Università degli Studi di Milano
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Magistrale in Matematica

Il problema di Gauss sul numero di classi di ideali

Soluzione mediante la teoria delle funzioni L associate a curve ellittiche

RELATORE: Prof. Massimo BERTOLINI

TESI DI
Martino BORELLO
Matr. 754381

ANNO ACCADEMICO 2009 - 2010

Agli amici e ai maestri che mi hanno accompagnato,
sostenuto ed educato in questi anni

Indice

Introduzione

Uno degli aspetti più affascinanti della teoria dei numeri è certamente il legame che stabilisce tra ambiti della matematica apparentemente distanti; il Problema di Gauss sul numero di classi di ideali, con la sua soluzione, è un esempio di questo.

Originato da un problema aritmetico di rappresentazione di numeri interi tramite espressioni quadratiche, il Problema di Gauss viene formalizzato e presentato in termini moderni come tentativo di stabilire l'andamento della cardinalità dei gruppi delle classi di ideali dei campi quadratici complessi $\mathbb{Q}(\sqrt{D})$, al variare dell'intero negativo D.

Molti furono i tentativi di risolvere tale problema, ma solo Goldfeld, nel 1976, intuì la strada giusta: il suo merito fu soprattutto quello di ricondurre il Problema di Gauss alla ricerca di una funzione L associata ad una curva ellittica che abbia uno zero triplo in un punto del piano complesso, legando proprietà analitiche e oggetti geometrici a un problema di natura algebrica.

In questa tesi presenteremo il problema da un punto di vista storico (Capitolo 1), daremo ampio spazio all'introduzione degli oggetti e degli strumenti fondamentali che intervengono nella sua soluzione (Capitoli 2, 3 e 4) e concluderemo con l'esposizione del lavoro di Gross-Zagier (Capitolo 5) e di Goldfeld (Capitolo 6).

Capitolo 1

Il Problema di Gauss sul numero di classi di ideali

Pensiamo che il modo migliore per comprendere il Problema di Gauss sul numero di classi di ideali sia introdurlo da un punto di vista storico, così da coglierne l'importanza, la difficoltà e alcune conseguenze.

In questo capitolo vedremo le origini di tale problema, partendo da alcuni fenomeni apparentemente poco attinenti ad esso fino ad arrivare alla formulazione precisa di Gauss. Evidenzieremo alcuni passi del suo sviluppo, nel diciannovesimo secolo e nella prima parte del ventesimo, osservando i limiti sostanziali di tutti i risultati ottenuti. Concluderemo infine con la presentazione del lavoro di Goldfeld, Gross e Zagier, che permette, a meno di un numero finito di calcoli, di risolvere il Problema di Gauss.

1.1 Le origini

Nel 1772 Eulero mise in evidenza il fatto che il polinomio

$$x^2 - x + 41$$

assume valori primi per $x = 1, 2, \ldots, 40$.

Nel 1798 Legendre tornò su tale argomento mettendo in rilievo che

$$x^2 + x + 41$$

assume anch'esso valori primi per $x = 0, 1, \ldots, 39$.

Questi due fatti, osservati da Eulero e Legendre, sono tra i primi segnali di un fenomeno più generale legato a quello che è noto come Problema di Gauss sul numero di classe 1. Tale legame è messo in evidenza da un risultato di Rabinovitch, enunciato nel 1913.

Teorema 1.1. *Sia $D < 0$ e $D \equiv 1$ (mod 4). Allora*

$$x^2 - x + \frac{1 + |D|}{4}$$

assume valori primi per $x = 1, 2, \ldots, \frac{|D|-3}{4}$ se e solo se l'anello degli interi algebrici del campo $\mathbb{Q}(\sqrt{D})$ è un dominio a fattorizzazione unica.

Un teorema analogo vale per il polinomio $x^2 + x + \frac{1+|D|}{4}$. É noto che l'anello degli interi algebrici di $\mathbb{Q}(\sqrt{-163})$ è un dominio a fattorizzazione unica e questo spiega i risultati osservati da Eulero e Legendre.

Il Problema di Gauss sul numero di classi di ideali ha una storia lunga, curiosa e interessante. Forse tale problema sarebbe da attribuire a Fermat, che nel 1654 enunciò teoremi come

$$p = 6n + 1 \;\Rightarrow\; p = x^2 + 3y^2$$

$$p = 8n + 1 \;\Rightarrow\; p = x^2 + 2y^2$$

con p primo, che furono provati da Eulero nel 1761 e nel 1763. Molti altri teoremi di rappresentazione di interi come somma di quadrati furono provati nel diciottesimo secolo.

Nel 1773 Lagrange, per primo, sviluppò una teoria generale sulle forme quadratiche binarie $Ax^2 + Bxy + Cy^2$ con discriminante $D = B^2 - 4AC$ per trattare il problema di quando un intero m sia rappresentabile nella forma

$$m = Ax^2 + Bxy + Cy^2$$

É chiaro che mediante un cambio di variabili lineare

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \qquad \text{con} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

abbiamo

$$Ax^2 + Bxy + Cy^2 = A'x'^2 + B'x'y' + C'y'^2$$

dove

$$\begin{aligned} A' &= Aa^2 + Bac + Cc^2 \\ B' &= 2Aab + B(ad + bc) + 2Ccd \\ C' &= Ab^2 + Bbd + Cd^2 \end{aligned}$$

e quindi le due forme quadratiche

$$Ax^2 + Bxy + Cy^2 \qquad \text{e} \qquad A'x'^2 + B'x'y' + C'y'^2$$

rappresentano lo stesso insieme di interi.

Indichiamo tali forme con (A, B, C) e (A', B', C') rispettivamente. Lagrange definì equivalenti due forme come le precedenti, dal momento che era interessato principalmente al problema della rappresentazione degli interi.

Scriviamo allora $(A, B, C) \sim (A', B', C')$ se la forma (A', B', C') può essere ottenuta dalla forma (A, B, C) mediante un cambio lineare di coordinate e ribadiamo che forme equivalenti rappresentano lo stesso intero.

Lagrange sviluppò una teoria di riduzione per le forme quadratiche binarie e mostrò che ogni forma è equivalente ad una certa forma ridotta scelta canonicamente. Questa idea fu sviluppata ulteriormente da Gauss. Diamo ora un'interpretazione moderna della teoria di riduzione per le forme quadratiche.

Date due forme equivalenti $(A, B, C) \sim (A', B', C')$ con discriminante

$$D = B^2 - 4AC = B'^2 - 4A'C' < 0$$

possiamo associare ad esse i due numeri complessi

$$z = \frac{-B + \sqrt{D}}{2A} \qquad \text{e} \qquad z' = \frac{-B' + \sqrt{D}}{2A'}$$

che giacciono sul semipiano complesso superiore, che chiamiamo $\mathfrak{H}$. Allora z è equivalente a z' nel senso che

$$z = \frac{az' + b}{cz' + d} \qquad \text{con} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

Una forma è detta ridotta se il numero complesso z che le è associato giace nel dominio fondamentale per il gruppo modulare $\mathrm{SL}_2(\mathbb{Z})$ (approfondiremo il significato di questi oggetti nel capitolo 2). É facile verificare che una forma ridotta soddisfa le condizioni

$$-A < B \leq A \leq C \qquad \text{o} \qquad 0 \leq B \leq A = C$$

Ogni forma è equivalente a un'unica forma ridotta canonica.

Definizione 1.1. *Denominiamo con $h(D)$ il numero delle forme quadratiche binarie $Ax^2 + Bxy + Cy^2$ di discriminante $D = B^2 - 4AC$ non equivalenti, ovvero il* ***numero di classi*** *(di equivalenza) di forme quadratiche binarie di discriminante D.*

Nel suo libro del 1798 Legendre semplificò il lavoro di Lagrange, dimostrò la legge di reciprocità quadratica assumendo che esistono infiniti numeri primi in ogni progressione aritmetica, introdusse la composizione di due forme e definì il simbolo di Legendre

$$\left(\frac{n}{p}\right) = \begin{cases} +1 & \text{se } n \equiv x^2 \pmod{p} \text{ (e } n \not\equiv 0 \pmod{p}) \\ -1 & \text{se } n \not\equiv x^2 \pmod{p} \\ 0 & \text{se } n \equiv 0 \pmod{p} \end{cases}$$

Il suo lavoro divenne quasi subito obsoleto con la pubblicazione, nel 1801, delle *Disquisitiones arithmeticae* di Gauss [Gau01]. Forse una delle parti più significative di tale libro è la sezione in cui Gauss definisce la composizione di due forme quadratiche binarie e prova che le classi di equivalenza di forme quadratiche binarie con lo stesso discriminante formano un gruppo finito con tale composizione come legge di gruppo.

Nell'articolo 303 delle *Disquisitiones arithmeticae*, Gauss enuncia la congettura che prende il suo nome.

Congettura 1.1. *Fissato un intero positivo h esiste un numero finito di discriminanti negativi D tali che $h(D) = h$.*

É significativo sottolineare che Gauss definiva le forme quadratiche binarie in modo leggermente diverso da Lagrange, poiché considerava le forme del tipo

$$Ax^2 + 2Bxy + Cy^2$$

definendo il discriminante come

$$D = B^2 - AC$$

Nell'articolo 303 Gauss dà delle tabelle di discriminanti aventi un numero di classi fissato e congettura che queste tabelle siano complete. Ipotizzò che $h(D)$ tende a ∞ per D che tende a $-\infty$ (**congettura di Gauss**).

Ritorniamo alla notazione di Lagrange ed enunciamo la versione moderna del **Problema di Gauss sul numero di classi**: ***trovare un algoritmo effettivo per determinare tutti i discriminanti negativi con un certo numero di classi*** h ***fissato***.

La notazione di Lagrange è più adatta per reinterpretare la teoria delle forme quadratiche binarie nei termini della teoria dei campi quadratici.
A ogni forma quadratica

$$Ax^2 + Bxy + Cy^2$$

di discriminante D possiamo associare un ideale del tipo

$$\mathbb{Z}\ A + \mathbb{Z}\ \frac{-B + \sqrt{D}}{2}$$

nell'anello degli interi algebrici di $\mathbb{Q}(\sqrt{D})$ (cfr. [Dav]).

Diciamo che due ideali $\mathcal{A}$ e $\mathcal{B}$ sono equivalenti se esistono due ideali principali (λ_1) e (λ_1) tali che

$$\mathcal{A}(\lambda_1) = \mathcal{B}(\lambda_2)$$

Si può mostrare che ideali equivalenti corrispondono a forme quadratiche equivalenti (nel senso di Lagrange) e viceversa, ovvero che c'è una corrispondenza biunivoca tra il gruppo delle classi di forme quadratiche binarie di discriminante D e il gruppo delle classi di ideali del campo quadratico $\mathbb{Q}(\sqrt{D})$, che denotiamo con $\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}$. Pertanto il Problema di Gauss sul numero di classi di forme quadratiche può essere riletto come **Problema di Gauss sul numero di classi di ideali**.

É particolarmente significativo determinare per quali D si ha $h(D) = 1$ (problema noto come Problema di Gauss sul numero di classe 1), in quanto in tal caso si ha che l'anello degli interi algebrici di $\mathbb{Q}(\sqrt{D})$ è un dominio a fattorizzazione unica. Il Problema di Gauss sul numero di classe 1 in forma più esplicita è: $h(D) = 1$ *per* $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$ *e per nessun altro* $D < -163$.

1.2 Gli sviluppi

Rispetto alla congettura originale di Gauss furono fatti pochissimi progressi fino al ventesimo secolo. Nel 1918 Landau pubblicò il teorema seguente, che attribuì a una lezione tenuta da Hecke.

Teorema 1.2. *Sia* $D < 0$. *Consideriamo* χ, *carattere mod* D, *dispari, reale e primitivo. Se per ogni* $s \in \mathbb{R}$ *tale che* $s > 1 - \frac{c_1}{\log|D|}$ *si ha*

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} \neq 0$$

allora

$$h(D) > c_2 \cdot \frac{\sqrt{|D|}}{\log|D|}$$

dove c_1 *e* c_2 *sono due costanti positive assolute fissate.*

L'Ipotesi di Riemann Generalizzata afferma che gli unici zeri non banali di $L(s,\chi)$ sono sulla linea $\mathrm{Re}(s) = \frac{1}{2}$. Hecke mostrò quindi che l'Ipotesi di Riemann Generalizzata implica la congettura di Gauss, dal momento che se tale ipotesi fosse vera, $h(D)$ crescerebbe con $|D|$.

Nel 1933 Deuring dimostrò un ulteriore teorema.

Teorema 1.3. *Se l'Ipotesi di Riemann classica è falsa, allora* $h(D) \geq 2$ *per* $|D|$ *sufficientemente grande.*

Questo risultato fu migliorato ulteriormente da Mordell nel 1934.

Teorema 1.4. *Se l'Ipotesi di Riemann classica è falsa, allora è vera la congettura di Gauss, ovvero* $h(D) \to \infty$ *per* $D \to -\infty$.

Sempre nel 1934, Heilbronn continuò su questa strada.

Teorema 1.5. *Se l'Ipotesi di Riemann Generalizzata è falsa, allora* $h(D) \to \infty$ *per* $D \to -\infty$.

Questo risultato, insieme al teorema di Hecke, dà una dimostrazione incondizionata della congettura di Gauss.

Teorema 1.6. $h(D) \to \infty$ *per* $D \to -\infty$.

Sfortunatamente il metodo della dimostrazione non è effettivo, poiché, se l'Ipotesi di Riemann Generalizzata fosse falsa, tutte le costanti dipenderebbero da uno zero sconosciuto di $L(s,\chi)$ situato fuori dalla retta $\mathrm{Re}(s) = \frac{1}{2}$. Questo zero, che presumibilmente non esiste, è noto come zero di Siegel.

Heilbronn e Linfoot precisarono la dimostrazione per trattare il caso $h(D) = 1$.

Teorema 1.7. *Esistono al più dieci discriminanti fondamentali negativi per cui* $h(D) = 1$, *ovvero* $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$ *e un decimo sconosciuto.*

La possibile esistenza di un decimo campo quadratico complesso con anello degli interi algebrici che è dominio a fattorizzazione unica riflette l'ineffettività della dimostrazione di Hecke-Deuring-Heilbronn. Se tale campo esistesse, l'Ipotesi di Riemann Generalizzata non sarebbe vera. Questo portò ad un fervente lavoro su tale problema.

Nel 1935, con i lavori di Siegel e Tatuzawa, si mostrarono definitivamente tutte le potenzialità e i limiti di questo approccio al problema. Siegel dimostrò un significativo teorema.

Teorema 1.8. *Per ogni $\epsilon > 0$, esiste una costante $c > 0$, che non può essere effettivamente calcolata, tale che*

$$h(D) > c\ |D|^{\frac{1}{2}-\epsilon}$$

Tatuzawa si limitò a precisare il risultato di Siegel, mostrando che il teorema è vero con una costante positiva effettivamente calcolabile per ogni $D < 0$ eccetto al più un caso eccezionale.

Tutti questi tentativi, in ogni caso, non risolsero il Problema di Gauss, a causa della loro ineffetività. Fatta eccezione per alcuni casi semplici, non si sapeva ancora se le tavole di Gauss fossero complete. Tutto quello che si sapeva è che se Gauss si sbagliava l'Ipotesi di Riemann Generalizzata era falsa. Si può immaginare facilmente quante discussioni generasse tale argomento tra gli anni 40 e 50.

Un professore di liceo, Kurt Heegner, diceva di aver risolto il Problema di Gauss sul numero di classe 1. Il lavoro di Heegner conteneva alcuni errori e in generale, al tempo, non gli fu dato credito. Morì prima che qualcuno avesse realmente capito quello che aveva fatto.

1.3 La soluzione

Bisogna aspettare la fine degli anni 60 per intravedere una soluzione definitiva del problema.

Baker nel 1966 e Stark nel 1967 dimostrarono che non esiste un decimo campo quadratico complesso con $h(D) = 1$, portando a conclusione la soluzione del Problema di Gauss sul numero di classe 1. La dimostrazione di Baker si basa sulla verifica che tre logaritmi sono linearmente independenti e riduce quindi il problema ad un numero finito di calcoli. La dimostrazione di Stark è totalmente differente da quella di Baker, ma ha molti tratti comuni al lavoro di Heegner.

Nel 1968 Deuring corresse gli errori della dimostrazione di Heegner e nello stesso anno Siegel diede un'ulteriore dimostrazione del problema $h(D) = 1$.

Nel 1970 Chowla portò a una sintesi unitaria tali lavori, scrivendo l'articolo *The Heegner-Stark-Baker-Deuring-Siegel theorem*.

Nel 1971 Baker e Stark mostrarono che esistono esattamente diciotto campi quadratici complessi che hanno numero di classe di ideali uguale a 2. Usarono entrambi il metodo della indipendenza lineare di certi logaritmi.

É a questo punto che si inserisce il lavoro di Goldfeld, oggetto principale del nostro studio. Nel presentarlo daremo per nota la nozione di alcuni oggetti che saranno illustrati nei capitoli successivi.

Sia E una curva ellittica su $\mathbb{Q}$ con funzione L associata $L_E(s)$. Sia $g = \text{rango}(E(\mathbb{Q}))$ e N il conduttore di E. Sia $D < 0$ un discriminante fondamentale e $\mathbb{Q}(\sqrt{D})$ un campo quadratico complesso. Sia infine $\chi_D(n)$ il carattere di Dirichlet associato al campo quadratico $\mathbb{Q}(\sqrt{D})$. Vale allora il seguente teorema.

Teorema 1.9. *Sia $\mu = 1, 2$ tale che $\chi_D(-N) = (-1)^{g-\mu}$.*
Se per E vale la congettura di Birch-Swinnerton-Dyer, ovvero se

$$L_E(s) \sim c_E(s-1)^g$$

per una certa costante c_E dipendente da E, allora, se $(N, D) = 1$, si ha

$$h(D) > \frac{c}{g^{4g}N^{13}}(\log|D|)^{g-\mu-1}e^{-21\sqrt{g\log\log|D|}}$$

dove c è una costante assoluta indipendente da E.

Vale un teorema analogo se $(D, N) > 1$.

Se la congettura di Birch-Swinnerton-Dyer è vera per un'opportuna curva ellittica di rango $g = 3$, allora il teorema di Goldfeld risolve effettivamente il Problema di Gauss sul numero di classi di ideali. Quindi l'ultimo passo che mancava era mostrare che esiste una curva ellittica la cui funzione L associata ha uno zero triplo in $s = 1$.

Nel 1981 Birch e Stephens utilizzarono il metodo introdotto da Heegner per la costruzione di punti canonici di ordine infinito su certe classi di curve ellittiche (i cosiddetti punti di Heegner).

Nel 1983 Gross e Zagier ottennero il risultato fondamentale (cfr. [Gro86]). Sia E una curva ellittica definita su $\mathbb{Q}$ con conduttore N e rango dispari g. Per $D < 0$, $D \equiv 1 \pmod{4N}$, sia $E^{(D)}$ la curva ellittica "twistata" di conduttore ND^2.

Teorema 1.10. *Se $L_E(s)$ ha uno zero di ordine dispari in $s = 1$, allora esiste un punto di Heegner $P_D \in E(\mathbb{Q})$ tale che*

$$L'_E(1)L_{E^{(D)}}(1) = \frac{\pi^2 w}{\sqrt{|D|}}\langle P_D, P_D\rangle$$

dove w è una costante dipendente da E e $\langle\ ,\ \rangle$ è un prodotto interno (che definiremo meglio più avanti).

Considerando

$$\bar{E} : -139y^2 = x^3 + 4x^2 - 48x + 80$$

con $N = 37 \cdot (139)^2$ e $g = 3$, si può mostrare che il punto di Heegner P_{-139} è banale.

Corollario 1.1. *$L_{\bar{E}}(s)$ ha uno zero triplo in $s = 1$.*

Tale risultato, unito al teorema di Goldfeld (cfr. [Gol76]), permette di ottenere il Teorema di Golfeld-Gross-Zagier.

Teorema 1.11. *Per ogni $\epsilon > 0$ esiste una costante effettivamente calcolabile $c_\epsilon > 0$ tale che*

$$h(D) > c_\epsilon (\log |D|)^{1-\epsilon}$$

A meno di un numero finito di calcoli, il Problema di Gauss sul numero di classi di ideali è risolto. Infatti, fissato h, abbiamo che se $h(D) = h$, allora

$$D < \exp\left\{ \left(\frac{h}{c} \right)^{\frac{1}{1-\epsilon}} \right\}$$

Pertanto "basta" verificare cosa accade fino a tale valore e ciò si può fare comunque con un numero finito di conti.

Nel 1984 Oesterlé precisò il risultato di Goldfeld in [Oes85], ottendendo la stima

$$h(D) > c \cdot \prod_{p|D} \left(1 - \frac{2}{\sqrt{p}} \right) \cdot \log |D|$$

per ogni D, dove c è una costante assoluta ed effettivamente calcolabile. In [Oes88] sono riportati i seguenti risultati, che danno un'idea dell'effettiva stima che si può ottenere con questo metodo, con diverse curve ellittiche di partenza:

$$\begin{aligned} h(D) = 3 &\quad \Rightarrow \quad \log |D| \leq 165 \\ h(D) = 4 &\quad \Rightarrow \quad \log |D| \leq 2640 \\ h(D) = 5 &\quad \Rightarrow \quad \log |D| \leq 275 \\ h(D) = 6 &\quad \Rightarrow \quad \log |D| \leq 1320 \end{aligned}$$

Capitolo 2

Curve ellittiche e curve modulari

Lo scopo di questo lungo capitolo è introdurre gli oggetti fondamentali per lo studio successivo. Incominceremo dalle curve ellittiche, ne vedremo i legami con i tori complessi e introdurremo infine la nozione di curva modulare.

2.1 Elementi di teoria delle curve ellittiche

Incominciamo dalla definizione di curva ellittica.

Definizione 2.1. *Una* ***curva ellittica*** *è una curva algebrica proiettiva di genere* 1*, nella quale viene specificato un punto* O*.*

Dato un campo K, si dice che la curva ellittica E è **definita su** K se i coefficienti della sua equazione appartengono a K e O è a coordinate in K. In tal caso i punti di E sono tutti i punti a coordinate in $\overline{K}$.

Ogni curva ellittica possiede una legge di composizione interna (indicata solitamente con $+$), che si può sintetizzare nel seguente modo: dati tre punti $P, Q, R \in E$, allora

$$P + Q + R = 0 \qquad \text{se e solo se} \qquad P, Q, R \text{ sono allineati}$$

Per dettagli cfr. [Sil], pag.55. L'insieme dei punti di E è gruppo abeliano rispetto a tale legge di composizione, con elemento neutro O.
Indichiamo con $E(K)$ il gruppo dei punti a coordinate in K.

Ogni curva ellittica E definita su K è isomorfa a una curva algebrica piana di equazione

$$y^2 + axy + by = x^3 + cx^2 + dx + e \qquad \text{con } a, b, c, d, e \in K$$

che chiamiamo **forma di Weierstrass** della curva E.
Se $\text{char}(K) \neq 2, 3$ l'equazione si può semplificare ulteriormente in

$$y^2 = 4x^3 - g_2 x - g_3 \qquad \text{con } g_2, g_3 \in K$$

In entrambe le forme, il punto O è l'unico punto all'infinito, ovvero $O = Y_\infty$ (cfr. [Sil], pag.47-50 e pag.63).
Ci sono due quantità associate a tale equazione:

$$\Delta = g_2^3 - 27g_3^2 \qquad\qquad j = 1728\,\frac{g_2^3}{\Delta}$$

Si può dimostrare che la curva E è non singolare se e solo se $\Delta \neq 0$ (cfr. [Sil], pag.50). La j invece caratterizza le curve ellittiche, nel senso che è invariante per isomorfismi, come vedremo più avanti nel dettaglio.

Le mappe che andiamo a considerare sulle curve ellittiche sono dette isogenie e tengono conto sia della struttura geometrica che di quella algebrica di questi oggetti. Cominciamo dalla definizione.

Definizione 2.2. *Siano E_1 ed E_2 curve ellittiche. Un'**isogenia** tra E_1 ed E_2 è un morfismo*

$$\phi : E_1 \to E_2$$

che soddisfa $\phi(O) = O$.
Denotiamo con $Hom(E_1, E_2)$ l'insieme delle isogenie tra E_1 ed E_2.
*Diciamo che E_1 ed E_2 sono **isogene** se esiste un'isogenia $\phi \in Hom(E_1, E_2)$ non nulla.*

La definizione data è prettamente geometrica, ma si dimostra immediatamente che le isogenie sono anche omomorfismi di gruppi.

