, sottolineando che è essenziale conoscere un limite

superiore dell'ordine del gruppo, soprattutto per riuscire a dare un criterio di arresto per l'algoritmo.
Forniamo anche in questo caso una pseudocodifica dell'algoritmo, preceduta da una breve descrizione in cui spieghiamo come ottenere ad ogni passo le colonne della matrice di relazione memorizzando gli esponenti degli elementi trovati durante ogni iterazione all'interno di particolari liste di liste.
A questo punto spieghiamo come adattare l'algoritmo al Gruppo delle Classi. I due problemi fondamentali sono come calcolare in $\mathrm{Cl}(D)$ e come ottenere un limite superiore di $h(D)$.
Il primo problema è risolto facilmente utilizzando un'operazione tra forme ridotte, detta composizione, che fu introdotta già da Gauss nel 1798. In particolare forniamo la pseudocodifica dell'algoritmo che, assegnata una forma, calcola la sua ridotta e di quello che, date due forme, ne fa la composizione.
Un limite superiore per $h(D)$ lo troviamo, invece, utilizzando ancora una volta la Teoria Analitica dei Numeri ed in particolar modo i prodotti di Eulero e le proprietà dei caratteri di Dirichlet. Tale limite è, sotto l'assunzione dell'Ipotesi Generalizzata di Riemann (cioè l'Ipotesi di Riemann per le L-serie di Dirichlet),

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

quando $P \to \infty$.
A questo punto, avendo a disposizione tutti gli strumenti, forniamo la pseudocodifica dell'algoritmo di Shanks applicato al Gruppo delle Classi e troviamo che il suo tempo di esecuzione è pari a $O\left(|D|^{1/4} \log^2(|D|^{1/4})\right)$.
La parte finale del capitolo è dedicata alla descrizione di altri algoritmi un po' più efficienti e ad una veloce panoramica dei risultati più importanti ottenuti fino ad oggi. In particolare ci soffermiamo sui cosiddetti algoritmi subesponenziali di Mc Curley e Atkin, che usano una strategia simile a quella del metodo di Shanks, ma lavorano su multipli del Numero di Classe invece che su divisori. I loro tempi di esecuzione sono dell'ordine di $O\left(L(|D|)^{\sqrt{9/8}}\right)$

dove $L(x)$ è una funzione definita come

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

Infine citiamo gli ultimi miglioramenti degli algoritmi descritti sopra. In particolare facciamo riferimento ad uno scritto recente di Jacobson, Ramachandran e Williams. Questo lavoro ci è stato inviato tramite posta elettronica dallo stesso Williams e sarà discusso durante il settimo Algorithm Number Theory Symposium (ANTS VII) alla fine di luglio. In esso gli autori descrivono le tecniche usate per calcolare, tramite un algoritmo con tempo di esecuzione $O(|d|^{1/4})$, il Numero di Classe e la struttura del Gruppo delle Classi di tutti i campi quadratici immaginari con discriminante d per $0 < |d| < 10^{11}$.

Riferimenti bibliografici

[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.