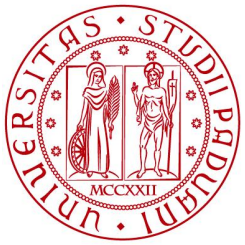


UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

Curve Modulari come Spazi di Moduli di Curve Ellittiche

Relatore:
Prof. Matteo Longo

Laureando: Orazio Giulio Cherubini
Matricola: 2033988

Anno Accademico 2023/2024

20/09/2024

Indice

Introduzione

La teoria delle forma modulari è uno strumento potente che connette diverse aree della matematica, a partire dall'analisi di Fourier fino ad arrivare alla teoria dei numeri. Lo studio delle curve modulari è strettamente connesso allo studio delle forme modulari in quanto queste ultime possono essere considerate come funzioni o forme differenziali sulle prime. Questa interpretazione impone delle condizioni sulle forme modulari che portano a una grande varietà di identità di particolare interesse. Se ne dà un breve esempio:

Esempio. A ciascuna forma modulare è associato un peso k che ha significato di grado nella corrispondenza tra forme modulari e 1-forme su curve modulari. Si indicano perciò $\mathcal{M}_k(\Gamma)$ gli spazi vettoriali di forme modulari di peso k relative al sottogruppo di congruenza Γ (si veda il Paragrafo 1.2). Si ha che $G_4^2, G_8 \in \mathcal{M}_8(SL_2(\mathbb{Z}))$, dove G_k è la serie di Eisenstein di peso k (si veda il Paragrafo 4.2). Avendo che $\mathcal{M}_8(SL_2(\mathbb{Z}))$ è in relazione con le 1-forme di grado 8 su $X(SL_2(\mathbb{Z}))$, di cui è noto il genere (si veda il Paragrafo 3.3), si ottiene che $\mathcal{M}_8(SL_2(\mathbb{Z}))$ ha dimensione 1 come spazio vettoriale su $\mathbb{C}$ grazie al teorema di Riemann-Roch. Allora si ottiene che $G_4^2 = G_8$ a meno di costanti moltiplicative. L'interesse in questa relazione è che l'espansione di Fourier di G_k ha la forma

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n,\ q = e^{2\pi i\tau}\ ,$$

dove ζ è la ζ di Riemann e $\sigma_k(n) = \sum_{m|n} m^k$. Allora dalla relazione $G_4^2 = G_8$ si ottiene

$$\sigma_7(n) = \sigma_3(n) + 120\sum_{i=1}^{n-1}\sigma_3(i)\sigma_3(n-i)\ .$$

Questo tipo di relazioni si rivelano spesso utili studiando funzioni generatrici che risultano forme modulari, come, per fare un altro esempio, nel problema dei quattro quadrati. Nel contesto delle curve modulari è impossibile non citare il Teorema di Modularità, che ha importanti conseguenze in teoria dei numeri come il conteggio di soluzioni modulo p di equazioni della forma $y^2 = 4x^3 - g_2x - g_3$ o, notoriamente, l'Ultimo Teorema di Fermat. Se ne dà una formulazione contenente la curva modulare compatta $X_0(N)$.

Teorema 1 (di Modularità)**.** *Sia E una curva ellittica con $j(E) \in \mathbb{Q}$. Allora esiste un intero positivo N e una funzione olomorfa $X_0(N) \to E$.*

L'obbiettivo di questa tesi è fornire un quadro generale della teoria delle curve modulari. Si parte dalla loro costruzione insiemistica, per poi dotarle di struttura topologica

e infine considerarle quali superficie di Riemann. La tesi si conclude con lo studio dei problemi di moduli di curve ellittiche con struttura di N-livello, determinando quali tra le curve modulari $Y_0(N), Y_1(N), Y(N)$ sono spazi di moduli fini di curve ellittiche.

Il Capitolo 1 dà le prime definizioni e proprietà delle azioni delle trasformazioni di Möbius sul semipiano complesso. Prosegue poi presentando i sottogruppi di congruenza, delineandone alcune proprietà algebriche e arrivando alla definizione di curva modulare. In seguito si discutono le proprietà topologiche delle curve modulari, ottenendone anche una rappresentazione attraverso i domini fondamentali. Per i Paragrafi 1.1 e 1.2 sono stati seguiti principalmente F. Diamond, J. Shurman, *A First Course in Modular Forms* [4] e K. Conrad, $SL_2(\mathbb{Z})$ [3]. Nei Paragrafi 1.3 e 1.4 sono stati seguiti perlopiù T. Miyake, *Modular Forms* [10] e N. Koblitz, *Introduction to Elliptic Curves and Modular Forms* [7].

Nel Capitolo 2 si dotano le curve modulari di una struttura di superficie di Riemann. Si introducono prima i punti ellittici per i sottogruppi di congruenza, attraverso considerazioni algebriche, per concludere costruendo un atlante per ciascuna curva modulare. In questo capitolo sono stati seguiti principalmente [4] e [10].

Lo scopo del Capitolo 3 è presentare un completamento delle curve modulari a delle superficie di Riemann compatte. Questo viene fatto attraverso l'aggiunta di cuspidi allo spazio precedentemente costruito, che saranno definite all'inizio del capitolo. Si procede poi dotando lo spazio ottenuto delle strutture necessarie. Si conclude il capitolo calcolando il genere delle superficie di Riemann compatte ottenute, il quale è fondamentale nel contesto della teoria delle forme modulari.

Il Capitolo 4 ha lo scopo di stabilire una corrispondenza tra le curve ellittiche su $\mathbb{C}$ e i tori complessi. Questa corrispondenza permetterà, nel Capitolo5, di usare i tori complessi per determinare gli spazi di moduli di curve ellittiche cercati. In questo capitolo si è fatto riferimento a [4], a J. H. Silverman, *The Arithmetic of Elliptic Curves* [11] e a R. Miranda, *Algebraic Curves and Riemann Surfaces* [9].

Il capitolo 5 inizia con la definizione dei problemi e gli spazi di moduli, con particolare attenzione ai problemi di moduli di strutture di N-livello. Procede presentando dei risultati sugli spazi di moduli di curve ellittiche prive di struttura di livello e con "framings". Infine stabilisce quali tra le curve modulari $Y_0(N), Y_1(N), Y(N)$ sono spazi di moduli fini di curve ellittiche. In particolare si otterranno i seguenti risultati:

Teorema 7: Per ogni intero positivo N, la curva modulare $Y_0(N)$ è lo spazio di moduli grezzo per le curve ellittiche con $\Gamma_0(N)$-struttura.

Teorema 11: Se $N > 3$, la curva modulare $Y_1(N)$ è lo spazio di moduli fine per le curve ellittiche con $\Gamma_1(N)$-struttura.

Teorema 10: Se $N > 2$, la curva modulare $Y(N)$ è lo spazio di moduli fine per le curve ellittiche con $\Gamma(N)$-struttura.

Per questo capitolo sono stati utilizzati in particolare i seguenti riferimenti bibliografici: D. Arapura, *Abelian Varieties and Moduli* [1]; B. Conrad, *Modular Curves* [2]; R. Hain, *Lectures on Moduli Spaces of Elliptic Curves* [5]; N. M. Katz, B. Mazur, *Arithmetic Moduli of Elliptic Curves* [6]; J. H. Silverman, *The Arithmetic of Elliptic Curves* [11].

Capitolo 1

Sottogruppi di congruenza e azioni sul semipiano complesso

In questo capitolo vengono introdotti i primi risultati per trattare le curve modulari e le curve ellittiche. In particolare si definiscono i sottogruppi di congruenza e si osservano alcune loro proprietà algebriche. Si studia inoltre l'azione dei sottogruppi di congruenza sul semipiano complesso deducendo alcune proprietà topologiche del quoziente rispetto a questa azione.

1.1 Azione di $SL_2(\mathbb{Z})$ su $\mathbb{H}$

In questo paragrafo vengono definite e studiate le azioni di alcuni gruppi, quali $GL_2(\mathbb{C})$, $SL_2(\mathbb{R})$ e $SL_2(\mathbb{Z})$, sul semipiano complesso.

Notazione. Si introducono alcune notazioni standard:

1. $\mathbb{H} = \{ z \in \mathbb{C} \mid Im(z) > 0 \}$ detto il *semipiano complesso*.
2. $\hat{K} = K \cup \{\infty\}$ con $K = \mathbb{C}, \mathbb{R}$ o $\mathbb{Q}$.
3. $M_2(R)$ l'anello delle matrici 2×2 su un anello R.
4. $GL_2(R) = \{ \gamma \in M_2(R) \mid \det \gamma \in U(R) \}$.
5. $SL_2(R) = \{ \gamma \in M_2(R) \mid \det \gamma = 1 \}$.

Il gruppo $GL_2(\mathbb{C})$ agisce transitivamente su $\hat{\mathbb{C}}$ tramite la legge

$$GL_2(\mathbb{C}) \times \hat{\mathbb{C}} \to \hat{\mathbb{C}}, \ \left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z \right) \mapsto \frac{az+b}{cz+d}$$

con le convenzioni $\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \infty \right) \mapsto \frac{a}{c}$ e $\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \frac{-d}{c} \right) \mapsto \infty$ se $c \neq 0$, altrimenti $\infty \mapsto \infty$.

Osservazione. Si osserva che tale azione non è fedele dato che l'automorfismo indotto da $\gamma \in GL_2(\mathbb{C})$ coincide con quello indotto da $-\gamma$. Per questo motivo in alcuni testi si sceglie di considerare il quoziente del gruppo $GL_2(\mathbb{C})$ per il sottogruppo $\{ \pm \mathbb{1} \}$ ottenendo il gruppo speciale lineare $PSL_2(\mathbb{C})$. Si segue invece l'approccio di [4] che rende più naturali alcuni argomenti successivi senza incontrare problemi causati dalla non fedeltà dell'azione.

Anche il gruppo $SL_2(\mathbb{R})$ agisce su $\hat{\mathbb{C}}$ come sottogruppo di $GL_2(\mathbb{C})$. L'azione di $SL_2(\mathbb{R})$ non è fedele per la stessa ragione osservata in precedenza ma a differenza di quella di $GL_2(\mathbb{C})$ non è transitiva. Infatti, la seguente proposizione implica la non transitività dell'azione oltre ad essere utile successivamente.

Proposizione 1.1. *L'azione di $SL_2(\mathbb{R})$ su $\hat{\mathbb{C}}$ preserva gli insiemi $\hat{\mathbb{R}}, \mathbb{H}, -\mathbb{H} \subseteq \hat{\mathbb{C}}$.*

Dimostrazione. Si dimostra prima l'invarianza di $\hat{\mathbb{R}}$. Sia $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{R})$. Se si ha $c = 0$, si ottiene che l'automorfismo indotto da γ è $\infty \mapsto \infty,\ x \mapsto \frac{ax+b}{d} \in \mathbb{R}, \forall x \in \mathbb{R}$. Se invece $c \neq 0$, si ottiene che l'automorfismo indotto da γ è dato da $\infty \mapsto a/c,\ -d/c \mapsto \infty$ e $x \mapsto \frac{ax+b}{cx+d} \in \mathbb{R}, \forall x \in \mathbb{R} \setminus \{ -d/c \}$. In ogni caso ogni elemento di $\hat{\mathbb{R}}$ è mappato su un elemento di $\hat{\mathbb{R}}$ dimostrando l'asserto.

Si dimostra ora l'invarianza di $\mathbb{H}$ per l'azione di $SL_2(\mathbb{R})$. L'invarianza di $-\mathbb{H}$ segue con un procedimento analogo. Sia $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{R})$ e sia $\tau \in \mathbb{H}$. In primo luogo si osserva che sia nel caso in cui $c = 0$, per cui $\infty \mapsto \infty$, che nel caso $c \neq 0$, per cui $\mathbb{R} \ni -d/c \mapsto \infty$, si ha $\tau \nmapsto \infty$ da cui $\gamma\tau \in \mathbb{C}$. É allora possibile calcolare la parte immaginaria di $\gamma\tau$

$$Im(\gamma\tau) = \frac{\gamma\tau - \overline{\gamma\tau}}{2} = \frac{\frac{a\tau+b}{c\tau+d} - \frac{a\overline{\tau}+b}{c\overline{\tau}+d}}{2} = \frac{(ad-bc)\tau - (ad-bc)\overline{\tau}}{2|c\tau+d|^2} = \frac{Im(\tau)}{|c\tau+d|^2} > 0\ .$$

Si deduce quindi che $\gamma\tau \in \mathbb{H}$ come si voleva dimostrare. □

La Proposizione 1.1 permette di considerare la restrizione dell'azione di $SL_2(\mathbb{R})$ su $\hat{\mathbb{C}}$ agli insiemi $\hat{\mathbb{R}}$ e $\mathbb{H}$ ottenendo così un'azione su ciascuno dei due. È utile per i paragrafi successivi osservare che l'azione di $SL_2(\mathbb{R})$ su $\hat{\mathbb{R}}$ e $\mathbb{H}$ è transitiva. Per $\hat{\mathbb{R}}$ il fatto è chiaro perchè ogni elemento può essere mappato a ∞ da un'opportuna trasformazione: $\infty \mapsto \infty$ tramite $\mathbb{1}$, $0 \mapsto \infty$ tramite $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ e per ogni altro $x \in \mathbb{R},\ x \mapsto \infty$ tramite $\left(\begin{smallmatrix} -1/x & 0 \\ 1 & -x \end{smallmatrix}\right)$. Per $\mathbb{H}$ invece si dimostra la seguente proposizione.

Proposizione 1.2. *L'azione di $SL_2(\mathbb{R})$ su $\mathbb{H}$ è transitiva.*

Dimostrazione. È sufficiente mostrare che $\forall \tau \in \mathbb{H}$ esiste un $\gamma \in SL_2(\mathbb{R})$ tale che $\gamma i = \tau$ per dedurre che l'azione è transitiva. Sia $\tau \in \mathbb{H}$ e si osservi che scelta

$$\widetilde{\gamma} = \begin{pmatrix} Im(\tau) & \mathrm{Re}(\tau) \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$$

vale $\widetilde{\gamma} i = \tau$. Ora avendo che $\det \widetilde{\gamma} = Im(\tau) > 0$, è ben definita $\gamma = \frac{1}{\sqrt{Im(\tau)}} \widetilde{\gamma} \in SL_2(\mathbb{R})$ e si ha che $\gamma i = \tau$ concludendo la dimostrazione. □

Questo fatto sarà usato nel Paragrafo 1.3 per dimostrare che l'azione del gruppo modulare su $\mathbb{H}$ è propriamente discontinua da cui si otterrà che lo spazio topologico $Y(\Gamma)$ è di Hausdorff.

Definizione. Il *gruppo modulare* è $SL_2(\mathbb{Z}) = \{ \gamma \in M_2(\mathbb{Z}) \mid \det \gamma = 1 \}$.

Il gruppo $SL_2(\mathbb{Z})$ è un sottogruppo di $SL_2(\mathbb{R})$ e in quanto tale agisce ench'esso sul semipiano complesso superiore e su $\hat{\mathbb{R}}$. L'azione di $SL_2(\mathbb{Z})$ non è transitiva su $\mathbb{H}$ e $\hat{\mathbb{R}}$. Con metodi simili a quelli già usati si ottiene che $\hat{\mathbb{Q}}$ è invariante per $SL_2(\mathbb{Z})$, quindi è possibile considerarne l'azione ristretta a tale insieme che risulta inoltre transitiva.

Proposizione 1.3. *L'azione di $SL_2(\mathbb{Z})$ su $\hat{\mathbb{C}}$ preserva $\mathbb{H}$ e $\hat{\mathbb{Q}}$, inoltre l'azione si $SL_2(\mathbb{Z})$ ristretta a $\hat{\mathbb{Q}}$ è transitiva.*

Dimostrazione. Risulta chiaro che $\mathbb{H}$ e $\hat{\mathbb{R}}$ siano invarianti per $SL_2(\mathbb{Z})$ dato che $SL_2(\mathbb{Z})$ è sottogruppo di $SL_2(\mathbb{R})$.

Per $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ vale $\gamma\infty = \infty \in \hat{\mathbb{Q}}$ se $c = 0$ e altrimenti risulta $\gamma\infty = a/c \in \mathbb{Q}$. Sia ora $\frac{n}{m} \in \mathbb{Q}$ con $n, m \in \mathbb{Z}$. Data $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ allora $(a\frac{n}{m}+b), (c\frac{n}{m}+d) \in \mathbb{Q}$. Ora se $c\frac{n}{m} + d \neq 0$ si ottiene $\gamma\frac{n}{m} \in \mathbb{Q}$, altrimenti si ha $\frac{n}{m} = \frac{-d}{c}$ e $\gamma\frac{n}{m} = \infty \in \mathbb{Q}$. Complessivamente è stata dimostrata l'invarianza di $\hat{\mathbb{Q}}$.

Analogamente a prima, si dimostra che per ogni $x \in \hat{\mathbb{Q}}$ esiste $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ tale che $\gamma\infty = x$, dimostrando in questo modo la transitività. Chiaramente $\mathbb{1}\infty = \infty$. Sia ora $\frac{n}{m} \in \mathbb{Q}$ con $n, m \in \mathbb{Z}$ coprimi. Allora, usando l'Algoritmo di Euclide Esteso, esistono $b, d \in \mathbb{Z}$ tali che $nd - mb = 1$ da cui $\gamma = \left(\begin{smallmatrix} n & b \\ m & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ con $\gamma\infty = \frac{n}{m}$. □

1.2 Sottogruppi di congruenza

In questo paragrafo si definiscono i sottogruppi di congruenza e si delineano alcune loro proprietà algebriche.

Sia λ_N l'applicazione

$$\lambda_N \colon SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z}), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$$

dove $\overline{x}$ indica la classe di equivalenza di x in $\mathbb{Z}/N\mathbb{Z}$. La mappa è definita dato che se $ad - bc = 1$ allora $ad - bc \equiv 1 \mod N$.

Proposizione 1.4. *L'applicazione λ_N è un omomorfismo di gruppi suriettivo.*

Dimostrazione. Si dimostra prima la suriettività. Sia $\bar{\gamma} = \left(\begin{smallmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{smallmatrix}\right) \in SL_2(\mathbb{Z}/N\mathbb{Z})$ di cui sicuramente esiste un sollevamento $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$. Si deve avere che $MCD(ad, cb, N) = 1$, altrimenti la condizione $ad - cb \equiv 1 \mod N$ sarebbe impossibile. Avendo di conseguenza che $MCD(a, b, N) = 1$ è possibile trovare $a' \in \bar{a},\ b' \in \bar{b}$ tali che $MCD(a', b') = 1$. Infatti uno tra a e b è diverso da 0 e si considera, a meno di scambi, $a \neq 0$. In tal caso di deve avere una soluzione $t \in \mathbb{Z}$ al sistema di congruenze

$$\begin{cases} t \equiv_p 1 & \text{se } p \mid MCD(a, b) \\ t \equiv_p 0 & \text{se } p \nmid MCD(a, b) \text{ e } a \mid c\,. \end{cases}$$

Un siffatto t è tale che $MCD(a, b+tN) = 1$. Si sostituiscano a e b con a' e b' per semplicità di notazione. Si ricorda che $ad - bc \equiv 1 \mod N$, che equivale a $ad - bc + kN = 1$ per

qualche $k \in \mathbb{Z}$. Avendo ora $MCD(a,b) = 1$, usando l'Algoritmo di Euclide Esteso, si ottiene che esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta b = 1$ da cui si deriva

$$1 = ad - bc + kN = ad - bc + kN\alpha a + kN\beta b = a(d + \alpha kN) - b(c - \beta kN) \ .$$

Sostituendo c con $c - \beta kN \in \bar{c}$ e d con $d + \alpha kN \in \bar{d}$ si è dimostrato che esiste almeno una $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ tale che $\lambda_N(\gamma) = \bar{\gamma}$.

Rimane da dimostrare che λ_N rispetta il prodotto. Si fissino due elementi di $SL_2(\mathbb{Z})$

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ \delta = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \ .$$

Si ha che

$$\begin{aligned} \lambda_N(\gamma\delta) = \lambda_N \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} &= \begin{pmatrix} \overline{ae + bg} & \overline{af + bh} \\ \overline{ce + dg} & \overline{cf + dh} \end{pmatrix} = \\ &= \begin{pmatrix} \overline{ae} + \overline{b}\overline{g} & \overline{a}\overline{f} + \overline{bh} \\ \overline{ce} + \overline{d}\overline{g} & \overline{c}\overline{f} + \overline{dh} \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \begin{pmatrix} \overline{e} & \overline{f} \\ \overline{g} & \overline{h} \end{pmatrix} = \\ &= \lambda_N(\gamma)\lambda_N(\delta) \end{aligned}$$

concludendo la dimostrazione. □

Definizione. Il *sottogruppo di congruenza principale* di livello $N \geqslant 1$ è

$$\Gamma(N) = \ker \lambda_N \ .$$

Definizione. Un *sottogruppo di congruenza* di livello $N \geqslant 1$ è Γ con $\Gamma(N) \leqslant \Gamma \leqslant SL_2(\mathbb{Z})$.

Notazione. Si introducono delle notazioni per i seguenti sottogruppi di congruenza di livello $N \geqslant 1$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \mod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, c \equiv 0, a \equiv 1 \mod N \right\} \ .$$

Vengono osservate alcune proprietà dei sottogruppi di congruenza sopra considerati.

Osservazione. Si ha che $\Gamma_0(1) = \Gamma_1(1) = \Gamma(1) = SL_2(\mathbb{Z})$ dato che ogni intero è congruente modulo 1.

Osservazione. Se si ha $N|M$ allora $\Gamma_0(M) \leqslant \Gamma_0(N)$, $\Gamma_1(M) \leqslant \Gamma_1(N)$ e $\Gamma(M) \leqslant \Gamma(N)$ dato che le congruenze modulo M sono rispettate anche modulo N.

Osservazione. Si ha che $\Gamma(N) \leqslant \Gamma_1(N) \leqslant \Gamma_0(N)$.