Teorema 2.1. *Consideriamo un'isogenia*

$$\phi : E_1 \to E_2$$

Si ha

$$\phi(P+Q) = \phi(P) + \phi(Q) \qquad \textit{per ogni } P, Q \in E_1$$

Dimostrazione. cfr. [Sil], pag. 75. □

2.2 Tori complessi

Introduciamo ora una seconda famiglia di oggetti, apparentemente diversi da quelli precedenti. Premettiamo una definizione.

Definizione 2.3. *Chiamiamo* ***reticolo*** *su* $\mathbb{C}$ *un sottogruppo* $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ *generato da due elementi* $\omega_1, \omega_2 \in \mathbb{C}$ *linearmente indipendenti su* $\mathbb{R}$

Da ogni reticolo possiamo ottenere una superficie di Riemann compatta, di genere 1, detta toro complesso.

Definizione 2.4. *Definiamo* ***toro complesso di dimensione*** 1 *il gruppo quoziente* $\mathbb{C}/\Lambda$*, dove* Λ *è un reticolo su* $\mathbb{C}$*, dotato di struttura di superficie di Riemann nel modo naturale.*

Considerando i tori complessi come superfici di Riemann, possiamo analizzare le funzioni meromorfe sui tori complessi. In realtà, si usa vedere tali funzioni come funzioni complesse a valori complessi invarianti rispetto agli elementi del reticolo.

Definizione 2.5. *Definiamo* ***funzione ellittica*** *rispetto a* Λ*, con* Λ *reticolo su* $\mathbb{C}$*, una funzione meromorfa su* $\mathbb{C}$ *tale che*

$$f(z+\omega) = f(z) \qquad \textit{per ogni } \omega \in \Lambda$$

Denotiamo con $\mathbb{C}(\Lambda)$ *l'insieme di tutte le funzioni ellittiche rispetto a* Λ*.*

Tra tutte le funzioni ellittiche, la più importante è certamente la funzione $\wp$ di Weierstrass, che definiamo insieme alla serie di Eisenstein, altro oggetto fondamentale per quanto seguirà.

Definizione 2.6. *Sia $\Lambda \subset \mathbb{C}$ un reticolo.*

*Definiamo la **funzione** $\wp(\Lambda)$ **di Weierstrass** come*

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

*Definiamo **serie di Eisenstein di peso** $2k$ la serie*

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^{2k}}$$

Per semplicità, se il reticolo Λ è fissato, scriveremo soltanto $\wp$ e G_{2k}.

Vale il seguente teorema, che descrive le proprietà basilari di questi due oggetti.

Teorema 2.2. *Sia $\Lambda \subset \mathbb{C}$ un reticolo. Allora*

1. *La serie che compare nella definizione della $\wp$ di Weierstrass converge assolutamente e uniformemente su ogni sottoinsieme compatto di $\mathbb{C} \setminus \Lambda$. Essa definisce quindi una funzione meromorfa ed ellittica con poli (di ordine 2) in tutti e soli i punti di Λ.*

2. *La serie di Eisenstein $G_{2k}(\Lambda)$ è assolutamente convergente per ogni $k > 1$.*

Dimostrazione. cfr. [Sil], pag.153. □

Ogni funzione ellittica è in realtà funzione razionale della $\wp$ di Weierstrass e della sua derivata, come afferma il seguente teorema.

Teorema 2.3. *Sia $\Lambda \subset \mathbb{C}$ un reticolo. Allora*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$$

Dimostrazione. cfr. [Sil], pag.154. □

2.3 Legame tra curve ellittiche e tori complessi

Abbiamo introdotto separatamente curve ellittiche e tori complessi. Andiamo ora a vedere i legami tra queste due famiglie di oggetti, evidenziando l'equivalenza tra la categoria delle curve ellittiche definite su $\mathbb{C}$ con morfismi le isogenie e la categoria dei tori complessi con morfismi le mappe olomorfe. Incominciamo da un teorema, che segnala un primo legame tra di esse.

Teorema 2.4. *Sia $\Lambda \subset \mathbb{C}$ un reticolo. Per ogni $z \in \mathbb{C} \setminus \Lambda$ si ha*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

dove $g_2 = g_2(\Lambda) = 60\ G_4(\Lambda)$ e $g_3 = g_3(\Lambda) = 140\ G_6(\Lambda)$.

Dimostrazione. cfr. [Sil], pag.157. □

Ogni toro complesso può essere visto come curva ellittica, come afferma il seguente teorema.

Teorema 2.5. *Sia $\Lambda \subset \mathbb{C}$ un reticolo.*

Il polinomio

$$f(x) = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

ha radici distinte.

Il suo discriminante

$$\Delta(\Lambda) = g_2^3 - 27g_3^2$$

è diverso da zero.

Allora

$$E : y^2 = 4x^3 - g_2x - g_3$$

è una curva ellittica su $\mathbb{C}$, non singolare.

La mappa

$$\begin{aligned} \phi : \quad \mathbb{C}/\Lambda &\to E \hookrightarrow \mathbb{P}^n(\mathbb{C}) \\ z \notin \Lambda &\mapsto (\wp(z) : \wp'(z) : 1) \\ \omega \in \Lambda &\mapsto (0 : 1 : 0) \end{aligned}$$

è un isomorfismo di superfici di Riemann che è omomorfismo di gruppi.

Dimostrazione. cfr. [Sil], pag.158. □

Siano ora Λ_1 e Λ_2 due reticoli. Se $\alpha \in \mathbb{C}$ ha la proprietà che $\alpha\Lambda_1 \subset \Lambda_2$, allora la moltiplicazione per α

$$\begin{array}{rccc} \phi_\alpha : & \mathbb{C}/\Lambda_1 & \to & \mathbb{C}/\Lambda_2 \\ & z \pmod{\Lambda_1} & \mapsto & \alpha z \pmod{\Lambda_2} \end{array}$$

è chiaramente un omomorfismo olomorfo.

Vediamo ora un teorema fondamentale per il nostro studio.

Teorema 2.6. *Valgono:*

1. *La corrispondenza*

$$\begin{array}{rcl} \{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subset \Lambda_2\} & \to & \left\{ \begin{array}{c} \textit{mappe olomorfe } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \textit{con } \phi(0) = 0 \end{array} \right\} \\ \alpha & \mapsto & \phi_\alpha \end{array}$$

   è biunivoca.

2. *Siano E_1 ed E_2 curve ellittiche corrispondenti ai reticoli Λ_1 e Λ_2. Allora l'inclusione naturale*

$$\{\textit{isogenie } \phi : E_1 \to E_2\} \hookrightarrow \left\{ \begin{array}{c} \textit{mappe olomorfe } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \textit{con } \phi(0) = 0 \end{array} \right\}$$

   è biunivoca.

Dimostrazione. 1. Se $\phi_\alpha = \phi_\beta$, allora per ogni $z \in \mathbb{C}$, $\alpha z \equiv \beta z \pmod{\Lambda_2}$. Quindi la mappa $z \mapsto (\alpha - \beta)z$ manda $\mathbb{C}$ in Λ_2. Poiché Λ_2 è discreto, questa mappa deve essere costante. Pertanto $\alpha = \beta$.

Sia ora $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ una mappa olomorfa con $\phi(0) = 0$. Allora, poiché $\mathbb{C}$ è semplicemente connesso, possiamo sollevare ϕ a una mappa olomorfa $f : \mathbb{C} \to \mathbb{C}$ con $f(0) = 0$, tale che il seguente diagramma commuta:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\phi} & \mathbb{C}/\Lambda_2 \end{array}$$

Per ogni $\omega \in \Lambda_1$, $f(z+\omega) \equiv f(z) \pmod{\Lambda_2}$ per ogni $z \in \mathbb{C}$. Ricordando ancora che Λ_2 è discreto, otteniamo che $f(z+\omega)-f(z)$ deve essere indipendente da z. Allora

$$f'(z+\omega) = f'(z) \qquad \text{per ogni } z \in \mathbb{C},\ \omega \in \Lambda_1$$

Quindi $f'(z)$ è una funzione ellittica olomorfa, perciò costante. Pertanto $f(z) = \alpha z + \gamma$ per qualche $\alpha, \gamma \in \mathbb{C}$. Poiché $f(0) = 0$, si ha $\gamma = 0$, e $f(\Lambda_1) \subset \Lambda_2$ implica $\alpha\Lambda_1 \subset \Lambda_2$, e quindi $\phi = \phi_\alpha$.

2. Notiamo che, poiché un'isogenia è data localmente da funzioni razionali definite ovunque, cioè è un morfismo, la mappa indotta sui corrispondenti tori complessi sarà olomorfa. Allora l'associazione

$$\mathrm{Hom}(E_1, E_2) \to \text{Mappe olomorfe}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$$

è ben definita ed è chiaramente iniettiva.

Proviamo ora la suriettività. Da (1.) è sufficiente considerare le mappe della forma ϕ_α con $\alpha \in \mathbb{C}^*$ che soddisfa $\alpha\Lambda_1 \subset \Lambda_2$. La mappa indotta sull'equazione di Weierstrass è data da

$$\begin{array}{ccc} E_1 & \to & E_2 \\ (\wp(z;\Lambda_1) : \wp'(z;\Lambda_1) : 1) & \mapsto & (\wp(\alpha z;\Lambda_2) : \wp'(\alpha z;\Lambda_2) : 1) \end{array}$$

quindi dobbiamo mostrare che $\wp(\alpha z;\Lambda_2)$ e $\wp'(\alpha z;\Lambda_2)$ possono essere espresse come funzioni razionali di $\wp(z;\Lambda_1)$ e $\wp'(z;\Lambda_1)$. Usando il fatto che $\alpha\Lambda_1 \subset \Lambda_2$, vediamo che per ogni $\omega \in \Lambda_1$,

$$\wp(\alpha(z+\omega);\Lambda_2) = \wp(\alpha z + \alpha\omega;\Lambda_2) = \wp(\alpha z;\Lambda_2)$$

e similmente per $\wp'(\alpha z;\Lambda_2)$. Pertanto $\wp(\alpha z;\Lambda_2)$ e $\wp'(\alpha z;\Lambda_2)$ appartengono a $\mathbb{C}(\Lambda_1)$. Per il Teorema 2.3 si ha la tesi. □

Corollario 2.1. *Siano E_1 ed E_2 due curve ellittiche definite su $\mathbb{C}$, corrispondenti ai reticoli Λ_1 e Λ_2.*

Allora E_1 ed E_2 sono isomorfe (su $\mathbb{C}$) se e solo se Λ_1 e Λ_2 sono omoteticamente equivalenti (i.e. $\Lambda_1 = \alpha\Lambda_2$ per un certo $\alpha \in \mathbb{C}^*$).

Dimostrazione. Se E_1 ed E_2 sono isomorfe vuol dire che esiste un isomorfismo tra $\mathbb{C}/\Lambda_1$ e $\mathbb{C}/\Lambda_2$. Dal Teorema 2.6 si ha che questo isomorfismo è del tipo ϕ_α, con $\alpha \in \mathbb{C}^*$ tale che $\alpha\Lambda_1 \subset \Lambda_2$. La mappa ϕ_α ha come inversa la mappa $\phi_{\alpha^{-1}}$, essendo la moltiplicazione per uno scalare. Quindi si ha che $\alpha^{-1}\Lambda_2 \subset \Lambda_1$, da cui $\alpha\Lambda_1 = \Lambda_2$.
Il viceversa è ovvio, sempre dal Teorema 2.6. □

Osservazione 2.1. Poiché la mappa ϕ_α è chiaramente un omomorfismo, il Teorema 2.6 implica che ogni mappa olomorfa da $E_1(\mathbb{C})$ a $E_2(\mathbb{C})$ che manda O in O è necessariamente un omomorfismo. Questo risultato è analogo a quello del Teorema 2.1.

Finora abbiamo definito le curve ellittiche e i tori complessi, le mappe tra di essi e abbiamo visto come passare dai tori complessi alle curve ellittiche tramite la funzione di Weiestrass. Con il **Teorema di Uniformizzazione** chiudiamo il cerchio.

Teorema 2.7. *Dati due numeri complessi a_2 e a_3 tali che $a_2^3 - 27a_3^2 \neq 0$, esiste un reticolo $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ tale che*

$$g_2(\Lambda) = a_2 \qquad g_3(\Lambda) = a_3$$

Dimostrazione. [Apo], pag.43. Noi ne daremo dimostrazione più avanti dopo aver introdotto le funzioni modulari. □

Corollario 2.2. *Sia E una curva ellittica. Allora esiste un reticolo $\Lambda \subset \mathbb{C}$, unico a meno di omotetie, e un isomorfismo*

$$\begin{aligned} \phi: \ \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\mapsto (\wp(z;\Lambda) : \wp'(z;\Lambda) : 1) \end{aligned}$$

di superfici di Riemann che è anche isomorfismo di gruppi.

Dimostrazione. L'esistenza è garantita dal Teorema 2.5 e dal Teorema 2.7. L'unicità è il Corollario 2.1. □

Data una curva ellittica su $\mathbb{C}$, possiamo ricostruire il reticolo grazie al seguente risultato.

Proposizione 2.1. *Sia E una curva ellittica definita su $\mathbb{C}$ con funzioni coordinate di Weiestrass x e y. Allora, dati α e β cammini su $E(\mathbb{C})$ che sono base per $H_1(E, \mathbb{Z})$,*

$$\omega_1 = \int_\alpha dx/y \qquad e \qquad \omega_2 = \int_\beta dx/y$$

sono numeri complessi linearmente indipendenti su $\mathbb{R}$.
Se $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, la mappa

$$\begin{aligned} F: \quad E(\mathbb{C}) &\to \mathbb{C}/\Lambda \\ P &\mapsto \textstyle\int_O^P dx/y \ (mod\ \Lambda) \end{aligned}$$

è un isomorfismo di superfici di Riemann che è anche isomorfismo di gruppi.

Quindi tori complessi (che sono superfici di Riemann, oggetti analitici complessi) e curve ellittiche definite su $\mathbb{C}$ (che sono insiemi degli zeri di certi polinomi, oggetti algebrici) sono interscambiabili.

Tenendo conto di quanto detto in questo paragrafo, il termine "curva ellittica" definita su $\mathbb{C}$ (sinteticamente, "complessa") sarà sinonimo di "toro complesso". In questa identificazione abbiamo anche evidenziato quali sono le mappe tra curve ellittiche e come si possano definire funzioni meromorfe su di esse, rifacendosi alla struttura di tori complessi.

2.4 Gruppo modulare

Introduciamo ora il gruppo modulare, oggetto fondamentale per dare un'ulteriore interpretazione delle curve ellittiche. Cominciamo ricordando una definizione basilare di algebra lineare.

Definizione 2.7. *Definiamo* ***gruppo speciale lineare*** $SL_2(\mathbb{Z})$ *il sottogruppo delle matrici invertibili a coefficienti in $\mathbb{Z}$, aventi determinante* 1.

Possiamo allora definire da subito il gruppo modulare.

Definizione 2.8. *Una* ***trasformazione lineare fratta*** *è una funzione complessa a valori complessi della forma:*

$$f(z) = \frac{az+b}{cz+d}$$

con $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

Definiamo ***gruppo modulare*** *il gruppo delle trasformazioni lineari fratte.*

Osservazione 2.2. Il gruppo modulare è isomorfo al gruppo proiettivo speciale lineare $PSL_2(\mathbb{Z})$, che è il quoziente $SL_2(\mathbb{Z})/\{\pm I\}$. Spesso identificheremo il gruppo modulare con $SL_2(\mathbb{Z})$, confondendo trasformazioni con matrici e sottointendendo che le matrici sono determinate a meno di segno. Indichiamo il gruppo modulare con Γ.

L'importanza del gruppo modulare è legata in gran parte al fatto che esso agisce come gruppo di trasformazioni del semipiano superiore

$$\mathfrak{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

Infatti, se $\alpha \in \Gamma$ è la trasformazione $\alpha : z \to \frac{az+b}{cz+d}$, si ha

$$\mathrm{Im}(\alpha(z)) = \frac{(ad-bc)\ \mathrm{Im}(z)}{|cz+d|^2} = \frac{\mathrm{Im}(z)}{|cz+d|^2}$$

da cui si ha che $z \in \mathfrak{H}$ implica $\alpha(z) \in \mathfrak{H}$. Tutte le altre verifiche sono ovvie.

Analogamente all'intero piano complesso, $\mathfrak{H}$ può essere considerato come superficie di Riemann. Un modo di pensare a Γ è come a un gruppo di "simmetrie" di $\mathfrak{H}$.

L'azione di un gruppo su un insieme determina delle classi di equivalenza, dette **orbite**: poniamo $z \sim w$ se e solo se esiste $\alpha \in \Gamma$ tale che $z = \alpha(w)$. Denotiamo con $\Gamma\backslash\mathfrak{H}$ il quoziente di $\mathfrak{H}$ rispetto a tale relazione d'equivalenza.

Definizione 2.9. *Un* ***dominio fondamentale*** *D per Γ in $\mathfrak{H}$ è un sottoinsieme di $\mathfrak{H}$ tale che ogni orbita di Γ ha un elemento in D e due elementi di D sono nella stessa orbita se e solo se appartengono al bordo di D.*

Solitamente si considera come dominio fondamentale quello definito nel seguente teorema.

Teorema 2.8. *Un dominio fondamentale per* Γ *in* $\mathfrak{H}$ *è l'insieme*

$$D = \left\{ z \in \mathfrak{H} \;\middle|\; -\frac{1}{2} \leq Re(z) \leq \frac{1}{2} \text{ e } |z| \geq 1 \right\}$$

Inoltre gli elementi

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad e \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

generano Γ.

Dimostrazione. [Lanb], pag.30. □

Insieme al gruppo modulare si possono definire delle funzioni, invarianti sotto la sua azione.

Definizione 2.10. *Definiamo* ***funzione modulare*** *una funzione meromorfa su* $\mathfrak{H}$ *invariante sotto l'azione di* Γ. *In altre parole,* f *funzione meromorfa è modulare se*

$$f(\alpha(z)) = f(z) \qquad \forall \alpha \in \Gamma$$

Notiamo che le funzioni modulari sono analoghe alle funzioni ellittiche, con diverso dominio e gruppo di simmetria.

Le funzioni modulari e quelle ellittiche sono casi speciali di **funzioni automorfe**, che sono funzioni meromorfe in una o più variabili complesse definite su una certa varietà complessa e invarianti sotto un certo gruppo di trasformazioni, dette simmetrie, della varietà.
Possiamo dare una definizione più debole.

Definizione 2.11. *Definiamo* ***funzione modulare di peso*** k, *con* $k \in \mathbb{Z}$, *una funzione meromorfa* f *tale che*

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

per ogni trasformazione in Γ.

Osservazione 2.3. Notiamo che k deve essere pari se f non è identicamente nulla. Infatti, se consideriamo $-I \in \Gamma$ abbiamo che $f(z) = (-1)^k f(z)$.

Osservazione 2.4. Ricordiamo che $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ e che il fattore $c\tau + d$ in questo caso è semplicemente 1. Quindi ogni funzione modulare (o modulare di peso k) f è periodica di periodo 1. Quindi f ha uno sviluppo in serie di Fourier del tipo

$$f(z) = \sum_{n=-m}^{\infty} c_n e^{2\pi i n z}$$

Sia $D = \{q \in \mathbb{C} \mid |q| < 1\}$ il disco aperto unitario, sia $D' = D \setminus \{0\}$ e ricordiamo dall'analisi complessa che la funzione olomorfa, di periodo 1,

$$\tau \mapsto e^{2\pi i \tau} = q$$

manda $\mathfrak{H}$ in D'. Allora, in corrispondenza di f, la funzione $g : D' \to \mathbb{C}$, dove $g(q) = f(\log(q)/(2\pi i))$ è ben definita, e $f(\tau) = g(e^{2\pi i \tau})$. Se f è olomorfa su $\mathfrak{H}$, allora g è olomorfa su D' e quindi g ha sviluppo in serie di Laurent $g(q) = \sum_{n \in \mathbb{Z}} c_n q^n$ per $q \in D'$.
La relazione $|q| = e^{-2\pi \mathrm{Im}(\tau)}$ mostra che $q \to 0$ se $\mathrm{Im}(\tau) \to \infty$. Quindi diciamo che f è **olomorfa in** ∞ se g si estende olomorficamente a $q = 0$, i.e. se la serie di Laurent è sugli interi non negativi. Questo significa che f ha sviluppo in serie di Fourier

$$f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi i n z}$$

Se f, funzione modulare, è olomorfa per ogni $z \in \mathfrak{H}$ ed in ∞, diciamo che è **forma modulare** (analogamente per le funzioni modulari di peso k). Spesso si parla di forme modulari anche per funzioni modulari olomorfe in $\mathfrak{H}$ e non in ∞. In tal caso parleremo di forme modulari in $\mathfrak{H}$. Definiamo infine $f(\infty) := c_0$. Se $c_0 = 0$ diciamo che f è una **forma cuspidale**.
Denotiamo con $\mathcal{M}_k(\Gamma)$ l'insieme delle forme modulari di peso k e con $\mathcal{S}_k(\Gamma)$ l'insieme delle forme modulari cuspidali di peso k. Si verifica facilmente che entrambi sono spazi vettoriali su $\mathbb{C}$.

2.5 $\Gamma \setminus \mathfrak{H}$ come spazio di moduli

Abbiamo introdotto $\Gamma \setminus \mathfrak{H}$ come oggetto geometrico. Possiamo ora reinterpretarlo come spazio di moduli, di cui richiamiamo la definizione.

Definizione 2.12. *Uno **spazio di moduli** è un oggetto geometrico i cui punti parametrizzano classi di isomorfismo di oggetti geometrici.*

Abbiamo visto che due tori complessi $\mathbb{C}/\Lambda_1$ e $\mathbb{C}/\Lambda_2$ sono isomorfi se e solo se esiste $\alpha \in \mathbb{C}^*$ tale che $\alpha\Lambda_1 = \Lambda_2$.
Sia $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Abbiamo

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \omega_2(\mathbb{Z}\tau \oplus \mathbb{Z}) = \omega_2\Lambda_\tau$$

dove $\tau = \frac{\omega_1}{\omega_2} \in \mathbb{C}/\mathbb{R}$.
Si ha perciò

$$\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda_\tau$$

Inoltre possiamo supporre $\tau \in \mathfrak{H}$ (altrimenti basta scambiare ω_1 con ω_2).
Si noti

$$\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z} = \Lambda_{\tau+1} = \mathbb{Z}(\tau+1) \oplus \mathbb{Z} = -\tau\Lambda_{-\frac{1}{\tau}} = -\tau\left(\mathbb{Z}\left(-\frac{1}{\tau}\right) \oplus \mathbb{Z}\right)$$

da cui

$$\mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{T(\tau)} \cong \mathbb{C}/\Lambda_{S(\tau)}$$

Generalizziamo. Notiamo innanzitutto che

$$\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2' \quad \Longleftrightarrow \quad \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

con ω_1, ω_2 e ω_1', ω_2' basi orientate $\left(\text{i.e. } \frac{\omega_1}{\omega_2}, \frac{\omega_1'}{\omega_2'} \in \mathfrak{H}\right)$ e $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

Abbiamo quindi la seguente proposizione.

Proposizione 2.2. *Siano $\tau, \tau' \in \mathfrak{H}$. Allora*

$$\mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'} \qquad \textit{se e solo se} \qquad \textit{esiste } \gamma \in \Gamma \textit{ tale che } \tau' = \gamma(\tau)$$

Dimostrazione. Abbiamo $\mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'}$ se e solo se esiste $\alpha \in \mathbb{C}^*$ tale che $\alpha\Lambda_\tau = \Lambda_{\tau'}$, cioè tale che $\mathbb{Z}(\alpha\tau) \oplus \mathbb{Z}\alpha = \mathbb{Z}\tau' \oplus \mathbb{Z}$.

Poiché $\tau, \tau' \in \mathfrak{H}$, questo accade se e solo se

$$\begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha\tau \\ \alpha \end{pmatrix}$$

con $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, come già osservato.

Quest'ultima condizione è equivalente a chiedere che

$$\tau' = \frac{a(\alpha\tau) + b\alpha}{c(\alpha\tau) + d\alpha} = \frac{a\tau + b}{c\tau + d} = \gamma(\tau) \qquad \text{con } \gamma \in \Gamma$$

□

Possiamo quindi concludere che $\Gamma\backslash\mathfrak{H}$ è spazio di moduli di curve ellittiche definite su $\mathbb{C}$, ovvero ogni punto di $\Gamma\backslash\mathfrak{H}$ rappresenta una classe di isomorfismo di curve ellittiche definite su $\mathbb{C}$.

