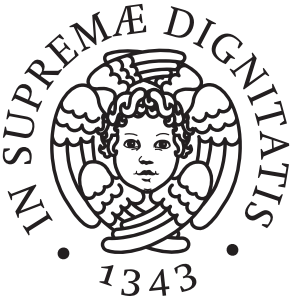
Università di Pisa




Facoltà di Matematica

# Fattorizzazione Unica negli Anelli degli Interi dei Campi Quadratici Immaginari

Tesi di Laurea Triennale
in Matematica

Candidato
**Lorenzo Furio**

Relatore
**Davide Lombardo**
Università di Pisa

Anno Accademico 2018 - 2019

# Indice

# Introduzione

Una domanda che sorge spontanea quando ci si approccia allo studio dei campi di numeri e dei relativi anelli degli interi è se essi siano o meno anelli a fattorizzazione unica. In generale, fissato un campo, si riesce sempre a calcolare il suo gruppo delle classi, tuttavia risulta un problema molto complesso determinare quali campi, all'interno di un insieme descritto da una proprietà fissata, hanno numero di classe 1. Se però ci limitiamo a considerare delle particolari famiglie di campi di numeri è talvolta possibile sfruttarne le relative caratteristiche per studiare la soluzione a questo problema. Nel nostro caso studieremo i campi quadratici immaginari fino a determinare per quali di essi il relativo anello degli interi ha fattorizzazione unica. Si può vedere facilmente che le estensioni quadratiche di $\mathbb{Q}$ sono tutte e sole quelle nella forma $\mathbb{Q}(\sqrt{m})$ per $m \in \mathbb{Z}$ libero da quadrati. Dunque i campi quadratici immaginari, ovvero quelli che ci limiteremo a studiare, risultano essere estensioni del tipo $\mathbb{Q}(\sqrt{-m})$ per $m \in \mathbb{N}$ libero da quadrati.
Nel 1801, nelle sue *Disquisitiones Arithmeticae* [Gau86], Gauss aveva congetturato che se $K = \mathbb{Q}(\sqrt{-m})$, allora $\mathcal{O}_K$ è un UFD se e solo se $m \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. In realtà la congettura originale di Gauss si presentava come un problema di forme quadratiche, che è però equivalente a quello sopra enunciato, che è una riformulazione dello stesso nei termini della matematica moderna. Tale congettura fu successivamente dimostrata da Heegner [Hee52], Baker [Bak67] e Stark [Sta67]. Serre [Ser89] ha dato una reinterpretazione moderna della dimostrazione di Heegner facendo uso della teoria delle curve ellittiche ed è questa la dimostrazione che ci proponiamo di ripercorrere in questa tesi. Si osservi che di fatto lavorare con i campi quadratici immaginari è essenziale: nel caso dei campi quadratici reali, ovvero $K = \mathbb{Q}(\sqrt{m})$ con $m \in \mathbb{N}$ libero da quadrati, si congettura che gli anelli degli interi a fattorizzazione unica siano infiniti, ma questo fatto sembra ancora ben lontano dall'essere dimostrato.
Per dimostrare la congettura di Gauss cominceremo notando che $\mathcal{O}_K$ è un reticolo di $\mathbb{C}$, pertanto il quoziente $\mathbb{C}/\mathcal{O}_K$ è biolomorfo ad una curva ellittica $E$. Possiamo dunque studiare le proprietà di tale curva per dedurre le proprietà di $\mathcal{O}_K$. Si può mostrare che $E$ è a moltiplicazione complessa e che il suo anello degli endomorfismi è proprio $\mathcal{O}_K$. Inoltre, supponendo che $\mathcal{O}_K$ sia a

fattorizzazione unica, mostreremo in un primo momento che il suo invariante $j$ è razionale, per poi ottenere successivamente che è intero. A questo punto concluderemo osservando come gli automorfismi di campo di $\mathbb{C}$ agiscono sui punti di torsione della curva, determinando delle condizioni stringenti su $j$, che ci permetteranno di mostrare ce esiste solo un numero finito di curve ellittiche ad invariante $j$ intero e con moltiplicazione complessa. Questo implica il risultato voluto, in quanto ogni anello del tipo $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ che sia a fattorizzazione unica corrisponde ad una diversa curva ellittica con queste proprietà. Per di più questo metodo permette di ottenere esplicitamente queste curve, rendendo possibile verificare tutti i numeri di classe di tutti i campi $\mathbb{Q}(\sqrt{-d})$ trovati.
Diamo ora una descrizione più precisa del contenuto della tesi. Nel primo capitolo introdurremo alcuni risultati di base sulla teoria delle curve ellittiche che utilizzeremo nel corso degli altri capitoli. Nel secondo capitolo mostreremo che, dato un campo quadratico immaginario $K$, a meno di isomorfismo esiste un numero finito di curve ellittiche il cui anello degli endomorfismi è isomorfo a $\mathcal{O}_K$; per raggiungere questo risultato studieremo come il gruppo $\mathrm{Aut}(\mathbb{C})$ agisce sull'insieme di tali curve. Nel terzo capitolo descriveremo la teoria della curva di Tate, ovvero una curva ellittica definita su un campo $p$-adico i cui punti possono essere identificati con un quoziente $\bar{K}^*/q^{\mathbb{Z}}$. Il vantaggio di tale strumento risiede nello sfruttare il fatto che gli elementi di $\mathrm{Gal}(\bar{K}/K)$ commutano con l'isomorfismo fra il quoziente $\bar{K}^*/q^{\mathbb{Z}}$ e il gruppo dei punti della curva. Infatti, dal momento che le curve ellittiche a invariante $j$ razionale possono essere definite sui razionali, le curve $\mathbb{C}/\mathcal{O}_K$ viste nel capitolo precedente possono essere studiate su un'estensione di $\mathbb{Q}$ diversa da $\mathbb{C}$, nel nostro caso, su un campo $p$-adico. Finiremo dunque per dedurre che se una curva ellittica ha invariante $j$ a valutazione $p$-adica negativa per qualche primo $p$, il suo anello degli endomorfismi è isomorfo a $\mathbb{Z}$, pertanto l'invariante $j$ delle curve ellittiche a moltiplicazione complessa ha valore assoluto minore o uguale a 1 per tutti i primi, ovvero è un intero algebrico. Da questo segue che se $\mathcal{O}_K$ ha fattorizzazione unica, la curva $\mathbb{C}/\mathcal{O}_K$ ha invariante $j$ intero. Infine nel quarto capitolo studieremo come il gruppo di Galois assoluto di $\mathbb{Q}$ agisce sui punti di torsione $E[\ell]$, per $\ell$ primo, rappresentando gli automorfismi in $GL_2(\mathbb{F}_\ell)$. La teoria delle curve modulari permette dunque di ottenere un'equazione diofantea che ha un numero finito di soluzioni, ovvero esiste un numero finito di curve ellittiche a meno di isomorfismo su $\mathbb{C}$ per cui $j$ rispetta tale equazione, in particolare esiste un numero finito di curve ellittiche il cui anello degli endomorfismi è della forma $\mathcal{O}_K$ ed è UFD. Inoltre conoscere il valore di $j$ ci permette di ricostruire le curve in questione e verificare che effettivamente gli anelli $\mathcal{O}_K$ a fattorizzazione unica sono solamente i 9 trovati da Gauss.

CAPITOLO 1

# Preliminari

In questa sezione enunceremo alcuni risultati di base che useremo in seguito nel corso della tesi.

## 1.1 Il gruppo delle classi

Innanzi tutto cominciamo osservando le proprietà algebriche di $\mathcal{O}_K$ :

**Proposizione 1.1.1.** *Sia $K$ un campo di numeri e $\mathcal{O}_K$ il suo anello degli interi, allora $\mathcal{O}_K$ è un UFD se e solo se è un PID.*

Questa proposizione ci porta a definire un particolare gruppo, il gruppo delle classi di ideali, nel modo seguente:

**Definizione 1.1.2.** Detti $\mathcal{F}(K)$ gli ideali frazionari di $\mathcal{O}_K$ e $\mathcal{P}(K)$ gli ideali principali fra i frazionari, si chiama gruppo delle classi di $\mathcal{O}_K$ il gruppo $Cl(K) := \frac{\mathcal{F}(K)}{\mathcal{P}(K)}$.

Infatti gli ideali frazionari formano un gruppo abeliano con l'operazione di moltiplicazione e gli ideali principali sono un loro sottogruppo, pertanto il gruppo quoziente è ben definito. Vale poi la seguente proprietà:

**Teorema 1.1.3.** *Sia $K$ un campo di numeri, allora $Cl(K)$ è un gruppo finito.*

In un certo senso, il gruppo delle classi "misura" quanto un anello di interi non è PID, in particolare non è difficile notare che $\mathcal{O}_K$ è PID (e quindi UFD) se e solo se $Cl(K)$ è banale.

## 1.2 Curve Ellittiche

I risultati successivi hanno l'obbiettivo di riportare le proprietà di base degli endomorfismi di una curva ellittica e di mostrarne il collegamento con gli anelli degli interi dei campi quadratici immaginari.
Quando lavoriamo nel campo dei numeri complessi, si può trovare una corrispondenza fra le curve ellittiche e i tori complessi, cioè dei quozienti di $\mathbb{C}$ per dei reticoli $\Lambda$, ovvero dei sottogruppi discreti di rango 2. D'ora in avanti quando parleremo di *toro* faremo sempre riferimento ad un quoziente $\mathbb{C}/\Lambda$.

**Definizione 1.2.1.** Dati due tori $T_1, T_2$ si chiama isogenia un omomorfismo additivo suriettivo olomorfo $c : T_1 \to T_2$.

**Proposizione 1.2.2.** *Per ogni isogenia $c : T_1 \to T_2$ esiste una costante $\alpha \in \mathbb{C}^*$ tale che $c([x]) = [\alpha \cdot x] \quad \forall x \in \mathbb{C}$.*

**Definizione 1.2.3.** Dato un toro $T$ si definiscono gli endomorfismi del toro come $\mathrm{End}(T) := \{c : T \to T | c \text{ è un'isogenia}\} \bigcup \{0\}$.

Nella precedente definizione le isogenie vengono intese come elementi di $\mathbb{C}^*$, piuttosto che come funzioni.

**Proposizione 1.2.4.** $\mathrm{End}(T)$ *è un sottoanello di $\mathbb{C}$ e i suoi elementi sono interi algebrici di grado al più 2.*

Si può osservare che $\mathbb{Z} \subset \mathrm{End}(T)$, inoltre $\mathrm{End}(T)$ è un sottogruppo discreto di $\mathbb{C}$, quindi è uno $\mathbb{Z}$-modulo libero generato da 1 o 2 elementi. Dunque, in particolare, $\mathrm{End}(T) = \mathbb{Z}$ o $\mathrm{End}(T) = \mathbb{Z}[\alpha]$, dove $\alpha$ è un intero algebrico di grado 2.
Un toro è una varietà complessa di dimensione 1, vogliamo quindi provare a cercare una curva in $\mathbb{P}^2\mathbb{C}$ biolomorfa ad esso, trovando quindi una corrispondenza fra i tori e tali curve.

**Definizione 1.2.5.** Dato un campo $K$, si chiama curva ellittica una curva algebrica piana non singolare definita su $K$ da un'equazione in $\mathbb{P}^2K$ nella forma

$$E : \ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Nel corso della trattazione vedremo principalmente curve complesse.

**Definizione 1.2.6.** Si chiama funzione di Weierstrass la funzione

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

La funzione di Weierstrass è biperiodica rispetto al reticolo $\Lambda$, pertanto possiamo vederla come una funzione $\wp : {}^{\mathbb{C}}\!/_{\Lambda} \to \mathbb{C}$. Inoltre non è difficile mostrare che tale funzione è meromorfa e ha poli di ordine 2 sugli elementi del reticolo; equivalentemente può essere vista come una funzione olomorfa $\wp : {}^{\mathbb{C}}\!/_{\Lambda} \to \mathbb{P}^2\mathbb{C}$.

**Proposizione 1.2.7.** *Le funzioni $\wp(z)$ e $\wp'(z)$ rispettano un'equazione del tipo*

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

*dove*

$$g_2 = 60 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^4}$$
$$g_3 = 140 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^6}$$

**Proposizione 1.2.8.** *La funzione seguente*

$$\begin{aligned} z &\longmapsto [\wp(z), \wp'(z), 1] \quad \text{se } z \neq 0 \\ z &\longmapsto [0,1,0] = O \quad \text{se } z = 0 \end{aligned}$$

*è un biolomorfismo fra $T = {}^{\mathbb{C}}\!/_{\Lambda}$ e la curva $E : Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ in $\mathbb{P}^2\mathbb{C}$.*

**Proposizione 1.2.9.** *Dato il reticolo $\Lambda$, ogni funzione meromorfa $\Lambda$-periodica è una funzione razionale di $\wp$ e $\wp'$.*

Generalmente rappresenteremo la curva con la sua equazione su $\mathbb{C}^2$, ammettendo che abbia anche un punto all'infinito che corrisponde a $O$.
Chiameremo $E_\Lambda$ la curva ottenuta da un toro di reticolo $\Lambda$.
Partendo dalla legge di gruppo additivo di $T$ è possibile definire una legge di gruppo sulla curva, in maniera tale da rendere il biolomorfismo della proposizione 1.2.8 un omomorfismo. Intuitivamente definiamo la somma fra i punti $P$ e $Q$ come il terzo punto di intersezione fra la retta passante per entrambi e la curva, la cui coordinata $y$ è cambiata di segno. Algebricamente, per $x_1 \neq x_2$, questo si traduce nella seguente relazione (sulle coordinate affini):

$$(x_1, y_1) + (x_2, y_2) = \left( \frac{k^2}{4} - x_1 - x_2 \ , \ -k\left(\frac{k^2}{4} - x_1 - x_2\right) - h \right) \qquad (1.1)$$

dove $k = \frac{y_2 - y_1}{x_2 - x_1}$ e $h = y_1 - kx_1$. Se invece $x_1 = x_2$ allora abbiamo due casi: o $y_1 = -y_2 \neq -y_1$, allora diremo che $(x_1, y_1) + (x_2, y_2) = O$, dove $O$ è il punto all'infinito della curva; oppure $(x_1, y_1) = (x_2, y_2)$, in questo caso la formula di addizione è una formula di duplicazione e vale la stessa relazione che in 1.1 ma con $k = \frac{12x_1^2 - g_2}{2y_1}$ e $h = y_1 - kx_1$.
Per le curve ellittiche che non si presentano nella forma $y^2 = 4x^3 - g_2x - g_3$

sappiamo che esiste un cambio di coordinate lineare che le porta in tale forma, pertanto la legge di gruppo su queste curve è definita, attraverso tale cambio di coordinate, come la legge della curva ellittica nella forma $y^2 = 4x^3 - g_2x - g_3$ associata ad essa.
Non è difficile osservare che la legge di gruppo descritta nell'equazione 1.1 è una funzione le cui coordinate sono funzioni razionali a coefficienti razionali dei punti della curva. Inoltre il cambio di coordinate che porta una curva ellittica nella forma $y^2 = 4x^3 - g_2x - g_3$ in una curva ellittica in forma di Weierstrass, ovvero nella forma $y^2 = x^3 + ax + b$, è a coefficienti razionali, pertanto anche la legge di gruppo sulle curve ellittiche in forma di Weierstrass avrà coordinate che sono funzioni razionali a coefficienti razionali.