Si vuole ora mostrare che per ogni $N \geqslant 1$ il gruppo modulare è di indice finito sul sottogruppo di congruenza principale di livello N. Questo implica che $SL_2(\mathbb{Z})$ è di indice finito su ogni sottogruppo di congruenza. Per mostrare la finitezza dell'indice viene data preliminarmente la Proposizione 1.5.

Proposizione 1.5. *La cardinalità di $SL_2(\mathbb{Z}/N\mathbb{Z})$ è*

$$|SL_2(\mathbb{Z}/N\mathbb{Z})| = N^3 \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{p^2}\right) .$$

Dimostrazione. Per il Teorema Cinese del Resto si ha $\mathbb{Z}/N\mathbb{Z} \simeq \prod_{\substack{p^\alpha||N \\ p \text{ primo}}} \mathbb{Z}/p^\alpha\mathbb{Z}$ da cui si ottiene che

$$SL_2(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{\substack{p^\alpha||N \\ p \text{ primo}}} SL_2(\mathbb{Z}/p^\alpha\mathbb{Z}) .$$

Allora la cardinalità cercata è

$$|SL_2(\mathbb{Z}/N\mathbb{Z})| = \prod_{\substack{p^\alpha||N \\ p \text{ primo}}} |SL_2(\mathbb{Z}/p^\alpha\mathbb{Z})|$$

per cui la dimostrazione si riduce a provare l'uguaglianza

$$|SL_2(\mathbb{Z}/p^\alpha\mathbb{Z})| = p^{3\alpha}\left(1 - \frac{1}{p^2}\right) \quad \text{per } p \text{ primo.}$$

Si supponga inizialmente che $\alpha = 1$ in modo da avere il campo $\mathbb{Z}/p\mathbb{Z}$. Si osserva che $SL_2(\mathbb{Z}/p\mathbb{Z})$ è il nucleo dell'omomorfismo suriettivo $\det\colon GL_2(\mathbb{Z}/p\mathbb{Z}) \to \left(\mathbb{Z}/p\mathbb{Z}\right)^*$ per cui

$$|SL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|GL_2(\mathbb{Z}/p\mathbb{Z})|}{p-1} .$$

Osservando che $|GL_2(\mathbb{Z}/p\mathbb{Z})|$ è il numero di basi ordinate per $(\mathbb{Z}/p\mathbb{Z})^2$, per le quali si hanno $p^2 - 1$ scelte per il primo vettore e $p^2 - p$ scelte per il secondo, si ottiene che

$$|SL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|GL_2(\mathbb{Z}/p\mathbb{Z})|}{p-1} = \frac{(p^2-1)(p^2-p)}{p-1} = p^3\left(1 - \frac{1}{p^2}\right)$$

dimostrando così il caso $\alpha = 1$.

Posto $\alpha > 1$ sia $\lambda\colon SL_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \to SL_2(\mathbb{Z}/p\mathbb{Z})$ la mappa indotta dall'omomorfismo suriettivo da $\mathbb{Z}/p^\alpha\mathbb{Z}$ su $\mathbb{Z}/p\mathbb{Z}$, in modo simile a come è stata definita λ_N. Si osserva che $\ker\lambda = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \;\middle|\; a, d \equiv 1,\ b, c \equiv 0 \mod p \right\}$. Per determinare un elemento di $\ker\lambda$ si possono scegliere liberamente $p^{\alpha-1}$ possibili $a \in \mathbb{Z}/p^\alpha\mathbb{Z}$ tali che $a \equiv 1 \mod p$, $p^{\alpha-1}$ possibili $b \in \mathbb{Z}/p^\alpha\mathbb{Z}$ tali che $b \equiv 0 \mod p$ e $p^{\alpha-1}$ possibili $c \in \mathbb{Z}/p^\alpha\mathbb{Z}$ tali che $c \equiv 0 \mod p$. Dati dei tali a, b, c, esiste un unico $d \in \mathbb{Z}/p^\alpha\mathbb{Z}$ tale che $d \equiv 1 \mod p$ e $ad - bc \equiv 1 \mod p^\alpha$. In questo modo si ottiene che $|\ker\lambda| = p^{3(\alpha-1)}$.

Essendo λ un omomorfismo suriettivo (allo stesso modo di λ_N), dal Primo Teorema di Isomorfismo risulta che

$$|SL_2(\mathbb{Z}/p^\alpha\mathbb{Z})| = |\ker\lambda||SL_2(\mathbb{Z}/p\mathbb{Z})| = p^{3(\alpha-1)}p^3\left(1 - \frac{1}{p^2}\right) = p^{3\alpha}\left(1 - \frac{1}{p^2}\right)$$

dimostrando la proposizione. □

Proposizione 1.6. *L'indice di* $SL_2(\mathbb{Z})$ *su* $\Gamma(N)$ *è*

$$[SL_2(\mathbb{Z})\colon \Gamma(N)] = N^3 \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{p^2}\right).$$

Inoltre l'indice in $SL_2(\mathbb{Z})$ *di ogni sottogruppo di congruenza* Γ *è finito.*

Dimostrazione. Dalla Proposizione 1.4 e dal Primo Teorema di Isomorfismo si ha che

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

per cui l'indice $[SL_2(\mathbb{Z})\colon \Gamma(N)]$ vale $|SL_2(\mathbb{Z}/N\mathbb{Z})|$ che è dato dalla Proposizione 1.5. Considerato ora un generico sottogruppo di congruenza Γ, si deve avere $\Gamma(N) \leqslant \Gamma$ per qualche $N \in \mathbb{N}$. Allora si ha che

$$[SL_2(\mathbb{Z})\colon \Gamma] \mid [SL_2(\mathbb{Z})\colon \Gamma(N)] < \infty\,. \qquad \square$$

Osservazione. La finitezza dell'indice sarà necessaria nel Paragrafo 1.3 per dimostrare che lo spazio quoziente $Y(\Gamma)$ è di Hausdorff per ogni sottogruppo di congruenza Γ. Inoltre verrà usata anche nel Paragrafo 1.4 per ottenere un dominio fondamentale per ogni sottogruppo di congruenza Γ. Infine sarà necessaria nel Capitolo 3 per determinare la finitezza delle cuspidi e di conseguenza una formula per il genere di $X(\Gamma)$

Proposizione 1.7. *Gli indici di* $\Gamma_1(N)$ *e* $\Gamma_0(N)$ *in* $SL_2(\mathbb{Z})$ *valgono*

$$[SL_2(\mathbb{Z})\colon \Gamma_1(N)] = N^2 \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{p^2}\right),$$

$$[SL_2(\mathbb{Z})\colon \Gamma_0(N)] = N \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right).$$

Dimostrazione. Le dimostrazioni delle due uguaglianze sono analoghe.

Dato che λ_N è suriettiva e $\ker \lambda_N = \Gamma(N) \leqslant \Gamma_1(N) \leqslant SL_2(\mathbb{Z})$ si ottiene dal Primo Teorema di Isomorfismo che

$$[SL_2(\mathbb{Z})\colon \Gamma_1(N)] = \frac{[SL_2(\mathbb{Z})\colon \Gamma(N)]}{[\Gamma_1(N)\colon \Gamma(N)]} = \frac{|SL_2(\mathbb{Z}/N\mathbb{Z})|}{|\lambda_N\big(\Gamma_1(N)\big)|}\,.$$

Sfruttando il fatto che

$$\lambda_N\big(\Gamma_1(N)\big) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \,\middle|\, b \in \mathbb{Z}/N\mathbb{Z} \right\}$$

si ricava che $|\lambda_N\big(\Gamma_1(N)\big)| = N$. Da questo, unitamente alla Proposizione 1.5, segue che

$$\begin{aligned}[SL_2(\mathbb{Z})\colon \Gamma_1(N)] &= N^3 \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{p^2}\right) \Big/ N \\ &= N^2 \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{p^2}\right).\end{aligned}$$

Si dimostra ora la seconda uguaglianza. Dato che λ_N è suriettiva e $\Gamma(N) \leqslant \Gamma_0(N)$, si ottiene, usando ancora il Primo Teorema di Isomorfismo, che

$$[SL_2(\mathbb{Z})\colon \Gamma_0(N)] = \frac{[SL_2(\mathbb{Z})\colon \Gamma(N)]}{[\Gamma_0(N)\colon \Gamma(N)]} = \frac{|SL_2(\mathbb{Z}/N\mathbb{Z})|}{|\lambda_N\big(\Gamma_0(N)\big)|}.$$

Sfruttando il fatto che

$$\lambda_N\big(\Gamma_0(N)\big) = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \,\middle|\, a \in \big(\mathbb{Z}/N\mathbb{Z}\big)^*, b \in \mathbb{Z}/N\mathbb{Z} \right\},$$

dove $\big(\mathbb{Z}/N\mathbb{Z}\big)^*$ indica il gruppo degli invertibili di $\mathbb{Z}/N\mathbb{Z}$, si ricava che

$$|\lambda_N\big(\Gamma_0(N)\big)| = N\phi(N) = N^2 \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Da questo, unitamente alla Proposizione 1.5, segue che

$$\begin{aligned}[SL_2(\mathbb{Z})\colon \Gamma_0(N)] &= N^3 \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{p^2}\right) \Big/ N^2 \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right) \\ &= N \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 + \frac{1}{p}\right)\end{aligned}$$

concludendo la dimostrazione. □

Proposizione 1.8. *Gli ordini degli elementi di $SL_2(\mathbb{Z})$ possono essere $1, 2, 3, 4, 6$ o ∞.*

Dimostrazione. Sia data $\gamma \in SL_2(\mathbb{Z})$ tale che $\gamma^n = \mathbb{1}$ per qualche n. Il polinomio caratteristico di γ deve essere $x^2 - tx + 1$ con t la traccia di γ. Dato che $\gamma^n = \mathbb{1}$ gli autovalori di γ devono essere radici n-esime dell'unità, da cui si deduce che $|t| \leqslant 2$. Quindi γ viene annullata dal massimo comun divisore dei polinomi $x^n - 1$ e $x^2 - tx + 1$, per cui si distinguono i seguenti casi in t:

t = 2 - Si ha che $\gamma = \mathbb{1}$, che ha ordine 1.

t = −2 - Si ha che il massimo comun divisore è $x + 1$ se n è pari e 1 se n è dispari. Considerando solo il primo caso, dato che l'altro non è possibile, si ottiene che $\gamma = -\mathbb{1}$, che ha ordine 2.

t = 1 - Dato che $x^2 - x + 1$ è un fattore di $x^3 + 1$ si deve avere che $\gamma^3 = -\mathbb{1}$. Dato che $-\mathbb{1}$ non annulla $x^2 - x + 1$ non si può avere $\gamma = -\mathbb{1}$, da cui γ ha ordine 6.

t = −1 - Dato che $x^2 + x + 1$ è un fattore di $x^3 - 1$ si deve avere che $\gamma^3 = \mathbb{1}$. Dato che $\mathbb{1}$ non annulla $x^2 + x + 1$ non si può avere $\gamma = \mathbb{1}$, da cui γ ha ordine 3.

t = 0 - Si ha $\gamma^2 = -\mathbb{1}$ da cui γ ha ordine 4. □

Le seguenti Proposizioni 1.9 e 1.10 saranno necessarie nel Capitolo 5 per dimostrare l'esistenza di uno spazio di moduli fine per le curve ellittiche con struttura di livello.

Proposizione 1.9. *Il sottogruppo di congruenza $\Gamma(N)$ è privo di torsione per $N > 2$.*

Dimostrazione. Sia fissata $\gamma \in \Gamma(N)$ tale che $\gamma^n = \mathbb{1}$ per qualche n e si denoti con $\varphi(x)$ il polinomio caratteristico di γ. Sono stati già studiati nella dimostrazione della Proposizione 1.8 i possibili valori di $\varphi(x)$. Avendo che $\gamma \equiv \mathbb{1} \mod N$ deve verificarsi che $\varphi(x) \equiv x^2 - 2x + 1 \mod N$. Allora detta t la traccia di γ deve valere $t \equiv 2 \mod N$.

Se N ⩾ 5 l'unica possibilità è $t = 2$ quindi $\gamma = \mathbb{1}$.

Se N = 4 le uniche possibilità sono $t = \pm 2$ quindi $\gamma = \pm\mathbb{1}$, di cui è da eliminare $-\mathbb{1}$ dato che non appartiene a $\Gamma(4)$.

Se N = 3 le uniche possibilità sono $t = 2$ o $t = -1$. Nel primo caso si ha $\gamma = \mathbb{1}$, altrimenti si deve avere $\gamma^3 = \mathbb{1}$. Per studiare il secondo caso, considerato che $\gamma \equiv \mathbb{1}$ mod 3, si pone $\gamma = \mathbb{1} + 3^k M$ con k un'intero positivo e $M \in M_2(\mathbb{Z})$ tale che $M \neq 0$ mod 3. Allora la condizione $\gamma^3 = \mathbb{1}$ impone che $3^{k+1}M + 3^{2k+1}M^2 + 3^{3k}M^3 = 0$ che è assurda dato che

$$3^{k+1}M + 3^{2k+1}M^2 + 3^{3k}M^3 \equiv 3^{k+1}M \not\equiv 0 \mod 3^{k+2}\,. \qquad \square$$

Osservazione. Si ha $-\mathbb{1} \in \Gamma(2)$ per cui $\Gamma(2)$ ha torsione non banale.

Proposizione 1.10. *Il sottogruppo di congruenza $\Gamma_1(N)$ è privo di torsione per $N > 3$.*

Dimostrazione. Si può seguire un procedimento analogo alla dimostrazione della Proposizione 1.9. Infatti essendo che $\gamma \in \Gamma_1(N)$ si riduce a $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mod N$ si ha comunque che il polinomio minimo di γ si riduce a $x^2 - 2x + 1 \mod N$. □

Osservazione. Si ha $-\mathbb{1} \in \Gamma_1(2)$ e $\left(\begin{smallmatrix} 1 & 1 \\ -3 & -2 \end{smallmatrix}\right) \in \Gamma_1(3)$ per cui $\Gamma_1(2)$ e $\Gamma_1(3)$ hanno torsione non banale.

Osservazione. Il sottogruppo di congruenza $\Gamma_0(N)$ ha torsione non banale per ogni intero positivo N. Infatti si ha $-\mathbb{1} \in \Gamma_0(N)$ per ogni intero positivo N.

I sottogruppi di congruenza agiscono sul semipiano complesso superiore $\mathbb{H}$ e su $\hat{\mathbb{Q}}$ in quanto sono sottogruppi di $SL_2(\mathbb{Z})$. L'azione su $\hat{\mathbb{Q}}$ verrà studiata nel Paragrafo 3.1. L'oggetto centrale della tesi è studiare le curve modulari per sottogruppi di congruenza qui di seguito definite.

Definizione. Sia Γ un sottogruppo di congruenza. La *curva modulare* per Γ è

$$Y(\Gamma) = \Gamma\backslash\mathbb{H}\,.$$

Si deve considerare questo spazio con la topologia quoziente indotta dalla proiezione naturale $\pi\colon \mathbb{H} \to Y(\Gamma)$. Alcune proprietà topologiche di tale spazio seguiranno da risultati noti di topologia generale: ad esempio il fatto che $Y(\Gamma)$ sia connesso e connesso per archi deriva dal fatto che $\mathbb{H}$ ha queste proprietà e il quoziente le conserva.

Notazione. Per $\Gamma = \Gamma(N), \Gamma_1(N), \Gamma_0(N)$ la curva modulare associata $Y(\Gamma)$ è denotata con $Y(N),\ Y_1(N),\ Y_0(N)$ rispettivamente.

1.3 Azioni propriamente discontinue

All'inizio di questo paragrafo saranno dati alcuni risultati generali su azioni di gruppi su spazi di Hausdorff che saranno usati per dedurre che le curve modulari sono spazi di Hausdorff.

Definizione. Sia X uno spazio topologico e sia G un gruppo. L'azione $G \times X \to X$, definita da $(g, x) \mapsto gx$ è *propriamente discontinua* se

$$\forall x, y \in X,\ \exists U \in \mathscr{N}(x), V \in \mathscr{N}(y)\colon\ |\{\, g \in G \mid g(U) \cap V \neq \varnothing \,\}| < \infty\,,$$

dove $\mathscr{N}(x)$ denota il filtro degli intorni di x.

Proposizione 1.11. *La definizione precedente è equivalente a*

$$\forall A, B \subseteq X \textit{ compatti},\ |\{\, g \in G \mid g(A) \cap B \neq \varnothing \,\}| < \infty\,.$$

Dimostrazione. É chiaro che la seconda formulazione implichi la prima, se si pongono al posto di A e B i singoletti $\{\, x \,\}$ e $\{\, y \,\}$.

Per dimostrare l'altra implicazione, si fissi $y \in B$. Si ha ora che $\forall x \in A$ vale

$$\exists U_x \in \mathscr{N}(x), V_x \in \mathscr{N}(y)\colon\ |\{\, g \in G \mid g(U_x) \cap V_x \neq \varnothing \,\}| < \infty\,.$$

La collezione $\{U_x\}_{x\in A}$ è un ricoprimento aperto di A, il quale è un insieme compatto. Pertanto, la collezione $\{U_x\}_{x\in A}$ ammette un sottoricoprimento finito $\{U_{x_1}, \ldots, U_{x_n}\}$ con $x_1, \ldots, x_n \in A$. Sia $V_y = \bigcap_{1\leqslant i\leqslant n} V_{x_i}$. Si ha ora che

$$|\{\, g \in G \mid g(A) \cap V_y \neq \varnothing \,\}| \leqslant \sum_{1\leqslant i\leqslant n} |\{\, g \in G \mid g(U_{x_i}) \cap V_y \neq \varnothing \,\}| < \infty\,.$$

La collezione $\{V_y\}_{y\in B}$ è un ricoprimento aperto di B, il quale è un insieme compatto. Pertanto, $\{V_y\}_{y\in B}$ ammette un sottoricoprimento finito $\{V_{y_1}, \ldots, V_{y_n}\}$ con $y_1, \ldots, y_n \in B$. Vale ora che

$$|\{\, g \in G \mid g(A) \cap B \neq \varnothing \,\}| \leqslant \sum_{1\leqslant i\leqslant n} |\{\, g \in G \mid g(A) \cap V_{y_i} \neq \varnothing \,\}| < \infty\,. \qquad \square$$

Definizione. Sia G un gruppo che agisce su un insieme X. Lo *Stabilizzatore* di $x \in X$ è

$$G_x = \{ g \in G \mid gx = x \} \ .$$

Proposizione 1.12. *Sia G un gruppo topologico, localmente compatto, con base della topologia numerabile, che agisce transitivamente su uno spazio topologico di Hausdorff X anch'esso localmente compatto. Allora si ha che*

$$\forall x \in X,\ G/G_x \text{ è omeomorfo a } X \text{ tramite } gG_x \mapsto gx \ .$$

Osservazione. Nella Proposizione 1.12 si dota G/G_x della topologia quoziente, ovvero la topologia indotta dalla proiezione naturale $\pi : G \to G/G_x$.

Dimostrazione. Si veda Theorem 1.2.1 di [10]. □

Si osserva a questo punto che il gruppo $SL_2(\mathbb{R})$ è un gruppo topologico localmente compatto con la topologia indotta dalla sua immersione in $\mathbb{R}^4$.

Proposizione 1.13. *Sia G un gruppo topologico, localmente compatto, che agisce transitivamente su uno spazio topologico di Hausdorff X anch'esso localmente compatto. Sia $\Gamma \leqslant G$, le seguenti proprietà sono equivalenti:*

1. *Γ è discreto in G;*
2. *L'azione di Γ su X è propriamente discontinua.*

Dimostrazione. Viene prima dimostrata l'implicazione 1⇒2. Siano $x \in X$ e $A, B \subseteq X$ due insiemi compatti. Si pongano $M = \{ g \in G \mid gx \in A \}$ e $N = \{ g \in G \mid gx \in B \}$. Poiché G agisce transitivamente su X si ha che $A = Mx$. Sia $\{ U_i \}_{i \in I}$ un ricoprimento aperto di M tale che $\overline{U_i}$ sia compatto $\forall i \in I$. Dalla Proposizione 1.12 si ha che $\{ U_i x \}_{i \in I}$ è un ricoprimento aperto di A, che è compatto, per cui esistono $U_1, \ldots, U_n$ tali che $\{ U_i x \}_{i=1,\ldots,n}$ è un sottoricoprimento aperto di A. Ora avendo

$$M \subseteq \bigcup_{i=1}^{n} U_i G_x = K$$

ed essendo M chiuso in K, che è compatto, M risulta compatto. In modo simile N è compatto in modo tale che NM^{-1} risulta compatto. Allora l'insieme

$$\{ \gamma \in \Gamma \mid \gamma(A) \cap B \neq \varnothing \} = \Gamma \cap NM^{-1}$$

è discreto, essendo sottoinsieme di Γ, ed è contenuto in NM^{-1}, che è compatto, implicando che è finito. Dalla Proposizione 1.11 si ottiene che Γ agisce in modo propriamente discontinuo su X provando l'implicazione 1⇒2.

Viene dimostrata ora l'implicazione 2⇒1. Sia $V \subseteq G$ un intorno compatto di 1_G, l'identità di G, e si fissi $x \in X$. Risulta, per la Proposizione 1.12, che Vx è compatto. Si ha quindi che $\Gamma \cap \{ \gamma \in \Gamma \mid \gamma x \in Vx \}$ risulta finito dato che $\{ x \}$ e Vx sono insiemi compatti in X. É possibile allora scegliere V in modo tale che $\Gamma \cap V = \{ 1_G \}$, per cui Γ risulta discreto in G. □

Dato che $SL_2(\mathbb{R})$ e $\mathbb{H}$ rispettano le condizioni della Proposizione 1.13, ogni sottogruppo discreto di $SL_2(\mathbb{R})$ agisce in modo propriamente discontinuo su $\mathbb{H}$. In particolare l'azione di $SL_2(\mathbb{Z})$ e dei sottogruppi di congruenza su $\mathbb{H}$ è propriamente discontinua.