Ricapitolando, presa una curva ellittica E, consideriamo il toro complesso $\mathbb{C}/\Lambda$ associatole mediante il Teorema di Uniformizzazione, ci riconduciamo a Λ_τ e consideriamo infine la classe di τ (mod Γ). Possiamo inoltre ridurci sempre a un rappresentante nel dominio fondamentale D.

2.6 La funzione modulare j

Sia Λ un reticolo e $k > 1$ intero. Consideriamo la serie di Eiesenstein $G_{2k}(\Lambda)$ di peso $2k$ relativa al reticolo Λ. Ricordiamo che

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda\backslash\{0\}} \omega^{-2k}$$

Grazie al Teorema 2.2, possiamo considerare G_{2k} come una funzione di reticolo, ovvero funzione dall'insieme dei reticoli su $\mathbb{C}$ a valori in $\mathbb{C}$. Come tale si verifica ovviamente che

$$G_{2k}(\alpha\Lambda) = \alpha^{-2k} G_{2k}(\Lambda)$$

per ogni $\alpha \in \mathbb{C}^*$.

Possiamo ora ridurci a considerare i reticoli del tipo Λ_τ, con $\tau \in \mathfrak{H}$. In tal modo possiamo considerare le serie di Eisenstein come funzioni complesse, con dominio il semipiano $\mathfrak{H}$, a valori complessi:

$$G_{2k}(\tau) = G_{2k}(\Lambda_\tau) = \sum_{(m,n)\in(\mathbb{Z}\times\mathbb{Z})\setminus(0,0)} \frac{1}{(m\tau+n)^{2k}}$$

Sempre dal Teorema 2.2 abbiamo che questa serie è assolutamente convergente per ogni $\tau \in \mathfrak{H}$ ed è facile osservare che per $k > 2$ è anche uniformemente convergente in ogni compatto di $\mathfrak{H}$. Pertanto $G_{2k}(\tau)$ è una funzione olomorfa su $\mathfrak{H}$.

Consideriamo ora $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. Da quanto detto finora, abbiamo che

$$G_{2k}(\gamma(\tau)) = (c\tau + d)^{2k} G_{2k}(\tau)$$

Pertanto ogni $G_{2k}(\tau)$, con $k > 2$, è una forma modulare di peso $2k$.

Consideriamo ora le due forme modulari

$$g_2(\tau) = 60\ G_4(\tau) \qquad \text{e} \qquad g_3(\tau) = 140\ G_6(\tau)$$

di peso rispettivamente 4 e 6.

Da queste otteniamo la forma modulare

$$\Delta(\tau) = g_2^3(\tau) - 27 g_3^2(\tau)$$

di peso 12. Dalle sezioni precedenti risulta che $\Delta(\tau)$ è olomorfa e non nulla su $\mathfrak{H}$.

Possiamo introdurre allora la funzione

$$j(\tau) = 1728\ \frac{g_2^3(\tau)}{\Delta(\tau)}$$

che, essendo rapporto di due forme modulari di peso 12, è una funzione modulare (di peso 0). Poiché poi $\Delta(\tau) \neq 0$ in $\mathfrak{H}$, si ha che $j(\tau)$ è una forma modulare su $\mathfrak{H}$.

Sia $\rho = e^{2\pi i/3}$. Si può allora mostrare che $j(\rho) = 0$, j ha un polo semplice in $i\infty$ (cfr. [Apo], pag. 39) ed è normalizzata in modo da avere in esso residuo 1.

Enunciamo ora un risultato generale che ci sarà utile.

Proposizione 2.3. *Sia f una funzione modulare di peso $2k$, $f \neq 0$. Allora*

$$\nu_{i\infty}(f) + \frac{1}{3}\nu_\rho(f) + \frac{1}{2}\nu_i(f) + \sum_{\tau \neq i,\rho} \nu_\tau(f) = \frac{k}{6}$$

in $\Gamma\backslash\mathfrak{H}$, dove per $\nu_\tau(f)$ si intende l'ordine di polo (con segno negativo) o di zero (con segno positivo) di f in τ.

Dimostrazione. cfr. [Lanb], pag. 33. □

Possiamo allora dimostrare facilmente il seguente teorema.

Teorema 2.9. *La mappa $j : \Gamma\backslash\mathfrak{H} \to \mathbb{C}$ è una biiezione.*

Dimostrazione. Applichiamo la Proposizione 2.3 alla funzione $j(\tau) - \alpha$ per $\alpha \in \mathbb{C}$:

$$\frac{1}{3}\nu_\rho(j-\alpha) + \frac{1}{2}\nu_i(j-\alpha) + \sum_{\tau \neq i,\rho} \nu_\tau(j-\alpha) = 1$$

I termini a sinistra dell'uguale sono tutti maggiori di 0 e questo è possibile se e solo se l'ordine di $j(\tau) - \alpha$ è diverso da 0 in un unico punto. In particolare la molteplicità è 3 in ρ, 2 in i e 1 negli altri punti. In ogni caso il teorema è provato. □

Data $j(\tau)$, possiamo ricostruire la j come funzione di reticolo nel seguente modo: dato un reticolo $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, con ω_1, ω_2 base orientata, poniamo $j(\Lambda) = j\left(\frac{\omega_1}{\omega_2}\right)$.

Se $\Lambda_1 = \alpha\Lambda_2$, per un certo $\alpha \in \mathbb{C}^*$ (fatto che ci assicura l'isomorfismo dei tori complessi corrispondenti), allora $j(\Lambda_1) = j(\Lambda_2)$. Viceversa, il Teorema 2.9 ci dice che, se $j(\Lambda_1) = j(\Lambda_2)$, allora i due tori complessi sono isomorfi e quindi i due reticoli sono omoteticamente equivalenti.

Da queste osservazioni si può dimostrare, come corollario del Teorema 2.9, il Teorema di Uniformizzazione.

Corollario 2.3. *Dati due numeri complessi a_2 e a_3 tali che $a_2^3 - 27a_3^2 \neq 0$, esiste un reticolo $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ tale che*

$$g_2(\Lambda) = a_2 \qquad g_3(\Lambda) = a_3$$

Dimostrazione. Dal Teorema 2.9 esiste un $\tau \in \mathfrak{H}$ tale che

$$j(\tau) = 1728 \, \frac{a_2^3}{a_2^3 - 27a_3^2}$$

Consideriamo Λ_τ. Ci sono 2 casi:

1. $a_2 = 0$. Allora $j(\tau) = 0$ e $\tau = \rho$, come osservato.
   Sia $\alpha \in \mathbb{C}^*$ tale che $\alpha^{-6} g_3(\Lambda_\tau) = a_3 \neq 0$ e sia $\Lambda = \alpha\Lambda_\tau$. Allora $g_3(\Lambda) = \alpha^{-6} g_3(\Lambda_\tau) = a_3$ e
   $$g_2(\Lambda) = \alpha^{-4} g_2(\Lambda_\tau) = \alpha^{-4} g_2(\rho) = a_2 = 0$$

2. $a_2 \neq 0$. Sia $\alpha \in \mathbb{C}^*$ tale che $\alpha^{-4} g_2(\Lambda_\tau) = a_2$ e sia $\Lambda = \alpha\Lambda_\tau$. Allora $g_2(\Lambda) = \alpha^{-4} g_2(\Lambda_\tau) = a_2$. Quindi
   $$\begin{aligned} 1728 \, \tfrac{a_2^3}{a_2^3 - 27a_3^2} &= j(\tau) = j(\Lambda_\tau) = j(\Lambda) = 1728 \, \tfrac{g_2^3(\Lambda)}{g_2^3(\Lambda) - 27g_3^2(\Lambda)} = \\ &= 1728 \, \tfrac{a_2^3}{a_2^3 - 27g_3^2(\Lambda)} \end{aligned}$$
   dove l'uguaglianza $j(\Lambda_\tau) = j(\Lambda)$ segue dal fatto che Λ_τ e Λ sono omoteticamente equivalenti. Questo mostra che $g_3^2(\Lambda) = a_3^2$, da cui $g_3(\Lambda) = \pm a_3$. Scambiando eventualmente α con meno $i\alpha$ (cosicché $g_2(\Lambda)$ rimanga invariato, mentre $g_3(\Lambda)$ cambi di segno), abbiamo la tesi.

□

Se E è una curva ellittica, indichiamo con j_E il valore di $j(\Lambda)$, dove Λ è un reticolo tale che $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Questo valore è indipendente da Λ ed è chiamato j-**invariante** della curva.

Quanto detto finora si può riformulare nel seguente modo: *due curve ellittiche E_1 ed E_2 sono isomorfe se e solo se $j_{E_1} = j_{E_2}$.*

Concludiamo questo paragrafo con una considerazione riguardante le funzioni modulari, in relazione alla funzione j.
Sia $q = q_\tau = e^{2\pi i \tau}$.

Teorema 2.10. *Sia f una forma modulare in $\mathfrak{H}$ e con sviluppo in serie di Laurent*

$$f(q) = \sum_{n=-m}^{\infty} c_n q^n$$

Allora f è un polinomio in j con coefficienti nello $\mathbb{Z}$-modulo generato dai coefficienti c_n.

Dimostrazione. Ricordiamo che una forma modulare in $\mathfrak{H}$ è una funzione modulare olomorfa in $\mathfrak{H}$. Scriviamo

$$f(q) = \frac{c_{-m}}{q^m} + \text{termini di grado superiore}$$

così che $f - c_{-m} j^m$ sia olomorfa su $\mathfrak{H}$ e abbia sviluppo che inizia con al più un termine polare di ordine $m - 1$. Ripetendo il procedimento, possiamo sottrarre a f un polinomio in j con coefficienti nello $\mathbb{Z}$-modulo generato dai coefficienti c_n fino ad ottenere una funzione modulare olomorfa in $\mathfrak{H}$ che si annulla all'infinito ed è quindi identicamente nulla. □

Corollario 2.4. *L'insieme di tutte le funzioni modulari è $\mathbb{C}(j)$.*

Dimostrazione. Ogni funzione modulare è rapporto di forme modulari in $\mathfrak{H}$. Poiché lo $\mathbb{Z}$-modulo generato dai coefficienti c_n di f è un sottoinsieme di $\mathbb{C}$, si ha che ogni forma modulare vive in $\mathbb{C}[j]$. Pertanto ogni funzione modulare appartiene a $\mathbb{C}(j)$. Il viceversa è ovvio. □

2.7 Sottogruppi di congruenza

Abbiamo parlato finora del gruppo modulare Γ e delle funzioni modulari come funzioni invarianti rispetto alla sua azione. Sostituendo Γ con un suo

sottogruppo Γ' possiamo generalizzare la condizione di modularità. Ci limiteremo a considerare i sottogruppi di congruenza, che andremo a definire, in quanto utili ai nostri fini.
In questo paragrafo sarà conveniente considerare Γ come $SL_2(\mathbb{Z})$, in quanto le nozioni che diamo sono più visibili da un punto di vista matriciale.
Da qui in avanti N indicherà un intero positivo.

Definizione 2.13. *Chiamiamo* ***sottogruppo principale di congruenza di livello*** N *il sottogruppo*

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ (mod\ N) \right\}$$

dove la congruenza $(mod\ N)$ *si intende su ogni entrata. In particolare, si ha* $\Gamma(1) = \Gamma$.

Il sottogruppo $\Gamma(N)$ è normale in Γ, essendo il nucleo dell'omomorfismo naturale $\phi : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$.
Si può mostrare che ϕ è suriettivo e quindi

$$\Gamma/\Gamma(N) \cong SL_2(\mathbb{Z}/N\mathbb{Z})$$

da cui si ha che $[\Gamma : \Gamma(N)]$ è finito per ogni N, in particolare

$$[\Gamma : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

dove il prodotto è fatto sui divisori primi di N.

Definizione 2.14. *Un sottogruppo* Γ' *di* Γ *è detto* ***sottogruppo di congruenza*** *se* $\Gamma(N) \subset \Gamma'$ *per qualche intero positivo* N *e in tal caso* Γ' *è detto sottogruppo di congruenza di livello* N.

Dalla definizione segue immediatamente che ogni sottogruppo di congruenza ha indice finito in Γ.

I più importanti sottogruppi di congruenza sono, oltre al sottogruppo principale di congruenza,

$$\Gamma_0(N) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL_2(\mathbb{Z}) \;\middle|\; \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \equiv \left(\begin{array}{cc} * & * \\ 0 & * \end{array} \right) \pmod{N} \right\}$$

e

$$\Gamma_1(N) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL_2(\mathbb{Z}) \;\middle|\; \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \equiv \left(\begin{array}{cc} 1 & * \\ 0 & 1 \end{array} \right) \pmod{N} \right\}$$

dove per "$*$" si intende "non specificato".

Tali sottogruppi soddisfano ovviamente le inclusioni

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \Gamma$$

Si dimostra facilmente che la mappa

$$\begin{array}{rcl} \Gamma_1(N) & \to & \mathbb{Z}/N\mathbb{Z} \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) & \mapsto & b \pmod{N} \end{array}$$

è suriettiva e ha nucleo $\Gamma(N)$. Pertanto $\Gamma(N)$ è normale in $\Gamma_1(N)$ e

$$[\Gamma_1(N) : \Gamma(N)] = N$$

Similmente si mostra che la mappa

$$\begin{array}{rcl} \Gamma_0(N) & \to & (\mathbb{Z}/N\mathbb{Z})^* \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) & \mapsto & d \pmod{N} \end{array}$$

è suriettiva con nucleo $\Gamma_1(N)$, così che $\Gamma_1(N)$ è normale in $\Gamma_0(N)$ e

$$[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N)$$

dove φ è la funzione di Eulero, da cui si deduce che

$$[\Gamma : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p} \right)$$

La nozione di funzione modulare rispetto a un sottogruppo di congruenza Γ' di Γ è la ovvia generalizzazione di quanto già visto. Notiamo che quando

$-I \notin \Gamma'$ esistono funzioni di peso dispari, al contrario del caso generale.

Sviluppiamo ora la definizione di forma modulare rispetto a Γ'.

Sia k un intero e Γ' sottogruppo di congruenza. Una funzione $f : \mathfrak{H} \to \mathbb{C}$ è una forma modulare di peso k rispetto a Γ' se è una funzione modulare rispetto a Γ' e se soddisfa le condizioni di olomorfia che andiamo ad illustrare.

Ogni sottogruppo di congruenza Γ' contiene una matrice di traslazione del tipo $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) : \tau \mapsto \tau + h$ per un certo h intero positivo, minimale. Questo perché Γ' contiene $\Gamma(N)$ per un certo N, quindi contiene $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) : \tau \mapsto \tau + N$, e se vogliamo h minimale abbiamo che h divide N.

Ogni funzione $f : \mathfrak{H} \to \mathbb{C}$ che sia modulare (modulare di peso k) rispetto a Γ' è quindi $h\mathbb{Z}$-periodica e ha pertanto una funzione corrispondente $g : D' \to \mathbb{C}$, dove D' è, come nel caso delle forme modulari, il disco unitario privo di 0, ma, in questo caso, $f(\tau) = g(q_h)$, con $q_h = e^{2\pi i\tau/h}$.

Come precedentemente, se f è olomorfa in $\mathfrak{H}$, la g è olomorfa su D' ed ha sviluppo in serie di Laurent. Diciamo che f è olomorfa in ∞ se g si estende olomorficamente a $q = 0$. Allora f ha sviluppo in serie di Fourier

$$f(\tau) = \sum_{n=0}^{\infty} c_n q_h^n = \sum_{n=0}^{\infty} c_n e^{2\pi i n\tau/h}$$

Per rendere lo spazio vettoriale delle forme modulari di dimensione finita, dobbiamo richiedere l'olomorfia non solo su $\mathfrak{H}$ ma anche nei punti limite. Per i sottogruppi di congruenza l'idea è di aggiungere non solo ∞, ma anche tutto $\mathbb{Q}$, e poi identificare i punti aggiunti equivalenti rispetto a Γ'.

Una classe di equivalenza di punti in $\mathbb{Q} \cup \{\infty\}$ è detta **cuspide** di Γ'.

Quando $\Gamma' = \Gamma$, tutti i razionali sono equivalenti a ∞, e quindi Γ ha una sola cuspide. Poiché ogni $s \in \mathbb{Q}$ ha la forma $s = \gamma(\infty)$ per qualche $\gamma \in \Gamma$, il numero di cuspidi è al più il numero dei laterali $\Gamma'\gamma$ in Γ, ma eventualemente meno, in ogni caso un numero finito, dato che $[\Gamma : \Gamma']$ è finito.

Una forma modulare rispetto a Γ' deve essere olomorfa nelle cuspidi. Scrivendo ogni $s \in \mathbb{Q} \cup \{\infty\}$ come $s = \gamma(\infty)$, con $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ l'olomorfia in s

è definita in termini di olomorfia in ∞ di $(c+d\tau)^{-k}f(\gamma(\tau))$.
Come prima possiamo definire le forme cuspidali. In questo caso richiediamo che $c_0 = 0$ nello sviluppo di Fourier di $(c+d\tau)^{-k}f(\gamma(\tau))$ per ogni $\gamma \in \Gamma$.
Denotiamo con $\mathcal{M}_k(\Gamma')$ e $\mathcal{S}_k(\Gamma')$ rispettivamente gli insiemi delle forme modulari e delle forme cuspidali rispetto a Γ'.

Consideriamo ora $\alpha_N = \left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right)$. Si ha $\alpha_N(\tau) = \frac{\tau}{N}$ e $\alpha_N^{-1}(\tau) = N\tau$. Chiamiamo $j_N(\tau) = j \circ \alpha_N^{-1}(\tau) = j(N\tau)$. Ovviamente j_N è invariante rispetto al gruppo $\alpha_N^{-1}\Gamma\alpha_N$, ed è facile mostrare che $\Gamma_0(N) = \Gamma \cap \alpha_N^{-1}\Gamma\alpha_N$. Pertanto j_N è una funzione modulare rispetto a $\Gamma_0(N)$.
Si può dimostrare il seguente risultato.

Teorema 2.11. *Sia $A \in GL_2(\mathbb{Q})$ con $\det(A) > 0$. Allora $\mathbb{C}(j, j \circ A)$ è il campo di tutte le funzioni modulari rispetto a $\Gamma \cap A^{-1}\Gamma A$. In particolare, $\mathbb{C}(j, j_N)$ è il campo di tutte le funzioni modulari rispetto a $\Gamma_0(N)$, dove $j_N(\tau) = j(N\tau)$.*

Dimostrazione. cfr. [Shi], pag.34. □

2.8 $\Gamma_0(N) \setminus \mathfrak{H}$ come spazio di moduli

In questa sezione ci limiteremo a considerare i sottogruppi di congruenza del tipo $\Gamma_0(N)$, che sono i più utili ai nostri scopi. Per una trattazione più ampia si veda [Dia], pag.37-42.

Sia N un intero positivo. Consideriamo la coppia (E, C), dove E è una curva ellittica complessa e C è un sottogruppo ciclico di E di ordine N. Diciamo che due coppie (E, C) ed (E', C') sono equivalenti (e scriviamo $(E, C) \sim (E', C')$) se esiste un isomorfismo tra E ed E' che manda C in C'. Denotiamo con

$$S_0(N) = \{\text{coppie } (E, C)\}/\sim$$

Denotiamo una classe di equivalenza di $S_0(N)$ con $[E, C]$.

Consideriamo ora il quoziente di $\mathfrak{H}$ rispetto all'azione del gruppo $\Gamma_0(N)$ che denotiamo, come nel caso generale, con $\Gamma_0(N)\backslash\mathfrak{H}$.
Ricordiamo che, dato $\tau \in \mathfrak{H}$, $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$. Data una curva ellittica E, ci possiamo ricondurre, tramite isomorfismi, alla curva ellittica $E_\tau = \mathbb{C}/\Lambda_\tau$. Possiamo quindi considerare il sottogruppo di E_τ generato da $\Lambda_\tau + \frac{1}{N}$.
Osserviamo che $N\left(\Lambda_\tau + \frac{1}{N}\right) = \Lambda_\tau$, e N è il minimo intero per cui ciò accade. Pertanto $\langle \Lambda_\tau + \frac{1}{N} \rangle$ è un sottogruppo di E_τ ciclico di ordine N. Abbiamo allora il seguente risultato.

Teorema 2.12. *Sia N un intero positivo. Allora*

$$S_0(N) = \left\{ \left[E_\tau, \left\langle \Lambda_\tau + \frac{1}{N} \right\rangle \right] \;\middle|\; \tau \in \mathfrak{H} \right\}$$

Inoltre $\left[E_\tau, \langle \Lambda_\tau + \frac{1}{N} \rangle\right] = \left[E_{\tau'}, \langle \Lambda_{\tau'} + \frac{1}{N} \rangle\right]$ se e solo se $\tau \sim \tau'$ rispetto a $\Gamma_0(N)$, ovvero se e solo esiste $\gamma \in \Gamma_0(N)$ tale che $\gamma(\tau) = \tau'$.
Quindi c'è una biiezione

$$\begin{array}{rccc} \psi_0 : & S_0(N) & \to & \Gamma_0(N)\backslash\mathfrak{H} \\ & \left[E_\tau, \langle \Lambda_\tau + \frac{1}{N} \rangle\right] & \mapsto & [\tau]_\sim \end{array}$$

Dimostrazione. Consideriamo una coppia (E, C).
Poiché $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_{\tau'}$ per qualche τ' in $\mathfrak{H}$, possiamo prendere $E = \mathbb{C}/\Lambda_{\tau'}$. Abbiamo allora $C = \left\langle \Lambda_{\tau'} + \frac{c\tau'+d}{N} \right\rangle$ per $c, d \in \mathbb{Z}$ tali che $(c, d, N) = 1$, in modo che l'ordine di $\Lambda_{\tau'} + \frac{c\tau'+d}{N}$ sia esattamente N.
Questo implica che $ad - bc - kN = 1$ per qualche $a, b, k \in \mathbb{Z}$.
Quindi $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, ridotta modulo N, appartiene a $SL_2(\mathbb{Z}/N\mathbb{Z})$. Modificare le entrate di γ modulo N non fa variare $\Lambda_{\tau'} + \frac{c\tau'+d}{N}$. Poiché l'omomorfismo di $\Gamma = SL_2(Z)$ in $SL_2(\mathbb{Z}/N\mathbb{Z})$ è suriettivo possiamo allora assumere $\gamma \in \Gamma$.
Sia $\tau = \gamma(\tau')$ e sia $\alpha = c\tau' + d$. Allora $\alpha\tau = a\tau' + b$, così che

$$\alpha\Lambda_\tau = \Lambda_{\tau'}$$

ovvero

$$\mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'}$$

e

$$\alpha\left(\Lambda_\tau + \frac{1}{N}\right) = \Lambda_{\tau'} + \frac{c\tau' + d}{N}$$

ovvero

$$\alpha\left(\left\langle\Lambda_\tau + \frac{1}{N}\right\rangle\right) = \left\langle\Lambda_{\tau'} + \frac{c\tau' + d}{N}\right\rangle$$

Questo mostra che $[E, C] = [C/\Lambda_\tau, \langle\Lambda_\tau + \frac{1}{N}\rangle]$, con $\tau \in \mathfrak{H}$, quindi la prima uguaglianza è provata.

Supponiamo ora $\tau, \tau' \in \mathfrak{H}$ equivalenti rispetto a $\Gamma_0(N)$, ovvero $\tau = \gamma(\tau')$ con $\gamma \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Come abbiamo appena mostrato, posto $\alpha = c\tau' + d$,

$$\alpha\Lambda_\tau = \Lambda_{\tau'} \qquad \text{e} \qquad \alpha\left(\Lambda_\tau + \frac{1}{N}\right) = \Lambda_{\tau'} + \frac{c\tau' + d}{N}$$

ma, poiché $c \equiv 0 \pmod{N}$, si ha $\alpha\left(\Lambda_\tau + \frac{1}{N}\right) = \Lambda_{\tau'} + \frac{d}{N}$.
É banale mostrare che $\langle\Lambda_{\tau'} + \frac{d}{N}\rangle = \langle\Lambda_{\tau'} + \frac{1}{N}\rangle$, quindi

$$[\mathbb{C}/\Lambda_\tau, \langle\Lambda_\tau + \frac{1}{N}\rangle] = [\mathbb{C}/\Lambda_{\tau'}, \langle\Lambda_{\tau'} + \frac{1}{N}\rangle]$$

Viceversa, supponiamo $[\mathbb{C}/\Lambda_\tau, \langle\Lambda_\tau + \frac{1}{N}\rangle] = [\mathbb{C}/\Lambda_{\tau'}, \langle\Lambda_{\tau'} + \frac{1}{N}\rangle]$, con $\tau, \tau' \in \mathfrak{H}$. Allora $\alpha\Lambda_\tau = \Lambda_{\tau'}$ per un certo $\alpha \in \mathbb{C}$. Pertanto, come visto precedentemente, esiste $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ tale che $\tau = \gamma(\tau')$. Con ragionamenti analoghi e inversi a prima, l'isomorfismo dei gruppi ciclici di ordine N ha come conseguenza che $c \equiv 0 \pmod{N}$, ovvero $\gamma \in \Gamma_0(N)$. □

Da quanto detto possiamo concludere che $\Gamma_0(N)\backslash\mathfrak{H}$ è spazio di moduli delle coppie (E, C), dove E è una curva ellittica complessa e C un suo sottogruppo ciclico di ordine N.