**Definizione 1.2.10.** Si chiama gruppo di $n$-torsione il gruppo

$$E[n] := \{P \in E | nP = 0\}$$

**Proposizione 1.2.11.** $E[n] \cong {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$

Diremo che due curve ellittiche complesse sono isomorfe se esiste un isomorfismo olomorfo fra di esse, ovvero una funzione fra le due curve le cui coordinate sono funzioni olomorfe e che sia anche un isomorfismo rispetto alla legge di gruppo della curva. Più in generale possiamo considerare degli omomorfismi olomorfi, in particolare, come per i tori, è possibile definire l'anello degli endomorfismi della curva $\mathrm{End}(E)$. Nel caso di una curva ellittica $E_\Lambda$ proveniente da un reticolo $\Lambda$, l'anello degli omomorfismi della curva è isomorfo all'anello degli endomorfismi del toro ${}^{\mathbb{C}}\!/_{\Lambda}$, in quanto esiste un isomorfismo olomorfo fra la curva e il toro, dunque sono ottenuti gli uni dagli altri tramite la composizione con esso.
Se stiamo trattando curve ellittiche su campi generici diversi da $\mathbb{C}$ la condizione di olomorfia non può più essere utilizzata per definire gli endomorfismi, pertanto essi si definiscono nel modo seguente:

**Definizione 1.2.12.** Sia $K$ un campo e ${}^{E}\!/_{K}$ una curva ellittica definita su di esso, chiameremo endomorfismo della curva una funzione algebrica $E \longrightarrow E$ che induca un omomorfismo di gruppi.

**Proposizione 1.2.13.** $E_{\Lambda_1} \cong E_{\Lambda_2} \iff \exists \alpha \in \mathbb{C}$ *tale che* $\Lambda_1 = \alpha\Lambda_2$.

Osserviamo che una trasformazione lineare delle coordinate è un isomorfismo di curve ellittiche. Inoltre, data una generica curva ellittica, definita su un campo di caratteristica diversa da 2 e da 3, nella forma $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, esiste sempre una trasformazione lineare delle coordinate che la manda in una curva ellittica in forma di Weierstrass, ovvero nella forma $y^2 = x^3 + ax + b$. Pertanto possiamo sempre assumere che a meno di isomorfismo una curva ellittica sia in forma di Weierstrass.

**Definizione 1.2.14.** Data una curva ellittica generica

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

definiamo:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2^2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6
\end{aligned}$$

Inoltre si definisce invariante $j$ della curva la quantità $j = \frac{c_4^3}{\Delta}$.

**Teorema 1.2.15.** *L'invariante $j$ di una curva ellittica è invariante per isomorfismo.*

Il precedente teorema ci dice che possiamo quindi definire senza perdita di generalità l'invariante $j$ su una curva ellittica in forma di Weierstrass, dunque per la curva $y^2 = x^3 + ax + b$ avremo che $\Delta = 4a^3 + 27b^2$ e $j = \frac{1728a^3}{\Delta}$.
La curva $y^2 = 4x^3 - g_2x - g_3$ ha dunque invariante $j = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$.

**Teorema 1.2.16.** *Due curve ellittiche definite su un campo algebricamente chiuso sono isomorfe se e solo se hanno lo stesso invariante $j$.*

**Teorema 1.2.17.** $\forall c \in \mathbb{C}\ \exists \Lambda$ *reticolo tale che* $j(E_\Lambda) = c$.

**Corollario 1.2.18.** *Ogni curva ellittica complessa, a meno di isomorfismo, proviene da un toro.*

**Proposizione 1.2.19.** *Per le curve ellittiche complesse la definizione di endomorfismo come in 1.2.12 coincide con quella di endomorfismo olomorfo ereditata dai tori.*

*Dimostrazione.* Le funzioni razionali sono chiaramente olomorfe nel piano proiettivo, quindi resta da dimostrare che gli omomorfismi olomorfi sono descritti da funzioni razionali.
Sappiamo che $E \cong E_\Lambda$ per un certo reticolo $\Lambda$, dunque $\forall \phi$ omomorfismo olomorfo di $E$ $\exists \alpha \in \mathrm{End}\left(\mathbb{C}/\Lambda\right)$ per cui $\phi(\wp(z), \wp'(z)) = (\wp(\alpha z), \wp'(\alpha z))$. Dato che $\alpha\Lambda \subseteq \Lambda$, la funzione $\wp(\alpha z)$ è $\Lambda$-periodica, pertanto, per la proposizione 1.2.9, è una funzione razionale di $\wp(z)$ e $\wp'(z)$, da cui la tesi. □

**Esempio 1.2.20.** Data la curva $E : \ y^2 = x^3 + x$, un endomorfismo è ad esempio la funzione $(x, y) \longmapsto (-x, iy)$, le cui coordinate sono funzioni razionali.

Fino ad ora abbiamo parlato principalmente di curve ellittiche complesse, questo perché su $\mathbb{C}$ è possibile stabilire una corrispondenza fra curve e tori. In generale però, per curve ellittiche definite su campi qualsiasi, non tutte le proprietà sopra elencate rimangono valide, tuttavia alcune proprietà non dipendono dalla particolare scelta del campo, ad esempio il teorema 1.2.16. Nel corso della tesi vedremo, oltre a curve ellittche definite su $\mathbb{C}$, curve ellittiche definite su campi di numeri e su loro completamenti rispetto a valori assoluti non archimedei.
Alla luce di quanto appena detto, per studiare l'anello $\mathcal{O}_K$ degli interi di $K = \mathbb{Q}(\sqrt{-n})$ cominceremo considerando le curve ellittiche il cui anello degli endomorfismi è isomorfo a $\mathcal{O}_K$.

CAPITOLO 2

# Razionalità dell'invariante $j$

## 2.1 L'Azione di $Cl(K)$ su $\mathcal{ELL}(\mathcal{O}_K)$

**Definizione 2.1.1.** Dato un anello $R$, definiamo l'insieme

$$\mathcal{ELL}(R) := \{E | \operatorname{End}(E) \cong R\}_{/\cong} \longleftrightarrow \{\Lambda | \operatorname{End}(E_\Lambda) \cong R\}_{/\text{omotetia}}$$

dove $E$ costituisce una curva ellittica complessa e $\Lambda$ un reticolo di $\mathbb{C}$.

**Lemma 2.1.2.** *Dato $n \in \mathbb{N} \setminus \{0\}$ e detto $K = \mathbb{Q}(\sqrt{-n})$, allora $\mathcal{ELL}(\mathcal{O}_K) \neq \emptyset$.*

*Dimostrazione.* Consideriamo il reticolo $\Lambda = \mathcal{O}_K$ e la curva $E = \mathbb{C}/\mathcal{O}_K$, allora $\mathcal{O}_K \cdot \mathcal{O}_K \subset \mathcal{O}_K$, dunque $\mathcal{O}_K \subset \operatorname{End}(E)$. Inoltre, se $\alpha \in \operatorname{End}(E)$, $\alpha\mathcal{O}_K \subset \mathcal{O}_K$, pertanto $\alpha \in K$. Tuttavia gli endomorfismi di una curva sono interi algebrici, quindi $\alpha \in \mathcal{O}_K$, da cui $\operatorname{End}(E) = \mathcal{O}_K$. Questo in particolare ci dice che $E \in \mathcal{ELL}(\mathcal{O}_K)$, a meno di considerare la sua classe di isomorfismo. □

D'ora in avanti, data una curva ellittica, scriveremo che essa appartiene a $\mathcal{ELL}(R)$ intendendo che la sua classe di isomorfismo appartiene a tale insieme. Un'altra convenzione che utilizzeremo spesso è la seguente: dati $A$ e $B$ due sotto $\mathbb{Z}$-moduli di $\mathbb{C}$, indicheremo con $AB$ il modulo $< \{ab \mid a \in A, b \in B\} >_{\mathbb{Z}}$, similmente alla notazione utilizzata per gli ideali frazionari.
Infine, aggiungiamo che d'ora in poi $K$ sarà sempre un campo quadratico immaginario, a meno che non sia specificato diversamente.
Consideriamo adesso un ideale frazionario $\mathfrak{a} \in \mathcal{F}(K)$. Questo è sempre uno $\mathbb{Z}$-modulo libero di rango $n = [K : \mathbb{Q}]$, quindi nel nostro caso, in cui $K = \mathbb{Q}(\sqrt{-n})$, $\mathfrak{a} \subset \mathbb{C}$ è uno $\mathbb{Z}$-modulo di rango 2; inoltre $\mathfrak{a} \subsetneq \mathbb{R}$, dunque $\mathfrak{a}$ è un reticolo di $\mathbb{C}$. Questo vuol dire che possiamo considerare la curva ellittica $E_{\mathfrak{a}}$

e notare che

$$\begin{aligned}\mathrm{End}(E_{\mathfrak{a}}) \cong \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = \{\alpha \in K \mid (\alpha)\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1}\} = \\ = \{\alpha \in K \mid (\alpha) \subseteq \mathcal{O}_K\} = \mathcal{O}_K\end{aligned}$$

Dunque $E_{\mathfrak{a}} \in \mathcal{ELL}(\mathcal{O}_K)$. Questa osservazione ci porta a formulare la seguente proposizione.

**Proposizione 2.1.3.** *Sia $\Lambda$ un reticolo tale che $\mathrm{End}(E_\Lambda) \cong \mathcal{O}_K$, allora $\exists\lambda \in \mathbb{C}$ e $\exists\mathfrak{a} \in \mathcal{F}(K)$ tali che $\Lambda = \lambda\mathfrak{a}$.*

*Dimostrazione.* Sappiamo che ogni reticolo può essere normalizzato, ovvero sappiamo che $\exists\lambda \in \Lambda$ tale che $\frac{1}{\lambda}\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$. Per ipotesi $\mathcal{O}_K\Lambda = \Lambda$, dunque

$$\mathcal{O}_K\frac{1}{\lambda}\Lambda = \frac{1}{\lambda}\Lambda \implies \mathcal{O}_K(\mathbb{Z} \oplus \tau\mathbb{Z}) = \mathbb{Z} \oplus \tau\mathbb{Z}$$

Tuttavia $\mathcal{O}_K\mathbb{Z} = \mathcal{O}_K$, pertanto

$$\mathcal{O}_K \subseteq \mathcal{O}_K \oplus \tau\mathcal{O}_K\mathbb{Z} = \mathbb{Z} \oplus \tau\mathbb{Z}$$

Inoltre vale che $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$, ma $\mathcal{O}_K \subseteq \mathbb{Z} \oplus \tau\mathbb{Z} \subseteq \mathbb{Q}(\tau)$, da cui otteniamo $K \subseteq \mathbb{Q}(\tau)$. Per la proprietà delle torri $\mathbb{Q}(\tau) = K$. Quanto detto finora ci porta a concludere che $\frac{1}{\lambda}\Lambda$ è un sotto $\mathcal{O}_K$-modulo di $K$, pertanto è un suo ideale frazionario, ovvero $\frac{1}{\lambda}\Lambda = \mathfrak{a} \in \mathcal{F}(K) \implies \Lambda = \lambda\mathfrak{a}$. □

**Proposizione 2.1.4.** *Sia $\mathfrak{a} \in \mathcal{F}(K)$ e sia $\Lambda$ un reticolo di $\mathbb{C}$ tale che $E_\Lambda \in \mathcal{ELL}(\mathcal{O}_K)$, allora $\mathfrak{a}\Lambda$ è un reticolo e $E_{\mathfrak{a}\Lambda} \in \mathcal{ELL}(\mathcal{O}_K)$.*

*Dimostrazione.* Per un certo $\mathfrak{b} \in \mathcal{F}(K)$ vale che $\mathfrak{a}\Lambda = \mathfrak{a}\lambda\frac{1}{\lambda}\Lambda = \lambda\mathfrak{a}\mathfrak{b}$ che è un reticolo di $\mathbb{C}$, inoltre

$$\begin{aligned}\mathrm{End}(E_{\mathfrak{a}\Lambda}) = \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda\} = \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}\} = \\ = \{\alpha \in K \mid (\alpha) \subseteq \mathcal{O}_K\} = \mathcal{O}_K\end{aligned}$$

ovvero $E_{\mathfrak{a}\Lambda} \in \mathcal{ELL}(\mathcal{O}_K)$. □

**Proposizione 2.1.5.** *Dati $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}(K)$ e $\Lambda$ reticolo di $\mathbb{C}$, allora*

$$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \iff \bar{\mathfrak{a}} = \bar{\mathfrak{b}} \text{ in } Cl(K)$$

*Dimostrazione.*

$$\begin{aligned}&E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \iff \\ &\exists\alpha \in \mathbb{C} \text{ tale che } \alpha\mathfrak{a}\Lambda = \mathfrak{b}\Lambda \iff \\ &\exists\alpha \in \mathbb{C} \text{ tale che } \alpha\Lambda = \mathfrak{a}^{-1}\mathfrak{b}\Lambda \iff \\ &\exists\alpha \in \mathbb{C} \text{ tale che } \alpha\frac{1}{\lambda}\Lambda = \mathfrak{a}^{-1}\mathfrak{b}\frac{1}{\lambda}\Lambda \iff \\ &\exists\alpha \in K \text{ tale che } \alpha = \mathfrak{a}^{-1}\mathfrak{b} \iff \\ &\mathfrak{a}^{-1}\mathfrak{b} \in \mathcal{P}(K) \iff \bar{\mathfrak{a}} = \bar{\mathfrak{b}} \text{ in } Cl(K)\end{aligned}$$

□

Le tre proposizioni precedenti gettano le basi per definire un'azione del gruppo delle classi sull'insieme $\mathcal{ELL}(\mathcal{O}_K)$. Il seguente teorema si pone l'obbiettivo di descrivere tale azione.