Proposizione 1.14. *Si fissi un gruppo Γ che agisce su uno spazio topologico X. Se vale*

$$\forall x, y \in X,\ \exists U \in \mathscr{N}(x), V \in \mathscr{N}(y)\colon\ \forall \gamma \in \Gamma,\ \gamma U \cap V \neq \varnothing \Rightarrow \gamma x = y$$

allora $\Gamma\backslash X$ è spazio di Hausdorff.

Dimostrazione. Sia $\pi\colon X \to \Gamma\backslash X$ la proiezione naturale di X su $\Gamma\backslash X$. Siano $x, y \in X$ e siano $U \in \mathscr{N}(x), V \in \mathscr{N}(y)$ tali che $\forall \gamma \in \Gamma,\ \gamma U \cap V \neq \varnothing \Rightarrow \gamma x = y$. Ora per definizione $\pi(U)$ e $\pi(V)$ sono intorni di $\pi(x)$ e $\pi(y)$ rispettivamente. Si ottiene

$$\begin{aligned} \pi(U) \cap \pi(V) \neq \varnothing &\iff \exists \gamma \in \Gamma\colon \gamma(U) \cap V \neq \varnothing \\ &\iff \exists \gamma \in \Gamma\colon \gamma x = y \\ &\iff \pi(x) = \pi(y) \end{aligned}$$

da cui per ogni $x, y \in X$, tali che $\pi(x) \neq \pi(y)$, esistono due intorni in $\Gamma\backslash X$ disgiunti di $\pi(x)$ e $\pi(y)$ rispettivamente. Ne consegue che $\Gamma\backslash X$ è uno spazio di Hausdorff. □

Proposizione 1.15. *Se Γ agisce in modo propriamente discontinuo su uno spazio di Hausdorff X allora $\Gamma\backslash X$ è spazio di Hausdorff.*

Dimostrazione. Siano $x, y \in X$ e siano U_0 e V_0 intorni di x e y rispettivamente tali che $|\{\, \gamma \in \Gamma\colon \gamma U_0 \cap V_0 \neq \varnothing \,\}| < \infty$. A meno di riordinamenti, si ha

$$\{\, \gamma \in \Gamma\colon \gamma U_0 \cap V_0 \neq \varnothing \,\} = \{\, \gamma_1, \ldots, \gamma_n \,\}$$

in modo da avere $\gamma_i x \neq y$ per ogni $i \leqslant k$ e $\gamma_i x = y$ per ogni $i > k$. Per ogni $i \leqslant k$ si scelgano W_i e Vi intorni di $\gamma_i x$ e y rispettivamente tali che $W_i \cap V_i = \varnothing$. Siano ora

$$U = U_0 \cap \bigcap_{i=1}^{k} \gamma_i^{-1} W_i \quad \text{e} \quad V = V_0 \cap \bigcap_{i=1}^{k} V_i\ .$$

Si verifica che $\gamma U \cap V \neq \varnothing \iff \gamma \in \{\, \gamma_{k+1}, \ldots, \gamma_n \,\} \iff \gamma x = y$ da cui, dalla Proposizione 1.14, segue che $\Gamma\backslash X$ è spazio di Hausdorff. □

Come già osservato $SL_2(\mathbb{Z})$ e i sottogruppi di congruenza agiscono in modo propriamente discontinuo su $\mathbb{H}$. Allora dalle Proposizioni 1.14 e 1.15 si deduce la Proposizione 1.16.

Proposizione 1.16. *Dato Γ sottogruppo di congruenza, $Y(\Gamma)$ è spazio di Hausdorff.*

Tale proprietà permette di dotare $Y(\Gamma)$ della struttura di superficie di Riemann come verrà discusso nel Capitolo 2.

1.4 Domini fondamentali di sottogruppi di congruenza

Viene dato in questo paragrafo un possibile modo di rappresentare le curve modulari $Y(\Gamma)$ attraverso dei loro domini fondamentali e si deduce che le curve modulari $Y(\Gamma)$ non possono essere compatte.

Definizione. Sia G un gruppo con un azione su $\mathbb{H}$. Un *domino fondamentale* per G è $\mathcal{F} \subseteq \mathbb{H}$ tale che

- $\mathcal{F}$ è connesso
- $\mathcal{F}$ è chiuso in $\mathbb{H}$
- Per ogni $z \in \mathbb{H}$, $Gz \cap \mathcal{F} \neq \varnothing$
- Per ogni $g \in G$ se $g\overset{\circ}{\mathcal{F}} \cap \overset{\circ}{\mathcal{F}} \neq \varnothing$ allora la trasformazione indotta da g è l'identità.

Un primo esempio di dominio fondamentale è dato dal dominio fondamentale del gruppo modulare di seguito definito.

Proposizione 1.17. *Un dominio fondamentale per $SL_2(\mathbb{Z})$ è*

$$\mathcal{D} = \left\{ z \in \mathbb{H} \;\middle|\; |\mathrm{Re}\,(z)| \leqslant \tfrac{1}{2},\ |z| \geqslant 1 \right\} .$$

Dimostrazione. Chiaramente l'insieme è connesso e chiuso in $\mathbb{H}$.

Si useranno le notazioni $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ e $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Sia fissato $z \in \mathbb{H}$. È già stato osservato, nella dimostrazione della Proposizione 1.1, che data $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ si ha

$$Im(\gamma z) = \frac{Im(z)}{|cz+d|^2} .$$

I termini $cz+d$ al variare di c e d in $\mathbb{Z}$ costituiscono il reticolo $\mathbb{Z}z \oplus \mathbb{Z}$ che è un sottoinsieme discreto di $\mathbb{C}$. Dato che per costruzione non si può avere $c = d = 0$, esiste una matrice $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ tale che $|cz + d| > 0$ sia minimale. In tal caso si ha che $Im(\gamma z)$ è massimale al variare di γ in $SL_2(\mathbb{Z})$. Sostituendo γ con $T^j\gamma$ per un opportuno j, si può supporre, dato che T preserva la parte immaginaria, che γz realizzi $-\frac{1}{2} \leqslant \mathrm{Re}\,(\gamma z) \leqslant \frac{1}{2}$. Supponendo ora che $\gamma z \notin \mathcal{D}$, cioè che $|\gamma z| < 1$, si avrebbe che

$$Im(S\gamma z) = \frac{Im(\gamma z)}{|\gamma z|^2} > Im(\gamma z)$$

in contrasto con la massimalità di γ. Si ottiene quindi che $\gamma z \in \mathcal{D}$, dimostrando che $\mathcal{D}$ rispetta il terzo requisito di dominio fondamentale.

Si dimostrerà ora che $\gamma\overset{\circ}{\mathcal{D}} \cap \overset{\circ}{\mathcal{D}} \neq \varnothing \Rightarrow \gamma = \pm\mathbb{1}$ per ogni $\gamma \in SL_2(\mathbb{Z})$. Siano $z_1, z_2 \in \mathcal{D}$ tali che $z_2 = \gamma z_1$ per qualche $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ e si supponga che $Im(z_2) \geqslant Im(z_1)$. Si deve avere allora che

$$Im(z_2) = Im(\gamma z_1) = \frac{Im(z_1)}{|cz_1 + d|^2} \geqslant Im(z_1)$$

da cui si deduce che $|cz_1 + d| \leqslant 1$. Si osserva che, avendo $z_1 \in \mathcal{D}$, si ha $Im(z_1) \geqslant \sqrt{3}/2$. Allora se si avesse $|c| \geqslant 2$, si otterrebbe $|Im(cz_1 + d)| \geqslant \sqrt{3} > 1$, che implicherebbe $|cz_1 + d| > 1$ in contrasto con l'osservazione precedente.

Si studiano allora i casi $c = 0$ e $c = \pm 1$.

Se $c = 0$ si avrebbe $|d| \leqslant 1$ da cui, non potendo avere $c = d = 0$, si otterrebbe che $d = \pm 1$ e che γ è della forma $\left(\begin{smallmatrix} \pm 1 & n \\ 0 & \pm 1 \end{smallmatrix}\right)$ per qualche $n \in \mathbb{Z}$. Allora si avrebbe $z_2 = z_1 \pm n$ che è possibile solo se $n = 0$ o se $n = \pm 1$. Nel primo caso ($n = 0$) la trasformazione è semplicemente l'identità e quindi si concluderebbe $\gamma = \pm \mathbb{1}$. Nel secondo caso ($n = \pm 1$) si deve avere $\operatorname{Re}(z_1) = -\operatorname{Re}(z_2) = \pm 1/2$ da cui si otterrebbe $z_1, z_2 \notin \overset{\circ}{\mathcal{D}}$.

Se $c = \pm 1$, dato che $|Im(cz_1+d)| = |Im(z_1)| \geqslant \sqrt{3}/2$, si dovrebbe avere $|\operatorname{Re}(cz + d)| \leqslant 1/2$ che, avendo $|\operatorname{Re}(z_1)| \leqslant 1/2$, implicherebbe $|d| \leqslant 1$. Si distinguono allora i seguenti tre casi: $d = 0$, $d = c$ e $d = -c$.

Se $\mathbf{d = 0}$ si ottiene che $|z_1| = 1$ e che γ è della forma $\left(\begin{smallmatrix} a & \mp 1 \\ \pm 1 & 0 \end{smallmatrix}\right) = \pm T^a S$. Osservando che

$$|\operatorname{Re}(z_2)| = |\operatorname{Re}(\gamma z_1)| = |\operatorname{Re}(a - 1/z_1)| \geqslant |a| - |\operatorname{Re}(z_1)| \geqslant |a| - 1/2$$

e avendo $\operatorname{Re}(z_2) \leqslant 1/2$, si ottiene che $|a| \leqslant 1$. Se $a = 0$, si ha $z_2 = Sz_1 = -1/z_1$. Se $a = \pm 1$, si deve avere $\operatorname{Re}(z_1) = \pm 1/2$, quindi $z_1 = z_2 = \pm\frac{1}{2} + i\frac{\sqrt{3}}{2}$. In ogni caso si ha che z_1 e z_2 non appartengono a $\overset{\circ}{\mathcal{D}}$.

Se $\mathbf{d = c}$ si ottiene che $z_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ e che γ è della forma $\left(\begin{smallmatrix} a & a\mp 1 \\ \pm 1 & \pm 1 \end{smallmatrix}\right)$. Allora

$$z_2 = \gamma z_1 = \pm a - \tfrac{1}{z_1+1} = \pm a + z_1$$

da cui si ottiene che $z_2 = z_1$ oppure $z_2 = z_1 + 1$ e in ogni caso si ha $z_1, z_2 \notin \overset{\circ}{\mathcal{D}}$.

Se $\mathbf{d = -c}$ si ottiene che $z_1 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ e che γ è della forma $\left(\begin{smallmatrix} a & -a\mp 1 \\ \pm 1 & \mp 1 \end{smallmatrix}\right)$. Allora

$$z_2 = \gamma z_1 = \pm a - \tfrac{1}{z_1-1} = \pm a + z_1$$

da cui si ottiene che $z_2 = z_1$ oppure $z_2 = z_1 - 1$ e in ogni caso si ha $z_1, z_2 \notin \overset{\circ}{\mathcal{D}}$.

Avendo concluso i casi possibili per i valori di c e d, si osserva che in tutti questi casi, escluso quello che portava ad avere $\gamma = \pm \mathbb{1}$, si ha che $z_1, z_2 \notin \overset{\circ}{\mathcal{D}}$ da cui si deduce che $\gamma\overset{\circ}{\mathcal{D}} \cap \overset{\circ}{\mathcal{D}} \neq \varnothing \Rightarrow \gamma = \pm \mathbb{1}$ per ogni $\gamma \in SL_2(\mathbb{Z})$. È stato quindi dimostrato che $\mathcal{D}$ rispetta anche la quarta condizione di dominio fondamentale, concludendo la dimostrazione. □

Osservazione. Nel corso della dimostrazione è stato ricavato anche il seguente fatto: dati due punti distinti z_1, z_2 sul bordo di $\mathcal{D}$ questi sono nella stessa classe di equivalenza modulo $SL_2(\mathbb{Z})$ se e solo se $\operatorname{Re}(z_1) = -\operatorname{Re}(z_2) = \pm 1/2$ e $z_2 = z_1 \pm 1$ oppure $|z_1| = 1$ e $z_2 = -1/z_1$. Questo risultato definisce una legge di identificazione per i bordi di $\mathcal{D}$ che lo rendono omeomorfo a $Y(1)$. Si veda la Figura 1.1.

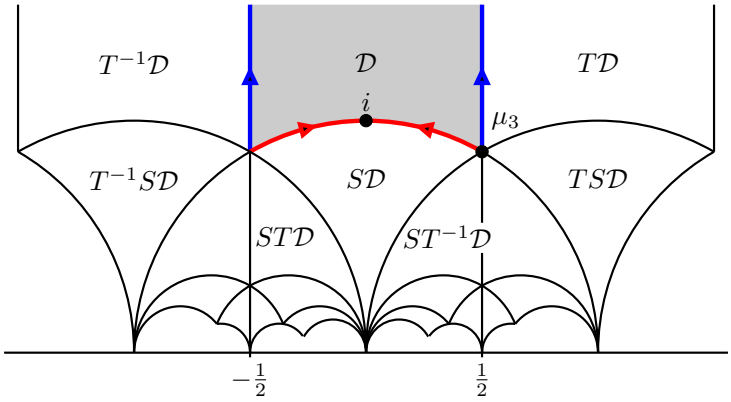


Figura 1.1: Una rappresentazione di $\mathcal{D}$ e alcune sue trasformazioni

Osservazione. Usando $\mathcal{D}$ come rappresentazione di $Y(SL_2(\mathbb{Z}))$ risulta molto facile osservare che $Y(SL_2(\mathbb{Z}))$ non è compatto e questo sarà valido per ogni $Y(\Gamma)$. Nel Capitolo 3 saranno costruite le curve $X(\Gamma)$, superficie di Riemann compatte tali che $X(\Gamma) = Y(\Gamma)$ a meno di finiti punti detti cuspidi.

Un'applicazione del fatto che $\mathcal{D}$ è dominio fondamentale per $SL_2(\mathbb{Z})$ è il seguente fatto algebrico.

Proposizione 1.18. *Il gruppo modulare è generato da* $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ *e* $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$

$$SL_2(\mathbb{Z}) = \langle S, T \rangle \ .$$

Dimostrazione. Il gruppo $\Gamma = \langle S, T \rangle$ è chiaramente sottogruppo di $SL_2(\mathbb{Z})$. Si mostrerà che, data $\gamma \in SL_2(\mathbb{Z})$, esiste $\gamma' \in \langle S, T \rangle$ tale che $\gamma\gamma' = \pm\mathbb{1}$. Essendo che $-\mathbb{1} = S^2 \in \Gamma$ si ottiene che, eventualmente moltiplicando per $-\mathbb{1}$, l'inversa di γ appartiene a Γ concludendo che $SL_2(\mathbb{Z}) \subseteq \Gamma$.

Sia $\gamma \in SL_2(\mathbb{Z})$, si fissi $z \in \overset{\circ}{\mathcal{D}}$ e si consideri $\gamma z \in \mathbb{H}$. Analogamente alla dimostrazione della Proposizione 1.17, si considera $\gamma'\gamma z$ al variare di $\gamma' \in \Gamma$ e se ne deduce che deve esistere $\gamma' \in \Gamma$ tale che $\gamma'\gamma z \in \mathcal{D}$. Per la quarta proprietà di $\mathcal{D}$ come dominio fondamentale, avendo che $\gamma'\gamma\overset{\circ}{\mathcal{D}} \cap \mathcal{D} \supseteq \{z\} \neq \varnothing$, si ottiene che $\gamma'\gamma = \pm\mathbb{1}$ come si voleva. □

Si procede ora a descrivere un metodo per ottenere un dominio fondamentale per un qualsiasi sottogruppo di congruenza Γ a partire da $\mathcal{D}$.

Osservazione. Si osserva che gli unici elementi $\alpha \in SL_2(\mathbb{Z})$ di $\mathcal{D}$ tali che l'intersezione $\mathcal{D} \cap \alpha^{-1}\mathcal{D}$ non sia il vuoto o un punto sono $\pm T, \pm S, \pm T^{-1}$. Allora si ha anche che per ogni $\alpha \in SL_2(\mathbb{Z})$ gli unici elementi $\beta \in SL_2(\mathbb{Z})$ di $\mathcal{D}$ tali che l'intersezione $\alpha^{-1}\mathcal{D} \cap \alpha^{-1}\beta^{-1}\mathcal{D}$ non sia il vuoto o un punto sono $\pm T, \pm S, \pm T^{-1}$.

Come già osservato nel Capitolo 1, dalla Proposizione 1.6 si ricava che l'indice di $SL_2(\mathbb{Z})$ su un qualsiasi sottogruppo di congruenza Γ è finito. Allora, dato Γ sottogruppo di congruenza, si ha $SL_2(\mathbb{Z})/\Gamma = \{\alpha_1\Gamma, \ldots, \alpha_n\Gamma\}$ e $SL_2(\mathbb{Z})$ può essere espresso come unione disgiunta di $\alpha_i\Gamma$.

Proposizione 1.19. *Dato un sottogruppo di congruenza* Γ *esiste sempre una scelta di rappresentanti* $\{\alpha_1, \ldots, \alpha_n\}$ *di* $SL_2(\mathbb{Z})/\Gamma$ *tale che*

$$\mathcal{F} = \bigcup_{i=1}^{n} {\alpha_i}^{-1}\mathcal{D} \tag{1.1}$$

è un dominio fondamentale per Γ.

Osservazione. In generale l'unione dei ${\alpha_i}^{-1}\mathcal{D}$ non è disgiunta. In particolare per ottenere un dominio fondamentale per Γ è necessario che ogni trasformato di $\mathcal{D}$ abbia intersezione con almeno un altro di essi, dato che un dominio fondamentale deve essere connesso. Si osserva però che se $\alpha^{-1}\mathcal{D} \cap \beta^{-1}\mathcal{D} \neq \varnothing$ con $\alpha \neq \pm\beta$ si ha $\alpha^{-1}\overset{\circ}{\mathcal{D}} \cap \beta^{-1}\overset{\circ}{\mathcal{D}} = \varnothing$. Infatti, se non fosse vero, si otterrebbe che $\alpha\beta^{-1}\overset{\circ}{\mathcal{D}} \cap \overset{\circ}{\mathcal{D}} \neq \varnothing$ da cui, dato che $\mathcal{D}$ è un dominio fondamentale, si avrebbe che $\alpha\beta^{-1} = \pm\mathbb{1}$ contro l'ipotesi $\alpha \neq \pm\beta$.

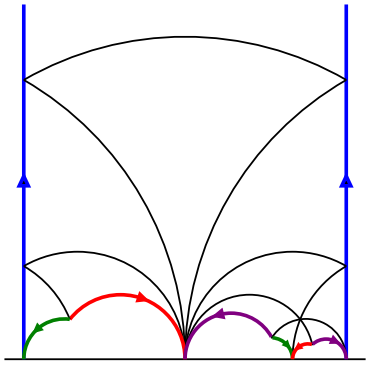


Figura 1.2: Un dominio fondamentale di $\Gamma_0(11)$ con evidenziate le leggi di identificazione.

Dimostrazione. In generale, indipendentemente dalla scelta dei rappresentanti α_i, un insieme $\mathcal{F}$ definito come nella 1.1 rispetta la definizione di dominio fondamentale, ad esclusione soltanto dell'essere connesso.

Il fatto che $\mathcal{F}$ sia chiuso è verificato in quanto $\mathcal{D}$ è chiuso, le α_i sono omeomorfismi e l'unione è finita.

Si verifica ora che $\mathcal{F}$ rispetta il terzo requisito di dominio fondamentale per Γ, ovvero che per ogni $z \in \mathbb{H}$, $\Gamma z \cap \mathcal{F} \neq \varnothing$. Si fissi $z \in \mathbb{H}$. Dato che $\mathcal{D}$ è un dominio fondamentale per $SL_2(\mathbb{Z})$ esiste $\gamma \in SL_2(\mathbb{Z})$ tale che $\gamma z \in \mathcal{D}$. Allora, essendo che $\gamma = \alpha_i\gamma'$ per qualche i e qualche $\gamma' \in \Gamma$, si ha che $\alpha_i\gamma' z = \gamma z \in \mathcal{D}$ da cui si ottiene che $\gamma' z \in {\alpha_i}^{-1}\mathcal{D} \subseteq \mathcal{F}$.

Si verifica ora che $\mathcal{F}$ rispetta il quarto requisito di dominio fondamentale per Γ, ovvero che per ogni $\gamma \in \Gamma$ se $\gamma\overset{\circ}{\mathcal{F}} \cap \overset{\circ}{\mathcal{F}} \neq \varnothing$ allora $\gamma = \pm\mathbb{1}$. Sia allora $\gamma \in \Gamma$ tale che $\gamma\overset{\circ}{\mathcal{F}} \cap \overset{\circ}{\mathcal{F}} \neq \varnothing$. In tal caso devono esistere α_i, α_j tali che $\gamma{\alpha_i}^{-1}\overset{\circ}{\mathcal{D}} \cap {\alpha_j}^{-1}\overset{\circ}{\mathcal{D}} \neq \varnothing$, il che, per l'osservazione precedente, implica che $\alpha_i\gamma^{-1} = \pm\alpha_j$. Nel caso in cui si abbia $\alpha_i\gamma^{-1} = -\alpha_j$ si osserva che, avendo ${\alpha_j}^{-1}\mathcal{D} = -{\alpha_j}^{-1}\mathcal{D}$, si ha anche $\alpha_i\gamma^{-1} = \alpha_j$. Da $\alpha_i\gamma^{-1} = \alpha_j$ si deduce che $\alpha_i = \alpha_j$, dato che questi sono rappresentanti di classi laterali, da cui si ottiene che $\alpha_i\gamma^{-1}{\alpha_i}^{-1} = \pm\mathbb{1}$.