2.9 Cenni sulle curve modulari

Possiamo a questo punto introdurre gli oggetti fondamentali alla trattazione dei capitoli successivi: le curve modulari.

Ogni sottogruppo di congruenza $\Gamma' \subset \Gamma$ agisce sul semipiano complesso $\mathfrak{H}$, che è una superficie di Riemann, e si può studiare il quoziente $\Gamma'\backslash\mathfrak{H}$

analogamente ai casi Γ e $\Gamma_0(N)$. Tale insieme di classi di equivalenza, o orbite, rispetto all'azione del gruppo Γ' si denota normalmente con $Y(\Gamma')$. In particolare

$$Y(N) = Y(\Gamma(N)) \qquad Y_1(N) = Y(\Gamma_1(N)) \qquad Y_0(N) = Y(\Gamma_0(N))$$

Ogni $Y(\Gamma')$ può essere dotato di una topologia e di una struttura di superficie di Riemann (il riferimento per questa sezione e per tutti i risultati enunciati e non dimostrati è [Dia], capitoli 2 e 3).

È a partire da questa considerazione che tali insiemi vengono chiamati **curve modulari**.

Come superfici di Riemann, tutte le $Y(\Gamma')$ possono essere compattificate: indichiamo con $X(\Gamma')$ il compattificato di $Y(\Gamma')$. In particolare

$$X(N) = X(\Gamma(N)) \qquad X_1(N) = X(\Gamma_1(N)) \qquad X_0(N) = X(\Gamma_0(N))$$

Possiamo riassumere le proprietà topologiche di ogni $X(\Gamma')$ nel seguente teorema.

Teorema 2.13. *Ogni curva modulare $X(\Gamma')$ è di Hausdorff, connessa e compatta.*

Topologicamente parlando, ogni superficie di Riemann compatta è un toro con g buchi, per un certo g intero non negativo, detto **genere**. Ogni curva ellittica complessa, in particolare, ha genere 1.

È facile osservare che la curva modulare $X(\Gamma)$, dove Γ è l'intero gruppo modulare, è una superficie di Riemann compatta di genere 0 (cioè una sfera). Lo si può facilmente osservare considerando il dominio fondamentale D.

Molto più complesso è determinare il genere delle altre curve modulari.

Considerato $\tau \in \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\} = \overline{\mathfrak{H}}$, definiamo lo stabilizzatore di τ in Γ come

$$\mathrm{Stab}(\tau) = \{\gamma \in \Gamma \mid \gamma(\tau) = \tau\}$$

e chiamiamo

$$e_\tau = \#(\mathrm{Stab}(\tau)/(\mathrm{Stab}(\tau) \cap \Gamma'))$$

Si può mostrare che e_τ dipende solo dall'orbita di $\tau \in \overline{\mathfrak{H}}$ rispetto a Γ' e che $e_\tau = 1$ per quasi tutti i $\tau \in X(\Gamma')$. Usando la formula di Riemann-Hurwitz si può mostrare che il genere g di $X(\Gamma')$ è dato da

$$g = g(X(\Gamma')) = 1 - [\Gamma : \Gamma'] + \frac{1}{2} \sum_{\tau \in X(\Gamma')} (e_\tau - 1)$$

(cfr. [Dar95], pag. 24). Non è facile determinare tale numero, nemmeno nel caso particolare di $\Gamma_0(N)$.

Per ogni Γ', un dominio fondamentale D' per Γ' contiene un dominio fondamentale D per Γ. Esiste poi una mappa suriettiva naturale $Y(\Gamma') \to Y(\Gamma)$, poiché ogni orbita di $\Gamma' \backslash \mathfrak{H}$ è contenuta in un orbita di $\Gamma \backslash \mathfrak{H}$. Tecnicamente, questa mappa è chiamata **ricoprimento**, dal momento che ogni punto di $Y(\Gamma)$ ha un intorno aperto la cui retrimmagine è un'unione disgiunta di aperti omeomorfi ad esso. Possiamo fare l'analogo per le curve modulari compattificate. Il grado del ricoprimento è utile per determinare il genere di $X(\Gamma')$ (per dettagli si veda [Dia], pag. 68).

Dalla geometria complessa sappiamo che ogni superficie di Riemann compatta ammette un'immersione in $\mathbb{P}^n(\mathbb{C})$ (per un certo n) come varietà proiettiva, in particolare si può immergere in $P^3(\mathbb{C})$, e come tale è una curva algebrica. Per quanto riguarda le curve modulari del tipo $X_0(N)$ abbiamo un'immersione "privilegiata": abbiamo visto che la funzione j è modulare, quindi è modulare anche rispetto a $\Gamma_0(N)$, così come j_N. Si può mostrare (cfr. [Dar95], pag.35) che j e j_N sono legate da un'equazione polinomiale $\Phi_N(j, j_N) = 0$ a coefficienti in $\mathbb{Q}$ e la mappa

$$\tau \mapsto (j(\tau), j_N(\tau))$$

dà un'equivalenza birazionale tra $X_0(N)$ e la curva algebrica piana definita dall'equazione $\Phi_N(x, y) = 0$. Tale curva è ellittica solo in un numero finito di casi, in particolare (cfr. [Bir70], pag.29) per

$$N = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49$$

Ribaltando il punto di vista, potremmo vedere $\tau \mapsto (j(\tau), j_N(\tau))$ come una parametrizzazione della curva $\Phi_N(x, y) = 0$.
Una versione analitica complessa del **Teorema di Modularità** (cfr. [Dia], pag.63) afferma che ogni curva ellittica complessa E con invariante j_E razionale può essere parametrizzata come curva modulare tramite mappe olomorfe, vedendo entrambe le curve come superfici di Riemann compatte.

Teorema 2.14. *Sia E una curva ellittica complessa con $j_E \in \mathbb{Q}$. Allora per qualche intero positivo N esiste una funzione olomorfa ϕ di superfici di Riemann compatte*

$$\phi : X_0(N) \to E$$

Tale mappa è detta solitamente parametrizzazione.

La dimostrazione di questo teorema è ben oltre i nostri scopi, ma ne faremo ampio uso. Quando si considera una curva ellittica con la sua parametrizzazione, la si chiama normalmente **curva ellittica modulare** (sottolineiamo la differenza con le curve modulari ellittiche, che sono invece curve modulari di genere 1).
É degno di nota il fatto che la dimostrazione completa di questo teorema è molto recente (pubblicata nel 2001, opera congiunta di Breuil, Conrad, Diamond, e Taylor, i quali utilizzarono molte delle tecniche usata da Wiles nella dimostrazione dell'Ultimo Teorema di Fermat) e quindi successiva alla soluzione del Problema di Gauss sul numero di classi di ideali. In realtà, tale teorema fu congetturato da Taniyama nel 1955 e verificato in molti casi anche prima del 2001, ed è sulla base di queste verifiche che svilupparono il loro lavoro Gross, Zagier e Goldfeld.

Capitolo 3

Punti di Heegner

In questo capitolo definiremo i punti di Heegner, particolari punti delle curve ellittiche che si costruiscono a partire dalla interpretazione modulare di queste. Essi hanno importanti proprietà e interverranno in modo fondamentale nei risultati di Gross e Zagier, e quindi di Goldfeld.
Vedremo diverse definizioni dei punti di Heegner, che legheremo tra loro, dando via via una panoramica del contesto algebrico-geometrico entro il quale si sviluppa il problema, soffermandoci soprattutto sull'aspetto costruttivo.

3.1 Divisori e legge di gruppo

Iniziamo ricordando alcuni elementi di teoria dei divisori che ci saranno utili per la costruzione dei punti di Heegner.

Definizione 3.1. *Il* ***gruppo dei divisori*** *di una curva C, indicato con $Div(C)$, è il gruppo abeliano libero generato dai punti di C. Quindi un divisore $D \in Div(C)$ è la somma formale*

$$D = \sum_{P \in C} n_P(P)$$

con $n_P \in \mathbb{Z}$ e $n_P = 0$ per tutti i $P \in C$ tranne un numero finito.

Definizione 3.2. *Chiamiamo* ***grado*** *di $D \in Div(C)$ l'intero*

$$\deg(D) = \sum_{P \in C} n_P$$

I divisori di grado 0 formano un sottogruppo di $\mathrm{Div}(C)$, che indichiamo con $\mathrm{Div}^0(C)$.

Se C è definita su K, il gruppo di Galois dell'estensione $\bar{K}$, che denotiamo con $G_{\bar{K}/K}$, agisce su $\mathrm{Div}(C)$ nel seguente modo

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma)$$

dove $\sigma \in G_{\bar{K}/K}$ e P^σ è il punto di C con coordinate modificate mediante σ. Diciamo che D **è definito su** K se $D^\sigma = D$ per ogni $\sigma \in G_{\bar{K}/K}$. Notiamo che se $D = n_1(P_1) + \ldots + n_r(P_r)$, dire che D è definito su K non significa che $P_1, \ldots, P_r \in C(K)$. Basta che $G_{\bar{K}/K}$ permuti i P_i in modo opportuno.

Assumiamo ora che la curva C sia liscia e sia $f \in \bar{K}(C)^*$. Possiamo allora associare a f il divisore $\mathrm{div}(f)$ dato da

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P)$$

Definizione 3.3. *Un divisore $D \in Div(C)$ è* ***principale*** *se esiste una $f \in \bar{K}(C)^*$ tale che $D = div(f)$.*

Due divisori D_1 e D_2 sono ***linearmente equivalenti****, e scriviamo $D_1 \sim D_2$, se $D_1 - D_2$ è principale.*

Il ***gruppo delle classi di divisori****, o* ***gruppo di Picard*** *$Pic(C)$, è il quoziente di $Div(C)$ rispetto al sottogruppo dei divisori principali $P(C)$.*

Infine il gruppo $Pic^0(C)$ è il quoziente di $Div^0(C)$ rispetto a $P(C)$.

Date due curve lisce C_1 e C_2 e data una mappa non costante $\phi : C_1 \to C_1$, questa induce una mappa ϕ_* sul gruppo dei divisori come segue

$$\begin{array}{rccc} \phi_* : & \mathrm{Div}(C_1) & \to & \mathrm{Div}(C_2) \\ & \sum_{P \in C} n_P(P) & \mapsto & \sum_{P \in C} n_P(\phi(P)) \end{array}$$

Introdurre tutte le definizioni e i risultati che portano a uno dei teoremi fondamentali della teoria dei divisori, il Teorema di Riemann-Roch, esulerebbe dallo scopo di questo paragrafo. Per approfondimenti a riguardo cfr. [Sil], pag. 37. Noi ci limiteremo a considerare le conseguenze di questo teorema per quanto riguarda le curve ellittiche.

Abbiamo già visto che sui punti di una curva ellittica è possibile definire una legge di gruppo. Utilizzeremo Riemann-Roch per introdurre tale legge da un altro punto di vista. Iniziamo con un lemma.

Lemma 3.1. *Sia C una curva di genere 1 e siano $P, Q \in C$. Allora*

$$(P) \sim (Q) \qquad \textit{se e solo se} \qquad P = Q$$

Dimostrazione. Supponiamo $(P) \sim (Q)$ e sia $f \in \bar{K}(C)$ tale che

$$(P) - (Q) = \mathrm{div}(f)$$

Allora f appartiene allo spazio di Riemann-Roch associato al divisore (Q), che, per il Teorema di Riemann-Roch, ha dimensione 1. Abbiamo perciò che f è costante (in $\bar{K}$) e quindi $P = Q$. □

Abbiamo allora il seguente risultato.

Proposizione 3.1. *Sia E una curva ellittica. Allora:*

1. *Per ogni divisore $D \in Div^0(E)$ esiste un unico punto $P \in E$ tale che*

$$D \sim (P) - (O)$$

quindi

$$\begin{aligned} \sigma : \quad Div^0(E) &\to E \\ D &\mapsto P \end{aligned}$$

è ben definita.

2. *La mappa σ è suriettiva.*

3. *Siano* $D_1, D_2 \in Div^0(E)$. *Allora*

$$\sigma(D_1) = \sigma(D_2) \qquad \textit{se e solo se} \qquad D_1 \sim D_2$$

Quindi σ *induce una biiezione*

$$\sigma : Pic^0(E) \xrightarrow{\sim} E$$

4. *La mappa inversa di* σ *è*

$$\begin{aligned} \kappa : \quad E &\xrightarrow{\sim} Pic^0(E) \\ P &\mapsto [(P) - (O)] \end{aligned}$$

5. *La legge di gruppo "geometrica" sui punti di* E *e la legge di gruppo indotta da* $Pic^0(E)$ *usando* σ *coincidono.*

Dimostrazione. cfr. [Sil], pag.66. □

3.2 Isogenie e endomorfismi

Ricordiamo che un'isogenia tra due curve ellittiche non è altro che un morfismo che manda O in O, che si dimostra essere omomorfismo di gruppi.
Abbiamo chiamato $\mathrm{Hom}(E_1, E_2)$ l'insieme delle isogenie tra le curve ellittiche E_1 ed E_2 e si verifica facilmente che esso è un gruppo.
Chiamiamo **anello degli endomorfismi** di una curva ellittica E l'insieme $\mathrm{End}(E) = \mathrm{Hom}(E, E)$.
Se le curve ellittiche sono definite su K, possiamo restringere l'attenzione alle isogenie definite su K. In tal caso consideriamo $\mathrm{Hom}_K(E_1, E_2)$ e $\mathrm{End}_K(E)$.
Per ogni $m \in \mathbb{Z}$ possiamo definire l'isogenia **moltiplicazione per** m

$$[m] : E \to E$$

nel modo naturale. Se la curva E è definita su K, $[m]$ è definita su K.

Si può dimostrare il seguente risultato.

Teorema 3.1. *Siano E, E_1 ed E_2 curve ellittiche definite su un campo K. Sia $m \in \mathbb{Z}$, $m \neq 0$. Allora $[m] \in End(E)$ è non costante. Inoltre si ha che:*

1. *$Hom(E_1, E_2)$ è uno $\mathbb{Z}$-modulo privo di elementi di torsione.*
2. *$End(E)$ è un dominio di integrità di caratteristica 0.*

Denotiamo con $E[m]$ il sottogruppo di E di m-torsione, ovvero

$$E[m] = \{P \in E \mid [m]P = O\}$$

Supponiamo ora che $\mathrm{char}(K) = 0$. In generale la mappa

$$[\ ] : \mathbb{Z} \to \mathrm{End}(E)$$

è biunivoca, ma ci sono alcuni casi in cui è soltanto iniettiva.

Definizione 3.4. *E ha **moltiplicazione complessa** se $\mathbb{Z} \subsetneq End(E)$.*

Notiamo infine che, poiché ogni isogenia ϕ è un omomorfismo di gruppi, $\ker(\phi)$ è un sottogruppo e si verifica facilmente che è un sottogruppo finito di ordine al più $\deg(\phi)$. Si ha anche una sorta di viceversa (cfr. [Sil], pag.78).

Proposizione 3.2. *Sia E una curva ellittica, e sia C un sottogruppo finito di E. Allora esiste un'unica curva ellittica E' e un'isogenia*

$$\phi : E \to E'$$

tale che

$$C = \ker \phi$$

La curva ellittica E' non è nient'altro che il quoziente E/C: il punto cruciale è dimostrare che tale quoziente è ancora una curva ellittica. Abbiamo comunque stabilito una corrispondenza biunivoca tra le coppie (E, C), dove E è una curva ellittica e C un suo sottogruppo finito, e i diagrammi $\phi : E \to E'$, con ϕ isogenia.

3.3 Ordini in campi quadratici

Sia K un campo di numeri e sia $\mathcal{O}_K$ l'anello degli interi algebrici di K.

Definizione 3.5. *Un* ***ordine*** $\mathcal{O}$ *in* K *è un sottoanello di* $\mathcal{O}_K$ *la cui dimensione su* $\mathbb{Z}$ *è pari a* $[K:\mathbb{Q}]$.

Andiamo subito a restringerci al caso in cui K è un campo quadratico complesso. Si può dimostrare facilmente il seguente risultato.

Proposizione 3.3. *Sia* $\mathcal{O}$ *un ordine di* K. *Allora esiste un unico intero positivo* c, *detto* ***conduttore*** *di* $\mathcal{O}$, *tale che*

$$\mathcal{O} = \mathbb{Z} + c\,\mathcal{O}_K$$

Dimostrazione. cfr. [Lanb], pag.91. □

Sia ora $\Lambda \subset K \subset \mathbb{C}$ un reticolo. Consideriamo l'insieme degli $\alpha \in K$ tali che $\alpha\Lambda \subset \Lambda$, che chiamiamo l'**ordine** di Λ. Ovviamente, nell'ipotesi $\Lambda \subset K$, tale insieme coincide con l'insieme di tutti gli $\alpha \in \mathbb{C}$ tali che $\alpha\Lambda \subset \Lambda$.
Sia ora $\tau \in \mathfrak{H}$ radice di un'equazione quadratica

$$Az^2 + Bz + C = 0$$

con $A, B, C \in \mathbb{Z}$, $(A, B, C) = 1$ e $A > 0$. Il discriminante di tale equazione è

$$D = B^2 - 4AC$$

così che

$$\tau = \frac{-B + \sqrt{D}}{2A}$$

Notiamo che

$$B \equiv D \pmod 2$$

Mantenendo queste notazioni si ha il seguente teorema.

Teorema 3.2. *Sia* $\mathcal{O} = \mathbb{Z}\ \frac{B+\sqrt{D}}{2} + \mathbb{Z}$. *Allora*

$$\mathbb{Z}\ \frac{B+\sqrt{D}}{2} + \mathbb{Z} = \mathbb{Z}\ \frac{D+\sqrt{D}}{2} + \mathbb{Z}$$

e $\mathcal{O}$ *è l'ordine del reticolo* Λ_τ.

Dimostrazione. L'uguaglianza

$$\mathbb{Z}\ \frac{B+\sqrt{D}}{2} + \mathbb{Z} = \mathbb{Z}\ \frac{D+\sqrt{D}}{2} + \mathbb{Z}$$

è ovvia ricordando $B \equiv D \pmod 2$.

Si ha ovviamente $1 \cdot \Lambda_\tau \subset \Lambda_\tau$. Poi

$$\left.\begin{array}{ll} \frac{B+\sqrt{D}}{2}\tau & = -C \\ \frac{B+\sqrt{D}}{2} & = A\tau + B \end{array}\right\} \in \Lambda_\tau$$

Quindi $\mathcal{O}$ è contenuto nell'ordine di Λ_τ.

Proviamo ora il viceversa. Innanzitutto mostriamo che

$$\Lambda_\tau \cdot \Lambda_{\overline{\tau}} = \frac{1}{A}\mathcal{O}$$

dove $\overline{\tau} = \frac{-B-\sqrt{D}}{2A}$. Infatti

$$\begin{aligned} \Lambda_\tau \cdot \Lambda_{\overline{\tau}} &= \mathbb{Z}\ \tfrac{B^2-D}{4A^2} + \mathbb{Z}\ \tfrac{-B+\sqrt{D}}{2A} + \mathbb{Z}\ \tfrac{-B-\sqrt{D}}{2A} + \mathbb{Z} \\ &= \tfrac{1}{A}\left(\mathbb{Z}\ C + \mathbb{Z}\ B + \mathbb{Z}\ A + \mathbb{Z}\ \tfrac{B+\sqrt{D}}{2}\right) \\ &= \tfrac{1}{A}\left(\mathbb{Z} + \mathbb{Z}\ \tfrac{B+\sqrt{D}}{2}\right) = \tfrac{1}{A}\mathcal{O} \end{aligned}$$

Ora consideriamo $\alpha \in K$ tale che $\alpha\Lambda_\tau \subset \Lambda_\tau$. Allora

$$\alpha\mathcal{O} = \alpha\Lambda_\tau \cdot A\Lambda_{\overline{\tau}} \subset \Lambda_\tau \cdot A\Lambda_{\overline{\tau}} = \mathcal{O}$$

e poiché $1 \in \mathcal{O}$ si ha $\alpha \in \mathcal{O}$, da cui la tesi. □

Notiamo che $D \equiv B^2 \pmod 4$, quindi $D \equiv 0, 1 \pmod 4$.

Viceversa, ogni $D \equiv 0, 1 \pmod 4$ è discriminante di un'equazione quadratica.

Ogni discriminante può essere scritto come $D = c^2\widetilde{D}$, con c intero positivo

e $\widetilde{D}$ discriminante di un'equazione quadratica. Se in ogni decomposizione di questo tipo si ha che $c = 1$, allora D si dice **discriminante fondamentale**. Si può mostrare facilmente che i discriminanti fondamentali sono del tipo:
$D = d \equiv 1 \pmod 4$ e privo di fattori quadratici;
$D = 4d$ e $d \equiv 2, 3 \pmod 4$ e privo di fattori quadratici.
Quindi in generale abbiamo che ogni discriminante D di un'equazione quadratica

$$Az^2 + Bz + C = 0$$

con $A, B, C \in \mathbb{Z}$, $(A, B, C) = 1$ e $A > 0$ è del tipo:
$D = c^2 d$ con $d \equiv 1 \pmod 4$ e privo di fattori quadratici;
$D = (2c)^2 d$ con $d \equiv 2, 3 \pmod 4$ e privo di fattori quadratici.
In ogni caso, se $\tau \in \mathfrak{H}$ è radice di un'equazione quadratica di questo tipo, abbiamo che $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$ e che l'ordine $\mathcal{O}$ di Λ_τ è della forma

$$\mathcal{O} = \mathbb{Z} + c\, \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$$

dove ricordiamo che
se $d \equiv 1 \pmod 4$, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$;
se $d \equiv 2, 3 \pmod 4$, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$.
La cosa più importante da notare è che l'ordine di Λ_τ è determinato totalmente dal discriminante D. Notiamo anche che nel caso D sia un discriminante fondamentale, l'ordine di Λ_τ coincide con l'anello degli interi algebrici di $\mathbb{Q}(\tau)$.

3.4 Punti di Heegner

Consideriamo la curva modulare $X_0(N)$. Abbiamo già visto che ogni suo punto non cuspidale può essere considerato come una classe di isomorfismo di coppie (E, C), con E curva ellittica complessa e C sottogruppo finito di ordine N. Da quanto detto precedentemente abbiamo quindi che ogni

punto non cuspidale di $X_0(N)$ può essere visto come un diagramma del tipo $(\phi : E \to E')$, con ϕ isogenia con nucleo isomorfo a $\mathbb{Z}/N\mathbb{Z}$.

Consideriamo $K = \mathbb{Q}(\sqrt{D})$ campo quadratico complesso con D discriminante fondamentale tale che $(D, N) = 1$. Sia $\mathcal{O}$ un **ordine** di K. Possiamo dare la prima definizione di punto di Heegner.

Definizione 3.6. *Diciamo che un punto non cuspidale $\tau \in X_0(N)$ è **punto di Heegner di discriminante** D se, visto τ come $(\phi : E \to E')$, si ha $End(E) = End(E') = \mathcal{O}$.*

Rileggiamo questa definizione alla luce dell'identificazione tra curve ellittiche e tori complessi, tenendo conto dei risultati precedenti.

Abbiamo visto che possiamo scegliere come rappresentante di ogni classe di $X_0(N)$ una coppia del tipo

$$\left(\mathbb{C}/\Lambda_\tau, \left\langle \Lambda_\tau + \frac{1}{N} \right\rangle\right)$$

Possiamo scegliere

$$\begin{array}{rccc} \phi: & \mathbb{C}/\Lambda_\tau & \to & \mathbb{C}/\Lambda_{\tau,\frac{1}{N}} \\ & \Lambda_\tau + z & \mapsto & \Lambda_{\tau,\frac{1}{N}} + z \end{array}$$

dove $\Lambda_{\tau,\frac{1}{N}} = \mathbb{Z}\tau \oplus \mathbb{Z}\frac{1}{N}$.
Poiché $N \cdot \Lambda_{\tau,\frac{1}{N}} = \Lambda_{N\tau}$, abbiamo che $\mathbb{C}/\Lambda_{\tau,\frac{1}{N}} \cong \mathbb{C}/\Lambda_{N\tau}$ e possiamo quindi considerare

$$\tilde{\phi} : \mathbb{C}/\Lambda_\tau \to \mathbb{C}/\Lambda_{N\tau}$$

Vediamo ora un teorema fondamentale.