**Teorema 2.1.6.** *Il gruppo $Cl(K)$ agisce su $\mathcal{ELL}(\mathcal{O}_K)$ tramite l'azione*

$$\begin{array}{ccc} Cl(K) \times \mathcal{ELL}(\mathcal{O}_K) & \longrightarrow & \mathcal{ELL}(\mathcal{O}_K) \\ \bar{\mathfrak{a}} * E_\Lambda & \longmapsto & E_{\mathfrak{a}\Lambda} \end{array}$$

*Inoltre, tale azione è semplicemente transitiva.*

*Dimostrazione.* Innanzi tutto cominciamo notando che l'azione è ben definita, ovvero che $E_{\mathfrak{a}\Lambda}$ non dipende dal rappresentante della classe di $\mathfrak{a}$ scelto, infatti per la proposizione 2.1.5 se due ideali frazionari $\mathfrak{a}$ e $\mathfrak{b}$ appartengono alla stessa classe allora $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$.
Adesso vogliamo mostrare che è semplicemente transitiva, ovvero che per ogni coppia di elementi di $\mathcal{ELL}(\mathcal{O}_K)$ esiste un'unica classe di $Cl(K)$ che manda un elemento nell'altro. Siano allora $\Lambda_1, \Lambda_2$ due reticoli tali che $E_{\Lambda_1}, E_{\Lambda_2} \in \mathcal{ELL}(\mathcal{O}_K)$, avremo che, per la proposizione 2.1.3, $\Lambda_1 = \lambda_1\mathfrak{a}$ e $\Lambda_2 = \lambda_2\mathfrak{b}$ con $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}(K)$. Dunque

$$\begin{aligned} &\exists \mathfrak{c} \in \mathcal{F}(K) \text{ tale che } E_{\mathfrak{c}\Lambda_1} \cong E_{\Lambda_2} \iff \\ &\exists \alpha \in \mathbb{C} \text{ tale che } \alpha\mathfrak{c}\Lambda_1 = \Lambda_2 \iff \\ &\frac{\alpha\lambda_1}{\lambda_2}\mathfrak{c}\mathfrak{a} = \mathfrak{b} \iff \\ &\overline{\mathfrak{c}\mathfrak{a}} = \overline{\mathfrak{b}} \text{ in } Cl(K) \iff \bar{\mathfrak{c}} = \overline{\mathfrak{a}^{-1}\mathfrak{b}} \end{aligned}$$

Pertanto l'azione è transitiva, in quanto $\overline{\mathfrak{a}^{-1}\mathfrak{b}} * E_{\Lambda_1} = E_{\Lambda_2}$. Per mostrare che la transitività è semplice basta osservare che per la proposizione 2.1.5 se avessi che gli ideali frazionari $\mathfrak{a}$ e $\mathfrak{b}$ mandano la curva $E_\Lambda$ nello stesso elemento allora $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \implies \bar{\mathfrak{a}} = \bar{\mathfrak{b}}$. □

**Corollario 2.1.7.** *$|\mathcal{ELL}(\mathcal{O}_K)| = |Cl(K)|$, in particolare $\mathcal{ELL}(\mathcal{O}_K)$ ha cardinalità finita.*

## 2.2 Algebricità dell'invariante $j$

A questo punto cerchiamo di capire come si comportano le operazioni di anello di $\mathrm{End}(E)$. Se la curva ellittica complessa $E$ proviene da un toro $T$, allora $\mathrm{End}(T)$ è un sottoanello di $\mathbb{C}$ e ne eredita le operazioni, pertanto, per capire come si comportano le operazioni di $\mathrm{End}(E)$ dobbiamo guardare le operazioni

di $\mathrm{End}(T)$ attraverso la funzione $z \longmapsto (\wp(z), \wp'(z))$. Quindi se $\alpha, \beta \in \mathrm{End}(T)$, in $\mathrm{End}(E)$ si traducono nelle funzioni

$$\phi = \{(\wp(z), \wp'(z)) \mapsto (\wp(\alpha z), \wp'(\alpha z))\}\ ,\ \psi = \{(\wp(z), \wp'(z)) \mapsto (\wp(\beta z), \wp'(\beta z))\}$$

Dunque

$$\begin{aligned}\phi \cdot \psi &= \{(\wp(z), \wp'(z)) \mapsto (\wp(\alpha\beta z), \wp'(\alpha\beta z))\} = \\ &= \phi(\{(\wp(z), \wp'(z)) \mapsto (\wp(\beta z), \wp'(\beta z))\}) = \phi \circ \psi\end{aligned}$$

da cui vediamo che il prodotto dell'anello $\mathrm{End}(E)$ è la composizione di funzioni. Per quanto riguarda la somma invece, se $(x, y) = (\wp(z), \wp'(z))$, abbiamo

$$\begin{aligned}(\phi + \psi)(x, y) &= (\wp((\alpha + \beta)z), \wp'((\alpha + \beta)z)) = \\ &= (\wp(\alpha z + \beta z), \wp'(\alpha z + \beta z)) = \\ &= (\wp(\alpha z), \wp'(\alpha z)) + (\wp(\beta z), \wp'(\beta z)) = \phi(x, y) + \psi(x, y)\end{aligned}$$

Dove la somma dei punti della curva è la legge di gruppo descritta nell'equazione 1.1, in particolare le sue coordinate sono funzioni razionali delle coordinate di $\phi(x, y)$ e $\psi(x, y)$.

*Osservazione* 2.2.1. $\mathrm{End}(E) \cong \mathrm{End}(T)$ è un anello commutativo, pertanto la composizione di endomorfismi di una curva ellittica è sempre commutativa.

A questo punto cominceremo a studiare come gli automorfismi di campo di $\mathbb{C}$ intervengono sulle proprietà delle curve ellittiche complesse. In particolare data la curva $E:\ y^2 = x^3 + ax + b$, indicheremo con $\sigma E$ la curva ottenuta applicando l'automorfismo $\sigma \in \mathrm{Aut}(\mathbb{C})$ alla sua equazione, ovvero $\sigma E$ è la curva ellittica definita dall'equazione $\sigma E:\ y^2 = x^3 + \sigma(a)x + \sigma(b)$.

**Proposizione 2.2.2.** *Sia $\sigma \in \mathrm{Aut}(\mathbb{C})$, $E$ una curva ellittica complessa, allora* $\mathrm{End}(\sigma E) \cong \mathrm{End}(E)$.

*Dimostrazione.* Cominciamo mostrando che $\mathrm{End}(\sigma E) = \sigma\,\mathrm{End}(E)$, dove $\sigma$ agisce sugli endomorfismi agendo sui loro coefficienti di funzioni razionali. Se $E:\ y^2 = x^3 + ax + b$, allora $\sigma E:\ y^2 = x^3 + \sigma(a)x + \sigma(b)$ e i punti $(x, y) \in E$ vengono mandati in punti $(\sigma(x), \sigma(y)) \in \sigma E$. Dal momento che ogni $\phi \in \mathrm{End}(\sigma E)$ è una funzione razionale, essa può essere espressa nella forma

$$\phi(u, v) = \left(\frac{p_1(u, v)}{q_1(u, v)}, \frac{p_2(u, v)}{q_2(u, v)}\right) \quad \text{dove} \quad p_1, p_2, q_1, q_2 \in \mathbb{C}[u, v]$$

dunque otteniamo che

$$\phi\left(\sigma(x), \sigma(y)\right) = \left(\frac{p_1(\sigma(x), \sigma(y))}{q_1(\sigma(x), \sigma(y))}, \frac{p_2(\sigma(x), \sigma(y))}{q_2(\sigma(x), \sigma(y))}\right)$$

ma per ogni polinomio $f(x,y) = \sum_{i,j} c_{i,j} x^i y^j \in \mathbb{C}[x,y]$ vale che

$$f(\sigma x, \sigma y) = \sum_{i,j} c_{i,j} \sigma(x)^i \sigma(y)^j = \sum_{i,j} \sigma(\sigma^{-1}(c_{i,j}) x^i y^j) = \sigma((\sigma^{-1} f)(x,y))$$

Pertanto $\phi(\sigma(x), \sigma(y)) = \sigma((\sigma^{-1}\phi)(x,y))$, da cui $(\sigma^{-1}\phi)(x,y) \in E$. Da questo segue che $\sigma^{-1}\phi(E) \subset E$, quindi per mostrare che $\sigma^{-1}\phi \in \mathrm{End}(E)$ ci resta da vedere che è un omomorfismo. Per ottenere la relazione cercata basta considerare la seguente catena di uguaglianze:

$$\begin{aligned}
(\sigma^{-1}\phi)((x,y)+(x',y')) &= \sigma^{-1}(\phi(\sigma((x,y)+\sigma(x',y')))) = \\
&= \sigma^{-1}(\phi((\sigma(x),\sigma(y))+(\sigma(x'),\sigma(y')))) = \\
&= \sigma^{-1}(\phi(\sigma(x),\sigma(y))+\phi(\sigma(x'),\sigma(y'))) \overset{*}{=} \\
&\overset{*}{=} \sigma^{-1}(\phi(\sigma(x),\sigma(y))) + \sigma^{-1}(\phi(\sigma(x'),\sigma(y'))) = \\
&= (\sigma^{-1}\phi)(x,y) + (\sigma^{-1}\phi)(x',y')
\end{aligned}$$

dove l'uguaglianza (*) è dovuta al fatto che la legge di gruppo della curva è data da funzioni razionali a coefficienti razionali e pertanto commuta con $\sigma$. Abbiamo quindi mostrato l'inclusione $\mathrm{End}(\sigma E) \subseteq \sigma\,\mathrm{End}(E)$, tuttavia ripercorrendo il ragionamento appena concluso in senso opposto è facile vedere che vale anche l'altra inclusione, ottenendo l'uguaglianza desiderata.
A questo punto ci basta mostrare che $\mathrm{End}(E) \cong \sigma\,\mathrm{End}(E)$. Per farlo è sufficiente mostrare che $\sigma$ è un omomorfismo con le operazioni di anello di $\mathrm{End}(E)$ e che è iniettivo. Se $\phi, \psi \in \mathrm{End}(E)$ allora $\forall (x,y) \in E$

$$\begin{aligned}
\sigma(\phi \circ \psi)(x,y) &= \sigma(\phi(\psi(\sigma^{-1}(x), \sigma^{-1}(y)))) = \\
&= \sigma\phi(\sigma(\psi(\sigma^{-1}(x), \sigma^{-1}(y)))) = \\
&= \sigma\phi(\sigma\psi(x,y))
\end{aligned}$$

Ovvero $\sigma(\phi \circ \psi) = \sigma\phi \circ \sigma\psi$. Inoltre

$$\begin{aligned}
\sigma(\phi+\psi)(x,y) &= \sigma((\phi+\psi)(\sigma^{-1}(x), \sigma^{-1}(y))) = \\
&= \sigma(\phi(\sigma^{-1}(x), \sigma^{-1}(y)) + \psi(\sigma^{-1}(x), \sigma^{-1}(y))) \overset{*}{=} \\
&\overset{*}{=} \sigma(\phi(\sigma^{-1}(x), \sigma^{-1}(y))) + \sigma(\psi(\sigma^{-1}(x), \sigma^{-1}(y))) = \\
&= \sigma\phi(x,y) + \sigma\psi(x,y)
\end{aligned}$$

dove l'uguaglianza (*) è vera poiché la legge di gruppo della curva è data da funzioni razionali a coefficienti razionali. Dall'ultima uguaglianza otteniamo che $\sigma(\phi+\psi) = \sigma\phi + \sigma\psi$, quindi effettivamente $\sigma$ è un omomorfismo. L'iniettività deriva dal fatto che se $\sigma\phi = \sigma\psi$ allora $\phi = \sigma^{-1}\sigma\phi = \sigma^{-1}\sigma\psi = \psi$. □

**Corollario 2.2.3.** *Sia $\sigma \in \mathrm{Aut}(\mathbb{C})$, allora $E \in \mathcal{ELL}(R) \implies \sigma E \in \mathcal{ELL}(R)$*

*Dimostrazione.* $\mathrm{End}(\sigma E) \cong \mathrm{End}(E) \cong R$. □

*Osservazione* 2.2.4. Se $E \in \mathcal{ELL}(\mathcal{O}_K)$ allora $\sigma E$ rappresenterà un numero finito di curve a meno di isomorfismo al variare di $\sigma \in \mathrm{Aut}(\mathbb{C})$, questo perché $\mathcal{ELL}(\mathcal{O}_K)$ è un insieme finito.