Essendo che $\pm\mathbb{1}$ sono gli unici elementi di $SL_2(\mathbb{Z})$ di ordine 1 e 2, come si deduce dalla Proposizione 1.8, e il coniugio preserva l'ordine, si ottiene che $\gamma = \pm\mathbb{1}$.

Per ottenere un dominio fondamentale per ciascun sottogruppo di congruenza Γ rimane da mostrare che esiste sempre una scelta di rappresentanti di classi laterali modulo Γ tali che $\mathcal{F}$ sia connesso.

Si ponga $\mathcal{D}_1 = \mathcal{D}$ e $\alpha_1 = \mathbb{1}$. Se $SL_2(\mathbb{Z}) = \Gamma = \alpha_1\Gamma$ si termina il processo dato che $\mathcal{D}_1$ è un dominio fondamentale per Γ. Altrimenti sia

$$\mathcal{S}_1 = \{\alpha \in SL_2(\mathbb{Z}) \backslash \alpha_1\Gamma \mid \alpha^{-1}\mathcal{D} \cap \mathcal{D}_1 \neq \varnothing\} .$$

Avendo ora $\Gamma \neq SL_2(\mathbb{Z})$ deve esistere $\alpha_2 \in \mathcal{S}_1$ tale che $\Gamma = \alpha_1\Gamma \neq \alpha_2\Gamma$. Infatti, come già osservato, $\mathcal{D} \cap S^{-1}\mathcal{D} \neq \varnothing$ e $\mathcal{D} \cap T^{-1}\mathcal{D} \neq \varnothing$, quindi una tra S e T appartiene a $\mathcal{S}_1$, dato che altrimenti si avrebbe $S, T \in \Gamma$ che implicherebbe $\Gamma = SL_2(\mathbb{Z})$. Si pone allora $\mathcal{D}_2 = \mathcal{D}_1 \cup {\alpha_2}^{-1}\mathcal{D}$ e si osserva che $\mathcal{D}_2$ è connesso dato che $\mathcal{D}_1$ e ${\alpha_2}^{-1}\mathcal{D}$ sono connessi e ${\alpha_2}^{-1}\mathcal{D} \cap \mathcal{D}_1 \neq \varnothing$.

Iterativamente si supponga di avere $\mathcal{D}_i$ connesso e $\{\alpha_1, \ldots, \alpha_i\}$ tali che $\mathcal{D}_i = \bigcup_{j=1}^{i} {\alpha_j}^{-1}\mathcal{D}$ e $\alpha_j\Gamma \neq \alpha_{j'}\Gamma$ per ogni $j \neq j'$. Se $SL_2(\mathbb{Z}) = \alpha_1\Gamma \cup \cdots \cup \alpha_i\Gamma$ allora $\mathcal{D}_i$ è un dominio fondamentale per Γ dato che è connesso per ipotesi e rispetta le altre condizioni di dominio fondamentale come è già stato mostrato. Altrimenti si pone

$$\mathcal{S}_i = \{\alpha \in SL_2(\mathbb{Z}) \backslash (\alpha_1\Gamma \cup \cdots \cup \alpha_i\Gamma) \mid \alpha^{-1}\mathcal{D} \cap \mathcal{D}_i \neq \varnothing\} .$$

Avendo ora che $\alpha_1\Gamma \cup \cdots \cup \alpha_i\Gamma \neq SL_2(\mathbb{Z})$ si dimostrerà successivamente che deve esistere $\alpha_{i+1} \in \mathcal{S}_i$ tale che $\alpha_{i+1} \notin \alpha_1\Gamma \cup \cdots \cup \alpha_i\Gamma$. Si pone allora $\mathcal{D}_{i+1} = \mathcal{D}_i \cup {\alpha_{i+1}}^{-1}\mathcal{D}$ e si osserva che $\mathcal{D}_{i+1}$ è connesso dato che $\mathcal{D}_i$ e ${\alpha_{i+1}}^{-1}\mathcal{D}$ sono connessi e ${\alpha_{i+1}}^{-1}\mathcal{D} \cap \mathcal{D}_i \neq \varnothing$.

Si dimostra ora che se non esistesse un tale α_{i+1} si arriverebbe ad un assurdo. Infatti, come già osservato, ${\alpha_j}^{-1}T^{-1}\mathcal{D} \cap \mathcal{D}_i \supseteq {\alpha_j}^{-1}T^{-1}\mathcal{D} \cap {\alpha_j}^{-1}\mathcal{D} \neq \varnothing$ per ogni $j \leqslant i$. Allora, supponendo di avere $T\alpha_j, S\alpha_j \in (\alpha_1\Gamma \cup \cdots \cup \alpha_i\Gamma)$ per ogni $j \leqslant i$, si ottiene che per ogni $j \leqslant i$ esiste un k_j tale che $T\alpha_j\Gamma = \alpha_{k_j}\Gamma$ e che per ogni $j \leqslant i$ esiste un ${k_j}'$ tale che $S\alpha_j\Gamma = \alpha_{k_j'}\Gamma$. Tali k_j sono unici per ciascun j dato che, se si avesse $k_j = k_{j'}$, si otterrebbe $T\alpha_j\Gamma = \alpha_{k_j}\Gamma = T\alpha_{j'}\Gamma$ da cui $\alpha_j\Gamma = \alpha_{j'}\Gamma$ che implica $j = j'$ secondo le ipotesi sugli α_j. Analogamente i k_j' sono unici. Si ottiene allora che

$$T(\alpha_1\Gamma \cup \cdots \cup \alpha_i\Gamma) = S(\alpha_1\Gamma \cup \cdots \cup \alpha_i\Gamma) = \alpha_1\Gamma \cup \cdots \cup \alpha_i\Gamma$$

che, avendo $SL_2(\mathbb{Z}) = \langle S, T \rangle$, implica

$$SL_2(\mathbb{Z}) = SL_2(\mathbb{Z})(\alpha_1\Gamma \cup \cdots \cup \alpha_i\Gamma) = \alpha_1\Gamma \cup \cdots \cup \alpha_i\Gamma$$

contro l'ipotesi di partenza.

Il processo iterativo deve avere un termine dato che gli α_j così costruiti rappresentano classi laterali distinte che sono al più $[SL_2(\mathbb{Z}) \colon \Gamma]$ che è finito per la Proposizione 1.6. Allora l'ultimo $\mathcal{D}_k$ ottenuto è un dominio fondamentale per Γ della forma 1.1 . □

Analogamente a quanto osservato per $\mathcal{D}$, il dominio fondamentale per un sottogruppo di congruenza Γ così costruito ha associate delle leggi di identificazione dei bordi che lo rendono omeomorfo a $Y(\Gamma)$. Si veda la Figura 1.2.

Osservazione. Essendo che è sempre possibile scegliere $\mathbb{1}$ come primo rappresentante, si può sempre avere $\mathcal{D} \subseteq \mathcal{F}$. Allora $Y(\Gamma)$ non potrà mai essere compatto dato che mancherà sempre il punto $i\infty$.

Capitolo 2

Curve modulari aperte

Sono già state introdotte le curve modulari $Y(\Gamma)$ dal punto di vista insiemistico e topologico nel capitolo precedente. In questo capitolo si studia la struttura di superficie di Riemann di cui si possono dotare gli spazi $Y(\Gamma)$. La scelta naturale sarebbe considerare un atlante per cui la proiezione $\pi\colon \mathbb{H} \to Y(\Gamma)$ sia una mappa olomorfa. Come sarà discusso nel Paragrafo 2.2 è possibile considerare quali carte locali delle inverse locali di π su tutta la superficie a meno di finiti punti detti ellittici.

2.1 Punti ellittici per sottogruppi di congruenza

In questo paragrafo vengono definiti e studiati i punti ellittici per i sottogruppi di congruenza. I risultati di questo paragrafo verrano applicati nel Paragrafo 2.3 per definire delle carte locali negli intorni dei punti ellittici.

Definizione. Sia Γ un sottogruppo di congruenza. Un punto $\tau \in \mathbb{H}$ è

- *semplice* per Γ se $\gamma\tau = \tau \Rightarrow \gamma = \pm\mathbb{1}, \forall\gamma \in \Gamma$;
- *ellittico* per Γ se $\pm\Gamma_\tau \neq \{\pm\mathbb{1}\}$.

I punti ellittici sono quindi i punti τ per cui esistono trasformazioni indotte da Γ non identiche che stabilizzano τ.

Osservazione. Dato che per $\gamma \in \Gamma$ e $\tau \in \mathbb{H}$ vale $\Gamma_{\gamma\tau} = \gamma\Gamma_\tau\gamma^{-1}$ il fatto che lo stabilizzatore sia non banale viene preservata dalle trasformazioni di Γ. In particolare se τ è ellittico o semplice allora $\tau' \in \Gamma\tau$ è, rispettivamente, ellittico o semplice. Risulta quindi naturale estendere la definizione di punto ellittico e punto semplice al quoziente $Y(\Gamma)$.

Proposizione 2.1. *Sia $\gamma \in SL_2(\mathbb{Z})$ la cui trasformazione ammette punto fisso, l'ordine di γ in $SL_2(\mathbb{Z})$ è $1, 2, 3, 4$ o 6.*

Dimostrazione. Sia $\tau \in \mathbb{H}$ punto fisso per $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Si ha

$$\frac{a\tau + b}{c\tau + d} = \tau \;\Rightarrow\; a\tau + b = c\tau^2 + d\tau \;.$$

Se fosse $c = 0$ allora si avrebbe $\tau \in \mathbb{Q}$ che è assurdo. Calcolando il discriminante dell'equazione si ottiene $a^2 + d^2 - 2ad + 4bc$ che, considerando che $ad - bc = 1$, si può scrivere come $(a + d)^2 - 4$. Se il discriminante fosse positivo si avrebbe $\tau \in \mathbb{R}$ che è assurdo, perciò si deduce che $|a + d| < 2$ quindi $a + d = 0, \pm 1$. Si calcola il polinomio caratteristico di γ

$$\begin{vmatrix} x-a & -b \\ -c & x-d \end{vmatrix} = x^2 - (a+d)x + ad - bc = x^2 - (a+d)x + 1$$

che può valere $x^2 + 1$ o $x^2 \pm x + 1$. Si deve avere quindi una tra $\gamma^4 = \mathbb{1}, \gamma^3 = \mathbb{1}, \gamma^6 = \mathbb{1}$. □

Osservazione. Se l'ordine di γ in $SL_2(\mathbb{Z})$ è 1 allora γ è $\mathbb{1}$ e se l'ordine è 2 allora γ è $-\mathbb{1}$. Infatti imponendo le condizioni sui coefficienti a, b, c, d in modo che $\gamma^2 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^2 = \mathbb{1}$ e $ad - bc = 1$ si ottengono come uniche soluzioni $\gamma = \pm\mathbb{1}$. In entrambi i casi la trasformazione indotta è l'identità di $\mathbb{H}$. Si studiano perciò le matrici γ di ordine $3, 4, 6$.

Osservazione. Se non si imponesse la condizione $\det \gamma = 1$ insieme alla condizione $\gamma^2 = \mathbb{1}$, ovvero se non si richiedesse che $\gamma \in SL_2(\mathbb{Z})$, si otterrebbero infinite soluzioni della forma $\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ con la restrizione $a^2 + bc = 1$ e determinante $-a^2 - bc = -1$.

Osservazione. Nella dimostrazione della Proposizione 2.1 è stato usato il fatto che, data una qualche $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, un eventuale punto fisso τ deve rispettare l'equazione $a\tau + b = c\tau^2 + d\tau$. Tale equazione è polinomiale di secondo grado a coefficienti in $\mathbb{Z}$ quindi ammette al più due radici e, se una di queste è in $\mathbb{H}$, l'altra deve essere la sua coniugata, quindi non appartenere al semipiano superiore. Se ne deduce quindi che ogni $\gamma \in SL_2(\mathbb{Z})$ ha al più un punto fisso in $\mathbb{H}$.

Proposizione 2.2. *Sia $\gamma \in SL_2(\mathbb{Z})$.*

- *Se γ ha ordine 3 allora è coniugata a $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)^{\pm 1}$ in $SL_2(\mathbb{Z})$.*
- *Se γ ha ordine 4 allora è coniugata a $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{\pm 1}$ in $SL_2(\mathbb{Z})$.*
- *Se γ ha ordine 6 allora è coniugata a $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)^{\pm 1}$ in $SL_2(\mathbb{Z})$.*

Dimostrazione. Si veda Proposition 2.3.3 di [4] . □

Conoscendo le caratteristiche delle $\gamma \in SL_2(\mathbb{Z})$ che ammettono punto fisso, si possono classificare i punti ellittici per $SL_2(\mathbb{Z})$ e poi di conseguenza i punti ellittici per Γ sottogruppo di congruenza.

Osservazione. Si ricorda che se τ è punto fisso per $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ allora, come nella dimostrazione della Proposizione 2.1, si deve avere $a\tau + b = c\tau^2 + d\tau$. Si calcolano quindi i punti fissi per le trasformazioni nella Proposizione 2.2.

- Per $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ il punto fisso è i.
- Per $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ e $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ il punto fisso è $\mu_3 = e^{2\pi i/3}$.

Osservazione. Risulta anche utile sapere $SL_2(\mathbb{Z})i \cap SL_2(\mathbb{Z})\mu_3 = \varnothing$. Infatti vale la relazione $\mathbb{Q}(i) \cap \mathbb{Q}(\mu_3) = \mathbb{Q}$ da cui si ottiene che non possono esistere $a, b, c, d \in \mathbb{Z}$ tali che $\frac{ai+b}{ci+d} = \mu_3$. Complessivamente non può esistere $\gamma \in SL_2(\mathbb{Z})$ tale che $\gamma i = \mu_3$.

Proposizione 2.3. *L'insieme dei punti ellittici per $SL_2(\mathbb{Z})$ è*

$$\{\, \tau \in \mathbb{H} \mid \tau \text{ ellittico per } SL_2(\mathbb{Z}) \,\} = SL_2(\mathbb{Z})i \cup SL_2(\mathbb{Z})\mu_3 \ .$$

Dimostrazione. L'inclusione delle due orbite nei punti ellittici è banale. Sia ora $\tau \in \mathbb{H}$ ellittico per $SL_2(\mathbb{Z})$ e sia $\gamma \in SL_2(\mathbb{Z})_\tau, \gamma \neq \pm\mathbb{1}$. Per la Proposizione 2.1 la matrice γ ha ordine $3, 4$ o 6 in $SL_2(\mathbb{Z})$. Dalla Proposizione 2.2 si ottiene che γ è coniugata a

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{\pm 1} \text{ o } \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}^{\pm 1}$$

tramite una qualche $\delta \in SL_2(\mathbb{Z})$.

- Se $\delta^{-1}\gamma\delta = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{\pm 1}$ allora $\delta\tau$ è punto fisso per $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{\pm 1}$ ovvero $\delta\tau = i$.
- Se $\delta^{-1}\gamma\delta = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)^{\pm 1}$ allora $\delta\mu_3$ è punto fisso per $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)^{\pm 1}$ ovvero $\delta\tau = \mu_3$.
- Se $\delta^{-1}\gamma\delta = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)^{\pm 1}$ allora $\delta\mu_3$ è punto fisso per $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)^{\pm 1}$ ovvero $\delta\tau = \mu_3$.

Complessivamente si ha $\tau \in SL_2(\mathbb{Z})i$ oppure $\tau \in SL_2(\mathbb{Z})\mu_3$. □

Osservazione. La Proposizione 2.3 implica che ogni punto ellittico per $SL_2(\mathbb{Z})$ ha stabilizzatore finito ciclico di ordine 2 o 3. Si mostra nella Proposizione 2.4 che questo fatto è vero anche per i punti ellittici di un sottogruppo di congruenza Γ. Inoltre come già osservato in precedenza $\Gamma_{\gamma\tau} = \gamma\Gamma_\tau\gamma^{-1}$ quindi l'ordine dello stabilizzatore è invariante in un'orbita. Si da quindi la seguente definizione.

Definizione. Il *periodo* di τ per Γ è

$$h_\tau = |\pm\Gamma_\tau/\pm\mathbb{1}| = \begin{cases} |\Gamma_\tau|/2 & \text{se } -\mathbb{1} \in \Gamma \\ |\Gamma_\tau| & \text{se } -\mathbb{1} \in \Gamma \ . \end{cases}$$

Il *periodo* di $P = \pi(\tau) \in Y(\Gamma)$ è h_τ.

La motivazione per il quiziente nella definizione di periodo ha lo scopo di tenere in considerazione che γ e $-\gamma$ inducono la stessa trasformazione. Definendolo in questo modo h_τ rappresenta il numero di trasformazioni che stabilizzano τ. Si osserva anche che $h_\tau = 1$ per τ semplice e $h_\tau > 1$ altrimenti.

Proposizione 2.4. *Sia Γ un sottogruppo di congruenza. La curva modulare $Y(\Gamma)$ ha finiti punti ellittici, inoltre questi hanno periodo 2 o 3.*

Dimostrazione. Dalla Proposizione 2.3 l'enunciato è vero per $\Gamma = SL_2(\mathbb{Z})$ dato che $Y(SL_2(\mathbb{Z}))$ ha come punti ellittici $\pi(i), \pi(\mu_3)$ di periodo 2 e 3 rispettivamente.

Dato Γ sottogruppo di congruenza, è già stato dimostrato che $[SL_2(\mathbb{Z}) : \Gamma] < \infty$. Esistono quindi $\gamma_j \in SL_2(\mathbb{Z})$ tali che $SL_2(\mathbb{Z}) = \bigcup_{j=1}^{d} \Gamma\gamma_j$. Si ha quindi

$$\{\, P \in Y(\Gamma) \mid P \text{ ellittico} \,\} \subseteq \{\, \Gamma(\gamma_j i), \Gamma(\gamma_j \mu_3) : j = 1, \ldots, d \,\}$$

che è finito. Inoltre per ogni $\gamma_j i$ si ha $\Gamma_{\gamma_j i} = \Gamma \cap \gamma_j SL_2(\mathbb{Z})_{\gamma_j i} {\gamma_j}^{-1}$ da cui si deduce che $h_{\gamma_j i} = 1$ oppure $h_{\gamma_j i} = 2$. Analogamente per ogni $\gamma_j\mu_3$ si ha $h_{\gamma_j\mu_3} = 1$ oppure $h_{\gamma_j\mu_3} = 3$. In ogni caso si ha un punto semplice oppure un punto ellittico di periodo 2 o 3. □

2.2 Carte locali per punti semplici

Per discutere le carte locali di $Y(\Gamma)$ è necessario discutere due casi distinti: i punti semplici e i punti ellittici della curva. L'ultimo caso richiede passaggi intermedi che saranno trattati nel paragrafo successivo.

Proposizione 2.5. *La proiezione $\pi\colon \mathbb{H} \to Y(\Gamma)$ è un omeomorfismo localmente ai punti semplici di $\mathbb{H}$.*

Dimostrazione. Si ottiene, in modo analogo alla dimostrazione della Proposizione 1.15, che

$$\forall \tau_1, \tau_2 \in \mathbb{H}\ \exists U_1 \in \mathscr{N}(\tau_1), U_2 \in \mathscr{N}(\tau_2)\colon\ \forall \gamma \in \Gamma\ \gamma U_1 \cap U_2 \neq \varnothing \Rightarrow \gamma\tau_1 = \tau_2\ .$$

Specializzando a $\tau = \tau_1 = \tau_2$ e considerando eventualmente l'intersezione di U_1 e U_2 si ottiene

$$\forall \tau \in \mathbb{H}\ \exists U \in \mathscr{N}(\tau)\colon\ \forall \gamma \in \Gamma\ \gamma U \cap U \neq \varnothing \Rightarrow \gamma\tau = \tau \Rightarrow \gamma = \pm\mathbb{1}\ .$$

Il che implica che la proiezione π ristretta a un intorno di τ è iniettiva.

Chiaramente la proiezione π è suriettiva sull'immagine dell'intorno ed è per definizione continua. Dalla Proposizione 1.12 la proiezione risulta anche aperta quindi è un omeomorfismo locale. □

L'intenzione è scegliere un'inversa locale di π come carta locale in un punto semplice della curva. Risulta quindi necessario discutere la compatibilità delle carte locali così scelte.

Proposizione 2.6. *Detto U_τ un intorno di $\tau \in \mathbb{H}$ punto semplice tale che*

$$\gamma U_\tau \cap U_\tau \neq \varnothing \Rightarrow \gamma = \pm\mathbb{1}$$

e detto $\mathbb{H}_s = \{\, \tau \in \mathbb{H} \mid \tau \text{ semplice} \,\}$, si ha che

$$\left\{\pi(U_\tau), (\pi|_{U_\tau})^{-1}\right\}_{\tau\in\mathbb{H}_s} \text{ è un atlante per } Y(\Gamma)\setminus\{\, P \in Y(\Gamma) \mid P \text{ ellittico} \,\}\ .$$

Dimostrazione. Siano U_1, U_2 due aperti con le proprietà richieste, siano $\tilde{U_1}, \tilde{U_2}$ le loro immagini tramite la proiezione π e siano $\varphi_i = (\pi|_{U_i})^{-1} : \tilde{U_i} \to U_i$. Le mappe φ_i sono omeomorfismi per la Proposizione 2.2. Considerato $\tau_1 \in \varphi_1(\tilde{U_1} \cap \tilde{U_2})$, la sua immagine $\tau_2 = \varphi_2 \circ \pi(\tau_1)$ è necessariamente nell'orbita di τ_1 ovvero $\tau_2 = \gamma\tau_1$ con $\gamma \in \Gamma$. Ora, dato $\tau \in \varphi_1(\tilde{U_1} \cap \tilde{U_2})$, si dimostra che deve valere $\gamma\tau = \varphi_2 \circ \pi(\tau)$. Infatti se $\varphi_2 \circ \pi(\tau) = \gamma'\tau$ con $\gamma' \in \Gamma$ allora si deve avere $\gamma\tau, \gamma'\tau \in U_2$. Si ottiene allora che $\gamma'\gamma^{-1}(U_2) \cap U_2 \neq \varnothing$, il che, per come sono stati scelte le carte locali, implica che $\gamma'\gamma^{-1} = \pm\mathbb{1}$ cioè che γ e γ' inducono la stessa trasformazione olomorfa su $\mathbb{H}$. Complessivamente è stato osservato che $\varphi_2 \circ {\varphi_1}^{-1} = \gamma$ per qualche $\gamma \in \Gamma$ e che quindi i cambi di carta locale sono olomorfi. □

2.3 Carte locali per punti ellittici

In questo paragrafo vengono definite delle carte locali negli intorni di punti ellittici per un sottogruppo di congruenza Γ. Viene perciò completata la costruzione di un atlante per le superficie di Riemann $Y(\Gamma)$.