Teorema 3.3. *Una curva ellittica complessa $E = \mathbb{C}/\Lambda$, con $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, ha moltiplicazione complessa se e solo se, posto $\tau = \frac{\omega_1}{\omega_2}$, esistono $a, b, c \in \mathbb{Z}$ tali che $a\tau^2 + b\tau + c = 0$.*

Dimostrazione. Ricordiamo che gli endomorfismi di $\mathbb{C}/\Lambda$ sono in corrispondenza biunivoca con gli $\alpha \in \mathbb{C}$ tali che $\alpha\Lambda \subset \Lambda$.

Consideriamo $\alpha \in \mathbb{C} \setminus \mathbb{Z}$, tale che $\alpha\Lambda \subset \Lambda$. Allora esistono $a', b', c', d' \in \mathbb{Z}$ tali che

$$\alpha\omega_1 = a'\omega_1 + b'\omega_2$$
$$\alpha\omega_2 = c'\omega_1 + d'\omega_2$$

Quindi $\alpha = c'\frac{\omega_1}{\omega_2} + d'$ e, sostituendo nella prima equazione, abbiamo

$$\left(c'\frac{\omega_1}{\omega_2} + d'\right)\omega_1 = a'\omega_1 + b'\omega_2$$

Dividendo per ω_2, abbiamo

$$c'\left(\frac{\omega_1}{\omega_2}\right)^2 + d'\frac{\omega_1}{\omega_2} = a'\frac{\omega_1}{\omega_2} + d'$$

ovvero

$$c'\tau^2 + (d' - a')\tau - d' = 0$$

Viceversa, siano $a, b, c \in \mathbb{Z}$ tali che $a\tau^2 + b\tau + c = 0$. Sia $\alpha = a\tau \notin \mathbb{Z}$. Allora

$$\alpha\omega_1 = a\omega_2 \in \Lambda$$
$$\alpha\omega_2 = a\frac{\omega_2^2}{\omega_1} = \omega_1 a\tau^2 = \omega_1(-b\tau - c) = -c\omega_1 - b\omega_2 \in \Lambda$$

Quindi $\alpha\Lambda \subset \Lambda$. □

Per studiare i punti di Heegner dobbiamo quindi restringerci ai $\tau \in \mathfrak{H}$ che sono radici di un'equazione quadratica a coefficienti interi. Sia τ radice dell'equazione

$$Az^2 + Bz + C = 0$$

e supponiamo che $(A, B, C) = 1$ e $A > 0$. Sia $D = B^2 - 4AC$. Abbiamo visto come D determini totalmente l'ordine di Λ_τ che ovviamente coincide con $\mathrm{End}(\mathbb{C}/\Lambda_\tau)$. In particolare abbiamo visto che

$$\mathrm{End}(\mathbb{C}/\Lambda_\tau) = \mathbb{Z} + c\,\mathcal{O}_{\mathbb{Q}(\tau)}$$

dove c è un intero positivo determinato da D.

Abbiamo tutti gli strumenti per dimostrare il seguente risultato.

Teorema 3.4. *Un punto non cuspidale $\tau \in X_0(N)$ è un punto di Heegner di discriminante D se e solo se è radice di un'equazione quadratica*

$$Az^2 + Bz + C = 0 \tag{3.1}$$

con $(A, B, C) = 1$, $A > 0$, $A \equiv 0 \ (mod\ N)$ e $D = B^2 - 4AC$.

Dimostrazione. Sia τ radice di un'equazione del tipo (3.1) e $A = NA'$. Allora $N\tau$ è radice dell'equazione

$$A'z^2 + Bz + NC = 0$$

e ovviamente si ha $(A', B, NC) = 1$, $A' > 0$ e il discriminante di tale equazione è ancora D. Quindi $\mathrm{End}(\mathbb{C}/\Lambda_\tau) = \mathrm{End}(\mathbb{C}/\Lambda_{N\tau})$ e in particolare sono lo stesso ordine nel campo quadratico complesso $\mathbb{Q}(\sqrt{D})$.
Viceversa, se $\tau \in \mathfrak{H}$ è punto di Heegner di discriminante D si ha che τ e $N\tau$ devono essere radici di equazioni quadratiche con stesso determinante. Siano

$$Az^2 + Bz + C = 0 \qquad \text{e} \qquad A'z^2 + B'z + C' = 0$$

equazioni con $(A, B, C) = 1$, $A > 0$, $(A', B', C') = 1$ e $A' > 0$ che hanno come radici rispettivamente τ e $N\tau$. Si ha allora che

$$A'N^2z^2 + B'Nz + C' = 0$$

ha come radice τ, quindi esiste k intero positivo tale che

$$kA = A'N^2 \qquad kB = B'N \qquad kC = C'$$

da cui

$$B'^2 - 4A'C' = \left(\frac{k}{N}\right)^2 (B^2 - 4AC)$$

Quindi k deve essere uguale ad N, da cui $A = A'N \equiv 0 \ (\mathrm{mod}\ N)$. □

É facile verificare (è un semplice calcolo) che la condizione del teorema è invariante sotto l'azione di $\Gamma_0(N)$. Affinché esistano punti di Heegner di discriminante D, si deve avere $D \equiv k^2 \pmod{4N}$ per qualche intero positivo k.

Rileggiamo quanto già visto da un ulteriore punto di vista.
Se $\tau = (\phi : E = \mathbb{C}/\Lambda \to E' = \mathbb{C}/\Lambda')$ è un punto di Heegner di discriminante D con anello degli endomorfismi $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{D})$, abbiamo visto come possiamo riportarci ad avere $\Lambda \subset \Lambda' \subset K$, con $\Lambda'/\Lambda \cong \mathbb{Z}/N\mathbb{Z}$ (basta prendere $\Lambda = \Lambda_\tau$ e $\Lambda' = \Lambda_{\tau,\frac{1}{N}}$). Abbiamo $\mathcal{O}\Lambda \subset \Lambda$ e $\mathcal{O}\Lambda' \subset \Lambda'$ e abbiamo visto come sia possibile trovare $\overline{\Lambda}$ e $\overline{\Lambda'}$ tali che $\Lambda \cdot \overline{\Lambda} = \mathcal{O}$ e $\Lambda' \cdot \overline{\Lambda'} = \mathcal{O}$. Quindi Λ e Λ' sono $\mathcal{O}$-moduli invertibili di rango 1. Poiché $\Lambda \subset \Lambda'$, abbiamo che $\mathcal{N} = \Lambda \cdot \overline{\Lambda'} \subset \mathcal{O}$ è un ideale di $\mathcal{O}$, tale che $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$, cioè primitivo di norma N.

Limitiamoci a considerare il caso in cui D è un discriminante fondamentale. Abbiamo visto che in questo caso $\mathcal{O} = \mathcal{O}_K$, anello degli interi algebrici di K. Λ e Λ' sono allora ideali frazionari e $\mathcal{N}$ ideale primitivo di norma N di $\mathcal{O}_K$. Osserviamo anche che $\Lambda' = \Lambda \cdot \mathcal{N}^{-1}$. Viceversa, dato un ideale frazionario $\mathcal{I}$ e un ideale primitivo $\mathcal{N}$ di norma N di $\mathcal{O}_K$, si può verificare che $\tau = (\mathrm{id} : \mathbb{C}/\mathcal{I} \to \mathbb{C}/\mathcal{I}\mathcal{N}^{-1})$ è un punto di Heegner di discriminante D. Due scelte $\mathcal{I}_1$, $\mathcal{N}_1$ e $\mathcal{I}_2$, $\mathcal{N}_2$ definiscono lo stesso punto di Heegner se e solo se $\mathcal{I}_1 = \alpha\mathcal{I}_2$ per un certo $\alpha \in K^*$ (ovvero se $\mathcal{I}_1$ e $\mathcal{I}_2$ appartengono alla stessa classe in Cl_K) e $\mathcal{N}_1 = \mathcal{N}_2$. Quindi c'è una corrispondenza biunivoca

$$\left\{ \begin{array}{c} \text{coppie } (\mathcal{I},\mathcal{N}) : \ \mathcal{I} \in \mathrm{Cl}_K \text{ e } \mathcal{N} \\ \text{ideale primitivo di norma } N \end{array} \right\} \ \leftrightarrow \ \left\{ \begin{array}{c} \text{Punti di Heegner in } X_0(N) \\ \text{di discriminante } D \end{array} \right\}$$
$$(\mathcal{I},\mathcal{N}) \ \mapsto \ (\mathrm{id} : \mathbb{C}/\mathcal{I} \to \mathbb{C}/\mathcal{I}\mathcal{N}^{-1})$$

3.5 Costruzione del punto $P_D \in E(K)$

Riprendiamo e sviluppiamo alcuni concetti a partire dall'ultima osservazione riguardo ai punti di Heegner.

Sia K un campo quadratico complesso, $\mathcal{O}_K$ l'anello degli interi algebrici

di K, Cl_K il gruppo di classi di ideali di $\mathcal{O}_K$. Ogni ideale Λ di $\mathcal{O}_K$ è reticolo di $\mathbb{C}$ e possiamo considerare la curva ellittica $\mathbb{C}/\Lambda$. A meno di isomorfismi la curva $\mathbb{C}/\Lambda$ dipende non tanto da Λ, quanto dalla sua classe in Cl_K. Si ha inoltre che

$$\mathrm{End}(\mathbb{C}/\Lambda) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} = \mathcal{O}_K$$

Viceversa, data una curva ellittica E definita su $\mathbb{C}$ tale che $\mathrm{End}(E) = \mathcal{O}_K$, $E \cong \mathbb{C}/\Lambda$ per un'unica classe in Cl_K. Riassumiamo questi risultati nella seguente proposizione.

Proposizione 3.4. *C'è una corrispondenza biunivoca tra le classi in Cl_K e le classi di isomorfismo di curve ellittiche E definite su $\mathbb{C}$ con $End(E) = \mathcal{O}_K$.*

Corollario 3.1. *Ci sono solo un numero finito di classi di isomorfismo di curve ellittiche E definite su $\mathbb{C}$ con $End(E) = \mathcal{O}_K$.*

Dimostrazione. Ovvio, poiché Cl_K è finito. □

Corollario 3.2. *Se $E = \mathbb{C}/\Lambda$ è una curva ellittica con $End(E) = \mathcal{O}_K$, allora $j(\Lambda)$ è algebrico su $\mathbb{Q}$.*

Dimostrazione. cfr. [Sil], pag.339. □

Ovviamente $j(\Lambda) = j(\Lambda')$ se Λ e Λ' appartengono alla stessa classe in Cl_K. Abbiamo visto che $j(\Lambda)$ è algebrico su $\mathbb{Q}$, in realtà si può mostrare che è un intero algebrico (cfr. [Lanb], pag. 57).

Consideriamo ora l'estensione abeliana non ramificata massimale di K, cioè il **campo di classe di Hilbert di** K, che denominiamo con H. Si può dimostrare (cfr. [Lanb], pag.123) il seguente teorema:

Teorema 3.5. *Dato $\Lambda \in Cl_K$ si ha $H = K(j(\Lambda))$.*
In più $[H : K] = [\mathbb{Q}(j(\Lambda)) : \mathbb{Q}] = h$ (con $h = \#Cl_K$) e, preso un sistema di rappresentanti $\{\Lambda_1, ..., \Lambda_h\}$ per Cl_K, $\{j(\Lambda_1), ..., j(\Lambda_h)\}$ formano un sistema completo di coniugati di $j(\Lambda)$ rispetto a $G_{H|K}$.

Tutto quanto detto si può estendere al caso più generale in cui si considera $\mathcal{O}$ ordine di K contenuto in $\mathcal{O}_K$. I risultati sono analoghi.

Consideriamo ora $\tau \in X_0(N)$, punto di Heegner di discriminante D. Abbiamo visto che D determina in modo univoco $\mathrm{End}(\mathbb{C}/\Lambda_\tau)$ e quindi anche H (cfr. Teorema 3.5), che indicheremo quindi con $H(D)$. Preso un punto di Heegner τ di discriminante D abbiamo che sia $j(\tau)$ che $j_N(\tau)$ appartengono a $H(D)$ e quindi il punto $(j(\tau), j_N(\tau))$ appartiene alla curva $X_0(N)$ su $H(D)$ nella sua "versione" di curva algebrica piana $\Phi_N(x, y) = 0$, che denotiamo con $X_0(N)_{\mathrm{alg}}$.

Prima di concludere questa sezione, andiamo a enunciare un'altra versione del **Teorema di Modularità** (cfr. [Dia], pag.292):

Teorema 3.6. *Sia E una curva ellittica definita su $\mathbb{Q}$. Allora esiste un intero positivo N e un morfismo ϕ su $\mathbb{Q}$ tra curve definite su $\mathbb{Q}$ suriettivo, dalla curva $X_0(N)_{alg}$ alla curva ellittica E*

$$\phi : X_0(N)_{alg} \to E$$

Questa versione del Teorema di Modularità implica facilmente quella precedente. Infatti ogni curva ellittica E con $j_E \in \mathbb{Q}$, vista come curva algebrica su $\mathbb{C}$, è isomorfa su $\mathbb{C}$ ai punti $E'(\mathbb{C})$ di una curva ellittica E' definita su $\mathbb{Q}$. Abbiamo allora un morfismo su $X_0(N)_{\mathrm{alg}} \to E'$ su $\mathbb{Q}$ che si estende ai punti su $\mathbb{C}$ e quindi un morfismo $X_0(N) \to E$ che può essere visto come mappa olomorfa tra superfici di Riemann. Vale anche l'implicazione inversa.

Consideriamo ora una curva ellittica E tale che $j_E \in \mathbb{Q}$. Consideriamo la sua parametrizzazione $\phi : X_0(N)_{\mathrm{alg}} \to E$. Preso un punto di Heegner τ di discriminante D, si ha che

$$P_{H(D)} = \phi(j(\tau), j_N(\tau)) \in E(H(D))$$

Possiamo allora considerarne la traccia

$$P_D = \mathrm{Tr}_{H(D)/K}(P_{H(D)}) = \sum_{\sigma \in G_{H(D)/K}} \sigma(P_{H(D)})$$

Si ha ovviamente $P_D \in E(K)$, infatti, preso un qualsiasi $\bar{\sigma} \in G_{H(D)/K}$ si ha che

$$\bar{\sigma}(P_D) = \bar{\sigma}\left(\sum_{\sigma \in G_{H(D)/K}} \sigma(P_{H(D)})\right) = \sum_{\sigma \in G_{H(D)/K}} \bar{\sigma}(\sigma(P_{H(D)})) = P_D$$

Si usa chiamare **punto di Heegner** anche il punto P_D.

Notiamo che la costruzione di tale punto può anche essere fatta nel seguente modo: consideriamo un insieme $\tau_1, \ldots, \tau_h \in X_0(N)$ (dove h è la cardinalità di Cl_K) di punti di Heegner di discriminante D, coniugati rispetto a $G_{H(D)/K}$. Prendiamo il divisore $(\tau_1) + \ldots + (\tau_h)$ e, data la parametrizzazione ϕ da $X_0(N)$ ad E, consideriamo

$$\phi_*((\tau_1) + \ldots + (\tau_h)) = (\phi(\tau_1)) + \ldots + (\phi(\tau_h)) = \phi(\tau_1) + \ldots + \phi(\tau_h)$$

Ricordando ora che ϕ è una mappa su $\mathbb{Q}$, abbiamo che $\phi(\tau_1), \ldots, \phi(\tau_h)$ sono ancora un insieme di punti coniugati rispetto a $G_{H(D)/K}$, pertanto

$$\phi(\tau_1) + \ldots + \phi(\tau_h)$$

è un punto di $E(K)$, che coincide con P_D.

Capitolo 4

Teoria delle Funzioni L associate a curve ellittiche

La svolta sostanziale nella soluzione del Problema di Gauss sul numero di classi di ideali avvenne con l'intuizione del possibile utilizzo della teoria che è introdotta in questo capitolo. Studieremo alcune proprietà delle curve ellittiche definite su campi finiti e su campi locali. In entrambi i casi il passo principale sarà andare a raccogliere le informazioni che otteniamo riguardo a una curva ellittica in un'unica funzione, rispettivamente la funzione Z e la funzione L associate alla curva. Un'altra versione del Teorema di Modularità ci permetterà infine di dedurre importanti proprietà delle funzioni L associate a curve ellittiche, in particolare l'equazione funzionale che soddisfano.

4.1 Curve ellittiche su campi finiti: il Teorema di Hasse

Sia p primo e q una potenza di p.

Sia K campo finito di caratteristica p e cardinalità q.

Vogliamo cercare di stimare la cardinalità di $E(K)$. Una prima osservazione è che ogni valore di x ci dà al più due valori per y, quindi una maggiorazione

banale per $\#E(K)$ è $2q+1$, ma un'equazione di secondo grado ha probabilità $1/2$ di essere risolubile in K, quindi ci aspettiamo che l'ordine di grandezza sia circa q. Questa osservazione euristica è confermata dal Teorema di Hasse.

Teorema 4.1. *Sia E una curva ellittica definita su un campo K con q elementi, allora*

$$|\#E(K) - q - 1| \leq 2\sqrt{q}$$

Prima di dimostrare il teorema ricordiamo alcuni risultati geometrici.

1. Se $\phi : C_1 \to C_2$ è una mappa separabile (cfr. [Sil], pag. 25-28) tra curve definite su K allora definiamo **grado** della mappa ϕ la cardinalità della generica retroimmagine, ovvero

   $$\deg \phi = \#\phi^{-1}(Q) \qquad \text{per ogni } Q \in C_2 \setminus F$$

   dove F è un sottoinsieme di C_2 di cardinalità finita.

2. Se $\phi : E_1 \to E_2$ è un'isogenia non costante tra curve ellittiche definite su K, si ha

   $$\deg \phi = \#\phi^{-1}(Q) \qquad \text{per ogni } Q \in E_2$$

   Infatti, per ogni Q e Q' in E_2, se scegliamo $R \in E_1$ con $\phi(R) = Q - Q'$, il fatto che ϕ sia un omomorfismo implica che c'è una corrispondenza biunivoca

   $$\begin{aligned} \phi^{-1}(Q) &\to \phi^{-1}(Q') \\ P &\mapsto P + R \end{aligned}$$

3. Data una curva $E : y^2 + axy + by = x^3 + cx^2 + dx + e$, definiamo $E^{(q)} : y^2 + a^q xy + b^q y = x^3 + c^q x^2 + d^q x + e^q$. Si definisce allora il **q-esimo morfismo di Frobenius** come

   $$\begin{aligned} \phi_q : \quad E &\to E^{(q)} \\ (x, y) &\mapsto (x^q, y^q) \end{aligned}$$

Si noti che, se $(x, y) \in E$, con E definita su K di caratteristica p, allora $(x^q, y^q) \in E^{(q)}$ (basta ricordare che, in un campo di caratteristica p, vale $a^p + b^p = (a+b)^p$). Inoltre in K si ha $a^q = a$ per ogni a, pertanto $E^{(q)} = E$ e il morfismo di Frobenius è in realtà un endomorfismo, il cui insieme dei punti fissi è esattamente $E(K)$ (questo segue dal fatto che $x^q - x = 0$ è di grado q, ed ha quindi q soluzioni in $\overline{K}$, che sono tutti e soli gli elementi di K).

4. Siano E_1 e E_2 curve ellittiche. Allora la mappa

$$\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$$

è una forma quadratica definita positiva (cfr. [Sil], pag. 88). Ad ogni forma quadratica definita positiva si può associare una forma bilineare, in questo caso $\langle \phi, \psi \rangle = \frac{1}{2}(\deg(\phi - \psi) - \deg(\phi) - \deg(\psi))$. È facile mostrare che vale la disuguaglianza di Cauchy-Schwarz

$$|\langle \phi, \psi \rangle| = \frac{1}{2}|\deg(\phi - \psi) - \deg(\phi) - \deg(\psi)| \leq \sqrt{\deg(\phi)\deg(\psi)}$$

Abbiamo tutti gli strumenti per dare la dimostrazione del teorema di Hasse.

Dimostrazione. Consideriamo un'equazione di Weiestrass per E, a coefficienti in K, e consideriamo il q-esimo endomorfismo di Frobenius. Come osservato l'insieme dei punti fissi di tale endomorfismo è esattamente $E(K)$, ovvero

$$P \in E(K) \qquad \text{se e solo se} \qquad \phi_q(P) = P$$

da cui

$$E(K) = \ker(\mathrm{id} - \phi_q)$$

La mappa $\mathrm{id} - \phi_q$ è separabile (cfr. [Sil], pag. 83) ed è un'isogenia della curva ellittica E in se stessa, quindi

$$\#E(K) = \#\ker(\mathrm{id} - \phi_q) = \#(\mathrm{id} - \phi_q)^{-1}(\mathrm{O}) = \deg(\mathrm{id} - \phi_q)$$

Si ha infine che

$$|\deg(\mathrm{id} - \phi_q) - \deg(\mathrm{id}) - \deg(\phi_q)| \leq 2\sqrt{\deg(\mathrm{id})\deg(\phi_q)}$$

Ovviamente $\deg(\mathrm{id}) = 1$, mentre $\deg(\phi_q) = q$ (cfr. [Sil], pag. 30), da cui la tesi. □

4.2 La funzione Z associata a una varietà proiettiva

Sia ora V una varietà proiettiva su K. Sia K_n un'estensione di K di grado n, quindi un campo finito di cardinalità q^n. Denotiamo con $V(K_n)$ l'insieme dei punti di V a coordinate in K_n.

Definizione 4.1. *La **funzione zeta di V su K** è la serie di potenze*

$$Z(V/K;t) = \sum_{k=0}^{\infty} \frac{\left(\sum_{n=1}^{\infty}(\#V(K_n))\frac{t^n}{n}\right)^k}{k!} = \exp\left(\sum_{n=1}^{\infty}(\#V(K_n))\frac{t^n}{n}\right)$$

Conoscendo la funzione zeta di una certa varietà V possiamo risalire ai valori di $\#V(K_n)$ mediante la formula

$$\#V(K_n) = \frac{1}{(n-1)!}\frac{\mathrm{d}^n}{\mathrm{d}t^n}\log Z(V/K;t)\bigg|_{t=0}$$

Abbiamo un teorema, congetturato da Weil nel 1949.

Teorema 4.2. *Sia V una varietà proiettiva liscia su K, campo con q elementi, di dimensione n. Allora:*

1. ***Razionalità**: $Z(V/K;t) \in \mathbb{Q}(t)$*
2. ***Equazione funzionale**: esiste $\epsilon \in \mathbb{Z}$ (la caratteristica di Eulero di V), tale che*
$$Z\left(V/K;\frac{1}{q^n t}\right) = \pm q^{\frac{n\epsilon}{2}} t^{\epsilon} Z(V/K;t)$$
3. ***Ipotesi di Riemann**: c'è una fattorizzazione*
$$Z(V/K;t) = \frac{P_1(t)\dots P_{2n-1}(t)}{P_0(t)P_2(t)\dots P_{2n}(t)}$$

con $P_i(t) \in \mathbb{Z}[t]$*, per ogni* i*,* $P_0(t) = 1 - t$*,* $P_{2n}(t) = 1 - q^n t$ *e per ogni* $1 \leq i \leq 2n-1$*,*

$$P_i(t) = \prod_j (1 - \alpha_{ij} t) \qquad \text{con } |\alpha_{ij}| = q^{\frac{i}{2}}$$

Dimostreremo la congettura di Weil solo nel caso di curve ellittiche.
Prima di rienunciare il teorema nel nostro caso e di darne dimostrazione premettiamo un risultato sugli endomorfismi di curve ellittiche. Cominciamo da una definizione.