**Teorema 2.2.5.** *Sia $E \in \mathcal{ELL}(\mathcal{O}_K)$, allora $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$, dove $h_K = |Cl(K)|$ è il numero di classe di $K$.*

*Dimostrazione.* Sappiamo che per ogni curva $E: \ y^2 = x^3 + ax + b$ vale che $\sigma E: \ y^2 = x^3 + \sigma(a)x + \sigma(b)$, dunque

$$j(\sigma E) = 1728\frac{\sigma(a)^3}{4\sigma(a)^3 + 27\sigma(b)^2} = \sigma\left(1728\frac{a^3}{4a^3 + 27b^2}\right) = \sigma(j(E))$$

Per l'osservazione 2.2.4 sappiamo che al variare di $\sigma \in \mathrm{Aut}(\mathbb{C})$ otteniamo un numero finito di curve $\sigma E$ a meno di isomorfismo, tuttavia $j$ è invariante per isomorfismo, pertanto al variare di $\sigma \in \mathrm{Aut}(\mathbb{C})$, $j(\sigma E) = \sigma(j(E))$ può assumere solo un numero finito di valori, in particolare ne assume al più $h_K = |\mathcal{ELL}(\mathcal{O}_K)|$. Siano $j_1, ..., j_r$, con $r \leq h_K$, i possibili valori di $j(\sigma E)$ al variare di $\sigma \in \mathrm{Aut}(\mathbb{C})$, consideriamo il polinomio $p(x) = \prod_{i=1}^{r}(x - j_i)$, allora notiamo che

$$\sigma(p(x)) = \sigma(\prod_{i=1}^{r}(x - j_i)) = \prod_{i=1}^{r}(x - \sigma(j_i)) = \prod_{i=1}^{r}(x - j_i) = p(x)$$

infatti sicuramente per quanto detto $\sigma(j_i) \in \{j_1, ..., j_r\}$, inoltre $i \neq l \implies \sigma(j_i) \neq \sigma(j_l)$, altrimenti avrei che

$$\sigma(j_i) = \sigma(j_l) \ \Rightarrow \ j_i = \sigma^{-1}\sigma(j_i) = \sigma^{-1}\sigma(j_l) = j_l$$

il che è assurdo. Dunque se $p(x)$ è fissato da ogni $\sigma \in \mathrm{Aut}(\mathbb{C})$ significa che $p(x) \in \mathbb{Q}[x]$, inoltre $p(j(E)) = 0$, da cui vediamo che $j(E)$ è algebrico. A questo punto segue facilmente la stima sul grado di $j(E)$ osservando che

$$[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq \deg(p(x)) \leq h_K$$

□

**Corollario 2.2.6.** *Se $\mathcal{O}_K$ è UFD e $E \in \mathcal{ELL}(\mathcal{O}_K)$, allora $j(E) \in \mathbb{Q}$.*

CAPITOLO 3

# Integralità dell'invariante $j$

In questo capitolo faremo uso della teoria della curva di Tate per arrivare a dimostrare l'integralità dell'invariante $j$ delle curve di $\mathcal{ELL}(\mathcal{O}_K)$. Nei contenuti elencati in seguito saranno talvolta omesse alcune dimostrazioni che possono essere rintracciate nei capitoli I e V del libro di Silverman [Sil94].
Prima di iniziare c'è però bisogno di raffinare il teorema 1.2.17 nel modo che segue

**Teorema 3.0.1.** *Sia $K$ un campo di caratteristica diversa da 2 e da 3, sia $c \in \bar{K}$, allora esiste una curva ellittica $E$ definita su $K(c)$ tale che $j(E) = c$.*

*Dimostrazione.* Se $c = 0$ allora mi basta considerare la curva $y^2 = x^3 + 1$.
Se $c = 1728$ allora mi basta considerare la curva $y^2 = x^3 + x$.
Se invece $c \neq 0, 1728$, posso definire $\gamma = \frac{4}{27}\left(\frac{1728}{c} - 1\right) \in K$ e vale che $\gamma \neq 0$.
Dunque $c = \frac{1728}{1+\frac{27}{4}\gamma}$, in particolare appare chiaro che $K(c) = K(\gamma)$, pertanto mi basta trovare una curva $E$ definita su $K(\gamma)$ tale che $j(E) = c$. Se consideriamo la curva $E: \ y^2 = x^3 + \frac{1}{\gamma}x + \frac{1}{\gamma}$ è facile vedere che essa è definita su $K(\gamma)$, inoltre

$$j(E) = 1728\frac{4\frac{1}{\gamma^3}}{4\frac{1}{\gamma^3} + 27\frac{1}{\gamma^2}} = \frac{1728}{1 + \frac{27}{4}\gamma} = c$$

□

Nel precedente capitolo abbiamo mostrato che una curva ellittica complessa con anello degli endomorfismi isomorfo ad un certo anello degli interi $\mathcal{O}_K$ a fattorizzazione unica ha invariante $j$ razionale, pertanto il teorema appena visto ci garantisce che, a meno di isomorfismo su $\mathbb{C}$, possiamo assumere che tale curva sia definita da un'equazione a coefficienti razionali.

## 3.1 Espansione in $q$

Dato $\Lambda$ un reticolo complesso, sappiamo che a meno di omotetia possiamo considerarlo normalizzato, dunque $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ con $\Im(\tau) > 0$. Abbiamo allora una funzione che associa ad ogni elemento del semipiano complesso superiore un reticolo. Possiamo notare che se scriviamo la funzione $q(z) = e^{2\pi i z}$, allora questa definisce un'isomorfismo $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^*$. Questa stessa funzione manda il sottogruppo discreto $\tau\mathbb{Z} < \mathbb{C}/\mathbb{Z}$ nel sottogruppo discreto $q^{\mathbb{Z}} < \mathbb{C}^*$. Quindi in particolare abbiamo definito un isomorfismo $\mathbb{C}/\Lambda \cong \mathbb{C}^*/q^{\mathbb{Z}}$.
Si può notare che considerando $\Lambda$ come una funzione $\Lambda(\tau) = \mathbb{Z} \oplus \tau\mathbb{Z}$ si può vedere la funzione di Weierstrass come una funzione in due variabili $\wp(z, \tau)$. Inoltre, l'idea di considerare la funzione $q = e^{2\pi i z}$ deriva dal fatto che la funzione di Weierstrass è periodica di periodo 1 sia in $z$ che in $\tau$, pertanto vorremmo riscriverla nelle variabili $2\pi i z$ e $2\pi i \tau$ in maniera analoga a quanto si fa per gli sviluppi in serie di Fourier.

**Lemma 3.1.1.** *Siano* $q = e^{2\pi i \tau}, u = e^{2\pi i z}, F(u, q) = \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2}$. *Allora:*

- *$F$ converge assolutamente e uniformemente sui sottospazi compatti di $\mathbb{C} \setminus \mathbb{Z} \oplus \tau\mathbb{Z}$*
- *$F$ è una funzione ellittica per il reticolo $\mathbb{Z} \oplus \tau\mathbb{Z}$, ha poli doppi in $z \in \mathbb{Z} \oplus \tau\mathbb{Z}$ e nessun altro polo.*
- *La serie di Laurent di $F$ intorno a $z = 0$ è del tipo*

$$F(u, q) = \frac{1}{(2\pi i z)^2} - \left( \frac{1}{12} - 2 \sum_{n \geq 1} \frac{q^n}{(1 - q^n)^2} \right) + (\textit{potenze di } z)$$

Omettiamo la dimostrazione di questo lemma in quanto si tratta semplicemente di una lunga serie di conti. Tale dimostrazione può essere rintracciata nel lemma [Sil94, cap. 1, lemma 6.1]. Faremo uso del lemma per dimostrare il teorema che segue:

**Teorema 3.1.2.** *Se* $q = e^{2\pi i \tau}$ *e* $u = e^{2\pi i z}$ *allora:*

- $\frac{1}{(2\pi i)^2} \wp(z, \tau) = \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2} + \frac{1}{12} - 2 \sum_{n \geq 1} \frac{q^n}{(1 - q^n)^2}$
- $\frac{1}{(2\pi i)^3} \wp'(z, \tau) = \sum_{n \in \mathbb{Z}} \frac{q^n u (1 + q^n u)}{(1 - q^n u)^3}$

*Dimostrazione.* Sia $F(u,q)$ come nel lemma 3.1.1, allora consideriamo la funzione

$$\frac{1}{(2\pi i)^2}\wp(z,\tau) - F(u,q) - \frac{1}{12} + 2\sum_{n\geq 1}\frac{q^n}{(1-q^n)^2}$$

per il lemma precedente questa è una funzione ellittica olomorfa in $\mathbb{C}\setminus\mathbb{Z}\oplus\tau\mathbb{Z}$. Sviluppando $\wp(z,\tau)$ e $F(u,q)$ secondo il precedente lemma otteniamo la funzione

$$\frac{1}{(2\pi i)^2}\left(\frac{1}{z^2} + \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)}\left(\frac{1}{(z-m-n\tau)^2} - \frac{1}{(m+n\tau)^2}\right)\right) - \frac{1}{(2\pi i z)^2} +$$
$$+ \text{(potenze di z)} =$$
$$= \frac{1}{(2\pi i)^2}\sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)}\left(\frac{1}{(z-m-n\tau)^2} - \frac{1}{(m+n\tau)^2}\right) + \text{(potenze di z)}$$

Dunque non è difficile notare che tale funzione è biperiodica olomorfa ovunque, pertanto limitata e quindi costante. Ma dal momento che si annulla in zero ne deduciamo che è costantemente nulla, da cui ricaviamo $\wp(z,\tau)$.
Per ricavare $\wp'(z,\tau)$ basta applicare $\frac{d}{dz} = 2\pi i u\frac{d}{du}$ al valore ottenuto per $\wp(z,\tau)$. □

**Proposizione 3.1.3.** *Se $j(\tau)$ è l'invariante associato al reticolo $\mathbb{Z}\oplus\tau\mathbb{Z}$, allora*

$$j(\tau) = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n$$

*dove $c(n)\in\mathbb{Z}$ $\forall n\in\mathbb{N}$.*

Anche di questo fatto omettiamo la dimostrazione, in quanto si tratta di un'altra lunga serie di conti a partire dagli sviluppi in $q$ delle funzioni modulari. Per una referenza si veda la proposizione [Sil94, cap. 1, prop. 7.4].

**Teorema 3.1.4.** *Per $u,q\in\mathbb{C}$ con $|q|<1$ definiamo*

$$s_k(q) = \sum_{n\geq 1}\frac{n^k q^n}{1-q^n}$$
$$a_4(q) = -5s_3(q) \qquad a_6(q) = -\frac{5s_3(q)+7s_5(q)}{12}$$
$$X(u,q) = \sum_{n\in\mathbb{Z}}\frac{q^n u}{(1-q^n)^2} - 2s_1(q)$$
$$Y(u,q) = \sum_{n\in\mathbb{Z}}\frac{(q^n u)^2}{(1-q^n)^3} + s_1(q)$$
$$E_q:\ y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

*Valgono le seguenti:*

1. *$E_q$ è una curva ellittica e abbiamo un isomorfismo olomorfo*

$$\begin{array}{rccl} \phi: & {\mathbb{C}^*}/{q^{\mathbb{Z}}} & \longrightarrow & E_q \\ & u & \longmapsto & \begin{cases} (X(u,q), Y(u,q)) & \text{se } u \notin q^{\mathbb{Z}} \\ O & \text{se } u \in q^{\mathbb{Z}} \end{cases} \end{array}$$

   *dove $O$ è il punto all'infinito*

2. $a_4(q), a_6(q) \in \mathbb{Z}[[q]]$

3. $j(E_q) = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n$, *dove i coefficienti sono gli stessi di 3.1.3*

4. $\forall E/\mathbb{C}\ \exists q \in \mathbb{C}^*$ *con* $|q| < 1$ *tale che* $E \cong E_q$

*Dimostrazione.* 1. Se $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ e $E_\Lambda:\ y^2 = 4x^3 - g_2x - g_3$, l'isomorfismo segue da 3.1.2 con il cambio di coordinate

$$\frac{1}{(2\pi i)^2}x = x' + \frac{1}{12}, \qquad \frac{1}{(2\pi i)^3}y = 2y' + x'$$

che porta all'equazione $y'^2 + x'y' = x'^3 + a_4x' + a_6$ con

$$\begin{aligned} a_4 &= -\frac{1}{4} \cdot \frac{1}{(2\pi i)^4} g_2(\tau) + \frac{1}{48}, \\ a_6 &= -\frac{1}{4} \cdot \frac{1}{(2\pi i)^6} g_3(\tau) - \frac{1}{48} \cdot \frac{1}{(2\pi i)^4} g_2(\tau) + \frac{1}{1728} \end{aligned}$$

2. La dimostrazione di questo fatto segue espandendo i denominatori $1-q^n$ nelle serie $s_k$ e riarrangiando le serie. Da questo appare chiaro che $a_4(q) \in \mathbb{Z}[[q]]$, mentre per quanto riguarda $a_6(q)$ basta notare che

$$a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12} = -\sum_{n\geq 1} \left( \sum_{d|n} \frac{5d^3 + 7d^5}{12} \right) q^n$$

   e $5d^3+7d^5 \equiv 0(12)$ per ogni $d \in \mathbb{Z}$, infatti $5d^3+7d^5 \equiv 2d+d \equiv 0(3)$ e se $d$ è dispari $5d^3+7d^5 \equiv d+3d \equiv 0(4)$, mentre se $d$ è pari $d^2(5d+7d^3) \equiv 0(4)$.

3. La formula nella proposizione 3.1.3 mi dà il valore di $j$ per le funzioni del teorema 3.1.2, ma dal primo punto di questo teorema vediamo che $X(u,q)$ e $Y(u,q)$ sono ottenuti da esse con un cambio lineare di coordinate, quindi $j$ rimane invariato, da cui segue la tesi.

4. Per il corollario 1.2.18 sappiamo che esiste un reticolo $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ normalizzato per cui $E \cong E_\Lambda$, dunque per il punto 1 se $q = e^{2\pi i\tau}$ sappiamo che $E \cong E_q$.