Come è stato osservato nel Paragrafo 2.1 ciascun punto ellittico $\tau \in \mathbb{H}$ ha stabilizzatore ciclico finito ed ha associato un periodo h_τ. Prima di iniziare la costruzione di una carta locale in un punto ellittico si fanno le seguenti osservazioni

Osservazione. Dato $\tau \in \mathbb{H}$ se $\gamma \in \Gamma_\tau$ allora $\gamma\bar{\tau} = \bar{\tau}$ poiché il coniugio rispetta le operazioni di somma e prodotto e le entrate di γ sono invarianti per il coniugio.

Osservazione. Come nella dimostrazione della Proposizione 2.2 si usa il fatto

$$\forall \tau_1, \tau_2 \in \mathbb{H}\ \exists U_1 \in \mathscr{N}(\tau_1), U_2 \in \mathscr{N}(\tau_2)\colon\ \forall \gamma \in \Gamma\ \gamma U_1 \cap U_2 \neq \varnothing \Rightarrow \gamma\tau_1 = \tau_2$$

per ottenere che

$$\forall \tau \in \mathbb{H}\ \exists U_\tau \in \mathscr{N}(\tau)\colon\ \forall \gamma \in \Gamma\ \gamma U_\tau \cap U_\tau \neq \varnothing \Rightarrow \gamma \in \Gamma_\tau\ .$$

È utile sapere che in U_τ l'unico punto ellittico è τ. Infatti se esistesse qualche $\tau' \in U_\tau$ ellittico, per una qualche $\gamma' \in \Gamma_{\tau'}$ si avrebbe che $\gamma' U_\tau \cap U_\tau \neq \varnothing$ da cui $\gamma' \in \Gamma_\tau$. Per l'unicità dei punti fissi osservata nel Paragrafo 2.1 se ne deduce che $\tau = \tau'$.

Sia $\tau \in \mathbb{H}$ un punto ellittico e si consideri $\delta_\tau = \left(\begin{smallmatrix} 1 & \tau \\ 1 & \bar{\tau} \end{smallmatrix}\right) \in GL_2(\mathbb{C})$ scelta in modo tale che $\tau \mapsto 0, \bar{\tau} \mapsto \infty$. L'azione di Γ non è preservata da questa trasformazione ma il gruppo coniugato $\delta_\tau \Gamma {\delta_\tau}^{-1}$ agisce su $\delta_\tau(\mathbb{H})$ in modo che i diagrammi

$$\begin{array}{ccc} \mathbb{H} & \xrightarrow{\ \gamma\ } & \mathbb{H} \\ {\scriptstyle \delta_\tau}\downarrow & & \downarrow{\scriptstyle \delta_\tau} \\ \delta_\tau(\mathbb{H}) & \xrightarrow[\delta_\tau \gamma {\delta_\tau}^{-1}]{} & \delta_\tau(\mathbb{H}) \end{array}$$

siano commutativi per ogni $\gamma \in \Gamma$. Lo stabilizzatore di un punto $\delta_\tau(z) \in \delta_\tau(\mathbb{H})$ nel gruppo $\delta_\tau \Gamma {\delta_\tau}^{-1}$ è il coniugato dello stabilizzatore di $z \in \mathbb{H}$ nel gruppo Γ quindi in particolare per $z = \tau$ vale $\left(\delta_\tau \Gamma {\delta_\tau}^{-1}\right)_0 = \delta_\tau \Gamma_\tau {\delta_\tau}^{-1}$.

Il gruppo coniugato $\delta_\tau \Gamma_\tau {\delta_\tau}^{-1}$ è costituito per definizione da trasformazioni lineari fratte che stabilizzano 0 e ∞ dato che questi sono immagine tramite δ_τ di τ e $\bar{\tau}$. Le mappe con questa proprietà sono tutte della forma $z \mapsto az$ con $a \in \mathbb{C}^*$. Poiché, come è stato osservato nel Paragrafo 2.1, lo stabilizzatore di un punto ellittico è sempre ciclico e finito, è possibile interpretare lo stabilizzatore di 0 come sottogruppo ciclico finito di ordine h_τ di $\mathbb{C}^*$. Così facendo si ottiene che $\delta_\tau \Gamma_\tau {\delta_\tau}^{-1}$ è generato dalla funzione $z \mapsto \zeta_{h_\tau} z$ dove ζ_{h_τ} è una radice primitiva h_τ-esima dell'unità. Si è quindi dedotto che $\delta_\tau \Gamma_\tau {\delta_\tau}^{-1}$ è il gruppo generato dalla rotazione di angolo $2\pi/h_\tau$ attorno a 0. Si veda la Figura 2.1.

Per l'osservazione fatta all'inizio dei questo paragrafo, esiste un intorno $\bar{U}$ di τ tale che $\gamma\bar{U} \cap \bar{U} = \varnothing,\ \forall \gamma \notin \Gamma_\tau$. L'insieme $\delta_\tau(\bar{U})$ è, di conseguenza, un intorno di 0 tale che $\gamma' \delta_\tau(\bar{U}) \cap \delta_\tau(\bar{U}) = \varnothing, \forall \gamma' \notin \delta_\tau \Gamma_\tau {\delta_\tau}^{-1}$. Deve esistere quindi un disco W_r di raggio $r > 0$ centrato nell'origine contenente solo 0 come punto ellittico per $\delta_\tau \Gamma {\delta_\tau}^{-1}$ e tale che

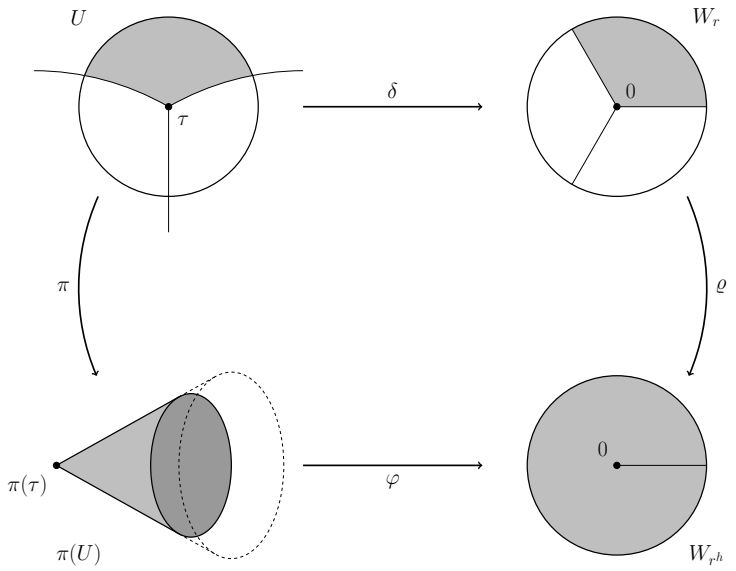


Figura 2.1: La costruzione di una carta locale per un punto ellittico.

$\gamma' W_r \cap W_r = \varnothing, \forall \gamma' \notin \delta_\tau \Gamma_\tau {\delta_\tau}^{-1}$. Rimane inoltre definita un'azione di $(\delta_\tau \Gamma {\delta_\tau}^{-1})_0$ su W_r dato che lo stabilizzatore di 0 è costituito da rotazioni, come è già stato osservato, le quali preservano i dischi centrati in 0.

Si ponga $U = {\delta_\tau}^{-1}(W_r)$ intorno di τ. Tale aperto mantiene le proprietà di $\bar{U}$ ed è omeomorfo tramite δ_τ a W_r. Dato che W_r è preservato dall'azione di $\delta_\tau \Gamma_\tau {\delta_\tau}^{-1}$ si deduce che U è preservato dall'azione di Γ_τ ed è quindi definito il quoziente $\Gamma_\tau \backslash U$. Risulta che $\Gamma_\tau \backslash U$ è omeomorfo a $\delta_\tau \Gamma_\tau {\delta_\tau}^{-1} \backslash W_r$. Infatti dati $z, z' \in U$ si ha che

$$[z]_{\Gamma_\tau} = [z']_{\Gamma_\tau} \iff [\delta_\tau z]_{\delta_\tau \Gamma_\tau {\delta_\tau}^{-1}} = [\delta_\tau z']_{\delta_\tau \Gamma_\tau {\delta_\tau}^{-1}}$$

da cui si deduce che δ_τ induce una mappa continua e iniettiva $\widetilde{\delta_\tau} : \Gamma_\tau \backslash U \to \delta_\tau \Gamma_\tau {\delta_\tau}^{-1} \backslash W_r$. Inoltre considerato che il seguente diagramma commuta

$$\begin{array}{ccc} U & \xrightarrow{\delta_\tau} & W_r \\ \downarrow & & \downarrow \\ \Gamma_\tau \backslash U & \xrightarrow{\widetilde{\delta_\tau}} & \delta_\tau \Gamma_\tau {\delta_\tau}^{-1} \backslash W_r \end{array}$$

si ottiene che $\widetilde{\delta_\tau}$ è effettivamente un omeomorfismo.

Anche $\pi(U)$ e $\Gamma_\tau \backslash U$ sono omeomorfi. Infatti considerati $z, z' \in U$ si ha

$$\pi(z) = \pi(z') \iff z \in \Gamma z' \iff z \in \Gamma_\tau z' \iff [z]_{\Gamma_\tau} = [z']_{\Gamma_\tau}$$

dove la seconda implicazione deriva dal fatto che $\gamma U \cap U \neq \varnothing \Rightarrow \gamma \in \Gamma_\tau$. Allora π induce una mappa continua e iniettiva $\widetilde{\pi} : \pi(U) \to \Gamma_\tau \backslash U$ che è anche suriettiva data la suriettività di $\widetilde{\pi} \circ \pi$. Il fatto che $\widetilde{\pi}$ sia una mappa aperta deriva dal fatto che π è continua e la proiezione naturale di U su $\Gamma_\tau \backslash U$ è aperta. Complessivamente si deduce che $\widetilde{\pi}$ è un omeomorfismo.

Definita $\varrho : W_r \to W_{r^{h_\tau}}$ con $\varrho(z) = z^{h_\tau}$, dove $W_{r^{h_\tau}}$ è la palla centrata nell'origine di raggio r^{h_τ}, si osserva che ϱ è invariante per l'azione di $\left(\delta_\tau \Gamma \delta_\tau{}^{-1}\right)_0$ su W_r quindi induce un omeomorfismo $\widetilde{\varrho} : \delta_\tau \Gamma_\tau \delta_\tau{}^{-1} \backslash W_r \to W_{r^{h_\tau}}$ in modo analogo a quanto discusso per $\widetilde{\delta_\tau}$ e $\widetilde{\pi}$.

Complessivamente è stato realizzato il seguente diagramma commutativo

$$\begin{array}{ccccccc} & & U & \xrightarrow{\delta_\tau} & W_r & & \\ & \swarrow^{\pi} & \downarrow & & \downarrow & \searrow^{\varrho} & \\ \pi(U) & \xrightarrow[\widetilde{\pi}]{} & \Gamma_\tau \backslash U & \xrightarrow[\widetilde{\delta_\tau}]{} & \delta_\tau \Gamma_\tau \delta_\tau{}^{-1} \backslash W_r & \xrightarrow[\widetilde{\varrho}]{} & W_{r^{h_\tau}} \end{array} \tag{2.1}$$

dal quale si deduce che $\pi(U)$ è omeomorfo a $W_{r^{h_\tau}}$ tramite $\widetilde{\varrho} \circ \widetilde{\delta_\tau} \circ \widetilde{\pi}$. Queste sono le carte locali che si intendono usare negli intorni di punti ellittici. Rimane da dimostrare che questa scelta induce una struttura olomorfa su $Y(\Gamma)$.

Osservazione. Il diagramma precedente rimane valido anche per punti semplici. Infatti in questo caso Γ_τ e il suo coniugato sono la trasformazione identica, per cui $U \simeq \Gamma_\tau \backslash U$ e $W_r \simeq \delta_\tau \Gamma_\tau \delta_\tau{}^{-1} \backslash W_r$. Inoltre ϱ è l'identità di W_r.

Proposizione 2.7. *Detto U_τ un intorno di $\tau \in \mathbb{H}$ tale che*

- $\gamma U_\tau \cap U_\tau \neq \varnothing \Rightarrow \gamma \in \Gamma_\tau$
- $\pi(U_\tau) \simeq W_{r^{h_\tau}}$ *tramite* $\widetilde{\varrho} \circ \widetilde{\delta_\tau} \circ \widetilde{\pi}$

secondo le notazioni introdotte nella precedente discussione

$$\left\{ \pi(U_\tau), \widetilde{\varrho} \circ \widetilde{\delta_\tau} \circ \widetilde{\pi} \right\}_{\tau \in \mathbb{H}} \text{ è un atlante per la superficie di Riemann } Y(\Gamma) \, .$$

Dimostrazione. Siano $U_i = U_{\widetilde{\tau_i}}$ due aperti con le proprietà richieste, siano $\left(\tilde{U}_i, \varphi_i\right)$ le carte locali relative agli U_i costruite come indicato sopra. È sufficiente verificare che la mappa di transizione $\varphi_2 \circ \varphi_1{}^{-1}$ sia olomorfa in un intorno di ciascun punto in $\varphi_1\left(\tilde{U}_1 \cap \tilde{U}_2\right)$ per ottenere che la mappa è olomorfa su tutto il dominio. Si consideri allora $P \in \tilde{U}_1 \cap \tilde{U}_2$. Si deve avere $P = \pi(\tau_1) = \pi(\tau_2)$ con $\tau_i \in U_i$ e quindi anche $\tau_2 = \gamma \tau_1$ per una qualche $\gamma \in \Gamma$. Dato che γ è un omeomorfismo $U_1 \cap \gamma^{-1} U_2$ è un intorno di τ_1 e avendo π mappa aperta $\pi\left(U_1 \cap \gamma^{-1} U_2\right)$ è un intorno di P contenuto in $\tilde{U}_1 \cap \tilde{U}_2$. Si considera ora $\varphi_1\Big(\pi\left(U_1 \cap \gamma^{-1} U_2\right)\Big)$ intorno di $\varphi_1(P)$ contenuto in $\varphi_1\left(\tilde{U}_1 \cap \tilde{U}_2\right)$.

Si assume inizialmente che $\varphi_1(P) = 0$ ovvero che $\tau_1 = \widetilde{\tau_1}$. In questo caso dato un qualche $z = \varphi_1(P') \in \varphi_1\Big(\pi\left(U_1 \cap \gamma^{-1} U_2\right)\Big)$ con $P' = \pi\left(\tau'\right)$ per un qualche $\tau' \in U_1 \cap \gamma^{-1} U_2$ si ha che

$$\begin{aligned} \varphi_2 \circ \varphi_1{}^{-1}(z) = \varphi_2(P') = \varphi_2\big(\pi(\tau')\big) = \varphi_2\big(\pi(\gamma\tau')\big) = \\ = \big(\delta_2(\gamma\tau')\big)^{h_2} = \Big(\delta_2 \gamma \delta_1{}^{-1}\big(\delta_1(\tau')\big)\Big)^{h_2} = \\ = \big(\delta_2 \gamma \delta_1{}^{-1}(z^{1/h_1})\big)^{h_2} \end{aligned}$$

dove $\delta_i = \delta_{\widetilde{\tau}_i}$ e $h_i = h_{\widetilde{\tau}_i}$. Se $h_1 = 1$, cioè se τ_1 fosse un punto semplice, la funzione $\varphi_2 \circ {\varphi_1}^{-1}$ risulta olomorfa come si voleva. Se $h_1 > 1$, cioè se τ_1 fosse ellittico, anche $\tau_2 = \gamma\tau_1$ sarebbe ellittico da cui si ottiene che $\tau_2 = \widetilde{\tau}_2$, dato che in $U_{\widetilde{\tau}_2}$ l'unico punto ellittico può essere eventualmente $\widetilde{\tau}_2$, e anche che $h_1 = h_2$. Ora, osservando che

$$0 \overset{{\delta_1}^{-1}}{\longmapsto} \tau_1 \overset{\gamma}{\longmapsto} \tau_2 \overset{\delta_2}{\longmapsto} 0 \qquad \text{e} \qquad \infty \overset{{\delta_1}^{-1}}{\longmapsto} \bar{\tau_1} \overset{\gamma}{\longmapsto} \bar{\tau_2} \overset{\delta_2}{\longmapsto} \infty$$

si ottiene, come già osservato, che $\delta_2\gamma{\delta_1}^{-1}(z) = az$ per qualche $a \in \mathbb{C}^*$. Avendo ciò si ottiene

$$\varphi_2 \circ {\varphi_1}^{-1}(z) = \left(\delta_2\gamma{\delta_1}^{-1}(z^{1/h_1})\right)^{h_2} = (az^{1/h_1})^{h_2} = a^{h_2}z$$

che è ancora una mappa olomorfa.

Nel caso in cui, invece che $\varphi_1(P) = 0$, si abbia $\varphi_2(P) = 0$ si possono scambiare i ruoli di φ_1 e φ_2 e verificare come prima che $\varphi_1 \circ {\varphi_2}^{-1}$ è olomorfa in $\varphi_2\big(\tilde{U}_1 \cap \tilde{U}_2\big)$. Per ottenere che $\varphi_2 \circ {\varphi_1}^{-1}$ è olomorfa è sufficiente osservare che l'inversa di una biiezione olomorfa è anch'essa olomorfa.

Se non si avesse né $\varphi_1(P) = 0$ né $\varphi_2(P) = 0$, è possibile considerare una carta $\big(U_3, \varphi_3\big)$ tale che $\varphi_3(P) = 0$. Infatti è sufficiente scegliere $U_3 = U_{\tau_1}$ con la relativa carta locale data dal diagramma 2.1. Avendo che $\varphi_2 \circ {\varphi_3}^{-1}$ e $\varphi_3 \circ {\varphi_1}^{-1}$ sono olomorfe per gli argomenti precedenti risulta che $\varphi_2 \circ {\varphi_1}^{-1} = (\varphi_2 \circ {\varphi_3}^{-1}) \circ (\varphi_3 \circ {\varphi_1}^{-1})$ è olomorfa. □

Capitolo 3

Curve modulari compatte

È già stato osservato nel Capitolo 1 che $SL_2(\mathbb{Z})$ agisce su $\hat{\mathbb{Q}}$. Questo implica che anche un qualsiasi sottogruppo di congruenza Γ agisce su $\hat{\mathbb{Q}}$. Nel Capitolo 1 inoltre si è osservato come nessuna curva modulare $Y(\Gamma)$ è compatta. Lo scopo di questo capitolo è definire, per ogni Γ sottogruppo di congruenza, la superficie di Riemann compatta $X(\Gamma)$ tale che $X(\Gamma) = Y(\Gamma)$ a meno di finiti punti.

3.1 Cuspidi di Γ

In questo paragrafo vengono definite e studiate le cuspidi per i sottogruppi di congruenza. Viene data inoltre una definizione delle curve modulari compatte $X(\Gamma)$ dal punto di vista insiemistico e topologico.

Definizione. Una *cuspide* per un sottogruppo di congruenza Γ è un elemento di $\Gamma\backslash\hat{\mathbb{Q}}$.

Osservazione. È già stato osservato nel Capitolo 1 che l'azione di $SL_2(\mathbb{Z})$ su $\hat{\mathbb{Q}}$ è transitiva. Questo implica che $SL_2(\mathbb{Z})\backslash\hat{\mathbb{Q}}$ è costituito da un solo elemento, ovvero che $SL_2(\mathbb{Z})$ ha una sola cuspide che verrà identificata con ∞.

Proposizione 3.1. *Le cuspidi per un sottogruppo di congruenza* Γ *sono al più* $[SL_2(\mathbb{Z})\colon \Gamma]$.

Dimostrazione. Si consideri una cuspide $\Gamma s \in \Gamma\backslash\hat{\mathbb{Q}}$. Dato che l'azione di $SL_2(\mathbb{Z})$ su $\hat{\mathbb{Q}}$ è transitiva esiste $\alpha \in SL_2(\mathbb{Z})$ tale che $s = \alpha_s\infty$. Allora $\Gamma s = \Gamma\alpha_s\infty$ e per ogni $\Gamma s' \in \Gamma\backslash\hat{\mathbb{Q}}$ si ha $\Gamma s = \Gamma s' \iff \Gamma\alpha_s = \Gamma\alpha_{s'}$. Esiste quindi un'iniezione da $\Gamma\backslash\hat{\mathbb{Q}}$ a $\Gamma\backslash SL_2(\mathbb{Z})$ che implica

$$|\Gamma\backslash\hat{\mathbb{Q}}| \leqslant |\Gamma\backslash SL_2(\mathbb{Z})| = [SL_2(\mathbb{Z})\colon \Gamma]\,. \qquad \square$$

Osservazione. Come già stato osservato nel Paragrafo 1.4, identificando $Y(\Gamma)$ con la sua rappresentazione con un dominio fondamentale per Γ, si ottiene facilmente che $Y(\Gamma)$ non è compatta. Si può vedere nella Figura 1.1 che aggiungendo un punto a ∞ e alcuni punti sull'asse reale, che sono più precisamente elementi di $\mathbb{Q}$, e dotandolo di opportuni intorni ai punti aggiunti, si ottiene un insieme compatto. Questi punti sono una rappresentazione geometrica delle cuspidi che sono appena state definite, il che motiva le costruzioni successive.