Definizione 4.2. *Sia* E *una curva ellittica e* $l \in \mathbb{Z}$ *un primo. Il* ***modulo (*l***-adico) di Tate di*** E *è il gruppo*

$$T_l(E) = \varprojlim_n E[l^n]$$

dove il limite inverso è fatto rispetto alle mappe naturali

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n]$$

ovvero l'insieme

$$\varprojlim_n E[l^n] = \left\{ (P_i) \in \prod_i E[l^i] \;\middle|\; P_i = [l^{j-i}]P_j \quad \text{per ogni } i \leq j \right\}$$

Poiché ogni $E[l^n]$ è uno $\mathbb{Z}/l^n\mathbb{Z}$-modulo vediamo che il modulo di Tate ha una struttura naturale come $\mathbb{Z}_l$-modulo. Nell'ipotesi $l \neq \mathrm{char}(K)$ si ha che $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ (cfr [Sil], pag. 91). D'ora in avanti per noi sarà $l \neq \mathrm{char}(K)$.
Il modulo di Tate è uno strumento utile per studiare le isogenie. Se

$$\phi : E_1 \to E_2$$

è un'isogenia di curve ellittiche, allora ϕ induce mappe

$$\phi_{l^n} : E_1[l^n] \to E_2[l^n]$$

e quindi una mappa $\mathbb{Z}_l$-lineare

$$\phi_l : T_l(E_1) \to T_l(E_2)$$

Abbiamo quindi definito un omomorfismo

$$\begin{aligned} \mathrm{Hom}(E_1, E_2) &\to \mathrm{Hom}(T_l(E_1), T_l(E_2)) \\ \phi &\mapsto \phi_l \end{aligned}$$

In particolare, se $E_1 = E_2 = E$, la mappa

$$\mathrm{End}(E) \to \mathrm{End}(T_l(E))$$

è anche un omomorfismo di anelli.
Se scegliamo una $\mathbb{Z}_l$-base per $T_l(E)$, possiamo scrivere ϕ_l come una matrice 2×2 e possiamo valutare $\det(\phi_l), \mathrm{tr}(\phi_l) \in \mathbb{Z}_l$, che, come sempre, non dipendono dalla base scelta.

Lemma 4.1. *Sia $\phi \in End(E)$. Allora*

$$\det(\phi_l) = \deg(\phi) \qquad tr(\phi_l) = 1 + \deg(\phi) - \deg(id - \phi)$$

In particolare, $\det(\phi_l)$ *e* $tr(\phi_l)$ *sono in* $\mathbb{Z}$ *e sono indipendenti da* l*.*

Dimostrazione. cfr. [Sil], pag.134. Notiamo solo che il risultato sulla traccia $\mathrm{tr}(\phi_l)$ è conseguenza del fatto che per ogni A, matrice 2×2, vale

$$\mathrm{tr}(A) = 1 + \det(A) - \det(\mathrm{id} - A)$$

□

Consideriamo ora il q-esimo endomorfismo di Frobenius ϕ (usiamo questa notazione per non appesantire la scrittura). Abbiamo già mostrato che $\#E(K) = \deg(\mathrm{id} - \phi)$. Similmente, per ogni intero $n \geq 1$, ϕ^n è il q^n-esimo endomorfismo di Frobenius, quindi $\#E(K_n) = \deg(\mathrm{id} - \phi^n)$.
Il polinomio caratteristico di ϕ_l,

$$\chi_{\phi_l}(t) = \det(t \cdot \mathrm{id} - \phi_l) = t^2 - \mathrm{tr}(\phi_l)t + \det(\phi_l) \in \mathbb{Z}[t]$$

Per il lemma 4.1 e considerazioni già fatte abbiamo che

$$\begin{aligned} \chi_{\phi_l}(t) &= t^2 - (1 + \deg(\phi) - \deg(\mathrm{id} - \phi))t - \deg(\phi) = \\ &= t^2 - (1 + q - \#E(K))t + q = \\ &= (t - \alpha)(t - \beta) \end{aligned}$$

con $\alpha\beta = q$.

Poiché per ogni $\frac{m}{n} \in \mathbb{Q}$ si ha

$$\chi_{\phi_l}\left(\frac{m}{n}\right) = \det\left(\frac{m}{n}\mathrm{id} - \phi_l\right) = \frac{\det\left(m \cdot \mathrm{id} - n\phi_l\right)}{n^2} = \frac{\deg\left(m \cdot \mathrm{id} - n\phi_l\right)}{n^2} \geq 0$$

Quindi abbiamo che α e β sono radici coniugate complesse, pertanto

$$|\alpha| = |\beta| = \sqrt{q}$$

Infine notiamo che il polinomio caratteristico di ϕ_l^n è dato da

$$\chi_{\phi_l^n}(t) = \det(t \cdot \mathrm{id} - \phi_l^n) = (t - \alpha^n)(t - \beta^n)$$

Per verificare questo possiamo porre ϕ_l in forma di Jordan, così che sia triangolare superiore con α e β sulla diagonale. In particolare,

$$\#E(K_n) = \deg(\mathrm{id} - \phi^n) = \det(\mathrm{id} - \phi_l^n) = \chi_{\phi_l^n}(1) = 1 - \alpha^n - \beta^n + q^n$$

Date queste premesse è facile dimostrare la congettura di Weil per le curve ellittiche.

Teorema 4.3. *Sia K un campo con q elementi ed E una curva ellittica su K. Allora esiste $a \in \mathbb{Z}$ (in particolare $a = 1 + q - \#E(K)$), tale che*

$$Z(E/K; t) = \frac{1 - at + qt^2}{(1 - t)(1 - qt)}$$

Con

$$1 - at + qt^2 = (1 - \alpha t)(1 - \beta t) \qquad |\alpha| = |\beta| = \sqrt{q}$$

Inoltre

$$Z\left(E/K; \frac{1}{qt}\right) = Z(E/K; t)$$

Dimostrazione. Consideriamo il logaritmo della funzione zeta di E

$$\begin{aligned} \log(Z(E/K;t)) &= \textstyle\sum_{n=1}^{\infty}(\#E(K_n))\frac{t^n}{n} \\ &= \textstyle\sum_{n=1}^{\infty}(1 - \alpha^n - \beta^n + q^n)\frac{t^n}{n} \\ &= -\log(1-t) + \log(1-\alpha t) + \log(1-\beta t) + \log(1-qt) \end{aligned}$$

Da cui

$$Z(E/K;t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)}$$

con i coefficienti α e β che soddisfano tutte le richieste.

Scriviamo $Z(E/K;t)$ nella forma

$$Z(E/K;t) = \frac{1-at+qt^2}{1-(1+q)t+qt^2}$$

da cui risulta più evidente l'equazione funzionale. Infatti:

$$Z\left(E/K;\frac{1}{qt}\right) = \frac{1-\frac{a}{qt}+\frac{1}{qt^2}}{1-\frac{1+q}{qt}+\frac{1}{qt^2}} = \frac{\frac{qt^2-at+1}{qt^2}}{\frac{qt^2-(1+q)t+1}{qt^2}} = Z(E/K;t)$$

□

4.3 Curve ellittiche su campi locali

Citiamo brevemente alcuni fatti sui campi locali.

Dato un dominio d'integrità D definiamo **valore assoluto** una mappa $|\cdot| : D \to \mathbb{R}$ che soddisfa, per ogni $x, y \in D$, le seguenti proprietà

1. $|x| \geq 0$ e $|x| = 0$ se e solo se $x = 0$;
2. $|x \cdot y| = |x| \cdot |y|$;
3. $|x + y| \leq |x| + |y|$.

Se inoltre si ha $|x + y| \leq \max(|x|, |y|)$ allora $|\cdot|$ si dice **valore assoluto non-archimedeo**. Chiamiamo **banale** un valore assoluto tale che $|x| = 1$ per ogni $x \neq 0$.

Siano $|\cdot|_1$ e $|\cdot|_2$ due valori assoluti sullo stesso dominio D. Diciamo che $|\cdot|_1$ e $|\cdot|_2$ sono **equivalenti** se $|x|_1 < 1$ se e solo se $|x|_2 < 1$. Se due valori assoluti non banali sono equivalenti, allora esiste k tale che $|x|_1 = |x|_2^k$, per ogni $x \in D$. I valori assoluti a meno di equivalenze, o più precisamente, le classi di equivalenza di valori assoluti, sono chiamati **posti**.

Il Teorema di Ostrowski afferma che ogni posto non banale su $\mathbb{Q}$ è o il valore assoluto ordinario, o il valore assoluto p-adico $|\cdot|_p$ (ricordiamo che, preso $q \in \mathbb{Q}$, si può scrivere $q = p^n \frac{a}{b}$, con $(p, a) = 1$ e $(p, b) = 1$, e si ha allora che $|q|_p = p^{-n}$).

Definiamo **campo locale** un campo topologico rispetto a una topologia non discreta, localmente compatto. Dato un campo locale si può definire un valore assoluto su di esso. Chiamiamo **campi locali non-archimedei** quelli in cui tale valore assoluto è non-archimedeo. Si può mostrare che i campi locali non-archimedei di caratteristica zero sono tutti estensioni finite del campo dei numeri p-adici $\mathbb{Q}_p$ per un certo primo p.
Dato un campo K, definiamo **valutazione discreta** una mappa

$$v : K \to \mathbb{Z} \cup \{\infty\}$$

che, per ogni $x, y \in K$, soddisfa le seguenti proprietà:

1. $v(x \cdot y) = v(x) + v(y)$;
2. $v(x + y) \geq \min(v(x), v(y))$;
3. $v(x) = \infty$ se e solo se $x = 0$.

La valutazione p-adica su $\mathbb{Q}$ è quella che a $q = p^n \frac{a}{b}$, come prima, associa $v_p(q) = n$, che non è nient'altro che $-\log_p |q|_p$.

Dato un valore assoluto non-archimedeo su un campo locale K, si possono definire alcuni oggetti:

1. l'**anello degli interi algebrici** $\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$;
2. gli elementi **unitari** di tale anello $\mathcal{O}_K^* = \{x \in K \mid |x| = 1\}$;
3. l'**ideale massimale** $\mathcal{M} = \{x \in K \mid |x| < 1\}$;
4. un genatore m di $\mathcal{M}$ chiamato **uniformizzante** di K;
5. il **campo residuo** $k = \mathcal{O}_K/\mathcal{M}$, che è finito.

Ogni elemento non nullo di K può essere scritto come um^n, dove u è unitario e n è un intero. La **valutazione normalizzata** di K è la mappa

$$v : um^n \mapsto n$$

Nel caso di $\mathbb{Q}_p$ l'anello degli interi algebrici è $\mathbb{Z}_p$, l'ideale massimale è $p\mathbb{Z}_p$ e il campo residuo è $\mathbb{Z}/p\mathbb{Z}$.

Consideriamo ora una curva ellittica E definita su K campo locale. Sia $\mathcal{O}_K$ l'anello degli interi algebrici di K, $\mathcal{M}$ il suo unico ideale massimale e k il campo residuo. Consideriamo una sua equazione di Weierstrass minimale (ovvero tale che $v(\Delta)$ sia minimo). Chiamiamo $\tilde{E}$ la riduzione modulo $\mathcal{M}$ di E (presa cioè l'equazione di Weierstrass minimale, consideriamo i suoi coefficienti ridotti modulo $\mathcal{M}$). La curva $\tilde{E}$ può essere singolare.
Diciamo che

1. E ha **buona** (o **stabile**) **riduzione** se $\tilde{E}$ è non singolare;
2. E ha **riduzione moltiplicativa** (o **semi-stabile**) se $\tilde{E}$ ha un nodo (in particolare se le direzioni delle tangenti nel nodo sono definite su k_v la riduzione si dice **spezzata**);
3. E ha **riduzione additiva** (o **instabile**) se $\tilde{E}$ ha una cuspide.

4.4 La funzione L associata a una curva ellittica

Possiamo finalmente introdurre l'oggetto principale del nostro studio, che, come anticipato, racchiude in sè molte informazioni sulle curve ellittiche.
Sia K un campo di numeri,
M_K un insieme completo di valori assoluti non equivalenti su K,
M_K^0 il sottoinsieme dei valori assoluti non-archimedei,
$v(x) = -\log|x|_v$ per ogni $|\cdot|_v \in M_K$,
K_v il completamento di K su v, per ogni $v \in M_K$,

$\mathcal{O}_v$, $\mathcal{M}_v$ e k_v l'anello degli interi algebrici, l'ideale massimale e il campo residuo associati a K_v, per ogni $v \in M_K^0$.

Consideriamo ora una curva ellittica E definita su K. Sia $|\cdot|_v \in M_K$ un valore assoluto tale che k_v è finito (denotiamo $q_v = \#k_v$) e la curva E ha buona riduzione in K_v. Chiamiamo $\tilde{E}_v$ la riduzione di E modulo $\mathcal{M}_v$. Ricordiamo che la funzione zeta di $\tilde{E}$ su k_v è

$$Z(\tilde{E}_v/k_v; t) = \exp\left(\sum_{n=1}^{\infty}(\#\tilde{E}_v(k_{v,n}))\frac{t^n}{n}\right)$$

dove ricordiamo che $k_{v,n}$ è l'estensione di grado n di k_v.

Abbiamo anche provato che

$$Z(\tilde{E}_v/k_v; t) = \frac{1 - a_v t + q_v t^2}{(1-t)(1-q_v t)}$$

dove $a_v = q_v + 1 - \#\tilde{E}_v(k_v)$.

Chiamiamo

$$L_v(t) = 1 - a_v t + q_v t^2$$

Notiamo che $L_v(t) \in \mathbb{Z}[t]$.

Estendiamo la definizione di $L_v(t)$ ai casi in cui E ha cattiva riduzione:

$$L_v(t) = \begin{cases} 1-t & \text{se } E \text{ ha riduzione moltiplicativa spezzata in } v \\ 1+t & \text{se } E \text{ ha riduzione moltiplicativa non spezzata in } v \\ 1 & \text{se } E \text{ ha riduzione additiva in } v \end{cases}$$

Possiamo allora dare un'importante definizione.

Definizione 4.3. *La **funzione** L di E su K è definita dal prodotto di Eulero*

$$L_{E/K}(s) = \prod_{v \in M_K^0} L_v(q_v^{-s})^{-1}$$

Sfruttando il Teorema di Hasse possiamo mostrare che tale prodotto converge a una funzione olomorfa su $\mathrm{Re}(s) > \frac{3}{2}$, la quale ha sviluppo in serie di Dirichlet

$$L_{E/K}(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

per certi coefficienti $a_n \in \mathbb{C}$. Vedremo che vale ben di più, come corollario di un'ulteriore versione del Teorema di Modularità.

Sia ora

$$f_v = \begin{cases} 0 & \text{se } E \text{ ha buona riduzione in } v \\ 1 & \text{se } E \text{ ha riduzione moltiplicativa in } v \\ 2+\delta_v & \text{se } E \text{ ha riduzione additiva in } v \end{cases}$$

dove δ_v è un certo intero non negativo, che "misura la ramificazione". In particolare $\delta_v = 0$ se $\mathrm{char}(k_v) \neq 2, 3$.

Definizione 4.4. *Il **conduttore** di E, curva ellittica definita su K, è l'ideale*

$$\mathcal{N}_{E/K} = \prod_{v \in M_K^0} \mathcal{M}_v^{f_v}$$

Consideriamo ora il caso $K = \mathbb{Q}$.

Abbiamo visto che i valori assoluti non banali su $\mathbb{Q}$ sono quello ordinario e quelli p-adici e questi ultimi sono non-archimedei. Rispetto ai valori assoluti p-adici, il completamento di $\mathbb{Q}$ è $\mathbb{Q}_p$, l'anello degli interi algebrici è $\mathbb{Z}_p$, l'ideale massimale $p\mathbb{Z}_p$ e il campo residuo $\mathbb{Z}/p\mathbb{Z}$.

Data una curva ellittica E definita su $\mathbb{Q}$ possiamo considerare il conduttore di E su $\mathbb{Q}$ come numero intero positivo, in particolare

$$N_E = N_{E/\mathbb{Q}} = \prod_{p \in \mathcal{P}} p^{f_p}$$

dove per $\mathcal{P}$ si intende l'insieme dei numeri primi.

Si ottiene pertanto che la funzione L di E è della forma

$$L_E(s) = L_{E/\mathbb{Q}}(s) = \prod_{p | N_E} \frac{1}{1 + t_p p^{-s}} \cdot \prod_{p \not| N_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

dove $t_p = 0, \pm 1$, a seconda della cattiva riduzione.

Poiché i primi che dividono N_E sono ovviamente in numero finito, si può scrivere in modo informale

$$L_E(s) \sim \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \prod_p \frac{1}{(1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})}$$

con $\alpha_p \cdot \beta_p = p$ e $|\alpha_p| = |\beta_p| = \sqrt{p}$, come visto precedentemente.

4.5 La funzione L di una forma modulare

Concludiamo introducendo alcuni elementi di teoria delle funzioni L associate a forme modulari.

Sia f una forma modulare, con sviluppo in serie di Fourier

$$f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi i n z}$$

con $z \in \mathfrak{H}$ e $c_n \in \mathbb{C}$.

Abbiamo già visto che possiamo interpretarla come

$$f(q) = \sum_{n=0}^{\infty} c_n q^n$$

con $q = e^{2\pi i z}$.

Ricordiamo che $f(z)$ si dice olomorfa all'infinito se $f(q)$ lo è in 0, e in tal caso

$$f(\infty) = c_0$$

Dato uno sviluppo di Fourier di questo tipo, esiste un modo "standard" di costruire una serie di Dirichlet associata, utilizzando una trasformazione integrale detta **trasfomata di Mellin**:

$$M(f(z), s) = \int_0^{\infty} f(t) t^{s-1} dt$$

Se poniamo $\bar{f}(z) = f(iz) - f(\infty)$, allora possiamo definire la **funzione** L di f come

$$L(f, s) = (2\pi)^2 M(\bar{f}, s)/\Gamma(s)$$

dove ricordiamo

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt = M(e^{-z}, s)$$

Da questo si mostra facilmente, con un cambio di variabili, che

$$L(f, s) = \sum_{n=1}^{\infty} c_n n^{-s}$$

La funzione $L(f,s)$ è chiamata la **funzione L della forma modulare f.** Se f ha peso k, si ha $f\left(-\frac{1}{z}\right) = z^k f(z)$. Supponiamo che f sia una forma cuspidale, così che $f(\infty) = 0$.

Sia

$$L^*(f,s) = (2\pi)^{-2}\Gamma(s)L(f,s) = M(\bar{f}(z),s) = \int_0^\infty f(it)t^s\frac{dt}{t}$$

Abbiamo allora il seguente risultato.

Proposizione 4.1. *Data una forma cuspidale di peso k, si ha*

$$L^*(f,k-s) = (-1)^{\frac{k}{2}}L^*(f,s)$$

Dimostrazione. Poiché

$$f(it) = f\left(-\frac{1}{\left(\frac{i}{t}\right)}\right) = \left(\frac{i}{t}\right)^k f\left(\frac{i}{t}\right)$$

si ha

$$L^*(f,k-s) = \int_0^\infty f(it)t^{k-s}\frac{dt}{t} = (i)^k\int_0^\infty f\left(\frac{i}{t}\right)t^{-s}\frac{dt}{t}$$

e, operando il cambio di variabile $t \rightsquigarrow \frac{1}{t}$ si ottiene

$$L^*(f,k-s) = (i)^k L^*(f,s) = (-1)^{\frac{k}{2}}L^*(f,s)$$

□

Se consideriamo forme modulari rispetto a $\Gamma_1(N)$ (che hanno come sottoinsieme le forme modulari rispetto a $\Gamma_0(N)$) e non all'intero Γ, le cose cambiano. In particolare, non abbiamo più che $f\left(-\frac{1}{z}\right) = z^k f(z)$, perché $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \notin \Gamma_1(N)$.

Fortunatamente le cose non cambiano troppo: definita infatti

$$L^*(f,s) = N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(f,s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s\Gamma(s)L(f,s)$$

si ottiene il seguente importante risultato.

Teorema 4.4. *Sia f forma cuspidale di peso k rispetto a $\Gamma_1(N)$, tale che*

$$i^k N^{-\frac{k}{2}} z^{-2} f\left(-\frac{1}{Nz}\right) = wf(z)$$

dove $w = \pm 1$. Allora $L^*(f,s)$ si estende a una funzione intera che soddisfa l'equazione funzionale

$$L^*(f, k-s) = wL^*(f,s)$$

Quindi $L(f,s)$ ha un prolungamento analitico a tutto il piano complesso.

Dimostrazione. cfr. [Dia], pag.204. □

Abbiamo già definito la funzione $L_E(s)$ di una curva ellittica E definita su $\mathbb{Q}$, avente sviluppo in serie di Dirichlet

$$L_E(s) = \sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} a_n(E) n^{-s}$$

Citiamo allora una versione del Teorema di Modularità che ha importanti conseguenze.

Teorema 4.5. *Sia E una curva ellittica su $\mathbb{Q}$ con conduttore N_E. Allora esiste una parametrizzazione ϕ definita su $\mathbb{Q}$,*

$$\phi : X_0(N_E) \to E$$

Inoltre esiste una forma cuspidale di peso 2 rispetto a $\Gamma_0(N_E)$ tale che

$$L(f,s) = L_E(s)$$

Più precisamente, tale forma è esattamente

$$f(z) = \sum_{n=1}^{\infty} a_n(E) e^{2\pi i n z}$$

e soddisfa le condizioni del Teorema 4.4.

Abbiamo perciò che $L_E(s)$ ammette prolungamento analitico a tutto il piano complesso, e soddisfa l'equazione funzionale

$$\left(\frac{\sqrt{N_E}}{2\pi}\right)^{2-s} \Gamma(2-s) L_E(2-s) = w \left(\frac{\sqrt{N_E}}{2\pi}\right)^{s} \Gamma(s) L_E(s)$$

Faremo ampio uso di questo risultato.

Capitolo 5

Il risultato di Gross-Zagier

Questo capitolo ha lo scopo di introdurre gli oggetti e gli strumenti necessari per comprendere il significato del risultato di Gross-Zagier. Non daremo quasi nessuna dimostrazione, in quanto farlo esulerebbe ampiamente dallo scopo del nostro studio.

Alla fine del capitolo vedremo come è possibile utilizzare il risultato di Gross-Zagier nello studio delle funzioni L associate alle curve ellittiche.

5.1 Operatori di Hecke

Abbiamo già introdotto il concetto di forma modulare e di forma cuspidale. Andiamo ora a studiare in modo più approfondito lo spazio delle forme cuspidali e gli operatori che agiscono su di esso.
Sia Γ' sottogruppo del gruppo modulare tale che

$$\Gamma_1(N) \subset \Gamma' \subset \Gamma_0(N)$$

per un certo N intero positivo.
Consideriamo $\mathcal{S}_2(\Gamma')$, spazio delle forme cuspidali di peso 2 rispetto a Γ', e $\Omega^1(X(\Gamma'))$, spazio delle 1-forme olomorfe su $X(\Gamma')$.

Abbiamo il seguente risultato.

Proposizione 5.1. *La mappa*

$$\begin{aligned} \mathcal{S}_2(\Gamma') &\to \Omega^1(X(\Gamma')) \\ f(z) &\mapsto \omega_f = 2\pi i f(z)\, dz \end{aligned}$$

è un isomorfismo

Dimostrazione. cfr. [Dar95], pag.26. □

Corollario 5.1. *Lo spazio $\mathcal{S}_2(\Gamma')$ è finito dimensionale e la sua dimensione è uguale al genere g di $X(\Gamma')$*

Dimostrazione. É conseguenza diretta della Proposizione 5.1 e del Teorema di Riemann-Roch. □

Lo spazio $\mathcal{S}_2(\Gamma')$ è dotato di un prodotto interno Hermitiano, detto **prodotto interno di Petersson**, dato da

$$\langle f, g\rangle = \frac{i}{8\pi^2}\int_{X(\Gamma')} \omega_f \wedge \bar{\omega}_g = \int_{\Gamma'\backslash\mathfrak{H}} f(z)\ \bar{g}(z)\ dx\ dy$$

dove $z = x + iy$, con $x, y \in \mathbb{R}$.

Restringiamo l'attenzione a $S_2(\Gamma_0(N))$.

Possiamo definire su tale spazio degli operatori, detti **operatori di Hecke**, con indice p primo, nel seguente modo (cfr. [Dara], pag.14, o, per una trattazione più approfondita, cfr. [Atk70]):

se $f \in S_2(\Gamma_0(N))$

$$T_p(f) := \begin{cases} \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) + pf(pz) & \text{se } p \not| N \\ \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) & \text{se } p|N \end{cases}$$

Questi operatori agiscono linearmente su $S_2(\Gamma_0(N))$ e, se $f = \sum a_n q^n$, si ha

$$T_p f = T_p(f) := \begin{cases} \sum_{p|n} a_n q^{n/p} + p\sum a_n q^{pn} & \text{se } p \not| N \\ \sum_{p|n} a_n q^{n/p} & \text{se } p|N \end{cases}$$

É conveniente estendere la definizione a ogni intero positivo n imponendo

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p \not| N} \frac{1}{1 - T_p p^{-s} + p^{1-2s}} \cdot \prod_{p|N} \frac{1}{1 - T_p p^{-s}}$$

Tale condizione può essere vista in modo più diretto (cfr. [Dar95], pag.29): sia m intero positivo, allora

$$T_{p^{m+1}} = \begin{cases} T_p T_{p^m} - p T_{p^{n-1}} & \text{se } p \not| N \\ T_p^m & \text{se } p|N \end{cases}$$

Se $n = \prod_{p \in \mathcal{P}} p^{e_p}$ definiamo allora

$$T_n = \prod_{p \in \mathcal{P}} T_{p^{e_p}}$$

É facile osservare che gli operatori di Hecke sono moltiplicativi, ovvero

$$T_m T_n = T_{mn} \qquad \text{se } (m, n) = 1$$

Possiamo allora dare la seguente definizione.