□

## 3.2 La curva di Tate

Fino ad ora abbiamo considerato solamente curve ellittiche definite su $\mathbb{C}$, tuttavia può essere interessante anche considerare curve ellittiche definite su altri campi. Nel capitolo 2 abbiamo dimostrato che una curva ellittica a moltiplicazione complessa ha invariante $j$ algebrico, quindi a meno di isomorfismo (su $\mathbb{C}$) può essere definita su un campo di numeri $\mathbb{Q}(\alpha)$. Possiamo allora studiare questa curva su un'estensione di $\mathbb{Q}(\alpha)$ non contenuta in $\mathbb{C}$, ad esempio, se $\mathfrak{p}$ è un ideale primo di $\mathbb{Q}(\alpha)$, possiamo considerare il completamento $\mathfrak{p}$-adico $K = \mathbb{Q}(\alpha)_{\mathfrak{p}}$. D'ora in avanti parleremo di campi $p$-adici come completamenti di campi di numeri rispetto ad un primo $p$, o, equivalentemente, come estensioni finite di $\mathbb{Q}_p$. In particolare in questa sezione ci occuperemo di studiare curve ellittiche definite su campi $p$-adici.
Come prima osservazione notiamo che l'approccio utilizzato per descrivere le curve ellittiche complesse a partire dai tori fallisce nel caso $p$-adico, infatti se in un campo $p$-adico $K$ esistesse un sottogruppo discreto non nullo, questo conterrebbe un elemento $x \neq 0$, dunque sommando $p^n$ volte $x$ otterrei che $p^n x$ appartiene a tale sottogruppo $\forall n \in \mathbb{N}$. Ma dato che $\lim_{n\to\infty} |p^n x| = 0$, ne deriva che 0 è un punto di accumulazione e quindi il sottogruppo non può essere discreto.
Tuttavia l'espansione in $q$ studiata precedentemente nel caso complesso ci permette, per analogia, di definire una curva ellittica anche nel caso $p$-adico, infatti $K^*$ ammette sottogruppi discreti del tipo $q^{\mathbb{Z}}$, pertanto possiamo identificare i quozienti $K^*/q^{\mathbb{Z}}$ con curve ellittiche opportune.

**Teorema 3.2.1.** *Sia $K$ un campo $p$-adico con valore assoluto $|\cdot|$, sia $q \in K^*$ tale che $|q| < 1$, allora riprendendo le notazioni del teorema 3.1.4 abbiamo:*

1. *$a_4(q), a_6(q)$ convergono in $K$, inoltre la curva $E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$, che chiameremo curva di Tate, ha invariante $j$ descritto dall'equazione 3.1.3.*

2. *Le serie $X(u,q), Y(u,q)$ convergono per ogni $u \in \bar{K} \setminus q^{\mathbb{Z}}$, inoltre definiscono un omomorfismo iniettivo*

$$\begin{array}{rccl} \phi : & \bar{K}^*/q^{\mathbb{Z}} & \longrightarrow & E_q(\bar{K}) \\ & u & \longmapsto & \begin{cases} (X(u,q), Y(u,q)) & \text{se } u \notin q^{\mathbb{Z}} \\ O & \text{se } u \in q^{\mathbb{Z}} \end{cases} \end{array}$$

3. *La mappa $\phi$ del punto precedente è compatibile con l'azione del gruppo di Galois $\mathrm{Gal}\left(\bar{K}/K\right)$, ovvero $\forall \sigma \in \mathrm{Gal}\left(\bar{K}/K\right)$ vale*

$$\sigma \circ \phi(u) = \phi \circ \sigma(u) \qquad \forall u \in \bar{K}^*$$

*Dimostrazione.* 1. Perché $a_4$ e $a_6$ convergano è sufficiente che convergano le $s_k$. Dal momento che $|q| < 1$, vale che $|1 - q^n| = 1$, quindi è sufficiente che converga la serie $\sum_{n\geq 1} |n^k q^n| \leq \sum_{n\geq 1} |q^n|$, che difatti converge. Allo stesso modo anche la serie $j(q) = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n$ converge e dal teorema 3.1.3 otteniamo che è un'identità di serie formali in $\mathbb{Z}[[q]]$, dunque è un'identità per ogni $q$ per cui converge in un campo completo rispetto a una norma, in particolare nel nostro caso è un'identità su $K$.

2. Analogamente al punto 1 non è difficile notare che $X$ e $Y$ convergono $\forall u \in \bar{K} \setminus q^{\mathbb{Z}}$. La buona definizione di $X$ e $Y$ su $\bar{K}^*/q^{\mathbb{Z}}$ appare evidente dal fatto che moltiplicare $u$ per una potenza di $q$ non fa altro che riarrangiare i termini della sommatoria. Inoltre $\forall u \in \bar{K}^*/q^{\mathbb{Z}}$ il punto $(X(u,q), Y(u,q))$ appartiene alla curva $E_q(\bar{K})$, perché il teorema 3.1.4 ci garantisce che nel caso complesso $X$ e $Y$ rispettano l'equazione della curva, dunque questo è vero come serie formali su $\mathbb{Q}(u)[[q]]$, quindi in particolare vale anche su $\bar{K}$. Anche le proprietà di omomorfismo sono ereditate dall'identità di serie formali. Infine per vedere l'iniettività basta notare che il nucleo è composto da tutti i valori di $u$ per cui $\phi(u) = O$ è il punto all'infinito, ovvero tutti quei valori per cui $X$ e $Y$ non convergono, che sono tutti e soli i valori di $q^{\mathbb{Z}}$. Dunque il nucleo è banale in $\bar{K}^*/q^{\mathbb{Z}}$, da cui segue l'iniettività.

3. Gli automorfismi di campo che fissano $K$ non modificano la norma $p$-adica di un elemento, pertanto non è difficile mostrare che gli automorfismi commutano con l'operazione di limite della serie, ovvero che data una serie $\sum_{n\geq 0} x_n$ allora $\sigma \sum_{n\geq 0} x_n = \sum_{n\geq 0} \sigma x_n$. Da questo segue che

$$\begin{aligned}\phi \circ \sigma(u) &= (X(\sigma(u), q), Y(\sigma(u), q)) = \\ &= (X(\sigma(u), \sigma(q)), Y(\sigma(u), \sigma(q))) = \\ &= (\sigma X(u,q), \sigma Y(u,q)) = \\ &= \sigma \circ \phi(u)\end{aligned}$$

□

**Lemma 3.2.2.** *Sia $K$ un campo $p$-adico e $\alpha \in \bar{K}$ tale che $|\alpha| > 1$, allora $\exists! q \in \bar{K}^*$ tale che $|q| < 1$ e $j(E_q) = \alpha$, inoltre $q \in K(\alpha)$.*

*Dimostrazione.* Sappiamo da 3.1.3 che, se $c(-1) = 1$, allora

$$j(q) = j(E_q) = \frac{\sum_{n\geq 0} c(n-1)q^n}{q}$$

Chiamiamo

$$f(q) = \frac{1}{j(q)} = \frac{q}{1 + c(0)q + c(1)q^2 + ...} = q - c(0)q^2 + (c(0)^2 - c(1))q^2 + ... \in \mathbb{Z}[[q]]$$

allora $\exists g(q) \in \mathbb{Z}[[q]]$ tale che $g(f(q)) = q$ come serie formali. Chiaramente vale anche che $f(g(q)) = q$. Dal momento che $g(q) \in \mathbb{Z}[[q]]$ e $|\alpha| > 1$, la serie $g(\frac{1}{\alpha})$ converge in $K(\alpha)$. Se indichiamo con $q$ il valore di tale serie vediamo che

$$q = g\left(\frac{1}{\alpha}\right) \quad \Longrightarrow \quad \frac{1}{j(q)} = f(q) = f\left(g\left(\frac{1}{\alpha}\right)\right) = \frac{1}{\alpha}$$

e pertanto $j(q) = \alpha$.
Ora che abbiamo mostrato l'esistenza di un tale $q$ mostriamone l'unicità. Se esistessero $q, q'$ tali che $|q|, |q'| < 1$ e $j(q) = j(q')$ allora avremmo che $f(q) = f(q')$, da cui

$$\begin{aligned} 0 &= |f(q) - f(q')| = \\ &= |q - q'| \cdot |1 - c(0)(q + q') + (c(0)^2 - c(1))(q^2 + qq' + q'^2) + ...| = \\ &= |q - q'| \end{aligned}$$

e pertanto $q = q'$. □

Ora che abbiamo introdotto la curva di Tate possiamo studiare come applicare le sue proprietà per ricavare l'integralità dell'invariante $j$ delle curve ellittiche a moltiplicazione complessa. Prima di farlo, però, introduciamo il seguente lemma, che in un certo senso raffina il risultato del teorema 1.2.16.

**Lemma 3.2.3.** *Siano $E, E'$ due curve ellittiche definite sul campo $K$ tali che $E \cong E'$ in $\bar{K}$, allora esiste un'estensione $K'/K$ tale che $5 \neq [K' : K] \leq 6$ e $E \cong E'$ su $K'$.*

*Dimostrazione.* Supponiamo che le due curve siano in forma di Weierstrass, infatti è possibile portarle in tale forma tramite cambi lineari di coordinate a coefficienti in $K$, allora siano

$$E : \ y^2 = x^3 + ax + b \qquad \text{e} \qquad E' : \ y^2 = x^3 + cx + d$$

Per il teorema 1.2.16 sappiamo che $j(E) = j(E') = j \in K$, dunque se $j \neq 0, 1728$, dalla formula di $j$ si vede facilmente che $a, b, c, d \neq 0$, pertanto abbiamo che

$$\frac{1728}{1 + \frac{27}{4}\frac{b^2}{a^3}} = \frac{1728}{1 + \frac{27}{4}\frac{d^2}{c^3}} \implies \frac{b^2}{a^3} = \frac{d^2}{c^3} \implies \left(\frac{a}{c}\right)^3 = \left(\frac{b}{d}\right)^2$$

Sia $\gamma = \frac{bc}{ad} \in K$, allora dalla relazione precedente è facile osservare che $\gamma^2 = \frac{a}{c}$ e $\gamma^3 = \frac{b}{d}$. Vediamo allora che la funzione

$$\begin{aligned} x &\longmapsto \gamma x \\ y &\longmapsto \sqrt{\tfrac{b}{d}}y \end{aligned}$$

è un isomorfismo $E \longrightarrow E'$, dove $\sqrt{\frac{b}{d}}$ è una qualunque radice di $\frac{b}{d}$. Infatti

$$\begin{aligned} &\left(\sqrt{\frac{b}{d}}y\right)^2 = (\gamma x)^3 + a\gamma x + b \implies \\ \implies &\frac{b}{d}y^2 = \frac{b}{d}x^3 + \frac{a}{c}\gamma c x + \frac{b}{d}d = \frac{b}{d}(x^3 + cx + d) \implies \\ \implies &y^2 = x^3 + cx + d \end{aligned}$$

Dunque le curve $E, E'$ sono isomorfe su un'estensione quadratica (o banale) $K\left(\sqrt{\frac{b}{d}}\right)$.
Se invece $j = 1728$ notiamo che $b, d = 0$ e $a, c \neq 0$. Dunque consideriamo la funzione

$$\begin{aligned} x &\longmapsto \sqrt{\tfrac{a}{c}}x \\ y &\longmapsto \sqrt{\tfrac{a}{c}}\sqrt[4]{\tfrac{a}{c}}y \end{aligned}$$

Similmente a prima si può mostrare che è un isomorfismo fra $E$ e $E'$, inoltre è definito su $K\left(\sqrt[4]{\frac{a}{c}}\right)$, quindi su un'estensione di grado divisore di 4.
Infine, se $j = 0$ allora $a, c = 0$ e $b, d \neq 0$, dunque la funzione

$$\begin{aligned} x &\longmapsto \sqrt[3]{\tfrac{b}{d}}x \\ y &\longmapsto \sqrt{\tfrac{b}{d}}y \end{aligned}$$

è un isomorfismo fra $E$ e $E'$ definito su $K\left(\sqrt[6]{\frac{b}{d}}\right)$, quindi su un'estensione di grado divisore di 6. □

**Proposizione 3.2.4.** *Sia $K$ un campo $p$-adico con valutazione $v$, $E/K$ una curva ellittica tale che $|j(E)| > 1$, $\ell > 3$ un primo tale che $\ell \nmid v(j(E))$, allora esiste $\sigma \in \mathrm{Gal}(\bar{K}/K)$ che agisce sul gruppo $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ come una matrice del tipo $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, ovvero esistono $P_1, P_2 \in E[\ell]$ tali che*

$$E[\ell] = < P_1, P_2 > \quad e \quad \sigma(P_1) = P_1, \quad \sigma(P_2) = P_1 + P_2$$

*Dimostrazione.* Cominciamo considerando un'estensione di Galois finita $L/K$ tale che $\ell \nmid [L:K]$, allora, se $w$ è la valutazione su $L$ che estende $v$, ne consegue che $w(j(E)) = e_{w/v}v(j(E))$, dove $e_{w/v}|[L:K]$ è l'indice di ramificazione, dunque è coprimo con $\ell$, da cui $\ell \nmid v(j(E)) \iff \ell \nmid w(j(E))$. Quindi $L$ rispetta le ipotesi del teorema, inoltre se dimostrassimo la tesi per $L$ allora la avremmo anche per $K$, in quanto se trovassimo l'automorfismo $\sigma$ della tesi varrebbe $\sigma \in \mathrm{Gal}(\bar{K}/L) \subset \mathrm{Gal}(\bar{K}/K)$.
Per il lemma 3.2.2 $\exists q \in K$ per cui $E \cong E_q$ su $\bar{K}$, quindi in particolare per il lemma 3.2.3 le due curve sono isomorfe su un'estensione finita il cui grado non è mai divisibile per $\ell$, dal momento che $\ell > 3$. Quindi ci basta dimostrare la tesi per $E_q$, in quanto su tale estensione gli automorfismi commutano con l'isomorfismo tra le curve. Sia $\zeta = \zeta_\ell$, allora possiamo assumere che $\zeta \in K$, in quanto altrimenti ci basterebbe considerare l'estensione $K(\zeta)/K$ che ha grado divisore di $\ell - 1$, che è coprimo con $\ell$. Sia allora $Q = q^{\frac{1}{\ell}} \in \bar{K}$ una radice $\ell$-esima di $q$ fissata, dal momento che $v(q) = -v(j(E))$, ne segue che $(\ell, v(q)) = (\ell, v(j(E))) = 1$, dunque $K(Q)/K$ è totalmente ramificata di grado $\ell$ ed essendo un'estensione di Kummer è ciclica di grado $\ell$, pertanto $\exists \sigma \in \mathrm{Gal}(K(Q)/K)$ tale che $\sigma(Q) = \zeta Q$. Vediamo che tale $\sigma$ è l'automorfismo cercato.
È facile notare che $< \zeta, Q > < \frac{\bar{K}^*}{q^{\mathbb{Z}}}$ è un sottogruppo di cardinalità $\ell^2$, inoltre tutti i suoi elementi hanno ordine che divide $\ell$, pertanto l'omomorfismo del teorema 3.2.1 manda elementi di tale sottogruppo in elementi di $\ell$-torsione della curva $E_q$. Tuttavia, sempre dal teorema 3.2.1, sappiamo che tale omomorfismo è iniettivo e dunque per motivi di cardinalità esso è un isomorfismo $\phi : < \zeta, Q > \longrightarrow E[\ell]$. Sappiamo poi che $\phi$ deve commutare con l'automorfismo $\sigma$ scelto precedentemente, pertanto vediamo che se $P_1 = \phi(\zeta)$ e $P_2 = \phi(Q)$ segue che

$$\sigma(P_1) = \phi(\sigma(\zeta)) = \phi(\zeta) = P_1$$
$$\sigma(P_2) = \phi(\sigma(Q)) = \phi(\zeta Q) = \phi(\zeta) + \phi(Q) = P_1 + P_2$$