Definizione. Il *semipiano superiore esteso* è $\mathbb{H}^* = \mathbb{H} \cup \hat{\mathbb{Q}} = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

Osservazione. Il nuovo spazio così definito può contenere anche le cuspidi per un sottogruppo di congruenza Γ. Essendo che è necessario poter isolare le cuspidi non è possibile dotare $\mathbb{H}^*$ della topologia indotta da $\mathbb{C}$. Infatti in tal caso per ogni intorno di un punto razionale si avrebbero infiniti altri punti razionali, possibilmente non appartenenti alla stessa classe di equivalenza modulo Γ.

Per l'osservazione precedente si definiranno dei sistemi di intorni dei punti aggiunti a $\mathbb{H}$ a partire dagli intorni di ∞.

Definizione. Dato $M > 0$ sia $\mathcal{N}_M = \{\tau \in \mathbb{H} | Im(\tau) > M\} \cup \{\infty\}$.

Questi insiemi costituiscono una base per gli intorni di ∞ in $\mathbb{H}^*$. Data $\alpha \in SL_2(\mathbb{Z})$ si ha che $\alpha\infty \in \hat{\mathbb{Q}}$, ed essendo che le trasformazioni di $SL_2(\mathbb{Z})$ preservano i cerchi in $\mathbb{P}^1(\mathbb{C})$, se $\alpha\infty \in \mathbb{Q}$ si ha che l'immagine tramite α di $\mathcal{N}_M$ è un cerchio tangente in $\alpha\infty$ all'asse reale.

Definizione. Si dota $\mathbb{H}^*$ della topologia generata dagli aperti di $\mathbb{H}$ e dagli aperti del tipo $\alpha\mathcal{N}_M$ al variare di $\alpha \in SL_2(\mathbb{Z})$ e $M > 0$.

Osservazione. Con la topologia appena definita, data una qualsiasi $\gamma \in SL_2(\mathbb{Z})$, l'applicazione $\tau \mapsto \gamma\tau$ è un omeomorfismo di $\mathbb{H}^*$ in sé stesso. Infatti è chiaro che tale applicazione è continua per i punti appartenenti a $\mathbb{H}$. Inoltre, se si considera l'intorno $\alpha\mathcal{N}_M$ di $\gamma s \in \hat{\mathbb{Q}}$, la sua antiimmagine tramite $\tau \mapsto \gamma\tau$ è $\gamma^{-1}\alpha\mathcal{N}_M$, il quale è un intorno di s per definizione.

Definizione. La *curva modulare compatta* per un sottogruppo di congruenza Γ è

$$X(\Gamma) = \Gamma\backslash\mathbb{H}^* .$$

Come per $Y(\Gamma)$, si intende considerare $X(\Gamma)$ dotato della topologia indotta dalla proiezione naturale $\pi\colon \mathbb{H}^* \to X(\Gamma)$.

Osservazione. Si osserva che $X(\Gamma) = \Gamma\backslash\mathbb{H}^* = \Gamma\backslash(\mathbb{H} \cup \hat{\mathbb{Q}}) = Y(\Gamma) \cup \Gamma\backslash\hat{\mathbb{Q}}$. Lo spazio $X(\Gamma)$ è compatto per la Proposizione 3.2 ed è ottenuto a partire da $Y(\Gamma)$ aggiungendo un numero finito di punti come precedentemente anticipato.

Proposizione 3.2. *Dato un sottogruppo di congruenza Γ, si ha che $X(\Gamma)$ è uno spazio di Hausdorff connesso e compatto.*

Dimostrazione. La connessione di $X(\Gamma)$ deriva dalla connessione di $\mathbb{H}^*$. Infatti se $\mathbb{H}^*$ è connesso, allora $X(\Gamma)$, che è sua immagine tramite π, è connesso. Si supponga allora che $\mathbb{H}^* = A_1 \mathbin{\mathring{\cup}} A_2$ con A_1 e A_2 aperti. Considerando $(A_1 \cap \mathbb{H}) \mathbin{\mathring{\cup}} (A_2 \cap \mathbb{H}) = \mathbb{H}$ e ricordando che $\mathbb{H}$ è connesso, si ottiene, a meno di cambiare gli indici, che $A_1 \cap \mathbb{H} = \mathbb{H}$ e $A_2 \cap \mathbb{H} = \varnothing$. Dalla seconda si ottiene che $A_2 \subseteq \hat{\mathbb{Q}}$, il che implica che l'unica possibilità per avere A_2 aperto è $A_2 = \varnothing$. Complessivamente $\mathbb{H}^*$ è connesso come si voleva.

Per la compattezza di $X(\Gamma)$ si consideri $\mathcal{D}^* = \mathcal{D} \cup \{\infty\}$. L'insieme $\mathcal{D}^*$ è compatto nella topologia di $\mathbb{H}^*$. Infatti dato un ricoprimento aperto $\mathcal{U}$ di $\mathcal{D}^*$ deve esistere $U \in \mathcal{U}$ tale che $\infty \in U$. Inoltre deve esistere $\mathcal{N}_M \subseteq U$ dato che i $\mathcal{N}_M$ costituiscono una base per

gli intorni di ∞ in $\mathbb{H}^*$. Allora $\mathcal{U}$ costituisce, nella topologia di $\mathbb{H}$, un ricoprimento aperto di $\mathcal{D}\backslash\mathcal{N}_M$ che è compatto nella topologia di $\mathbb{H}$. Deve esistere quindi un sottoricoprimento finito di $\mathcal{U}$ che, aggiungendo eventualmente U, è anche un sottoricoprimento finito di $\mathcal{D}^*$.

Vale che $\mathbb{H}^* = SL_2(\mathbb{Z})\mathcal{D}^* = \big(\bigcup_j \Gamma\alpha_j\big)\mathcal{D}^* = \bigcup_j \Gamma\alpha_j\mathcal{D}^*$ dove gli α_j sono rappresentanti delle classi laterali di $SL_2(\mathbb{Z})/\Gamma$. Allora $X(\Gamma) = \pi(\mathbb{H}^*) = \bigcup_j \pi(\alpha_j\mathcal{D}^*)$ è compatto dato che gli insiemi $\alpha_j\mathcal{D}^*$ sono compatti, quindi anche la loro proiezione è compatta, e l'unione è finita, dato che il numero di α_j è $[SL_2(\mathbb{Z})\colon \Gamma]$.

Si dimostra ora che $X(\Gamma)$ è uno spazio di Hausdorff. Siano allora $P_1, P_2 \in X(\Gamma)$ due punti con $P_i = \Gamma x_i$ per $x_i \in \mathbb{H}^*$. Il caso $x_1, x_2 \in \mathbb{H}$ è già stato discusso nella Proposizione 1.13. Si studiano allora i casi $x_1 \in \mathbb{H}, x_2 \in \hat{\mathbb{Q}}$ e $x_1, x_2 \in \hat{\mathbb{Q}}$.

Siano $x_1 \in \mathbb{H}$ e $x_2 \in \hat{\mathbb{Q}}$ e sia U un intorno di x_1 in $\mathbb{H}$ tale che $\bar{U}$ sia compatto. È già stato osservato, nella dimostrazione della Proposizione 1.1, che data $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ si ha

$$Im(\gamma\tau) = \frac{Im(\tau)}{|c\tau + d|^2} \quad \text{per ogni } \tau \in \mathbb{H}\ .$$

Si osserva che se $c = 0$ si ha $Im(\gamma\tau) \leqslant Im(\tau)/d^2 \leqslant Im(\tau)$, se invece $c \neq 0$ si ha $Im(\gamma\tau) \leqslant \frac{Im(\tau)}{Im(\tau)^2 + (d/c)^2} \leqslant 1/Im(\tau)$. In ogni caso risulta che

$$Im(\gamma\tau) \leqslant \max\left\{\ Im(\tau), \frac{1}{Im(\tau)}\ \right\} \text{ per ogni } \gamma \in SL_2(\mathbb{Z})\ .$$

Dato che il massimo di $Im(\tau)$ e $1/Im(\tau)$ è una funzione continua su $\mathbb{H}$ questa ammette massimo M su $\bar{U}$ dato che questo è compatto. Allora, per la disuguaglianza appena mostrata, si ottiene che $SL_2(\mathbb{Z})\bar{U} \cap \mathcal{N}_M = \varnothing$ da cui, fissata $\alpha \in SL_2(\mathbb{Z})$ tale che $\alpha\infty = x_2$, si ha $\Gamma\bar{U} \cap \alpha\mathcal{N}_M = \varnothing$. Gli insiemi $\pi(U)$ e $\pi(\alpha\mathcal{N}_M)$ sono intorni di P_1 e P_2 rispettivamente e sono disgiunti come si voleva.

Siano ora $x_1, x_2 \in \hat{\mathbb{Q}}$. Per avere P_1 e P_2 distinti è necessario imporre $\Gamma x_1 \neq \Gamma x_2$. Fissate $\alpha_1, \alpha_2 \in SL_2(\mathbb{Z})$ tali che $\alpha_i\infty = x_i$ si considerino gli intorni $\alpha_i\mathcal{N}_2$. Se si avesse $\gamma\alpha_1\mathcal{N}_2 \cap \alpha_2\mathcal{N}_2 \neq \varnothing$, ovvero se esistessero $\tau_1, \tau_2 \in \mathcal{N}_2$ tali che $\tau_2 = {\alpha_2}^{-1}\gamma\alpha_1\tau_1$, si otterrebbe che ${\alpha_2}^{-1}\gamma\alpha_1 = \pm T^m$ per qualche m. Infatti si ha che $\mathcal{N}_2 = \bigcup_j T^j\big(\mathcal{D} \cap \mathcal{N}_2\big)$ e che $\mathcal{N}_2$ è privo di punti ellittici. Dal fatto che ${\alpha_2}^{-1}\gamma\alpha_1 = \pm T^m$ si dedurrebbe che ${\alpha_2}^{-1}\gamma\alpha_1$ fissa ∞ da cui si otterrebbe che $\gamma x_1 = \gamma\alpha_1\infty = \alpha_2\infty = x_2$ contro l'ipotesi $\Gamma x_1 \neq \Gamma x_2$. Gli insiemi $\pi(\alpha_i\mathcal{N}_2)$ sono intorni dei P_i disgiunti come si voleva. □

Per arrivare alla compattificazione di $Y(\Gamma)$ come superficie di Riemann rimane da dotare $X(\Gamma)$ di un'opportuna struttura di superficie di Riemann. Per le carte locali in $Y(\Gamma) \subseteq X(\Gamma)$ vengono usate le stesse carte locali definite nel Capitolo 2.

3.2 $X(\Gamma)$ come superficie di Riemann

In questo paragrafo saranno definite delle carte locali negli intorni delle cuspidi di un sottorguppo di congruenza, completando così la struttura di superficie di Riemann per le curve modulari compatte. Viene usato un approccio simile a quello visto nel Paragrafo 2.3 per i punti ellittici.

Osservazione. Una difficoltà nel seguire lo stesso approccio delle carte locali per i punti ellittici è che nel caso delle cuspidi lo stabilizzatore di una cuspide può essere di ordine infinito. Ad esempio $SL_2(\mathbb{Z})_\infty = \{\pm\mathbb{1}\}\langle T\rangle$.

Definizione. Sia $s \in \hat{\mathbb{Q}}$. Dato un sottogruppo di congruenza Γ, l'*ampiezza* di s per Γ è

$$h_{s,\Gamma} = [SL_2(\mathbb{Z})_s \colon \{\pm\mathbb{1}\}\Gamma_s] \,.$$

L'*ampiezza* di $\pi(s) \in X(\Gamma)$ è $h_{s,\Gamma}$.

Osservazione. Sia dato un sottogruppo di congruenza Γ. Considerando s ed s' elementi di $\hat{\mathbb{Q}}$ tali che $\gamma s = s'$, per una qualche $\gamma \in \Gamma$, si ottiene che $h_{s,\Gamma} = h_{s',\Gamma}$. Infatti si ha che $[SL_2(\mathbb{Z})_{s'} \colon \{\pm\mathbb{1}\}\Gamma_{s'}] = [\gamma SL_2(\mathbb{Z})_s\gamma^{-1} \colon \gamma\{\pm\mathbb{1}\}\Gamma_s\gamma^{-1}] = [SL_2(\mathbb{Z})_s \colon \{\pm\mathbb{1}\}\Gamma_s]$. Allora l'ampiezza degli elementi di $\hat{\mathbb{Q}}$ è invariante nelle orbite di Γ, giustificando la definizione di ampiezza delle cuspidi appena data.

Proposizione 3.3. *Sia $s \in \hat{\mathbb{Q}}$, si ha che $h_{s,\Gamma} < \infty$ per ogni sottogruppo di congruenza Γ.*

Dimostrazione. Sia $\delta \in SL_2(\mathbb{Z})$ tale che $\delta s = \infty$ e si consideri $\delta\{\pm\mathbb{1}\}\Gamma\delta^{-1}$. Se Γ è sottogruppo di congruenza anche $\{\pm\mathbb{1}\}\Gamma$ è sottogruppo di congruenza dato che si deve avere $\Gamma(N) \subseteq \Gamma \subseteq \{\pm\mathbb{1}\}\Gamma$ per qualche $N \in \mathbb{N}$. Allora, avendo che $\Gamma(N)$ è normale in $SL_2(\mathbb{Z})$, anche $\delta\{\pm\mathbb{1}\}\Gamma\delta^{-1}$ è sottogruppo di congruenza, dato che si deve avere $\Gamma(N) = \delta\Gamma(N)\delta^{-1} \subseteq \delta\{\pm\mathbb{1}\}\Gamma\delta^{-1}$. Si usa ora il fatto che $\Gamma(N) \trianglelefteq SL_2(\mathbb{Z})$ e il Secondo Teorema di Isomorfismo per ottenere che

$$\frac{SL_2(\mathbb{Z})_\infty}{\Gamma(N)_\infty} \simeq \frac{\Gamma(N)SL_2(\mathbb{Z})_\infty}{\Gamma(N)}$$

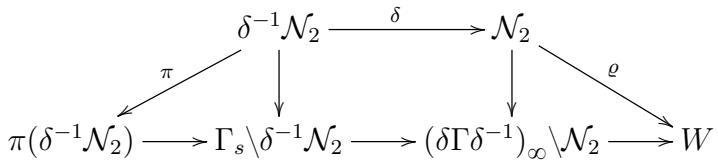
dato che $\Gamma(N)_\infty = \Gamma(N) \cap SL_2(\mathbb{Z})_\infty$. Ora, considerato il fatto che $\Gamma(N)_\infty \leqslant (\delta\{\pm\mathbb{1}\}\Gamma\delta^{-1})_\infty$ e che $\Gamma(N)SL_2(\mathbb{Z})_\infty \leqslant SL_2(\mathbb{Z})$, si ottiene che

$$[SL_2(\mathbb{Z})_\infty \colon (\delta\{\pm\mathbb{1}\}\Gamma\delta^{-1})_\infty] \mid [SL_2(\mathbb{Z})_\infty \colon \Gamma(N)_\infty] \mid [SL_2(\mathbb{Z}) \colon \Gamma(N)] < \infty$$

dove è stato usato che $[SL_2(\mathbb{Z})_\infty \colon \Gamma(N)_\infty] = [\Gamma(N)SL_2(\mathbb{Z})_\infty \colon \Gamma(N)]$. Complessivamente è stato ottenuto che $h_{s,\Gamma} = [SL_2(\mathbb{Z})_s \colon \{\pm\mathbb{1}\}\Gamma_s] = [SL_2(\mathbb{Z})_\infty \colon (\delta\{\pm\mathbb{1}\}\Gamma\delta^{-1})_\infty] < \infty$ come si voleva dimostrare. □

Osservazione. In modo analogo alla dimostrazione della Proposizione 3.2, si dimostra che per ogni $s \in \hat{\mathbb{Q}}$, posto $U = \alpha\mathcal{N}_2$ con $\alpha\infty = s$, vale che $\gamma U \cap U \neq \varnothing \Rightarrow \gamma \in \Gamma_s$. In modo simile agli intorni delle cuspidi descritti nel Paragrafo 2.3, si ha che, dato un tale U, si ha un omeomorfismo $\Gamma_s\backslash U \simeq \pi(U)$.

Si costruisce ora un diagramma commutativo analogo al diagramma 2.1. Si consideri $s \in \hat{\mathbb{Q}}$ con ampiezza h e si fissi $\delta \in SL_2(\mathbb{Z})$ tale che $\delta s = \infty$. Il seguente diagramma è commutativo



dove ϱ è la funzione su $\mathcal{N}_2$ definita da

$$\varrho(\tau) = \begin{cases} 0 & \text{se } \tau = \infty \\ e^{\frac{2\pi i \tau}{h}} & \text{se } \tau \neq \infty \end{cases}$$

e W è l'immagine di $\mathcal{N}_2$ tramite ϱ. Le frecce orizzontali nel diagramma sono omeomorfismi e la loro composizione verrà detta φ in modo da avere $\pi(\delta^{-1}\mathcal{N}_2) \simeq_\varphi W$.

Proposizione 3.4. *Si indichi con $\mathcal{A}$ l'atlante definito nella Proposizione 2.7. Usando le notazioni sopra introdotte*

$$\mathcal{A} \cup \left\{ \pi({\delta_s}^{-1}\mathcal{N}_2), \varphi_s \right\}_{s\in\hat{\mathbb{Q}}} \text{ è un atlante per la superficie di Riemann } X(\Gamma) \,.$$

Dimostrazione. Si mostra prima la compatibilità delle nuove carte locali con l'atlante $\mathcal{A}$. Siano $\big(\tilde{U}_i, \varphi_i\big)$ due carte locali tali che $\tilde{U}_i = \pi(U_i)$ con $U_1 = U_{\widetilde{\tau}_1}$, per qualche $\widetilde{\tau}_1 \in \mathbb{H}$ di periodo h_1 e $U_2 = \delta_2^{-1}(\mathcal{N}_2)$ con $\delta_2^{-1}\infty = s$ di ampiezza h_2. Si consideri anche $\delta_1 \in GL_2(\mathbb{C})$ come nella dimostrazione della Proposizione 2.7. È sufficiente verificare che la mappa di transizione ${\varphi_2 \circ \varphi_1}^{-1}$ sia olomorfa in un intorno di ciascun punto in $\varphi_1\big(\tilde{U}_1 \cap \tilde{U}_2\big)$ per ottenere che la mappa è olomorfa su tutto il dominio. Si consideri allora $P \in \tilde{U}_1 \cap \tilde{U}_2$. Si deve avere $P = \pi(\tau_1) = \pi(\tau_2)$ con $\tau_i \in U_i$ e quindi anche $\tau_2 = \gamma\tau_1$ per una qualche $\gamma \in \Gamma$. Come nella dimostrazione della Proposizione 2.7, si considera l'intorno $\varphi_1\Big(\pi\big(U_1 \cap \gamma^{-1}U_2\big)\Big)$ di $\varphi_1(P)$ contenuto in $\varphi_1\big(\tilde{U}_1 \cap \tilde{U}_2\big)$. Si osserva che $\widetilde{\tau}_1 \notin U_1 \cap \gamma^{-1}U_2$, altrimenti $\gamma\widetilde{\tau}_1$ sarebbe un punto ellittico di $\delta_2^{-1}(\mathcal{N}_2)$, il quale non contiene punti ellittici.

Si considera allora $z = \varphi_1(P') \in \varphi_1\Big(\pi\big(U_1 \cap \gamma^{-1}U_2\big)\Big)$ con $P' = \pi(\tau')$ per un qualche $\tau' \in U_1 \cap \gamma^{-1}U_2$. Si ha allora che

$$\begin{aligned} {\varphi_2 \circ \varphi_1}^{-1}(z) = \varphi_2(P') = \varphi_2\big(\pi(\tau')\big) = \varphi_2\big(\pi(\gamma\tau')\big) = \\ = \exp\left(\frac{2\pi i \delta_2\gamma(\tau')}{h_2}\right) = \exp\left(\frac{2\pi i \delta_2\gamma {\delta_1}^{-1}(\delta_1\tau')}{h_2}\right) \\ = \exp\left(\frac{2\pi i \delta_2\gamma {\delta_1}^{-1}(z^{1/h_1})}{h_2}\right) . \end{aligned}$$

La mappa considerata è olomorfa ad esclusione, nel caso in cui $h_1 > 0$, del punto $z = 0$. Nel caso in cui si avesse $h_1 > 0$ è già stato osservato che $\widetilde{\tau}_1 \notin U_1 \cap \gamma^{-1}U_2$ e avendo $\varphi_1\big(\pi(\widetilde{\tau}_1)\big) = 0$ si deduce che $0 \notin \varphi_1\Big(\pi\big(U_1 \cap \gamma^{-1}U_2\big)\Big)$ da cui la mappa è olomorfa.