Definizione 5.1. *Chiamiamo* ***algebra di Hecke*** $\mathbb{T}$ *la sottoalgebra commutativa di* $End_{\mathbb{C}}(S_2(N))$ *generata su* $\mathbb{Z}$ *dagli operatori di Hecke* T_n.
Denotiamo con $\mathbb{T}^0$ *la sottoalgebra generata solo dai* T_n *con* $(n, N) = 1$.

Si può dimostrare il seguente risultato (cfr. [Dara], pag.15).

Proposizione 5.2. *Le algebre di Hecke* $\mathbb{T}$ *e* $\mathbb{T}^0$ *sono finitamente generate come* $\mathbb{Z}$*-moduli, in particolare il rango di* $\mathbb{T}$ *è esattamente* g*, genere di* $X_0(N)$.

Sia $\mathbb{T}_{\mathbb{C}} = \mathbb{T} \otimes \mathbb{C}$. Si può definire una forma bilineare su $\mathbb{C}$ in modo naturale

$$\begin{aligned} \langle\ ,\ \rangle : \quad \mathbb{T}_{\mathbb{C}} \times S_2(\Gamma_0(N)) &\to \mathbb{C} \\ (T_n, f) &\mapsto a_n(f) \end{aligned}$$

dove $a_n(f)$ è l'n-esimo coefficiente nello sviluppo in serie di Fourier di f.

Si può dare una interpretazione degli operatori di Hecke in termini di spazi di moduli (per dettagli circa la connessione tra le due interpretazioni

cfr. [Dia], capitolo 5).

Consideriamo la curva modulare $X_0(N)$, i cui punti non cuspidali possono essere interpretati, in termini di spazi di moduli, come diagrammi

$$x = (\phi : E \to E')$$

con $\ker \phi$ sottogruppo ciclico di ordine N.

Sia n intero positivo. Consideriamo un sottogruppo C di E di ordine n tale che $C \cap \ker \phi = \{0\}$ e definiamo $x_C = \left(\overline{\phi} : E/C \to E'/\phi(C)\right)$. Allora

$$\begin{array}{rccc} T_n : & \mathrm{Div}(X_0(N)) & \to & \mathrm{Div}(X_0(N)) \\ & (x) & \mapsto & \sum_C (x_C) \end{array}$$

dove la sommatoria è fatta al variare dei sottogruppi descritti sopra.

5.2 La teoria di Atkin-Lehner

Introduciamo il concetto di forme vecchie e di forme nuove.

Abbiamo innanzitutto che ogni $T \in \mathbb{T}^0$ è autoaggiunto rispetto al prodotto interno di Petersson (cfr. [Kna], pag.280), ovvero

$$\langle Tf, g\rangle = \langle f, Tg\rangle \qquad \text{per ogni } f, g \in S_0(N)$$

Grazie al teorema spettrale per gli operatori commutativi autoaggiunti, abbiamo che

$$S_0(N) = \bigoplus_{\lambda} S_\lambda^0$$

su tutti gli omomorfismi di $\mathbb{C}$-algebra $\lambda : \mathbb{T}^0 \to \mathbb{C}$, dove S_λ^0 denota il corrispondente autospazio in $S_2(N)$.

L'autospazio S_λ^0 non è necessariamente unidimensionale, mentre se $\lambda : \mathbb{T} \to \mathbb{C}$ è un omomorfismo di anelli definito sull'intera algebra di Hecke $\mathbb{T}$, e S_λ è il suo autospazio associato, si ha che tale autospazio è unodimensionale.

Lo spazio $S_2(N)$ non si decompone in generale in somma diretta di autospazi unodimensionali. Comunque, esiste un sottospazio si $S_2(N)$, il cosiddetto

spazio delle forme nuove, che si decompone in somma diretta di autospazi unodimensionali sia sotto l'azione di $\mathbb{T}$ che di $\mathbb{T}^0$. Più precisamente, una forma cuspidale in $S_0(N)$ è detta **forma vecchia** se è combinazione lineare di funzioni della forma $f(d'z)$, con $f \in S_2(N/d)$ e $d'|d > 1$. Denotiamo l'insieme delle forme vecchie con il simbolo $S_2^{\text{old}}(N)$. Introduciamo allora lo spazio delle **forme nuove**, $S_2^{\text{new}}(N)$, come complemento ortogonale di $S_2^{\text{old}}(N)$ rispetto al prodotto interno di Petersson.

Abbiamo un teorema dovuto a Atkin e Lehner (cfr. [Atk70]).

Teorema 5.1. *Sia $f \in S_2^{new}(N)$ un'autoforma per l'azione di $\mathbb{T}^0$ e sia S un insieme finito di numeri primi. Sia infine $g \in S_2(N)$ un'autoforma per T_p, per ogni $p \notin S$.*
Se $a_p(f) = a_p(g)$ per ogni $p \notin S$, allora $g = \lambda f$ per qualche $\lambda \in \mathbb{C}$.

Corollario 5.2. *Abbiamo*

$$S_0(N) = S_2^{old}(N) \bigoplus_{\lambda} \mathbb{C} f_\lambda$$

dove la somma è fatta su tutti i $\lambda : \mathbb{T} \to \mathbb{C}$ corrispondenti ad autovettori in $S_2^{new}(N)$, e

$$f_\lambda(z) = \sum_{n=1}^{\infty} \lambda(T_n) e^{2\pi i n z}$$

L'autovettore f_λ è chiamato **autoforma normalizzata** o semplicemente **forma nuova di livello** N. Si dimostra che $a_1(f) = 1$.

5.3 La varietà Jacobiana

Sia X una superficie di Riemann compatta di genere $g \geq 1$ e sia x_0 un punto fissato di X. Lasciando variare $x \in X$ e vedendo l'integrazione lungo cammini come una funzione degli integrali olomorfi ω su X, la mappa

$$x \mapsto \left(\omega \mapsto \int_{x_0}^{x} \omega \right)$$

è un'iniezione

$$X \to \left\{ \begin{array}{c} \text{funzioni lineari di differenziali olomorfi su } X \\ \text{modulo integrazione su cammini chiusi} \end{array} \right\}$$

Quando $g = 1$ questo è un isomorfismo di gruppi abeliani. Quando $g > 1$ il dominio X non è più un gruppo, ma il codominio sì. Il codominio è la **Jacobiana** di X, che da un punto di vista analitico complesso è un toro g-dimensionale $\mathbb{C}/\Lambda_g$ con $\Lambda_g \cong \mathbb{Z}^{2g}$.

Vedendo X come una sfera con g manici, siano $A_1, \ldots, A_g$ i lacci longitudinali che circondano ogni manico e siano $B_1, \ldots, B_g$ i lacci latitudinali che fanno da equatore a ogni manico.

Si può dimostrare che per ogni intero non negativo N, ogni N-upla di interi $l_1, \ldots, l_N$ e ogni N-upla di lacci $\alpha_1, \ldots, \alpha_N$, esistono unici degli interi $m_1, \ldots, m_g, n_1, \ldots, n_g$ tali che

$$\sum_{i=1}^{N} l_i \int_{\alpha_1} \omega = \sum_{i=1}^{g} m_i \int_{A_i} \omega + \sum_{i=1}^{g} n_i \int_{B_i} \omega$$

per ogni $\omega \in \Omega^1_{\text{hol}}(X)$.

Detto

$$H_1(X, \mathbb{Z}) = \mathbb{Z} \int_{A_1} \oplus \ldots \oplus \mathbb{Z} \int_{A_g} \oplus \mathbb{Z} \int_{B_1} \oplus \ldots \oplus \mathbb{Z} \int_{B_g}$$

si ha che $H_1(X, \mathbb{Z})$ è isomorfo a $\mathbb{Z}^{2g}$ ed è ovviamente sottogruppo dello spazio duale di $\Omega^1_{\text{hol}}(X)$, che denotiamo con $\Omega^1_{\text{hol}}(X)^*$.

Si può dimostrare che

$$\Omega^1_{\text{hol}}(X)^* = \mathbb{R} \int_{A_1} \oplus \ldots \oplus \mathbb{R} \int_{A_g} \oplus \mathbb{R} \int_{B_1} \oplus \ldots \oplus \mathbb{R} \int_{B_g}$$

Possiamo allora dare una definizione più precisa della Jacobiana di X.

Definizione 5.2. *La **Jacobiana** di X è il gruppo quoziente*

$$Jac(X) = \Omega^1_{hol}(X)^* / H_1(X, \mathbb{Z})$$

Ricordiamo ora che $\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)/P(X)$. Se X ha genere maggiore di zero e x_0 è un punto base di X, allora X si immerge nel suo gruppo di Picard (di grado 0) tramite la mappa

$$x \mapsto P(X) + x - x_0$$

Possiamo allora enunciare il **Teorema di Abel**.

Teorema 5.2. *La mappa*

$$\begin{aligned} Div^0(X) &\to Jac(X) \\ \textstyle\sum_x n_x x &\mapsto \textstyle\sum_x n_x \int_{x_0}^{x} \end{aligned}$$

è ben definita, passa al quoziente e induce un isomorfismo

$$Pic^0(X) \tilde{\to} Jac(X)$$

Nel caso $X = X_0(N)$ indicheremo la Jacobiana con $J_0(N)$. Abbiamo visto come differenziali olomorfi su $X_0(N)$ possono essere identificati con forme cuspidali di peso 2. Possiamo pertanto interpretare la Jacobiana di $X_0(N)$ come

$$\mathrm{Jac}(X_0(N)) = S_0(N)^*/H_1(X_0(N), \mathbb{Z})$$

5.4 Teoria delle altezze

Come ultima premessa al risultato di Gross-Zagier, diamo alcuni elementi di teoria delle altezze.
In questo paragrafo ci limiteremo a dare, in sequenza, definizioni e proposizioni, omettendo tutte le dimostrazioni.

Definizione 5.3. *Sia $P \in \mathbb{P}^n(K)$ un punto con coordinate omogenee $(x_0, \ldots, x_n)$ con $x_i \in K$. L'**altezza di P relativa a K** è definita da*

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_n|_v\}^{n_v}$$

dove $n_v = [K_v : \mathbb{Q}_v]$.

Proposizione 5.3. *Sia $P \in \mathbb{P}^n(K)$. Allora:*

1. *$H_K(P)$ non dipende dalla scelta delle coordinate omogenee di P.*
2. *$H_K(P) \geq 1$.*
3. *Sia L un'estensione finita di K. Allora $H_L(P) = H_K(P)^{[L:K]}$.*

Dimostrazione. cfr. [Sil], pag.207. □

Definizione 5.4. *Sia $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$. L'**altezza assoluta di** P, denotata con $H(P)$, è definita come segue: scegliamo un qualsiasi campo K tale che $P \in \mathbb{P}^n(K)$, allora*

$$H(P) = H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}$$

dove si considera la radice positiva.

Definizione 5.5. *L'**altezza** (assoluta logaritmica) sullo spazio proiettivo è la funzione*

$$\begin{aligned} h: \quad \mathbb{P}^n(\bar{\mathbb{Q}}) &\to \mathbb{R} \\ P &\mapsto \log H(P) \end{aligned}$$

Definizione 5.6. *Sia E una curva ellittica definita su K e $f \in \bar{K}(E)$ una funzione. Una **altezza su E (relativa ad f)** è la funzione*

$$\begin{aligned} h_f: \quad E(\bar{K}) &\to \mathbb{R} \\ P &\mapsto h(f(P)) \end{aligned}$$

Proposizione 5.4. *Sia E una curva ellittica definita su K, $f \in K(E)$ una funzione pari non costante e $P \in E(K)$. Allora il limite*

$$\frac{1}{\deg(f)} \lim_{n\to\infty} 4^{-n} h_f([2^n]P)$$

esiste ed è indipendente da f.

Definizione 5.7. *L'**altezza canonica (o altezza di Néron-Tate)** su E definita su K, denotata con $\hat{h}$ o $\hat{h}_E$, è la funzione*

$$\begin{aligned} \hat{h}: \quad E(\bar{K}) &\to \mathbb{R} \\ P &\mapsto \tfrac{1}{\deg(f)} \lim_{n\to\infty} 4^{-n} h_f([2^n]P) \end{aligned}$$

Enunciamo infine il **Teorema di Néron-Tate**.

Teorema 5.3. *Sia E una curva ellittica definita su K e sia $\hat{h}$ l'altezza canonica su E. Allora:*

1. *Per ogni $P, Q \in E(\bar{K})$ si ha*

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

2. *Per ogni $P \in E(\bar{K})$ e $m \in \mathbb{Z}$*

$$\hat{h}([m]P) = m^2\hat{h}(P)$$

3. *$\hat{h}$ è una forma quadratica su E.*

4. *Sia $P \in E(\bar{K})$. Allora $\hat{h}(P) \geq 0$ e $\hat{h}(P) = 0$ se e solo se P è un punto di torsione.*

Dal teorema possiamo definire il **prodotto interno di Néron-Tate**

$$\langle\ ,\ \rangle : E(\bar{K}) \times E(\bar{K}) \to \mathbb{R}$$

con

$$\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

5.5 Il risultato di Gross-Zagier

Sia $K = \mathbb{Q}(\sqrt{D})$ campo quadratico complesso con discriminante fondamentale D e H campo di classe di Hilbert di K.
Diamo alcuni elementi di teoria globale di campi di classe, riducendoci al nostro caso (per una trattazione più completa cfr. [Lana], capitolo 10).
H è l'estensione abeliana non ramificata massimale di K. Consideriamo un primo $\mathcal{P}_K \in K$ e sia $\mathcal{P}_H$ un primo di H che sta sopra $\mathcal{P}_K$ (i.e. tale che $\mathcal{P}_H \cap K = \mathcal{P}_K$). Abbiamo che $\mathcal{O}_H/\mathcal{P}_L$ è estensione finita di $\mathcal{O}_K/\mathcal{P}_K$.

Per restrizione otteniamo un omomorfismo dal gruppo di decomposizione di $\mathcal{P}_H$ al gruppo di Galois dei campi residui

$$\{\sigma \in G_{H/K} \mid \mathcal{P}_H^\sigma = \mathcal{P}_H\} \to G_{\mathcal{O}_H/\mathcal{P}_H \ / \ \mathcal{O}_K/\mathcal{P}_K}$$

Il gruppo di Galois $G_{\mathcal{O}_H/\mathcal{P}_H \ / \ \mathcal{O}_K/\mathcal{P}_K}$ è ciclico, generato dall'automorfismo di Frobenius.

Esiste un unico elemento $\sigma_{\mathcal{P}_K} \in G_{H/K}$, univocamente determinato da $\mathcal{P}_K$, che viene mandato nell'automorfismo di Frobenius.

Sia $I(K) = \{\text{ideali frazionari di } K\}$.

Possiamo allora definire la **mappa di Artin**

$$\begin{array}{rccc} (\ \cdot\ , H/K): & I(K) & \to & G_{H/K} \\ & (\mathcal{A}, H|K) = \left(\prod \mathcal{P}_K^{n_{\mathcal{P}_\mathcal{K}}}\right) & \mapsto & \prod \sigma_{\mathcal{P}_K}^{n_{\mathcal{P}_\mathcal{K}}} \end{array}$$

Si può mostrare che il nucleo di tale mappa è esattamente $P(K)$, l'insieme degli ideali frazionari principali di K, così da ottenere un isomorfismo

$$\mathrm{Cl}_K \xrightarrow{\sim} G_{H/K}$$

Consideriamo allora $\sigma \in G_{H/K}$ e sia $[\mathcal{A}] \in \mathrm{Cl}_K$ corrispondente a σ.

Definiamo

$$\theta_{[\mathcal{A}]}(z) = \frac{1}{2u} + \sum_{\mathcal{A} \text{ ideale in } [\mathcal{A}]} e^{2\pi i N(\mathcal{A}) z} = \sum_{n=0}^{\infty} r_{[\mathcal{A}]}(n) e^{2\pi i n z}$$

dove $2u$ è il numero di elementi unitari in $\mathcal{O}_K$, $r_{[\mathcal{A}]}(0) = \frac{1}{2u}$ e $r_{[\mathcal{A}]}(n)$, per $n \geq 1$, è il numero di ideali (interi) in $[\mathcal{A}]$ di norma n.

Sia

$$\chi_D : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$$

carattere associato a K,

$$f = \sum_{n=1}^{\infty} a_n q^{2\pi i n z} \in S_2^{\mathrm{new}}(\Gamma_0(N))$$

e poniamo

$$F = \{n \geq 1 \mid (n, ND) = 1\}$$

Definiamo

$$L_{[\mathcal{A}]}(f,s) = \sum_{n\in F} \chi_D(n) n^{1-2s} \cdot \sum_{n=1}^{\infty} a_n r_{[\mathcal{A}]}(n) n^{-s}$$

Se f è un autoforma sotto l'azione di $\mathbb{T}$, normalizzata con la condizione che $a_1 = 1$, e χ è un carattere complesso di Cl_K, definiamo la funzione

$$L(f,\chi,s) = \sum_{[\mathcal{A}]\in \mathrm{Cl}_K} \chi([\mathcal{A}]) L_{[\mathcal{A}]}(f,s)$$

Sia ora τ un punto di Heegner di discriminante D, con D privo di fattori quadratici (il che implica $d \equiv 1 \pmod 4$) e primo con N. Sia c la classe del divisore $(\tau) - (\infty)$ in $J(H)$. Il campo quadratico $K = \mathbb{Q}(\sqrt{D})$ ha numero di classi di ideali h e contiene $2u$ radici dell'unità. L'elemento $\sigma \in G_{H/K}$ corrisponde alla classe $[\mathcal{A}]$ tramite l'isomorfismo di Artin. Infine $\langle\ ,\ \rangle$ denota il prodotto interno derivato dalle altezze su $J(H)\otimes\mathbb{C}$ e $(\ ,\ )$ il prodotto interno di Petersson.

Possiamo allora enunciare il **Teorema di Gross-Zagier**.

Teorema 5.4. *La serie* $g_{[\mathcal{A}]} = \sum_{n=1}^{\infty} \langle c, T_n c^{\sigma}\rangle e^{2\pi i n z}$ *è una forma cuspidale di peso* 2 *su* $\Gamma_0(N)$ *che soddisfa*

$$(f, g_{[\mathcal{A}]}) = \frac{u^2\sqrt{|D|}}{8\pi^2} L'_{[\mathcal{A}]}(f,s)$$

per ogni $f \in S_2^{new}(\Gamma_0(N))$

Da questo si può dedurre il seguente teorema.

Teorema 5.5. *Si ha*

$$L'(f,\chi,1) = \frac{8\pi^2(f,f)}{u^2\sqrt{|D|}} h(f,\chi) = \frac{\|\omega_f\|^2}{u^2\sqrt{|D|}} h(f,\chi)$$

dove h *è una altezza (che non definiamo in modo preciso, ma che è l'analogo dell'altezza canonica sui punti di una curva ellittica) e* $\omega_f = 2\pi i f(z) dz$.

5.6 Conseguenze sulle funzioni L associate a curve ellittiche

Questi risultati, riportati e dimostrati nell'articolo di Gross e Zagier [Gro86] possono essere riletti, grazie al Teorema di Modularità, in termini di funzioni L associate a curve ellittiche.

Consideriamo E curva ellittica di conduttore N_E. La funzione $L_E(s)$ è olomorfa su tutto il piano complesso e la parità del suo ordine m in $s = 1$ è nota: m è pari o dispari in accordo con il segno ($w = +1$ o $w = -1$) dell'equazione funzionale di $L_E(s)$, e questo è determinato a sua volta dal fatto che f soddisfi $f\left(-\frac{1}{Nz}\right) = -Nz^2 f(z)$ o $f\left(-\frac{1}{Nz}\right) = +Nz^2 f(z)$.

Fissato un discriminante D e considerato il campo $K = \mathbb{Q}(\sqrt{D})$, abbiamo visto come è possibile costruire un punto $P_D \in E(K)$, che abbiamo chiamato punto di Heegner. Denominiamo $E^{(D)}$ la curva ellittica "twistata" (se $E : y^2 = 4x^3 - g_2x - g_3$, allora $E^{(D)} : dy^2 = 4x^3 - g_2x - g_3$).

Si può dimostrare che, grazie al Teorema di Gross-Zagier, il punto di Heegner P_D viene mandato tramite coniugazione complessa in $-wP_D$.

Abbiamo quindi due casi:

1. $w = -1$. Quindi $L_E(1) = 0$ e abbiamo che $2P_D \in E(\mathbb{Q})$ e la formula di Gross-Zagier si può rileggere nel seguente modo:

$$L_{E^{(D)}}(1)L'_E(1) = C \cdot \hat{h}_E(2P_D)$$

   dove C è una costante non nulla.

2. $w = +1$. Allora $2P_D = (x, y\sqrt{D})$ con $x, y \in \mathbb{Q}$, e quindi $P_D \in E^{(D)}(\mathbb{Q})$ e la formula di Gross-Zagier diventa:

$$L_E(1)L'_{E^{(D)}}(1) = C \cdot \hat{h}_{E^{(D)}}(2P_D)$$

   dove C è ancora una costante non nulla.

Utilizzeremo questo risultato nel seguito.

Capitolo 6

Il Teorema di Goldfeld

Tutto quello che è stato detto finora ci porta finalmente al capitolo centrale del nostro studio. Il risultato di Goldfeld, unito al lavoro di Gross e Zagier, come già detto, chiude definitivamente il Problema di Gauss sul numero di classi di ideali, a meno di un numero finito di calcoli.

Per semplicità, affronteremo dapprima il Problema di Gauss di numero di classe 1, per poi trattare il caso più generale. Incominceremo, in entrambi i casi, da osservazioni basilari sulla ramificazione di primi "piccoli" in campi quadratici complessi. Entreremo poi nel merito dell'utilità del lavoro di Gross-Zagier alla soluzione di Goldfeld del quale daremo, infine, un'idea dettagliata pur senza entrare nei tecnicismi. In questo senso, per non appesantire le notazioni, useremo spesso gli aggettivi "piccoli" e "grandi", senza specificarne meglio il significato.

6.1 Il fenomeno di Deuring-Heilbronn

Iniziamo con una semplice osservazione.

Proposizione 6.1. *Sia $\mathbb{Q}(\sqrt{D})$ un campo quadratico complesso con numero di classi di ideali $h(D) = 1$. Allora tutti i primi minori di $\frac{1+|D|}{4}$ sono inerti.*

Dimostrazione. Ricordiamo che, poiché $h(D) = 1$, si ha che $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ è un dominio a ideali principali.

Sia p un primo che spezza completamente in $\mathbb{Q}(\sqrt{D})$. Allora $(p) = \pi \cdot \bar{\pi}$ con $\pi = \left(\frac{m+n\sqrt{D}}{2}\right)$. Segue che

$$p = \frac{m^2 + n^2|D|}{4}$$

da cui otteniamo

$$p > \frac{1 + |D|}{4}$$

□

La Proposizione 6.1 è il caso più semplice di un fenomeno generale per cui, in campi quadratici $\mathbb{Q}(\sqrt{D})$ con numero di classi di ideali "piccolo" rispetto a D, molti primi "piccoli" devono essere inerti, come vedremo.

Se $\chi_D(n) = \left(\frac{D}{n}\right)$ è il carattere quadratico associato al campo $\mathbb{Q}(\sqrt{D})$ la Proposizione 6.1 si può rienunciare così: *sia* $\mathbb{Q}(\sqrt{D})$ *un campo quadratico complesso con numero di classi di ideali* $h(D) = 1$*; allora* $\chi_D(p) = -1$ *per* $p \leq \frac{1+|D|}{4}$.

Quindi $\chi_D(n)$ si comporta come la funzione di Liuville $\lambda(n)$, ovvero

$$\lambda(n) = (-1)^{\Omega(n)}$$

con $\Omega(n)$ numero di fattori primi di n contati con molteplicità.