□

*Osservazione* 3.2.5. Dal momento che $\ell$ è primo, $P_1, P_2$ sono una base di $E[\ell]$ come $\mathbb{F}_\ell$-spazio vettoriale, che è infatti isomorfo a $\mathbb{F}_\ell^2$. Dunque esiste una rappresentazione $\rho_\ell : \mathrm{Gal}(\bar{K}/K) \longmapsto GL_2(\mathbb{F}_\ell)$ che descrive come gli elementi del gruppo di Galois agiscono sui punti di torsione della curva, fissata una base di essi.

**Corollario 3.2.6.** *Sia $K$ un campo di numeri, $E/K$ una curva ellittica per cui $j(E) \notin \mathcal{O}_K$, allora per ogni primo $\ell$, tranne al più un numero finito, esiste un elemento $\sigma \in \mathrm{Gal}(\bar{K}/K)$ per cui $\rho_\ell(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.*

*Dimostrazione.* Sia $p$ un primo di $\mathcal{O}_K$ tale che $v_p(j(E)) < 0$, consideriamo allora il completamento $p$-adico $K_p$, dal momento che $E$ è definita su $K$ è possibile assumere che sia definita su $K_p$ e $|j(E)| > 1$. Fissata un'immersione $\bar{K} \hookrightarrow \bar{K_p}$, ricordiamo che essa determina un'immersione $\mathrm{Gal}(\bar{K_p}/K_p) \subseteq \mathrm{Gal}(\bar{K}/K)$. A questo punto sappiamo che $\exists \sigma \in \mathrm{Gal}(\bar{K_p}/K_p)$ tale che $\rho_\ell(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Ma per quanto osservato prima $\sigma \in \mathrm{Gal}(\bar{K}/K)$, inoltre le coordinate dei punti di $E[\ell]$ stanno in $\bar{K} \subset \bar{K_p}$, da cui segue la tesi. □

**Teorema 3.2.7.** *Sia $K$ un campo di numeri e $E$ una curva definita su $K$, allora se $j(E) \notin \mathcal{O}_K$ vale che* $\mathrm{End}(E) \cong \mathbb{Z}$.

*Dimostrazione.* A meno di considerare un'estensione finita di $K$, sappiamo che $\mathrm{End}_{\mathbb{C}}(E) = \mathrm{End}_K(E)$, infatti $\mathrm{End}_{\mathbb{C}}(E)$ è finitamente generato su $\mathbb{Z}$, dunque è sufficiente cosiderare il campo di definizione dei generatori, che è un'estensione finita grazie al lemma 3.2.3. Dimostrare il teorema per un'estensione finita di $K$ ci garantisce la tesi anche per $K$, dal momento che gli endomorfismi su $K$ sono un sottoinsieme di quelli definiti su una sua qualunque estensione. Sappiamo inoltre che $|j(E)| > 1$, dunque posso scegliere un primo $\ell$ sufficientemente grande che rispetti le ipotesi del corollario 3.2.6, in particolare per lo stesso corollario esiste una base $P_1, P_2$ di $E[\ell]$ e un automorfismo $\sigma \in \mathrm{Gal}(\bar{K}/K)$ per cui $\sigma$ agisce come $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_\ell)$. Dato $\phi \in \mathrm{End}(E)$, se restringiamo $\phi$ a $E[\ell]$ esso è ancora un endomorfismo, pertanto può essere espresso da una matrice $\phi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{F}_\ell)$, ottenendo quindi un omomorfismo

$$\begin{array}{rccc} \Phi_\ell : & \mathrm{End}(E) & \longrightarrow & M_2(\mathbb{F}_\ell) \\ & \phi & \longmapsto & \phi_\ell \end{array}$$

Siccome gli endomorfismi sono definiti sul campo fissato dal gruppo di Galois, $\phi$ e $\sigma$ commutano, perciò

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

da cui

$$\begin{cases} a + c = a \\ b + d = a + b \end{cases} \implies c = 0 \wedge a = d$$

dunque $\phi_\ell = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$.

Supponiamo adesso per assurdo che $\mathbb{Z} \subsetneq \mathrm{End}(E) \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ per un certo

$d \in \mathbb{N}$, ovvero che $\mathrm{End}(E)$ sia un ordine di $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, allora possiamo assumere che $\ell$ si spezzi completamente in $\mathbb{Q}(\sqrt{-d})$, dal momento che in ogni campo di numeri esistono infiniti primi che si spezzano completamente. Possiamo anche assumere che $\ell \nmid [\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} : \mathrm{End}(E)]$, poiché tale indice è un numero finito. A questo punto vediamo che lo $\mathbb{Z}$-modulo $\ell\,\mathrm{End}(E)$ ha immagine nulla tramite $\Phi_\ell$, inoltre se $\phi \in \ker \Phi_\ell$, visto come elemento di $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, deve essere un multiplo di $\ell$, pertanto $\ker \Phi_\ell = \ell\,\mathrm{End}(E)$. Da questo segue che $\Phi_\ell$ diventa iniettiva passando al quoziente per il nucleo:

$$\overline{\Phi}_\ell : \frac{\mathrm{End}(E)}{\ell\,\mathrm{End}(E)} \longrightarrow M_2(\mathbb{F}_\ell)$$

In particolare $\frac{\mathrm{End}(E)}{\ell\,\mathrm{End}(E)} \cong \mathrm{End}(E) \otimes \frac{\mathbb{Z}}{\ell\mathbb{Z}}$, quindi

$$\mathrm{End}(E) \otimes \mathbb{F}_\ell = \mathcal{O}_{\mathbb{Q}(\sqrt{-d})} \otimes \mathbb{F}_\ell = \frac{\mathbb{Z}[x]}{(x^2+d)} \otimes \mathbb{F}_\ell = \frac{\mathbb{F}_\ell[x]}{(x^2+d)} =$$
$$= \frac{\mathbb{F}_\ell[x]}{(x+\sqrt{d})} \times \frac{\mathbb{F}_\ell[x]}{(x-\sqrt{d})} \cong \mathbb{F}_\ell^2$$

dove la prima uguaglianza è data dal fatto che $\ell \nmid [\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} : \mathrm{End}(E)]$, la seconda dal fatto che $\ell \neq 2$, mentre la quarta è data dal teorema cinese del resto notando che $\ell$ si spezza completamente in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ e dunque $x^2 + d$ è riducibile.
A questo punto notiamo che

$$|\,\mathrm{End}(E) \otimes \mathbb{F}_\ell| = |\mathbb{F}_\ell^2| = \ell^2 = \left| \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M_2(\mathbb{F}_\ell) \right\} \right|$$

pertanto l'iniettività di $\overline{\Phi}_\ell$ e l'uguaglianza fra le cardinalità implicano che $\overline{\Phi}_\ell$ è suriettiva sull'insieme $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M_2(\mathbb{F}_\ell) \right\}$, ovvero è un isomorfismo fra esso e $\mathrm{End}(E) \otimes \mathbb{F}_\ell$. Dovrà quindi esistere $\phi \in \mathrm{End}(E) \otimes \mathbb{F}_\ell$ tale che $\phi_\ell = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, ma questo è assurdo perché in $\mathbb{F}_\ell^2$ non ci sono nilpotenti. □

**Corollario 3.2.8.** *Sia $K = \mathbb{Q}(\sqrt{-d})$ tale che $\mathcal{O}_K$ è UFD, sia $E \in \mathcal{ELL}(\mathcal{O}_K)$, allora $j(E) \in \mathbb{Z}$.*

*Dimostrazione.* Dal corollario 2.2.6 sappiamo che $j(E) \in \mathbb{Q}$, inoltre $\mathrm{End}(E) \supsetneq \mathbb{Z}$, dunque per il teorema 3.2.7 $j(E) \in \mathcal{O}_\mathbb{Q} = \mathbb{Z}$. □

CAPITOLO 4

# Dimostrazione della congettura di Gauss

**Proposizione 4.0.1.** *Sia $d \in \mathbb{Z}$ libero da quadrati tale che $d > 2$ e $d \not\equiv 3(4)$, allora se $K = \mathbb{Q}(\sqrt{-d})$ si ha che $\mathcal{O}_K$ non è UFD.*

*Dimostrazione.* Si ha $-d \not\equiv 1(4)$, dunque $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$. Per mostrare che esso non è un UFD mostreremo che 2 è irriducibile ma non è primo. Se avessi un elemento $a+b\sqrt{-d}$ tale che $a+b\sqrt{-d}|2$ passando alle norme otterrei $a^2 + b^2 d|4$. Tuttavia, date le ipotesi, $d \geq 5$, perciò $b = 0$ e $a \in \{\pm 1, \pm 2\}$, ovvero $a + b\sqrt{-d}$ è invertibile o è uguale a 2 a meno di moltiplicazione per un invertibile, dunque 2 è irriducibile.
A questo punto notiamo che se $d$ è pari $2| - d$ ma $2 \nmid \pm\sqrt{-d}$, mentre se $d$ è dispari $2|1 + d$ ma $2 \nmid 1 \pm \sqrt{-d}$, da cui segue che 2 non è primo. □

**Proposizione 4.0.2.** *Sia $d \equiv 3(4)$ tale che $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ sia UFD, allora $\forall p \in \mathbb{Z}$ tale che $p < \frac{d}{4}$, $p$ è inerte in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$.*

*Dimostrazione.* Si ha $-d \equiv 1(4)$, dunque $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$. Supponiamo che $p$ non sia inerte, allora

$$\begin{aligned} p &= \left(a + b\frac{1+\sqrt{-d}}{2}\right)\left(a + b\frac{1-\sqrt{-d}}{2}\right) = \\ &= a^2 + ab + b^2\frac{d+1}{4} = \\ &= a^2 + ab + b^2 + b^2\frac{d-3}{4} \;>\; \frac{d-3}{4} \end{aligned}$$

Dunque se $p < \frac{d}{4}$ allora è inerte. □

**Definizione 4.0.3.** Sia $E$ una curva ellittica razionale, si chiama campo di definizione degli endomorfismi il più piccolo campo $K/\mathbb{Q}$ tale che $\mathrm{End}_K(E) = \mathrm{End}_{\mathbb{C}}(E)$.

**Lemma 4.0.4.** *Sia $E$ una curva ellittica razionale, allora detto $K$ il suo campo di definizione degli endomorfismi vale che $[K : \mathbb{Q}] \leq 2$.*

*Dimostrazione.* Consideriamo una curva ellittica razionale $E$, se $\mathrm{End}(E) \cong \mathbb{Z}$ allora $K = \mathbb{Q}$ e quindi la tesi è banale, altrimenti sappiamo che $\mathrm{End}_{\mathbb{C}}(E) \cong \mathbb{Z}[\omega]$ come anello, dove $\omega$ è un intero algebrico di grado 2 e quindi soddisfa un'equazione del tipo $\omega^2 = a\omega + b$ con $a, b \in \mathbb{Z}$. Sappiamo inoltre che $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ agisce su $\mathrm{End}_{\mathbb{C}}(E)$ agendo sui coefficienti dei suoi elementi, quindi c'è un omomorfismo

$$\Psi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(\mathrm{End}_{\mathbb{C}}(E)) \cong \mathrm{Aut}(\mathbb{Z}[\omega])$$

Vediamo allora come è fatto $\mathrm{Aut}(\mathbb{Z}[\omega])$: sicuramente se $\phi \in \mathrm{Aut}(\mathbb{Z}[\omega])$ allora $\phi(1) = 1$, inoltre $\phi(\omega^2 - a\omega - b) = \phi(0) = 0$, pertanto $\phi(\omega)^2 - \phi(a)\phi(\omega) - \phi(b) = \phi(\omega)^2 - a\phi(\omega) - b = 0$. Da questo segue che $\phi(\omega)$ può assumere solo due valori, quindi $\mathrm{Aut}(\mathbb{Z}[\omega]) \cong \mathbb{Z}/2\mathbb{Z}$ .
A questo punto, se $K$ è il campo di definizione degli endomorfismi, $\mathrm{Gal}(\bar{\mathbb{Q}}/K) = \ker \Psi$, quindi in particolare $[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) : \mathrm{Gal}(\bar{\mathbb{Q}}/K)] \leq 2$, da cui segue la tesi. □

*Osservazione* 4.0.5. Come abbiamo già osservato esiste un'azione

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[\ell]) \cong GL_2(\mathbb{F}_\ell)$$

quindi per restrizione c'è anche un'azione

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/K) \longrightarrow GL_2(\mathbb{F}_\ell)$$

e siccome $[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) : \mathrm{Gal}(\bar{\mathbb{Q}}/K)] = 2$ otteniamo che

$$[\rho_\ell\left(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\right) : \rho_\ell\left(\mathrm{Gal}(\bar{\mathbb{Q}}/K)\right)] \leq 2$$

Dato il campo quadratico immaginario $\mathbb{Q}(\sqrt{-d})$, sia $2 \neq \ell \in \mathbb{Z}$ un primo inerte in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, allora

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} \otimes \mathbb{F}_\ell = \frac{\mathbb{Z}[x]}{(x^2 + d)} \otimes \mathbb{F}_\ell = \frac{\mathbb{F}_\ell[x]}{(x^2 + d)} \cong \mathbb{F}_{\ell^2}$$

Se abbiamo dunque una curva ellittica $E \in \mathcal{ELL}(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})})$ sappiamo che gli endomorfismi agiscono sui punti di $\ell$-torsione, dunque in particolare $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} \otimes \mathbb{F}_\ell \cong \mathbb{F}_{\ell^2}$ agisce fedelmente su $E[\ell]$. Da questo, per cardinalità, segue che $E[\ell]$

è un $\mathbb{F}_{\ell^2}$-spazio vettoriale di dimensione 1, dove gli endomorfismi rappresentano gli scalari. Ne deduciamo quindi che se $K$ è il campo di definizione degli endomorfismi, allora $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ commuta con gli endomorfismi, poiché essi sono funzioni razionali e $\sigma$ ne fissa i coefficienti, dunque $\sigma$ è un endomorfismo lineare di $E[\ell]$ come $\mathbb{F}_{\ell^2}$-spazio vettoriale.