Si dimostra ora la compatibilità delle carte locali negli intorni delle cuspidi. Siano $\big(\tilde{U}_i, \varphi_i\big)$ due carte tali che $\tilde{U}_i = \pi(U_i)$ con $U_i = \delta_i^{-1}(\mathcal{N}_2)$ con $\delta_i^{-1}\infty = s_i$ di ampiezza h_i. Se $\tilde{U}_1 \cap \tilde{U}_2 \neq \varnothing$ si deve avere che $\gamma U_1 \cap U_2 \neq \varnothing$ per qualche $\gamma \in \Gamma$. Allora, come nelle osservazioni precedenti, si deve avere $\gamma s_1 = s_2$ da cui $h_1 = h_2$ e anche che $\delta_2\gamma{\delta_1}^{-1} = \pm T^m$ per qualche m. Restringendosi come prima a $\varphi_1\Big(\pi\big(U_1 \cap \gamma^{-1}U_2\big)\Big)$ si ottiene che

$${\varphi_2 \circ \varphi_1}^{-1}(z) = \exp\left(\frac{2\pi i \delta_2\gamma {\delta_1}^{-1}(\delta_1\tau)}{h_2}\right) = \exp\left(\frac{2\pi i(\delta_1\tau + m)}{h_2}\right) = e^{\frac{2\pi i m}{h_2}}\, z,$$

dato che $z = \exp\left(\frac{2\pi i(\delta_1\tau)}{h_1}\right)$, da cui ${\varphi_2 \circ \varphi_1}^{-1}$ è chiaramente olomorfa. □

3.3 Calcolo del genere di $X(\Gamma)$

Nei Paragrafi 3.1 e 3.2 è stato stabilito che, dato un sottogruppo di congruenza Γ, la curva modulare $X(\Gamma)$ è una superficie di Riemann compatta. Pertanto, dal punto di vista topologico, $X(\Gamma)$ è somma connessa di g tori, dove g è il genere di $X(\Gamma)$. In questo paragrafo viene calcolato tale genere.

Osservazione. Si osserva che il genere di $X\big(SL_2(\mathbb{Z})\big)$ è 0. Infatti considerando la sua rappresentazione con il dominio fondamentale $\mathcal{D}^*$, si ottiene che $X\big(SL_2(\mathbb{Z})\big)$ è omeomorfa ad un triangolo con due lati identificati e le due metà del terzo lato identificate. Questa identificazione rende $X\big(SL_2(\mathbb{Z})\big)$ omeomorfa alla sfera che ha genere 0.

Viene data la Formula di Riemann-Hurwitz.

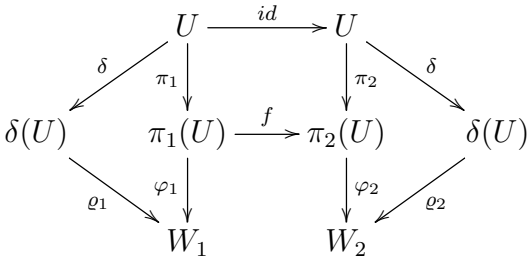
Teorema 2 (Formula di Riemann-Hurwitz)**.** *Sia $f\colon X \to Y$ una funzione olomorfa, non costante, tra due superficie di Riemann compatte X e Y con generi g_X, g_Y. Si indichi con e_x la ramificazione di f in ogni punto x di X e si ponga d il grado di f. Allora vale*

$$2g_X - 2 = d(2g_Y - 2) + \sum_{x \in X} (e_x - 1) \ .$$

La Formula di Riemann-Hurwitz mette in legame i generi di due superficie di Riemann compatte a patto di conoscere una funzione olomorfa tra esse. Viene data perciò, considerati due sottogruppi di congruenza Γ_1, Γ_2 con $\Gamma_1 \subseteq \Gamma_2$, una funzione olomorfa tra le curve modulari compatte ad essi associate.

Proposizione 3.5. *Dati due sottogruppi di congruenza Γ_1, Γ_2 con $\Gamma_1 \subseteq \Gamma_2$, la proiezione naturale $f\colon X(\Gamma_1) \to X(\Gamma_2),\ \Gamma_1\tau \mapsto \Gamma_2\tau$ è olomorfa.*

Dimostrazione. Si indicano con π_i le proiezioni $\mathbb{H}^* \to X(\Gamma_i)$. Sia $P = \pi_1(\widetilde{\tau}) \in X(\Gamma_1)$ e si consideri $\big(\pi_1(U), \varphi_1\big)$ la carta locale di $X(\Gamma_1)$ centrata in P e $\big(\pi_2(U), \varphi_2\big)$ la carta locale di $X(\Gamma_2)$ centrata in $f(P)$. Sia δ la trasformazione di $GL_2(\mathbb{C})$ tale che $\delta\widetilde{\tau} = \infty$ e siano ϱ_1 e ϱ_2 le mappe usate nella definizione delle carte locali φ_i. Considerato il fatto che $\pi_2(\tau) = \Gamma_2\tau = f(\Gamma_1\tau) = f\big(\pi_1(\tau)\big)$ si ha il seguente diagramma commutativo



che prova che $\varphi_2 \circ f \circ {\varphi_1}^{-1} = \varrho_2 \circ {\varrho_1}^{-1}$. Ora, se si ha $\widetilde{\tau} \in \mathbb{H}$, sono definiti i periodi h_i di $\widetilde{\tau}$ per Γ_1 e Γ_2 e si ottiene che $h_1 \mid h_2$. Allora, dato $z \in W_1$, si ha che

$$\varrho_2 \circ {\varrho_1}^{-1}(z) = (z^{1/h_1})^{h_2} = z^{h_2/h_1}$$

che è olomorfa. Se invece si ha $\widetilde{\tau} \in \hat{\mathbb{Q}}$, si ottiene che le ampiezze h_i di $\widetilde{\tau}$ per Γ_1 e Γ_2 verificano invece $h_2 \mid h_1$. Allora, dato $z \in W_1$, si ha che

$$\varrho_2 \circ {\varrho_1}^{-1}(z) = \exp\left(\frac{2\pi i {\varrho_1}^{-1}(z)}{h_2}\right) = \left(\exp\left(\frac{2\pi i {\varrho_1}^{-1}(z)}{h_1}\right)\right)^{\frac{h_1}{h_2}} = z^{\frac{h_1}{h_2}}$$

da cui si ottiene che $\varrho_2 \circ {\varrho_1}^{-1}$ è olomorfa. □

Si calcola ora il grado della funzione olomorfa f data nella Proposizione 3.5.

Proposizione 3.6. *Il grado della funzione olomorfa f data nella Proposizione 3.5 è*

$$\deg f = [\{\pm\mathbb{1}\}\Gamma_2 \colon \{\pm\mathbb{1}\}\Gamma_1] = \begin{cases} [\Gamma_2 \colon \Gamma_1]/2 & \textit{se } -\mathbb{1} \in \Gamma_2, -\mathbb{1} \notin \Gamma_1 \\ [\Gamma_2 \colon \Gamma_1] & \textit{altrimenti.} \end{cases}$$

Dimostrazione. Si consideri un punto semplice $\tau \in \mathbb{H}$ per Γ_2. Considerato il fatto che $\{\pm\mathbb{1}\}\Gamma_2 = \bigcup_j \{\pm\mathbb{1}\}\Gamma_1\gamma_j$, per alcuni $\gamma_j \in \Gamma_2$, si ottiene che $\{\pm\mathbb{1}\}\Gamma_2\tau = \bigcup_j \{\pm\mathbb{1}\}\Gamma_1\gamma_j\tau$. Si distinguono quindi i casi $-\mathbb{1} \in \Gamma_1$, $-\mathbb{1} \in \Gamma_2 \backslash \Gamma_1$ e $-\mathbb{1} \notin \Gamma_2$:

$-\mathbb{1} \in \mathbf{\Gamma_1}$ **-** Si ha che $\Gamma_2\tau = \{\pm\mathbb{1}\}\Gamma_2\tau = \bigcup_j \{\pm\mathbb{1}\}\Gamma_1\gamma_j\tau = \bigcup_j \Gamma_1\gamma_j\tau$, da cui si ottiene che $f^{-1}(\Gamma_2\tau) = \{\Gamma_1\gamma_j\tau\}$ che ha cardinalità $[\Gamma_2 \colon \Gamma_1]$.

$-\mathbb{1} \in \mathbf{\Gamma_2 \backslash \Gamma_1}$ **-** Si ha che $\Gamma_2\tau = \{\pm\mathbb{1}\}\Gamma_2\tau = \bigcup_j \{\pm\mathbb{1}\}\Gamma_1\gamma_j\tau = \bigcup_j \Gamma_1(\pm\gamma_j)\tau$, da cui si ottiene che $f^{-1}(\Gamma_2\tau) = \{\Gamma_1(\pm\gamma_j)\tau\}$ che ha cardinalità $[\Gamma_2 \colon \Gamma_1]/2$. Infatti tutti i $\pm\gamma_j$ rappresentano classi laterali distinte ma, avendo che$-\gamma_j\tau = \gamma_j\tau$, rappresentano la stessa antiimmagine.

$-\mathbb{1} \notin \mathbf{\Gamma_2}$ **-** Si ha che $[\Gamma_2 \colon \Gamma_1] = [\{\pm\mathbb{1}\}\Gamma_2 \colon \{\pm\mathbb{1}\}\Gamma_1]$ e che $\Gamma_2 = \bigcup_j \Gamma_1\gamma_j$. Allora si ottiene che $f^{-1}(\Gamma_2\tau) = \{\Gamma_1\gamma_j\tau\}$ che ha cardinalità $[\Gamma_2 \colon \Gamma_1]$.

Essendo che la cardinalità della fibra è stata calcolata per tutti tranne finiti punti di $X(\Gamma_2)$, la formula ottenuta rappresenta effettivamente il grado di f. □

Osservazione. Nella dimostrazione della Proposizione 3.6 è stato ottenuto anche che gli unici punti di ramificazione per f possono essere eventualmente le antiimmagini di punti ellittici o cuspidi di Γ_2. Infatti se $\tau \in \mathbb{H}$ è semplice per Γ_2 allora $|f^{-1}(\Gamma_2\tau)| = \deg f$ che implica che tutte le sue antiimmagini hanno ramificazione 1.

Si calcolano allora gli indici di ramificazione e_x di f in tutti i punti $x \in X(\Gamma_1)$.

Proposizione 3.7. *Sia $x = \Gamma_1\tau \in X(\Gamma_1)$. Si ha che*

$$e_x = [\{\pm\mathbb{1}\}\Gamma_{2,\tau} \colon \{\pm\mathbb{1}\}\Gamma_{1,\tau}] \,.$$

Dimostrazione. Si ricorda che dimostrando la Proposizione 3.5 è stato ottenuto che la localizzazione di f nell'intorno di un punto $x \in X(\Gamma_1)$ è $\varrho_2 \circ {\varrho_1}^{-1}(z)$.

Se $x = \pi_1(\tau)$ con $\tau \in \mathbb{H}$, la localizzazione è della forma $\varrho_2 \circ {\varrho_1}^{-1}(z) = z^{h_2/h_1}$. Questo implica che $e_x = h_2/h_1 = [\{\pm\mathbb{1}\}\Gamma_{2,\tau} \colon \{\pm\mathbb{1}\}\Gamma_{1,\tau}]$.

Se invece $x = \pi_1(s)$ con $s \in \hat{\mathbb{Q}}$, è stato ottenuto che $\varrho_2 \circ {\varrho_1}^{-1}(z) = z^{h_1/h_2}$. Questo implica che $e_x = h_1/h_2 = [\{\pm\mathbb{1}\}\Gamma_{2,\tau} \colon \{\pm\mathbb{1}\}\Gamma_{1,\tau}]$. □

Per calcolare il genere di una generica curva modulare $X(\Gamma)$ si specializza la discussione ponendo $\Gamma_2 = SL_2(\mathbb{Z})$ e $\Gamma_1 = \Gamma$.

Osservazione. Si indichino con y_2, y_3, y_∞ i punti ellittici di periodo 2 e 3 e la cuspide di $X\big(SL_2(\mathbb{Z})\big)$. Gli eventuali punti di ramificazione di f devono essere contenuti nelle antiimmagini di y_2, y_3, y_∞ ma non necessariamente ogni elemento di $f^{-1}(y_h)$ è un punto di ramificazione.

Proposizione 3.8. *Sia Γ un sottogruppo di congruenza. Siano ε_2 il numero di punti ellittici di periodo 2 in $X(\Gamma)$, ε_3 il numero di punti ellittici di periodo 3 in $X(\Gamma)$ e ε_∞ il numero di cuspidi in $X(\Gamma)$. Il genere g di $X(\Gamma)$ è*

$$g = 1 + \frac{1}{12}\Big([SL_2(\mathbb{Z})\colon \{\pm\mathbb{1}\}\Gamma] - 3\varepsilon_2 - 4\varepsilon_3 - 6\varepsilon_\infty\Big) .$$

Dimostrazione. Si consideri come prima la proiezione naturale

$$f\colon X(\Gamma) \to X(SL_2(\mathbb{Z})),\ \Gamma\tau \mapsto SL_2(\mathbb{Z})\tau$$

di cui si indica il grado con d.

L'antiimmagine tramite f di y_2 è costituita da ε_2 punti ellittici di $X(\Gamma)$ e $|f^{-1}| - \varepsilon_2$ punti semplici di $X(\Gamma)$. Come già osservato in questo paragrafo i punti ellittici di $X(\Gamma)$ hanno indice di ramificazione $h_{SL_2(\mathbb{Z})}/h_\Gamma = 2/2 = 1$, mentre i punti semplici hanno indice di ramificazione $h_{SL_2(\mathbb{Z})}/h_\Gamma = 2/1 = 2$. Si ottiene che

$$d = \sum_{x \in f^{-1}(y_2)} e_x = 2\big(|f^{-1}(y_2)| - \varepsilon_2\big) + 1\varepsilon_2$$

da cui si ricava, applicando la formula due volte, che

$$\sum_{x \in f^{-1}(y_2)} (e_x - 1) = 2\big(|f^{-1}(y_2)| - \varepsilon_2\big) + \varepsilon_2 - |f^{-1}(y_2)| =$$
$$= |f^{-1}(y_2)| - \varepsilon_2 = \frac{1}{2}\big(d - \varepsilon_2\big) .$$

Analogamente, considerando l'antiimmagine di y_3, si ottiene che

$$\sum_{x \in f^{-1}(y_3)} (e_x - 1) = \frac{2}{3}\big(d - \varepsilon_3\big) .$$

L'antiimmagine di y_∞ è costituita interamente dalle cuspidi di $X(\Gamma)$ e allora si ottiene che

$$\sum_{x \in f^{-1}(y_\infty)} (e_x - 1) = d - |f^{-1}(y_\infty)| = d - \varepsilon_\infty .$$

Complessivamente, avendo che gli unici punti di $X(\Gamma)$ con ramificazione eventualmente diversa da 1 sono nelle antiimmagini di y_2, y_3, y_∞ ed avendo, come già osservato, che il

genere di $X(SL_2(\mathbb{Z}))$ è 0, si ottiene che

$$\begin{aligned} g &= 1 + \frac{1}{2}\Big(-2d + \sum_{x \in X(\Gamma)} (e_x - 1)\Big) = \\ &= 1 + \frac{1}{2}\Big(-2d + \sum_{x \in f^{-1}(y_2)} (e_x - 1) + \sum_{x \in f^{-1}(y_3)} (e_x - 1) + \sum_{x \in f^{-1}(y_\infty)} (e_x - 1)\Big) = \\ &= 1 + \frac{1}{2}\Big(-2d + \frac{1}{2}(d - \varepsilon_2) + \frac{2}{3}(d - \varepsilon_3) + d - \varepsilon_\infty) = \\ &= 1 + \frac{1}{12}\Big(d - 3\varepsilon_2 - 4\varepsilon_3 - 6\varepsilon_\infty\Big) \end{aligned}$$

e usando la Proposizione 3.6 si conclude con la formula cercata. □

Capitolo 4

Curve ellittiche su $\mathbb{C}$

In questo capitolo verranno introdotte le curve ellittiche su $\mathbb{C}$ e le mappe tra di esse. Viene data inizialmente la loro rappresentazione come tori complessi e poi brevemente discussa l'equivalenza con la rappresentazione di cubiche lisce su $\mathbb{C}$.

4.1 Reticoli e tori complessi

In questo paragrafo verranno definiti i tori complessi e le relative mappe che rispettano la loro struttura, dette isogenie.

Definizione. Un *reticolo* in $\mathbb{C}$ è un sottogruppo additivo di $\mathbb{C}$ del tipo $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ con $\omega_1, \omega_2 \in \mathbb{C}$ linearmente indipendenti su $\mathbb{R}$.

Proposizione 4.1. *Due reticoli $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ e $\mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$ sono uguali se e solo se esiste $\gamma \in GL_2(\mathbb{Z})$ tale che*

$$\begin{pmatrix} \omega_2' \\ \omega_1' \end{pmatrix} = \gamma \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix} . \tag{4.1}$$

Dimostrazione. Si suppone prima l'esistenza di $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$. La condizione 4.1 corrisponde a

$$\begin{aligned} \omega_2' &= a\omega_2 + b\omega_1 \\ \omega_1' &= c\omega_2 + d\omega_1 \end{aligned}$$

e tali equazioni implicano chiaramente che $\mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2' \subseteq \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Poiché la matrice γ è invertibile, si ha che

$$\gamma^{-1} \begin{pmatrix} \omega_2' \\ \omega_1' \end{pmatrix} = \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}$$

da cui, analogamente a prima, si ottiene che $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subseteq \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$.

Per dimostrare l'altra implicazione, si ponga $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$. Si deve avere allora che $\omega_1', \omega_2' \in \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ e che $\omega_1, \omega_2 \in \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$, ottendendo che esistono dei

coefficienti $a, b, c, d, e, f, g, h \in \mathbb{Z}$ tali che

$$\begin{aligned}\omega_2' &= a\omega_2 + b\omega_1 \\ \omega_1' &= c\omega_2 + d\omega_1 \\ \omega_2 &= e\omega_2' + f\omega_1' \\ \omega_1 &= g\omega_2' + h\omega_1' \,.\end{aligned}$$

Questo implica che esistono due matrici $\gamma, \delta \in M_2(\mathbb{Z})$ tali che

$$\begin{aligned}\begin{pmatrix}\omega_1' \\ \omega_2'\end{pmatrix} &= \gamma \begin{pmatrix}\omega_1 \\ \omega_2\end{pmatrix} \\ \begin{pmatrix}\omega_1 \\ \omega_2\end{pmatrix} &= \delta \begin{pmatrix}\omega_1' \\ \omega_2'\end{pmatrix} \,.\end{aligned}$$

Dato che (ω_1, ω_2) e (ω_1', ω_2') sono entrambe basi di $\mathbb{C}$ su $\mathbb{R}$, si può dedurre che $\gamma^{-1} = \delta$ da cui γ e δ sono matrici invertibili in $M_2(\mathbb{Z})$ ovvero $\gamma, \delta \in GL_2(\mathbb{Z})$. □

Osservazione. Dato un reticolo $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, potendo eventualmente scambiare ω_1 e ω_2 con la matrice $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right) \in GL_2(\mathbb{Z})$, si può sempre supporre che $\omega_2/\omega_1 \in \mathbb{H}$. Infatti, non si può avere $\omega_2/\omega_1 \in \mathbb{R}$, dato che ω_1 e ω_2 sono linearmente indipendenti su $\mathbb{R}$, quindi almeno uno tra ω_1/ω_2 e ω_2/ω_1 deve appartenere ad $\mathbb{H}$.

Osservazione. Si supponga che i reticoli della Proposizione 4.1 siano tali che $\omega_2/\omega_1 \in \mathbb{H}$ e $\omega_2'/\omega_1' \in \mathbb{H}$, il che è possibile per quanto evidenziato nell'osservazione precedente. Allora la matrice γ della proposizione è tale che $\gamma \in SL_2(\mathbb{Z})$. Questo risultato deriva dal fatto che le condizioni $\omega_2/\omega_1, \omega_2'/\omega_1' \in \mathbb{H}$ impone un orientamento delle basi $\{\omega_1, \omega_2\}, \{\omega_1', \omega_2'\}$ su $\mathbb{R}$ e la matrice γ deve preservare tale orientamento. Di conseguenza si deve avere $\det \gamma = 1$.

Definizione. Un *toro complesso* è un quoziente $\mathbb{C}/\Lambda$, dove Λ è un reticolo in $\mathbb{C}$.

Un toro complesso ha una struttura di gruppo abeliano dato che è quoziente di un gruppo abeliano per un sottogruppo. Osservando che Λ è un sottogruppo discreto di $\mathbb{C}$, il quale agisce transitivamente su $\mathbb{C}$, si possono usare i risultati del Paragrafo 1.3 per ottenere che $\mathbb{C}/\Lambda$, con la topologia quoziente, è uno spazio di Hausdorff. Inoltre, dato un reticolo $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, si può facilmente riconoscere che l'insieme

$$\{\, t\omega_1 + s\omega_2 \mid t, s \in [0, 1] \,\}$$

è un dominio fondamentale per $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, detto parallelogramma fondamentale. Si veda la Figura 4.1.

Osservazione. Considerando un parallelogramma fondamentale per un reticolo Λ, con le opportune leggi di identificazione dei bordi, è chiaro che il toro complesso $\mathbb{C}/\Lambda$ è in effetti un toro dal punto di vista topologico. Dotando $\mathbb{C}/\Lambda$ di una struttura di superficie di Riemann si otterrà che esistono diversi tori complessi non biolomorfi tra loro.

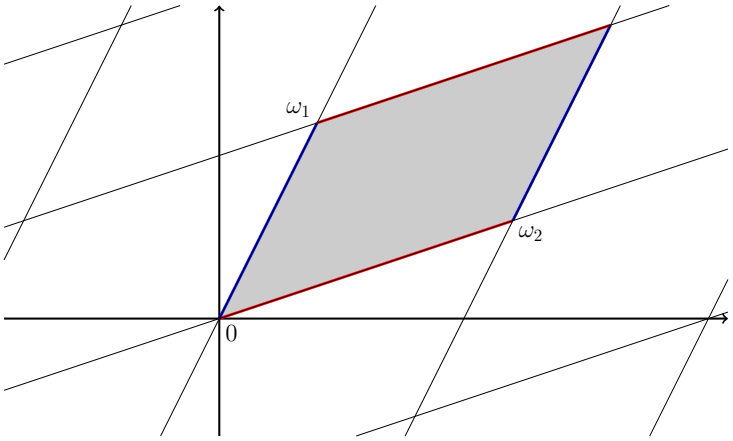


Figura 4.1: Un parallelogramma fondamentale per $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$.