Ci aspettiamo pertanto che, per $D \to -\infty$ e s fissato con $\mathrm{Re}(s) > \frac{1}{2}$, si abbia

$$\begin{array}{rcccc} L(s, \chi_D) & = & \sum \frac{\chi_D(n)}{n^s} & = & \prod \left(\frac{1}{1-\chi_D(p)p^{-s}}\right) \\ & \sim & \prod \left(\frac{1}{1+p^{-s}}\right) & = & \sum \frac{\lambda(n)}{n^s} \qquad = \frac{\zeta(2s)}{\zeta(s)} \end{array}$$

dove lasciamo al simbolo $\sim$ un significato intuitivo di approssimazione.

Questa osservazione sta alla base del cosiddetto effetto di repulsione dello zero (fenomeno di Deuring-Heilbronn) associato a campi quadratici immaginari con numero di classe di ideali piccolo.

Nel caso $h(D) = 1$ abbiamo che, se $D \to -\infty$ e D_1 è un discriminante fondamentale fissato, per $\mathrm{Re}(s) > \frac{1}{2}$

$$L(s, \chi_{D_1}) L(s, \chi_D \chi_{D_1}) \sim L(2s, \chi_{D_1}^2)$$

che implica (cfr. [Dav], capitolo 14) che la funzione $L(s, \chi_{D_1})$ non abbia zeri in $\mathrm{Re}(s) > \frac{1}{2}$.

6.2 Esistenza di una curva ellittica con funzione L associata con zero triplo

La costruzione che facciamo in questo paragrafo è molto particolare, ma può essere generalizzata ad altre curve ellittiche.
Sia E una curva ellittica definita su $\mathbb{Q}$.
Denotiamo con $L_E(s, \chi_D)$ la funzione L di E modificata con il carattere quadratico χ_D associato a un discriminante fondamentale D di un campo quadratico complesso, ovvero

$$L_E(s, \chi_D) = \sum_{n=1}^{\infty} \frac{\chi_D(n) a_n}{n^s}$$

dove $L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$. Si ha che

$$L_{E/\mathbb{Q}(\sqrt{D})}(s) = L_E(s) L_E(s, \chi_D)$$

Abbiamo che $L_{E/\mathbb{Q}(\sqrt{D})}(s) = L_{E^{(D)}}(s)$ dove $E^{(D)}$ è la curva ellittica "twistata".
Sia ora E la curva ellittica

$$E : y^2 = x^3 + 10x^2 - 20x + 8$$

con conduttore $N_E = 37$. Si ha $L_E(1) \neq 0$. Quindi il segno dell'equazione funzionale per $L_E(s)$ è positivo. Fissato $D = -139$, si ha allora

$$L_E(1) L'_{E^{(-139)}}(1) = C \cdot \hat{h}_{E^{(-139)}}(2P_{-139})$$

A questo punto si mostra tutta l'importanza dei punti di Heegner per il nostro problema. Dimostriamo infatti un lemma fondamentale.

Lemma 6.1. *P_{-139} è banale su una curva ellittica E di conduttore 37.*

Dimostrazione. Sia $K = \mathbb{Q}(\sqrt{-139})$. Il numero di classi di ideali di K è $h(-139) = 3$. Possiamo considerare 3 punti, radici di

$$Az^2 + Bz + C = 0$$

con $B^2 - 4AC = -139$ e $A \equiv 0 \pmod{37}$, coniugati rispetto a $G_{H(-139)/K}$. Scegliamo

$$\tau_1 = \frac{-3 + \sqrt{-139}}{2 \cdot 37} \qquad \tau_2 = \frac{71 + \sqrt{-139}}{10 \cdot 37} \qquad \tau_3 = \frac{-151 + \sqrt{-139}}{10 \cdot 37}$$

Essi soddisfano le relazioni

$$37 \cdot \tau_1 = \frac{-3\tau_1 - 1}{\tau_1} \qquad 37 \cdot \tau_2 = \frac{34\tau_2 - 7}{5\tau_2 - 1} \qquad 37 \cdot \tau_3 = \frac{-77\tau_3 - 31}{5\tau_3 + 2}$$

dove $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} -3 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 34 & -7 \\ 5 & -1 \end{smallmatrix}\right)$ e $\left(\begin{smallmatrix} -77 & -31 \\ 5 & 2 \end{smallmatrix}\right)$ sono matrici in $\mathrm{SL}_2(\mathbb{Z})$ tali che, per $z = \tau_1, \tau_2$ e τ_3 rispettivamente, si ha

$$(cz + d)^{-1} = -\frac{3 + \sqrt{-139}}{2}$$

Consideriamo ora la forma modulare $\Delta(z)$ di peso 12. Definiamo

$$g(z) = \sqrt[12]{\frac{\Delta(z)}{\Delta(37z)}} - \frac{3 + \sqrt{-139}}{2}$$

Per quanto detto, è immediato verificare che $g(z)$ si annulla in τ_1, τ_2 e τ_3. D'altra parte $g(z)$ è $\Gamma_0(37)$-invariante, ha un polo triplo all'infinito e non ha altri poli ($\Delta(z) \neq 0$ in $\mathfrak{H}$). Quindi ci sono solo questi 3 zeri. Pertanto

$$(\tau_1) + (\tau_2) + (\tau_3) - 3(\infty)$$

è un divisore principale su $X_0(37)$ e, considerata $\phi : X_0(37) \to E$, che soddisfa la proprietà $\phi(\infty) = 0$, si ha

$$P_{-139} = \phi_*((\tau_1) + (\tau_2) + (\tau_3)) = 0$$

□

Dal Lemma 6.1 segue quindi $\hat{h}(2P_{-139}) = 0$ e pertanto

$$L'_{E^{(-139)}}(1) = L'_{E/\mathbb{Q}(\sqrt{-139})}(1) = 0$$

Per semplicità chiamiamo ancora E la curva $E^{(-139)}$. Tale curva ha conduttore $N_E = 37 \cdot 139^2$. Per questa curva si ha

$$\left(\frac{\sqrt{N_E}}{2\pi}\right)^{2-s} \Gamma(2-s)L_E(2-s) = -\left(\frac{\sqrt{N_E}}{2\pi}\right)^{s} \Gamma(s)L_E(s)$$

Quindi $L_E(1) = 0$ e, poiché $L'_E(1) = 0$, si ha almeno uno zero triplo in $s = 1$. Si può verificare che $L'''_E(1) \neq 0$, quindi $L_E(s)$ ha uno zero esattamente triplo in $s = 1$.

6.3 Soluzione del Problema $h(D) = 1$

Sia E la curva definita nel paragrafo precedente.
Sia ora D, con $|D| > 163$, un discriminante fondamentale di un campo quadratico complesso tale che $h(D) = 1$. Si può mostrare che $(D, 37 \cdot 139) = 1$. Definiamo

$$\Lambda_D(s) = \left(\frac{N_E|D|}{4\pi^2}\right)^{s} \Gamma(s)^2 L_E(s)L_E(s, \chi_D)$$

Si può mostrare che $\Lambda_D(s)$ soddisfa l'equazione funzionale (cfr. [Shi])

$$\Lambda_D(1+s) = \chi_D(-N_E)\ \Lambda_D(1-s)$$

Poiché i primi più piccoli di $\frac{1+|D|}{4}$ sono inerti, e $|D| > 163$, si ha che $\chi_D(-N_E) = -\chi_D(37) = +1$, pertanto l'equazione funzionale è semplicemente

$$\Lambda_D(1+s) = \Lambda_D(1-s)$$

Allora $L_E(s)$ ha uno zero di ordine pari in $s = 1$ e quindi otteniamo che $L_{E/\mathbb{Q}(\sqrt{D})}(s) = L_E(s)L_E(s, \chi_D)$ ha uno zero di ordine almeno 4 in $s = 1$.
Consideriamo ora l'integrale

$$I_D = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \Lambda_D(1+s)\frac{ds}{s^3}$$

Lemma 6.2. *Abbiamo $I_D = 0$.*

Dimostrazione. Chiamiamo $f(s) = \frac{\Lambda_D(1+s)}{s^3}$. Abbiamo che

1. $f(s)$ ha uno zero di ordine almeno 1 in $s = 0$;
2. $f(s)$ è dispari;
3. $f(s)$ è olomorfa su tutto il piano complesso e si annulla all'infinito.

Consideriamo il rettangolo γ di vertici $2+ik$, $-2+ik$, $-2-ik$, $2-ik$ (come cammino, percorso in senso antiorario). Per il Teorema dei Residui e per le proprietà 1 e 3 di $f(s)$ si ha che

$$\frac{1}{2\pi i}\int_\gamma f(s)ds = 0$$

Per la proprietà 2 di $f(s)$ si ha che

$$\frac{1}{2\pi i}\int_\gamma f(s)ds = 2\left(\int_{2-ik}^{2+ik} f(s)ds + \int_{2+ik}^{-2+ik} f(s)ds\right)$$

Quindi, per ogni k, si ha che

$$\int_{2-ik}^{2+ik} f(s)ds + \int_{2+ik}^{-2+ik} f(s)ds = 0$$

Facendo tendere k a ∞ e ricordando la proprietà 3 abbiamo la tesi. □

Andiamo ora a modificare tale integrale per ottenere una contraddizione. Ricordiamo che

$$L_E(s) \sim \prod_p \frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})}$$

e

$$L_E(s,\chi_D) \sim \prod_p \frac{1}{(1-\chi_D(p)\alpha_p p^{-s})(1-\chi_D(p)\beta_p p^{-s})}$$

Se $h(D) = 1$ e D è sufficientemente grande, abbiamo visto che χ_D si comporta come la funzione di Liouville, e quindi il prodotto $L_E(s)L_E(s,\chi_D)$ si comporta come

$$\phi(s) := \prod_p \frac{1}{(1-\alpha_p^2 p^{-2s})(1-\beta_p^2 p^{-2s})}$$

Tale funzione non è altro che la **funzione zeta di Rankin** della forma modulare $\sum a(n)e^{2\pi inz}$. Si sa che tale funzione ha uno zero semplice in $s = 1$ (cfr. [Darb], nell'articolo di D. Goldfeld, *The Gauss Class Number Problem for Imaginary Quadratic Fields*, o [Zag84]).

Poiché $\phi(s)$ ha uno zero semplice in $s = 1$, potremmo pensare che, per ottenere una contraddizione, basti trovare una curva ellittica tale che $L_E(s)L_E(s, \chi_D)$ abbia zero doppio. In realtà, il ragionamento necessario è più sottile e richiede effettivamente uno zero quadruplo, come vedremo.
Definiamo

$$\Lambda_D^* = \left(\frac{N_E|D|}{4\pi^2}\right)^s \Gamma(s)^2\phi(s)$$

e

$$I_D^* = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \Lambda_D^*(1+s)\frac{ds}{s^3}$$

Scriviamo allora

$$0 = I_D = I_D^* + \text{Errore}$$

con

$$\text{Errore} = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \left(\frac{N_E|D|}{4\pi^2}\right)^{1+s} \Gamma(1+s)^2[L_E(1+s)L_E(1+s,\chi_D)-\phi(s)]\frac{ds}{s^3}$$

Definiamo infine dei coefficienti di Dirichlet $B(n)$ e $\nu_D(n)$ nel seguente modo

$$L_E(1+s)L_E(1+s,\chi_D) - \phi(s) = \sum_{n=1}^{\infty} B_n n^{-(1+s)}$$

e

$$\zeta(s)L(s,\chi_D) = \sum_{n=1}^{\infty} \nu_D(n)n^{-s}$$

Per $n < \frac{1+|D|}{4}$ si ha $B(n) = 0$ (come conseguenza della Proposizione 6.1).

Andiamo ad enunciare ora tre risultati. Non ci soffermeremo sulla loro dimostrazione, che risulta molto tecnica.

Lemma 6.3. *Definito*

$$d_4(n) = \sum_{d_1 d_2 d_3 d_4 = n} 1$$

si ha

$$|B(n)| \leq \begin{cases} 2\nu_D(n)\sqrt{n} & se\ \frac{1+|D|}{4} \leq n < \left(\frac{1+|D|}{4}\right)^2 \\ 2d_4(n)\sqrt{n} & se\ n \geq \left(\frac{1+|D|}{4}\right)^2 \end{cases}$$

Dimostrazione. cfr. [Darb], nell'articolo di D. Goldfeld, *The Gauss Class Number Problem for Imaginary Quadratic Fields*, Lemma 4. □

Lemma 6.4. *Sia $x > 1$. Allora*

$$\sum_{x \leq n \leq 2x} \nu_D(n)\sqrt{n} \leq 4ex^{\frac{3}{2}} L(1, \chi_D) + O\left(|D|^{\frac{3}{2}} x^{-\frac{1}{2}}\right)$$

Se in più $D > 4$ e $h(D) = 1$, allora

$$\sum_{x \leq n \leq 2x} \nu_D(n)\sqrt{n} \leq 4ex^{\frac{3}{2}} \pi |D|^{-\frac{1}{2}} + O\left(|D|^{\frac{3}{2}} x^{-\frac{1}{2}}\right)$$

Dimostrazione. cfr. [Darb], nell'articolo di D. Goldfeld, *The Gauss Class Number Problem for Imaginary Quadratic Fields*, Lemma 5. Per la seconda parte si usa semplicemente la formula di Dirichlet per il numero di classi di ideali $L(1, \chi_D) = \pi h(D)|D|^{-\frac{1}{2}}$ (cfr. [Dav], Capitolo 6). □

Lemma 6.5. *Per $y > 0$, definiamo*

$$G(y) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} y^{s+1} \Gamma(1+s)^2 \frac{ds}{s^3}$$

Allora

$$G(y) < 2y^2 e^{-\frac{1}{\sqrt{y}}}$$

Dimostrazione. cfr. [Darb], nell'articolo di D. Goldfeld, *The Gauss Class Number Problem for Imaginary Quadratic Fields*, Lemma 6. □

Utilizzando tutti questi risultati si ha che

$$\begin{aligned}
|\text{Errore}| &= \left| \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \left(\frac{N_E|D|}{4\pi^2}\right)^{1+s} \Gamma(1+s)^2 \left[\sum_{n=1}^{\infty} B(n) n^{-(1+s)}\right] \frac{ds}{s^3} \right| \\
&\leq \sum_{n \geq \frac{1+|D|}{4}} |B(n)| G\left(\frac{N_E|D|}{4\pi n}\right) \\
&\leq \sum_{\frac{1+|D|}{4} \leq n \leq \left(\frac{1+|D|}{4}\right)^2} 4\nu_D(n)\sqrt{n} \left(\frac{N_E|D|}{4\pi^2 n}\right)^2 e^{-\sqrt{\frac{4\pi^2 n}{N_E|D|}}} + \\
&\quad + \sum_{n > \left(\frac{1+|D|}{4}\right)^2} 4d_4(n)\sqrt{n} \left(\frac{N_E|D|}{4\pi^2 n}\right)^2 e^{-\sqrt{\frac{4\pi^2 n}{N_E|D|}}}
\end{aligned}$$

La seconda sommatoria è un $\mathrm{O}\left(e^{-c_1\sqrt{|D|}}\right)$ (per qualche $c_1 > 0$) e può quindi essere ignorato. Stimiamo allora Errore suddividendo ulteriormente la prima sommatoria:

$$\begin{aligned}
&|\text{Errore}| \leq \\
&\leq \frac{4N_E^2}{\pi^4} \sum_{k=1}^{\log_2\left(\frac{1+|D|}{4}\right)} \sum_{\frac{1+|D|}{4} 2^{k-1} \leq n \leq \frac{1+|D|}{4} 2^k} \left(\left(\frac{|D|}{4n}\right)^2 \nu_D(n)\sqrt{n} \cdot e^{-\sqrt{\frac{4\pi^2 n}{N_E|D|}}} \right) + \\
&+ \mathrm{O}\left(e^{-c_1\sqrt{|D|}}\right) \\
&\leq \frac{4N_E^2}{\pi^4} \sum_{k=1}^{\log_2\left(\frac{1+|D|}{4}\right)} \frac{1}{2^{2k-2}} \sum_{\frac{1+|D|}{4} 2^{k-1} \leq n \leq \frac{1+|D|}{4} 2^k} \left(\nu_D(n)\sqrt{n} \cdot e^{-\sqrt{\frac{4\pi^2 n}{N_E|D|}}} \right) + \\
&+ \mathrm{O}\left(e^{-c_1\sqrt{|D|}}\right) \\
&\leq \frac{4N_E^2}{\pi^4} \sum_{k=1}^{\log_2\left(\frac{1+|D|}{4}\right)} \frac{1}{2^{2k-2}} \sum_{\frac{1+|D|}{4} 2^{k-1} \leq n \leq \frac{1+|D|}{4} 2^k} \left(\nu_D(n)\sqrt{n} \cdot e^{-\sqrt{\frac{4\pi^2 n}{N_E|D|}}} \right) + \\
&+ \mathrm{O}\left(e^{-c_1\sqrt{|D|}}\right)
\end{aligned}$$

e, utilizzando il Lemma 6.4, si ottiene

$$\text{Errore} \ll |D|$$

da cui si ha che, per D sufficientemente grande, esiste una costante fissata c, effettivamente calcolabile, tale che

$$\text{Errore} < c \cdot |D|$$

per $|D| \to \infty$. Abbiamo allora che

$$|I_D^*| = |I_D - \text{Errore}| = |\text{Errore}| < c \cdot |D|$$

L'integrale I_D^* può essere calcolato analogamente a I_D, sfruttando il Teorema dei Residui. In questo caso abbiamo un polo doppio in $s = 0$. Si può mostrare che esiste una costante effetivamente calcolabile $C > 0$ tale che

$$|I_D^*| > C \cdot |D| \log |D|$$

che, insieme alla limitazione data, ci dà una contraddizione per D grandi. Quindi $h(D) \neq 1$ per D grandi.

6.4 Soluzione generale

Diamo ora un'idea della risoluzione del problema di Gauss nel caso generale (seguendo l'articolo [Zag84]). Vedremo come l'idea della dimostrazione sia fondamentalmente la stessa che nel caso $h(D) = 1$.

Supponiamo di avere un discriminate D con D grande. Vogliamo mostrare che $h(D)$ è anch'esso grande.

Il caso più semplice è quello in cui $\chi_D(37) = 1$. In tal caso infatti esiste in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ un ideale primo $\mathcal{P}$ di norma 37, e $\mathcal{P}^{h(D)}$ è un ideale principale di norma $37^{h(D)}$. Pertanto esistono $m, n \in \mathbb{Z}$, $n \neq 0$ tali che

$$37^{h(D)} = \frac{m^2 + n^2|D|}{4} > \frac{|D|}{4}$$

da cui

$$h(D) > \log_{37}\left(\frac{|D|}{4}\right)$$

Se invece $\chi_D(37) = 0$ o -1, consideriamo la curva ellittica E di conduttore $N_E = 37 \cdot 139^2$ dei paragrafi precedenti. Consideriamo ancora una volta la funzione $L_{E/\mathbb{Q}(\sqrt{D})}(s)$. Questa soddisfa un'equazione funzionale con segno positivo

$$\gamma(1+s)L_{E/\mathbb{Q}(\sqrt{D})}(1+s) = \gamma(1-s)L_{E/\mathbb{Q}(\sqrt{D})}(1-s)$$

per un opportuna funzione $\gamma(s)$. Quindi $L_{E/\mathbb{Q}(\sqrt{D})}(s)$ ha uno zero di ordine almeno 4 in $s = 1$. D'altra parte si può mostrare che $\chi_D(p) = -1$ per tutti

i primi piccoli che non dividono D, in particolare tutti i primi $p < \left|\frac{D}{4}\right|^{\frac{1}{h(D)}}$ (cfr. [Oes85]). Questo implica ancora che, per D grandi rispetto ad $h(D)$, $\chi_D(n)$ si comporti come la funzione di Liouville $\lambda(n)$.

Abbiamo

$$L_{E/\mathbb{Q}(\sqrt{D})}(s) = L_E(s)L_E(s,\chi_D)$$

e consideriamo come prima

$$\phi(s) = L_E(s)L_E(s,\lambda)$$

dove, se $L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, si ha $L_E(s,\lambda) = \sum_{n=1}^{\infty} \frac{\lambda(n)a_n}{n^s}$. Per quanto detto, queste due funzioni non devono differire molto.

Analogamente al caso $h(D) = 1$, non è sufficiente osservare che $L_{E/\mathbb{Q}(\sqrt{D})}(s)$ ha uno zero almeno quadruplo in $s = 1$ mentre $\phi(s)$ ha un zero semplice.

La contraddizione si ottiene come prima comparando i due integrali

$$I_D = \int_{2-i\infty}^{2+i\infty} \gamma(s+1)L_{E/\mathbb{Q}(\sqrt{D})}(s+1)\frac{ds}{s^3} \quad \text{e} \quad I_D^* = \int_{2-i\infty}^{2+i\infty} \gamma(s+1)\phi(s+1)\frac{ds}{s^3}$$

Il primo integrale è nullo, come dimostrato nel Lemma 6.2. Il secondo integrale è non nullo poiché è dominato da un residuo non banale in $s = 1$, della forma $m\log|D| + n$, per certi $m, n \in \mathbb{Z}$. Stimando poi la differenza $L_{E/\mathbb{Q}(\sqrt{D})}(s) - \phi(s)$ si può ottenere che la differenza $I_D^* - I_D$ è un $\mathrm{O}(h(D))$. Questa è una contraddizione per D grande rispetto a $h(D)$.

Si può allora concludere che $h(D) \to \infty$ per $D \to -\infty$ e si può anche dire in che modo.

Abbiamo quindi dato l'idea della dimostrazione del **Teorema di Goldfeld**.

Teorema 6.1. *Sia D un discriminante fondamentale di un campo quadratico complesso. L'esistenza di una curva ellittica E la cui funzione L associata $L_{E/\mathbb{Q}(\sqrt{D})}(s)$ ha uno zero di ordine maggiore o uguale a 4 in $s = 1$ implica che, per ogni costante $\epsilon > 0$, esiste una costante effettivamente calcolabile $c_\epsilon(E)$ tale che*

$$h(D) > c_\epsilon(E)(\log|D|)^{1-\epsilon}$$

Ricordiamo infine il risultato precisato di Oesterlé

$$h(D) > C \cdot \prod_{p|D} \left(1 - \frac{2}{\sqrt{p}}\right) \cdot \log |D|$$

per ogni D, dove C è una costante assoluta ed effettivamente calcolabile.

Questi risultati chiudono definitivamente il Problema di Gauss sul numero di classi di ideali dei campi quadratici complessi e con essi si conclude la nostra trattazione.

Bibliografia

[Apo] T.M. Apostol. *Modular functions and Dirichlet series in number theory*. Springer-Verlag.

[Atk70] A.O.L. Atkin, J.Lehner. Hecke operators on $\Gamma_0(N)$. *Math. Ann. 185*, pages 134–160, 1970.

[Bir70] B.J. Birch. Elliptic Curves and Modular Forms. *Symposia Math. IV (Roma, 1968/69), Academic Press*, pages 27–32, 1970.

[Dara] H. Darmon. *Rational Points on Modular Elliptic Curves*. American Mathematical Society.

[Darb] H. Darmon, S.W. Zhang. *Heegner Points and Rankin L-Series*. Mathematica Sciences Research Institute Publications.

[Dar95] R. Taylor H. Darmon, F. Diamond. Fermat's Last Theorem. *Current Developments in Mathematics 1, International Press*, pages 1–157, 1995.

[Dav] H. Davenport. *Multiplicative Number Theory*. Springer-Verlag.

[Dia] F. Diamond, J. Shurman. *A First Course in Modular Forms*. Springer.

[Gau01] C.F. Gauss. *Disquisitiones arithmeticae*. 1801.

[Gol76] D. Goldfeld. The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer. *Ann. Scuola Norm. Sup. Pisa (4) 3*, pages 623–663, 1976.

[Gro86] B. Gross, D.B. Zagier. Heegner points and derivatives of L-series. *Invent. Math. 84*, pages 225–320, 1986.

[Kna] A.W. Knapp. *Elliptic curves.* Princeton University Press.

[Lana] S. Lang. *Algebraic Number Theory.* Springer-Verlag.

[Lanb] S. Lang. *Elliptic Functions.* Springer-Verlag.

[Oes85] J. Oesterlé. Nombres de classes des corps quadratiques imaginaires. *Séminaire Nicolas Bourbaki, Astérisque 121-122*, pages 309–323, 1985.

[Oes88] J. Oesterlé. Le Probléme de Gauss sur le Nombre de Classes. *Enseign Math. 34*, pages 43–67, 1988.

[Shi] G. Shimura. *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press.

[Sil] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag.

[Zag84] D.B. Zagier. L-series of Elliptic Curves, the Birch-Swinnerton-Dyer Conjecture, and the Class Number Problem of Gauss. *Notices Am. Math. Soc. 31*, pages 739–743, 1984.