**Proposizione 4.0.6.** *Sia $E \in \mathcal{ELL}(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})})$ una curva ellittica razionale, $2 \neq \ell \in \mathbb{N}$ un primo inerte in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, allora esiste una base di $E[\ell]$ per cui*

$$\rho_\ell\left(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\right) \subseteq N_{GL_2(\mathbb{F}_\ell)}\left(\left\{\begin{pmatrix} a & -db \\ b & a \end{pmatrix} \in GL_2(\mathbb{F}_\ell)\right\}\right)$$

*Dimostrazione.* Sia $0 \neq v \in E[\ell]$, allora $v, \sqrt{-d}\cdot v$ sono sono una base di $E[\ell]$ come $\mathbb{F}_\ell$ spazio vettoriale, dove $\sqrt{-d}$ è un elemento di $\mathrm{End}(E) \cong \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$. Infatti dati $a, b \in \mathbb{F}_\ell$ vale che

$$\begin{aligned} & av + b\sqrt{-d}b = 0 \iff \\ \iff & (a + b\sqrt{-d})v = 0 \iff \\ \iff & a + b\sqrt{-d} = 0 \text{ in } \mathrm{End}(E) \otimes \mathbb{F}_\ell \iff \\ \iff & a, b = 0 \end{aligned}$$

Come fatto nel teorema 3.2.7 possiamo rappresentare $\mathrm{End}(E) \otimes \mathbb{F}_\ell$ in $M_2(\mathbb{F}_\ell)$ guardando la restrizione degli endomorfismi ai punti di $\ell$-torsione. Data la scelta di base fatta, vediamo che, dato un endomorfismo $a+b\sqrt{-d} \in \mathrm{End}(E)\otimes \mathbb{F}_\ell$,

$$\begin{cases} (a + b\sqrt{-d})v = av + b(\sqrt{-d}v) \\ (a + b\sqrt{-d})(\sqrt{-d}v) = -dbv + a(\sqrt{-d}v) \end{cases} \implies (a + b\sqrt{-d}) \mapsto \begin{pmatrix} a & -db \\ b & a \end{pmatrix}$$

Inoltre sappiamo che, dal momento che $\ell$ è inerte in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, vale l'isomorfismo $\mathrm{End}(E) \otimes \mathbb{F}_\ell \cong \mathbb{F}_{\ell^2}$. Chiamiamo allora

$$C := \left\{\begin{pmatrix} a & -db \\ b & a \end{pmatrix} \in GL_2(\mathbb{F}_\ell)\right\} = \left\{\begin{pmatrix} a & -db \\ b & a \end{pmatrix} \in M_2(\mathbb{F}_\ell) \middle| (a, b) \neq (0, 0)\right\}$$

è chiaro che $C \cong (\mathrm{End}(E) \otimes \mathbb{F}_\ell)^* \cong \mathbb{F}_{\ell^2}^*$ e quindi è ciclico.
A questo punto, come osservato in precedenza, gli elementi di $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ commutano con gli endomorfismi, pertanto

$$H := \rho_\ell(\mathrm{Gal}(\bar{\mathbb{Q}}/K)) \subseteq Z_{GL_2(\mathbb{F}_\ell)}(C) \subseteq N_{GL_2(\mathbb{F}_\ell)}(C)$$

Se $\rho_\ell(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) = H$ allora la precedente inclusione ci dà la tesi; ci resta quindi da considerare il caso in cui $[\rho_\ell(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) : H] = 2$. Cominciamo dimostrando che

$$N := N_{GL_2(\mathbb{F}_\ell)}\left(\left\{\begin{pmatrix} a & -db \\ b & a \end{pmatrix}\right\}\right) = \left\{\begin{pmatrix} a & -db \\ b & a \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} a & db \\ b & -a \end{pmatrix}\right\}$$

Sia $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{F}_\ell)$ tale che $\forall \begin{pmatrix} a & -db \\ b & a \end{pmatrix} \in C \quad \exists \begin{pmatrix} a' & -db' \\ b' & a' \end{pmatrix} \in C$ per cui valga l'equazione

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} a & -db \\ b & a \end{pmatrix} = \begin{pmatrix} a' & -db' \\ b' & a' \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{4.1}$$

dal momento che la traccia è invariante per coniugio, dall'equazione 4.1 otteniamo che

$$Tr\begin{pmatrix} a & -db \\ b & a \end{pmatrix} = Tr\begin{pmatrix} a' & -db' \\ b' & a' \end{pmatrix} \implies 2a = 2a' \implies a = a'$$

Dalla stessa equazione, prendendo i determinanti otteniamo che

$$a^2 + db^2 = a + db'^2 \implies b = \pm b'$$

Se scegliamo delle matrici per cui $b \neq 0$ possiamo sviluppare i conti dell'equazione 4.1 nel modo seguente:

$$\begin{cases} a\alpha + b\beta = a\alpha \mp db\gamma \\ -db\alpha + a\beta = a\beta \mp db\delta \\ a\gamma + b\delta = \pm b\alpha + a\gamma \\ -db\gamma + a\delta = \pm b\beta + a\delta \end{cases} \implies \begin{cases} \alpha = \pm\delta \\ \beta = \mp d\gamma \end{cases}$$

Abbiamo quindi ottenuto che

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & -d\gamma \\ \gamma & \alpha \end{pmatrix} \quad \vee \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & d\gamma \\ \gamma & -\delta \end{pmatrix}$$

da cui segue immediatamente l'uguaglianza cercata.
A questo punto non è difficile notare che se nell'equazione 4.1 le due matrici di $C$ coincidono, ovvero se $(a, b) = (a', b')$, ripercorrendo gli stessi conti otteniamo che $\alpha = \delta$ e $\beta = -d\gamma$. Questo ci dice che $Z_{GL_2(\mathbb{F}_\ell)}(C) \subseteq C$, inoltre sappiamo che $C$ è un gruppo ciclico, pertanto $Z_{GL_2(\mathbb{F}_\ell)}(C) = C$.
Questo ci dice che $H \subseteq C$. Se chiamo $H' = \rho_\ell\left(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\right)$, sappiamo che

$[H' : H] = 2$, dunque in particolare $H \lhd H'$, da cui $H' \subseteq N_{GL_2(\mathbb{F}_\ell)}(H)$. Se dimostriamo che $N_{GL_2(\mathbb{F}_\ell)}(H) \subseteq N$ allora segue la tesi.
Supponiamo che $H < C$ contenga un elemento che non è multiplo dell'identità, allora esso è una matrice nella forma $\begin{pmatrix} a & -db \\ b & a \end{pmatrix}$, con $b \neq 0$. Se $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in N_{GL_2(\mathbb{F}_\ell)}(H)$ allora essa deve rispettare l'equazione 4.1 per gli $a, b$ appena scelti e per certi $a', b'$, ma dal momento che $b \neq 0$ possiamo ripetere il ragionamento percorso precedentemente e ottenere che $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in N$, dunque in particolare $N_{GL_2(\mathbb{F}_\ell)}(H) \subseteq N$.
Se invece tutti gli elementi di $H$ sono multipli dell'identità allora $H$ è formato da multipli dell'identità per ogni scelta di base di $E[\ell]$, poiché il coniugio in $GL_2(\mathbb{F}_\ell)$ fissa i suoi elementi. Dato $h \in H' \setminus H$, sappiamo che il quoziente $H'/H$ è ciclico di ordine 2, pertanto $H' =< h, H >$; ci basta dunque trovare una base in cui $h \in N$, da cui segue che $H' =< h, H > < N$. Dal momento che $[H' : H] = 2$, $h$ è tale che $h^2 = \lambda I$ per un certo $\lambda \in \mathbb{F}_\ell^*$, dunque il suo polinomio minimo divide $x^2 - \lambda$, in particolare i suoi autovalori apparterranno all'insieme $\{\pm\sqrt{\lambda}\}$. Distinguiamo allora due casi:

- $\lambda$ **è un quadrato in** $\mathbb{F}_\ell$**:** in questo caso abbiamo diverse possibilità: o $h$ è simile alla matrice $\pm\sqrt{\lambda}I$ oppure è simile a $\begin{pmatrix} \sqrt{\lambda} & 0 \\ 0 & -\sqrt{\lambda} \end{pmatrix}$, infatti non può essere simile ad un blocco di Jordan dal momento che il suo polinomio minimo ha radici di molteplicità 1. Tali matrici appartengono a $N$, dunque $h$, nella base in cui è diagonale, appartiene a $N$, da cui segue la tesi.

- $\lambda$ **non è un quadrato in** $\mathbb{F}_\ell$**:** in questo caso, siccome $h$ non è un multiplo dell'identità, sappiamo che esiste $v \in E[\ell]$ per cui $v, hv$ sono una base di $E[\ell]$. In tale base $h(v) = (hv)$ e $h(hv) = \lambda v$, dunque $h$ sarà la matrice $\begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}$. Dal momento che $\ell$ è inerte in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ sappiamo che $-d$ non è un quadrato modulo $\ell$, allora $\exists \mu \in \mathbb{F}_\ell$ tale che $\mu^2 = \frac{\lambda}{-d}$. Dunque se coniughiamo la matrice $\begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}$ per la matrice $\begin{pmatrix} \mu^{-1} & 0 \\ 0 & 1 \end{pmatrix}$ otteniamo

$$\begin{pmatrix} \mu^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \mu^{-1}\lambda \\ \mu & 0 \end{pmatrix} = \begin{pmatrix} 0 & -\mu d \\ \mu & 0 \end{pmatrix} \in C$$

  Pertanto abbiamo trovato una base in cui $h \in N$, da cui la tesi.

□

A questo punto, cercheremo di mettere insieme i risultati ottenuti per trovare gli anelli degli interi di campi quadratici immaginari a fattorizzazione unica.
Quando Gauss elaborò la sua congettura calcolò il numero di classe di tutti i primi campi quadratici immaginari, trovando che per $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ l'anello $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ è a fattorizzazione unica. In particolare verificò che per $d \leq 163$ essi sono gli unici campi a numero di classe 1. Per dimostrare che essi sono gli unici campi in assoluto con questa proprietà possiamo quindi assumere che $d > 163$. Chiamiamo come al solito $K = \mathbb{Q}(\sqrt{-d})$, supponiamo che $\mathcal{O}_K$ sia UFD, allora per la proposizione 4.0.1 sappiamo che $d \equiv 3(4)$, dunque per la proposizione 4.0.2 ogni primo $p < \frac{d}{4}$ è inerte in $K$, in particolare tutti i primi minori di 41 sono inerti in $K$.
Introduciamo adesso il seguente teorema che sarà necessario per dimostrare la congettura.

**Teorema 4.0.7.** *Sia $\ell \in \mathbb{N}$ un numero primo, allora esiste una curva $Y_{ns}^{+}(\ell)$ definita su $\mathbb{Q}$ per cui esiste una corrispondenza*

$$Y_{ns}^{+}(\ell)(\mathbb{Q}) \longleftrightarrow \left\{ j(E) \middle| \, E/\mathbb{Q} \, , \; \rho_{E,\ell}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) \subseteq N_{GL_2(\mathbb{F}_\ell)}(C) \right\}$$

*dove tale inclusione vale in una base opportuna di $E[\ell]$ e dove, fissato $\epsilon \in \mathbb{F}_\ell^* \setminus \mathbb{F}_\ell^{*2}$,*

$$C = \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \in GL_2(\mathbb{F}_\ell) \right\}$$

Ometteremo la dimostrazione di questo teorema, che risulta lunga e complicata. Una referenza può essere trovata nel libro di Deligne e Rapoport [DR73] o nelle note di Siksek [Sik]. Proveremo a spiegare a grandi linee come può essere trovata la curva $Y_{ns}^{+}(\ell)$. Il gruppo indicato fino a questo momento con $C$ è detto sottogruppo di Cartan non-split; generalmente esso viene indicato come $C_{ns}(\ell)$, mentre il suo normalizzatore viene indicato con $C_{ns}^{+}(\ell)$. Sia $X(\ell)$ la curva modulare compattificata che classifica le classi di isomorfismo di curve ellittiche con struttura di livello $\ell$ completa. Possiamo definire le curve

$$X_{ns}(\ell) := X(\ell)/C_{ns}(\ell) \qquad \text{e} \qquad X_{ns}^{+}(\ell) := X(\ell)/C_{ns}^{+}(\ell)$$

che vengono dette curve modulari associate a $C_{ns}(\ell)$ e a $C_{ns}^{+}(\ell)$ rispettivamente. Indichiamo allora con $Y_{ns}(\ell)$ e $Y_{ns}^{+}(\ell)$ i rispettivi luoghi non cuspidali aperti. Per valori piccoli di $\ell$, in particolare per $\ell \leq 7$ (valore che ci interesserà per completare la dimostrazione della congettura), la curva $X_{ns}^{+}(\ell)$ è razionale, ovvero isomorfa a $\mathbb{P}^1\mathbb{Q}$. Fissando un isomorfismo $\mathbb{P}^1\mathbb{Q} \longrightarrow X_{ns}^{+}(\ell)$ possiamo parametrizzare i punti di $Y_{ns}^{+}(\ell)(\mathbb{Q})$ con $u \in \mathbb{Q}$, fatta eccezione per un numero

finito di valori, corrispondenti alle cuspidi di $X_{ns}^+(\ell)$.
Per definizione esiste un morfismo $j$ tale che

$$j : X_{ns}^+(\ell) \longrightarrow \frac{X(\ell)}{GL_2(\mathbb{F}_\ell)} \cong X(1) \cong \mathbb{P}^1$$

e per $P \in X_{ns}^+(\ell)(\mathbb{Q})$, che per il teorema 4.0.7 sappiamo rappresentare una certa curva ellittica $E$, vale $j(P) = j(E)$.
A questo punto sappiamo che ogni primo $\ell < 41$ è inerte in $K$, dunque per la proposizione 4.0.6, data una curva $E \in \mathcal{ELL}(\mathcal{O}_K)$, l'immagine di $\rho_\ell$ è contenuta in $C_{ns}^+(\ell)$, pertanto $E$ corrisponde, grazie al teorema 4.0.7, ad un punto $P_3$ di $X_{ns}^+(3)(\mathbb{Q})$ e ad un punto $P_7$ di $X_{ns}^+(7)(\mathbb{Q})$. A loro volta, questi punti corrispondono a numeri razionali $u_3$ e $u_7$. Dal momento che le equazioni per $X_{ns}^+(3)(\mathbb{Q})$ e $X_{ns}^+(7)(\mathbb{Q})$ sono note, otteniamo

$$j(E) = j_3(u_3) = u_3^3 \tag{4.2}$$

$$j(E) = j_7(u_7) = 64\frac{(u_7(u_7^2+7)(u_7^2-7u_7+14)(5u_7^2-14u_7-7))^3}{(u_7^3-7u_7^2+7u_7+7)^7} \tag{4.3}$$

Queste equazioni possono essere ritrovate nell'articolo di Baran [Bar10]. D'ora in poi scriveremo $u = u_7$.
Dal momento che $\mathcal{O}_K$ è UFD, dal corollario 3.2.8 sappiamo che $j(E) \in \mathbb{Z}$. In particolare, dall'equazione 4.3, otteniamo che

$$j(E) = j_7(u) = 64\frac{(u(u^2+7)(u^2-7u+14)(5u^2-14u-7))^3}{(u^3-7u^2+7u+7)^7} \in \mathbb{Z}$$

Se risolviamo questa equazione possiamo restringere l'insieme di possibili curve ellittiche il cui anello degli endomorfismi ha fattorizzazione unica. Innanzi tutto, dal momento che l'equazione è definita su $\mathbb{P}^1\mathbb{Q}$, vediamo che valutando $j_7$ nel punto all'infinito otteniamo $j_7(\infty) = 2^6 \cdot 5^3 = 8000$, dunque $\infty$ è una soluzione dell'equazione e pertanto produce un posssibile valore di $j$. Escluso questo caso possiamo quindi risolvere l'equazione su $\mathbb{Q}$. Chiamiamo

$$f(u) = u(u^2+7)(u^2-7u+14)(5u^2-14u-7) \quad \text{e} \quad g(u) = u^3-7u^2+7u+7$$

allora, poiché $f(u), g(u) \in \mathbb{Z}[u]$, sappiamo che esistono due polinomi $a(u), b(u) \in \mathbb{Z}[u]$ per cui

$$f(u)a(u) + g(u)b(u) = r$$

dove $r \in \mathbb{Z}$ è il risultante di $f$ e $g$. Non è difficile notare che $\deg(af) = \deg(bg) = n$, dunque, scrivendo $u = \frac{X}{Y}$ con $X, Y \in \mathbb{Z}$ coprimi, possiamo omogeneizzare i polinomi $f$ e $g$ nel modo seguente

$$F(X,Y) = f\left(\frac{X}{Y}\right) \cdot Y^7 \qquad \text{e} \qquad G(X,Y) = g\left(\frac{X}{Y}\right) \cdot Y^3$$

e sostituendo nell'equazione otteniamo

$$F(X,Y)A(X,Y) + G(X,Y)B(X,Y) = rY^n$$

Fissati dunque due interi coprimi $X$ e $Y$, appare chiaro che

$$(G(X,Y), F(X,Y))|rY^n$$

inoltre $G(X,Y) = X^3 - 7X^2Y + 7XY^2 + 7Y^3$, pertanto per divisione euclidea otteniamo che $(G(X,Y),Y) = (X^3,Y) = 1$, quindi in particolare $(G(X,Y),Y^n) = 1$, da cui segue che

$$(G(X,Y), F(X,Y))|r$$

A questo punto sappiamo che

$$64\frac{f(X/Y)^3}{g(X/Y)^7} = 64\frac{F(X,Y)^3}{G(X,Y)^7} \in \mathbb{Z}$$

dunque se $p \in \mathbb{Z}$ è un primo tale che $p|G(X,Y)$, necessariamente $p|2F(X,Y)$, quindi per quanto appena osservato $p|2r$.
Si può calcolare che il risultante è $r = -26985857024 = -2^{15} \cdot 7^7$, quindi $p = 2 \vee p = 7$. Vediamo che $7^2 \nmid G(X,Y)$, infatti

$$G(X,Y) \equiv 0(7) \iff X^3 - 7X^2Y + 7XY^2 + 7Y^3 \equiv 0(7) \iff X = 7Z$$

e sostituendo si ottiene

$$G(7Z,Y) = 7(7^2Z^2 - 7^2Z^2Y + 7ZY^2 + Y^3) \equiv 7(49)$$

dal momento che $7 \nmid Y$, in quanto $(X,Y) = 1$.
Sia allora $k = v_2(G(X,Y))$, supponiamo che $k > 15$, allora, siccome $j$ è intero,

$$v_2(64F(X,Y)^3) = 6 + 3v_2(F(X,Y)) \geq 7k$$

Tuttavia $(F(X,Y), G(X,Y))|2^{15} \cdot 7^7$, pertanto $v_2(F(X,Y)) \leq 15$, poiché $k > 15$. Mettendo insieme le disuguaglianze troviamo che

$$7k \leq 6 + 3v_2(F(X,Y)) \leq 6 + 3 \cdot 15 = 51$$

che non è mai rispettata, dal momento che $k > 15$. Questo ci dice che $v_2(G(X,Y)) \leq 15$. In particolare sappiamo che deve valere

$$X^3 - 7X^2Y + 7XY^2 + 7Y^3 = 2^a \cdot 7^b \qquad \text{con } 0 \leq a \leq 15\ ,\ 0 \leq b \leq 1$$

Tuttavia, dall'equazione 4.2 sappiamo che $j$ deve essere un cubo, ma questo è vero se e solo se $G(X,Y)$ è un cubo; quindi $a \equiv 0(3)$ e $b \equiv 0(3)$. Arrivamo pertanto ad ottenere solamente 6 equazioni:

$$X^3 - 7X^2Y + 7XY^2 + 7Y^3 = 2^{3a} \qquad \text{con } 0 \leq a \leq 5$$

Queste sono equazioni di Thue, che quindi hanno un numero finito di soluzioni; esse possono essere stimate e quindi calcolate. Risolvendo le equazioni per $X$ e $Y$ coprimi e $Y \neq 0$ si trovano le soluzioni

$$(2,1),\ (11,2),\ (-19,-9),\ (-5,-1),\ (-3,-1),\ (-3,5),\ (1,-1),\ (1,1)$$

Queste corrispondono ai seguenti invarianti $j$:

| Soluzione | $j$ | Fattori di $j$ |
|---|---|---|
| $(-3,5)$ | $-262537412640768000$ | $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ |
| $(2,1)$ | $-147197952000$ | $-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$ |
| $(-5,-1)$ | $-884736000$ | $-2^{18} \cdot 3^3 \cdot 5^3$ |
| $(1,1)$ | $-32768$ | $-2^{15}$ |
| $(-3,-1)$ | $1728$ | $2^6 \cdot 3^3$ |
| $(1,-1)$ | $287496$ | $2^3 \cdot 3^3 \cdot 11^3$ |
| $(11,2)$ | $6673554058125250 5802048$ | $2^6 \cdot 11^3 \cdot 23^3 \cdot 149^3 \cdot 269^3$ |
| $(-19,-9)$ | $6838755720062350457411072$ | $2^9 \cdot 17^6 \cdot 19^3 \cdot 29^3 \cdot 149^3$ |

Ognuno di essi individua in maniera unica una classe di isomorfismo di curve ellittiche e ognuna di esse ha un certo anello degli endomorfismi. Sappiamo che se $K = \mathbb{Q}(\sqrt{-d})$, per $d > 163$, e $\mathcal{O}_K$ è UFD, la curva $E \cong \mathbb{C}/\mathcal{O}_K$ deve essere tale che $j(E)$ appartiene alla lista appena prodotta. Quindi ci basta verificare se tali $j$, compreso il valore ottenuto nel punto all'infinito, producano curve ellittiche non CM oppure se i campi quadratici in cui si immergono i loro anelli di endomorfismi abbiano numero di classe 1 o meno. Tali $j$ elencati potrebbero anche restituire valori di $d$ minori o uguali a 163, in tal caso li possiamo ignorare, in quanto sono già stati verificati in precedenza.
La tabella successiva elenca i valori di $d$ per cui le curve associate a $j$, a meno di isomorfismo, hanno come anello degli endomorfismi un ordine in $\mathbb{Q}(\sqrt{-d})$:

| $j$ | Fattori di $j$ | $d$ |
|---|---|---|
| $-262537412640768000$ | $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ | 163 |
| $-147197952000$ | $-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$ | 67 |
| $-884736000$ | $-2^{18} \cdot 3^3 \cdot 5^3$ | 43 |
| $-32768$ | $-2^{15}$ | 11 |
| $1728$ | $2^6 \cdot 3^3$ | 1 |
| $8000$ | $2^6 \cdot 5^3$ | 2 |
| $287496$ | $2^3 \cdot 3^3 \cdot 11^3$ | 1 |
| $6673554058125250 5802048$ | $2^6 \cdot 11^3 \cdot 23^3 \cdot 149^3 \cdot 269^3$ | non CM |
| $6838755720062350457411072$ | $2^9 \cdot 17^6 \cdot 19^3 \cdot 29^3 \cdot 149^3$ | non CM |

Lo studio della curva modulare $X_{ns}^{+}(7)$ e la ricerca dei suoi punti interi per risolvere il problema del numero di classe 1 sono stati affrontati da Kenku [Ken85], che in fondo al suo articolo riporta una tabella di valori di $j$ che comprende quelli qui sopra riportati. Tali valori compaiono anche nell'articolo di Baran [Bar10, tabella 5.4], dove sono riportati tutti e soli i valori che abbiamo appena ottenuto.
Si noti che le soluzioni dell'equazione ci hanno portato ad ottenere alcuni valori di $d$ che già avevamo escluso, in quanto verificati da Gauss. Questo perché difatti l'unica ipotesi derivante dall'aver assunto che $d > 163$ consiste nel fatto che i primi $\ell < 41$ siano inerti in $\mathbb{Q}(\sqrt{-d})$, nel nostro caso specifico, che 3 e 7 siano inerti in $\mathbb{Q}(\sqrt{-d})$. È quindi logico che nella nostra tabella compaiano i valori $d = 43, 67, 163$, in quanto in questi casi $3, 7 < \frac{d}{4}$, dunque per la proposizione 4.0.2 essi sono inerti. Inoltre, è noto che i primi congrui a 3 modulo 4 sono inerti in $\mathbb{Q}(i)$, pertanto anche il valore $d = 1$ era logico che apparisse. Per $d = 11$ sappiamo che $-11 \equiv 3(7)$ che non è un quadrato, pertanto $x^2 + 11$ è irriducibile in $\mathbb{F}_7$, dunque 7 è inerte in $\mathbb{Q}(\sqrt{-11})$; tuttavia $11 \equiv 1(3)$ è un quadrato, ovvero 3 non è inerte. Per $\ell = 3$, però, il normalizzatore di un sottogruppo di Cartan split è contenuto nel normalizzatore di un sottogruppo di Cartan non-split, questo giustifica il fatto che 11 compaia nella nostra tabella. Un risultato in tal proposito può essere ritrovato nel libro di Serre [Ser89, appendice A, A.6]. Un discorso analogo vale per il caso $d = 2$. I valori trovati da Gauss che invece non sono comparsi sono $d = 3, 7, 19$, infatti 3 e 7 sono ramificati rispettivamente in $\mathbb{Q}(\sqrt{-3})$ e in $\mathbb{Q}(\sqrt{-7})$, mentre $-19 \equiv 2(7)$, dunque 7 non è inerte in $\mathbb{Q}(\sqrt{-19})$.
Questo completa la dimostrazione della congettura.

# Bibliografia


[Bak67] Alan Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[Bar10] Burcu Baran. Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem. *J. Number Theory*, 130(12):2753–2772, 2010.

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. 1973. Lecture Notes in Math., Vol. 349.

[Gau86] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[Hee52] Kurt Heegner. Diophantische Analysis und Modulfunktionen. *Math. Z.*, 56:227–253, 1952.

[Ken85] Monsuru A. Kenku. A note on the integral points of a modular curve of level 7. *Mathematika*, 32(1):45–48, 1985.

[Ser89] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

[Sik] Samir Siksek. Explicit arithmetic of modular curves. `https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/modcurves/lecturenotes.pdf`.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sta67] Harold M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.