Definizione. Sia $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ un reticolo e sia $\pi\colon \mathbb{C} \to \mathbb{C}/\Lambda$ la proiezione naturale. Si dota il toro complesso $\mathbb{C}/\Lambda$ dell'atlante

$$\left\{\pi(U_z), (\pi|_{U_z})^{-1}\right\}_{z\in\mathbb{C}}$$

con U_z la palla centrata in z di raggio $\min\big(|\omega_1|, |\omega_2|, |\omega_1+\omega_2|, |\omega_1-\omega_2|\big)$.

Osservazione. Siano $\mathbb{C}/\Lambda$ e $\mathbb{C}/\Lambda'$ due tori complessi con la struttura di superficie di Riemann sopra definita. Dati $m, b \in \mathbb{C}$ tali che $m\Lambda \subseteq \Lambda'$, la mappa

$$\varphi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda',\ \varphi(z+\Lambda) = mz + b + \Lambda'$$

è olomorfa.

Proposizione 4.2. *Sia $\varphi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ una funzione olomorfa tra due tori complessi. Allora esistono $m, b \in \mathbb{C}$ tali che $m\Lambda \subseteq \Lambda'$ e*

$$\varphi(z+\Lambda) = mz + b + \Lambda',\ \forall z + \Lambda \in \mathbb{C}/\Lambda\ .$$

La mappa φ è un isomorfismo se e solo se $m\Lambda = \Lambda'$.

Dimostrazione. Si osserva che le proiezioni naturali $\mathbb{C} \xrightarrow{p} \mathbb{C}/\Lambda$ e $\mathbb{C} \xrightarrow{p'} \mathbb{C}/\Lambda'$ sono i rivestimenti universali di $\mathbb{C}/\Lambda$ e $\mathbb{C}/\Lambda'$ rispettivamente. È possibile allora sollevare φ ad una mappa continua $\tilde{\varphi}$ tale che il seguente diagramma commuti

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{\varphi}} & \mathbb{C} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ \mathbb{C}/\Lambda & \xrightarrow{\varphi} & \mathbb{C}/\Lambda' \end{array}$$

Il sollevamento $\tilde{\varphi}$ risulta olomorfo, perciò anche $f_\lambda(z) = \tilde{\varphi}(z+\lambda) - \tilde{\varphi}(z)$, dato un qualsiasi $\lambda \in \Lambda$, è una funzione olomorfa. Dovendo avere che $\tilde{\varphi}(z+\lambda) + \Lambda' = \tilde{\varphi}(z) + \Lambda'$ per rispettare

il quoziente modulo Λ, si deduce che $f_\lambda(\mathbb{C}) \subseteq \Lambda'$. Allora f_λ è una mappa continua con immagine in un insieme discreto, da cui si ottiene che f_λ è costante. Considerando la derivata di f_λ, si deduce che $\tilde{\varphi}'(z+\lambda) = \tilde{\varphi}'(z)$, ottenendo complessivamente che $\tilde{\varphi}'$ è una funzione Λ-periodica e quindi limitata. Per il Teorema di Liouville, avendo che $\tilde{\varphi}'$ è una funzione intera limitata, si ottiene che $\tilde{\varphi}'$ è costante. La funzione $\tilde{\varphi}$ deve assumere quindi la forma

$$\tilde{\varphi}(z) = mz + b, \ \forall z \in \mathbb{C} \ \text{ per qualche } m, b \in \mathbb{C} \ .$$

Imponendo ancora la condizione $\tilde{\varphi}(z+\lambda) + \Lambda' = \tilde{\varphi}(z) + \Lambda'$ per ogni $\lambda \in \Lambda$, si deduce che $m\lambda \in \Lambda'$ per ogni $\lambda \in \Lambda$, ovvero che $m\Lambda \subseteq \Lambda'$, come si voleva.

Osservazione. Se si avesse $m\Lambda \subsetneq \Lambda'$, φ non potrebbe essere un isomorfismo. Infatti esisterebbe qualche $z \in \Lambda'$ tale che $z/m \notin \Lambda$. In tal caso si otterrebbe che

$$\varphi(z/m + \Lambda) = z + b + \Lambda' = b + \Lambda' = \varphi(\Lambda)$$

e φ non sarebbe iniettiva.

Supponendo che $m\Lambda = \Lambda'$, si ha anche $\frac{1}{m}\Lambda' = \Lambda$. Si definisce allora la mappa

$$\psi \colon \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda, \ \psi(z + \Lambda') = \frac{z}{m} - \frac{b}{m} + \Lambda \ .$$

Si osserva che $\psi = \varphi^{-1}$, da cui si ottiene che φ è un isomorfismo. □

Definizione. Siano $\mathbb{C}/\Lambda$ e $\mathbb{C}/\Lambda'$ due tori complessi. Un'*isogenia* tra $\mathbb{C}/\Lambda$ e $\mathbb{C}/\Lambda'$ è una mappa olomorfa non costante $\varphi \colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ che sia anche un omomorfismo di gruppi.

Si dirà che due tori complessi sono *equivalenti* se esiste un'isogenia tra di essi che sia anche un isomorfismo di gruppi.

Osservazione. Poiché un'isogenia φ è una funzione olomorfa, l'insieme dei suoi zeri, ovvero $\ker\varphi$, deve essere discreto nel dominio. Dato che un toro complesso è compatto, si ottiene che $\ker\varphi$ è finito per ogni isogenia φ.

Proposizione 4.3. *Sia $\varphi \colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ una funzione olomorfa tra due tori complessi, allora φ è un'isogenia se e solo se $\varphi(0) = 0$.*

Dimostrazione. Si rappresenta φ nella forma data dalla Proposizione 4.2

$$\varphi(z + \Lambda) = mz + b + \Lambda' \ \text{ con } m\Lambda \subseteq \Lambda', \ m, b \in \mathbb{C} \ .$$

Chiaramente se φ è un'isogenia deve valere $\varphi(0) = 0$. Se $\varphi(0) = 0$, si ottiene che $b \in \Lambda'$ e anche che $\varphi(z + \Lambda) = mz + \Lambda'$. Allora si ha

$$\varphi(z + \Lambda + w + \Lambda) = m(z + w) + \Lambda' = \varphi(z + \Lambda) + \varphi(w + \Lambda)$$

che implica che φ è omomorfismo di gruppi e quindi è anche un'isogenia. □

Un risultato che sarà particolarmente utile nel Capitolo 5 è la Proposizione 4.4.

Proposizione 4.4. *Sia $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ un reticolo con $\omega_2/\omega_1 \in \mathbb{H}$ e si ponga $\tau = \omega_2/\omega_1$ e $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$. I tori complessi $\mathbb{C}/\Lambda$ e $\mathbb{C}/\Lambda_\tau$ sono equivalenti.*

Dimostrazione. Dato che $\Lambda_\tau = (\frac{1}{\omega_1})\Lambda$, dalla Proposizione 4.2 si ottiene che la mappa $\varphi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda_\tau$, definita da $\varphi(z+\Lambda) = z/\omega_1 + \Lambda_\tau$, è un'isogenia iniettiva. □

Osservazione. Unendo i risultati delle Proposizioni 4.1 e 4.4 si ottiene che due tori complessi $\mathbb{C}/\Lambda_\tau$, $\mathbb{C}/\Lambda_{\tau'}$ sono equivalenti se e solo se $\tau' = \gamma\tau$ con $\gamma \in GL_2(\mathbb{Z})$.

Verranno date nel corso del paragrafo due classi notevoli di isogenie: la moltiplicazione per interi e i quozienti ciclici.

Definizione. Siano $N \geqslant 1$ un intero e Λ un reticolo. La *moltiplicazione per N* è l'isogenia

$$[N]\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda,\ z+\Lambda \mapsto Nz+\Lambda\ .$$

Definizione. Sia dato un intero $N \geqslant 1$. Il *sottogruppo di N-torsione* di $E = \mathbb{C}/\Lambda$ è

$$E[N] = \ker[N]\ .$$

Osservazione. Siano $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ e $E = \mathbb{C}/\Lambda$. Si osserva che

$$E[N] = \left\langle \frac{\omega_1}{N} + \Lambda \right\rangle \times \left\langle \frac{\omega_2}{N} + \Lambda \right\rangle \simeq (\mathbb{Z}/N\mathbb{Z})^2\ .$$

Osservazione. Siano $N \geqslant 1$ un intero e $E = \mathbb{C}/\Lambda$ un toro complesso. Si fissi $C \leqslant E[N]$ un sottogruppo ciclico del gruppo di N-torsione. Gli elementi di C sono classi $\{z+\Lambda\}$ quindi, considerandone l'unione, si può interpretare C come un reticolo tale che $\Lambda \subseteq C$.

Definizione. Siano $N \geqslant 1$ un intero, $E = \mathbb{C}/\Lambda$ un toro complesso e $C \leqslant E[N]$ un sottogruppo ciclico del gruppo di N-torsione. Un *quoziente ciclico* è l'isogenia

$$\pi\colon \mathbb{C}/\Lambda \mapsto \mathbb{C}/C,\ z+\Lambda \mapsto z+C\ .$$

Proposizione 4.5. *Sia $\varphi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ un'isogenia. Si ha il seguente diagramma commutativo*

$$\mathbb{C}/\Lambda \xrightarrow{[N]} \mathbb{C}/\Lambda \xrightarrow{\pi} \mathbb{C}/C \xrightarrow{\simeq} \mathbb{C}/\Lambda'$$
$$\mathbb{C}/\Lambda \xrightarrow[\varphi]{} \mathbb{C}/\Lambda'$$

dove $[N]$ è la moltiplicazione per un opportuno intero N, π è un opportuno quoziente ciclico, e $\mathbb{C}/C$ è isomorfo a $\mathbb{C}/\Lambda$.

Dimostrazione. Si veda [4]. □

Definizione. Sia N un intero positivo e si indichi con $\sqrt[N]{1}$ il gruppo delle radici N-esime dell'unità. Siano $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, con $\omega_2/\omega_1 \in \mathbb{H}$ e $E = \mathbb{C}/\Lambda$. Il *Weil pairing* è

$$e_N\colon E[N] \times E[N] \to \sqrt[N]{1},\ e_N(P,Q) = \exp\left(\frac{2\pi i \det\gamma}{N}\right)$$

con $\gamma \in M_2(\mathbb{Z}/N\mathbb{Z})$ tale che

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} \omega_1/N + \Lambda \\ \omega_2/N + \Lambda \end{pmatrix}\ .$$

Di seguito sono riportate sinteticamente alcune proprietà del Weil pairing che saranno determinanti per il suo utilizzo nel Capitolo 5. Non verrà data una dimostrazione di queste proprietà, per la quale si può consultare [4] oppure anche [11], contenente un approccio maggiormente astratto.

Proposizione 4.6. *Siano Λ un reticolo, N un intero positivo e si ponga $E = \mathbb{C}/\Lambda$.*

1. *La definizione di e_N è indipendente dalla base di Λ (fintanto che questa è orientata come richiesto dalla definizione).*
2. *Se P, Q generano $E[N]$, allora $e_N(P, Q)$ è una radice primitiva dell'unità.*
3. *Il Weil pairing e_N è bilineare, alternante e non degenere.*
4. *Il seguente diagramma commuta*

$$\begin{array}{ccc} E[dN] \times E[dN] & \xrightarrow{e_{dN}} & \sqrt[dN]{1} \\ \Big\downarrow{\scriptstyle d} & & \Big\downarrow{\scriptstyle d} \\ E[N] \times E[N] & \xrightarrow{e_N} & \sqrt[N]{1} \end{array}$$

5. *L'isomorfismo di tori complessi preserva il Weil pairing.*

4.2 Tori complessi e curve ellittiche

In questo paragrafo si stabilisce una forte corrispondenza tra tori complessi e curve ellittiche in modo da poterli complessivamente trattare come il medesimo oggetto. Verranno riportati solo i risultati principali senza una dimostrazione. Per una discussione più completa si veda [9].

Definizione. Sia $f \in \mathbb{C}[X]$ un polinomio di terzo grado con tutte le radici distinte. Una *curva ellittica* su $\mathbb{C}$ è una superficie di Riemann definita sull'insieme

$$\left\{ (x, y) \in \mathbb{C}^2 \;\middle|\; y^2 = f(x) \right\} \cup \{\infty\}$$

con la specifica di un punto sulla curva denotato con O.

Si riporta di seguito un risultato della teoria delle superficie di Riemann che introduce la discussione successiva.

Teorema 3. *Ogni superficie di Riemann compatta di genere* 1 *è biolomorfa ad una curva ellittica.*

Da questo si deduce che ogni toro complesso è biolomorfo ad un'opportuna curva ellittica. Le Proposizioni 4.7 e 4.8 daranno un risultato più preciso.

Su ciascuna curva ellittica (E, O) esiste una legge di gruppo abeliano, che verrà denotata con $\oplus$. Prima di darne la definizione si riporta una versione del Teorema di Bézout limitata alle curve piane su $\mathbb{C}$.

Teorema 4 (di Bézout)**.** *Siano $\mathscr{C}, \mathscr{D}$ due curve proiettive piane su $\mathbb{C}$ che non abbiano componenti comuni. La somma delle molteplicità dei punti di intersezione è uguale al prodotto dei gradi di $\mathscr{C}$ e $\mathscr{D}$.*

Si dà ora la definizione di $\oplus$: $E \times E \to E$. Considerati $P, Q \in E$, si denoti con R il terzo punto appartenente ad E e alla retta passante per P e Q. Il punto $P \oplus Q \in E$ è il terzo punto appartenente ad E e alla retta passante per O e R. Il terzo punto è univocamente determinato dato che per il Teorema di Bézout l'intersezione tra una retta e una curva di grado tre, quali sono le curve ellittiche, è costituita da tre punti contati con la loro molteplicità. Nel caso in cui due punti coincidano, ad esempio se $P = Q$ o $O = R$, si deve considerare la retta tangente al punto in questione.

Definizione. Due curve ellittiche $(E, O), (E', O')$ sono *equivalenti* se esiste un biolomorfismo f tale che $f(O) = O'$.

Come si vedrà alla fine del paragrafo la condizione $f(O) = O'$ è necessaria per garantire che (E, O) e (E', O') siano isomorfi come gruppi abeliani.

Definizione. Sia Λ un reticolo. La *funzione $\wp$ di Weierstrass* associata a Λ è

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right), \ z \in \mathbb{C} \setminus \Lambda \ .$$

Osservazione. Si osserva che la derivata di $\wp_\Lambda$ è Λ-periodica

$$\wp'_\Lambda(z) = -2 \sum_{\omega \in \Lambda} \left(\frac{1}{(z-\omega)^3} \right) .$$

Questo, unito al fatto che $\wp_\Lambda$ è una funzione pari, implica che $\wp_\Lambda$ è Λ-periodica.

Nella la Proposizione 4.7 verranno usate le *serie di Eisenstein*, anche se solo come coefficienti. Queste fanno parte della teoria delle forme modulari e non verranno trattate in questa tesi.

Definizione. Si fissi un intero pari $k > 2$. La *serie di Eisenstein* di peso k, valutata in un reticolo Λ, è

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

Il fatto che $\wp$ sia una funzione Λ-periodica permette di considerarla come una funzione definita sul toro complesso $\mathbb{C}/\Lambda$. Questo permette, a seguito della Proposizione 4.7, di definire una funzione dal toro complesso $\mathbb{C}/\Lambda$ ad una curva ellittica.

Proposizione 4.7. *Si hanno le seguenti proprietà della funzione $\wp_\Lambda$.*

1. *La serie di Laurent in $W \setminus \{0\}$ di $\wp_\Lambda$ è*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n=0}^{\infty} (2n+1) G_{2n+2}(\Lambda) z^{2n}$$

con W la palla centrata in zero di raggio $\min\big(|\omega_1|, |\omega_2|, |\omega_1 + \omega_2|, |\omega_1 - \omega_2|\big)$.

2. *Vale la seguente relazione*

$$(\wp'_\Lambda)^2 = 4(\wp_\Lambda)^3 - 60G_4(\Lambda)\wp_\Lambda - 140G_6(\Lambda)\ . \tag{4.2}$$

3. *Sia* $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ *e si ponga* $\omega_3 = \omega_1 + \omega_2$*. L'equazione precedente*

$$y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$$

è equivalente all'equazione

$$y^2 = 4(x - \wp(\omega_1/2))(x - \wp(\omega_2/2))(x - \wp(\omega_3/2))$$

in cui il polinomio sulla destra ha tre radici distinte.

In particolare la Proposizione 4.7 mostra che esiste una biiezione tra il toro complesso $\mathbb{C}/\Lambda$ e la curva ellittica di equazione $y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$, che sarà denotata da (E_Λ, ∞), definita da

$$z + \Lambda \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z)),\ \text{per}\ z \in \mathbb{C}\backslash\Lambda\ \ \text{e}\ \ \Lambda \mapsto \infty\ .$$

Per ora è stato mostrato che ad ogni toro complesso è associata una determinata curva ellittica isomorfa ad esso, cosa che si poteva dedurre anche dal Teorema 3. Si mostra, con la Proposizione 4.8, che vale anche un risultato inverso.

Proposizione 4.8. *Sia* (E, ∞) *una curva ellittica definita dell'equazione*

$$y^2 = 4x^3 - a_2x - a_3,\ \textit{con}\ a_2^3 - 27a_3^2 \neq 0\ .$$

Esiste un reticolo Λ *tale che* $60G_4(\Lambda) = a_2$ *e* $140G_6(\Lambda) = a_3$*, per cui* $E = E_\Lambda$*.*

Proposizione 4.9. *La* $\wp_\Lambda$ *trasporta la somma di* $\mathbb{C}/\Lambda$ *nella somma* $\oplus$ *di* (E_Λ, ∞)

$$\wp_\Lambda(z + w) = \wp_\Lambda(z) \oplus \wp_\Lambda(w)\ .$$

Questo mostra che, oltre a essere isomorfi come superficie di Riemann, i tori complessi e le curve ellittiche sono isomorfi come gruppi abeliani. Per questo motivo, soprattutto nel capitolo successivo, le espressioni "tori complessi" e "curve ellittiche" saranno usate intercambiabilmente.

Capitolo 5

Spazi di moduli di curve ellittiche

Lo scopo di uno spazio di moduli è rappresentare le classi di equivalenza di un determinato oggetto e i modi in cui queste possono variare in modo regolare. In questo contesto per regolarità si intende analiticità, quindi uno spazio di moduli deve rappresentare famiglie analitiche dell'oggetto in considerazione. In questo capitolo si introducono quindi i concetti di famiglia analitica e spazio di moduli. Vengono poi discusse le condizioni per cui le curve modulari $Y(N)$, $Y_1(N)$, $Y_0(N)$ sono spazi di moduli di curve ellittiche con opportune condizioni sui punti di N-torsione.

Notazione. Data $\pi\colon \mathcal{E} \to T$ una funzione olomorfa surietiva di rango massimo tra due varietà analitiche, si userà la notazione $\mathcal{E}_t = \pi^{-1}(t)$.

5.1 Famiglie di curve ellittiche e spazi di moduli

In questo paragrafo si definiscono i problemi di moduli e gli spazi di moduli corrispondenti. Si definiscono poi le famiglie di curve ellittiche con le opportune strutture di N-livello associate. Si introducono quindi i problemi di moduli associati a ciascuna struttura di N-livello.

Definizione. Un *problema di moduli* è un funtore controvariante dalla categoria delle varietà analitiche su $\mathbb{C}$ alla categoria degli insiemi.

Definizione. Sia $\mathcal{F}$ un problema di moduli. Uno *spazio di moduli fine* per $\mathcal{F}$ è una varietà analitica M tale che esiste un $\mathcal{U} \in \mathcal{F}(M)$, detto *oggetto universale*, con la seguente proprietà: per ogni varietà analitica T e ogni $\mathcal{E} \in \mathcal{F}(T)$ esiste un'unica mappa olomorfa $f\colon T \to M$ tale che $\mathcal{E} = \mathcal{F}(f)(\mathcal{U})$.

Proposizione 5.1. *M è uno spazio di moduli fine per $\mathcal{F}$ se e solo se esiste un isomorfismo naturale $\mathcal{F} \simeq Hom(\_, M)$, ovvero se e solo se M è una rappresentazione di $\mathcal{F}$.*

Dimostrazione. Se M è uno spazio di moduli per $\mathcal{F}$ con oggetto universale $\mathcal{U}$, la posizione

$$Hom(T, M) \ni f \mapsto \mathcal{F}(f)(\mathcal{U}) \in \mathcal{F}(T)$$

è una trasformazione naturale.

Supposto invece di avere una trasformazione naturale $\mathcal{F} \simeq Hom(\_, M)$, si ponga $\mathcal{U}$ l'immagine in $\mathcal{F}(M)$ dell'identità $id_M \in Hom(M, M)$. Data ora $\mathcal{E} \in \mathcal{F}(T)$, esiste un'unica $j \in Hom(T, M)$ che corrisponde a $\mathcal{E}$. Osservando il seguente diagramma commutativo

$$\begin{array}{ccc} \mathcal{F}(T) & \xleftarrow[\mathcal{F}(j)]{} & \mathcal{F}(M) \\ \updownarrow\wr & & \updownarrow\wr \\ Hom(T, M) & \xleftarrow[\circ j]{} & Hom(M, M) \end{array}$$

e seguendo le immagini di id_M lungo i due possibili percorsi da $Hom(M, M)$ a $\mathcal{F}(T)$, si riconosce che $\mathcal{F}(j)(\mathcal{U}) = \mathcal{E}$. □

Definizione. Sia $\mathcal{F}$ un problema di moduli. Uno *spazio di moduli grezzo* per $\mathcal{F}$ è una varietà analitica M tale che esiste una trasformazione naturale $I \colon \mathcal{F} \to Hom(\_, M)$ con la seguente proprietà: per ogni altra trasformazione naturale $J \colon \mathcal{F} \to Hom(\_, N)$ deve esistere un'unica mappa olomorfa $f \colon M \to N$ tale che $J = (\_ \circ f) \circ I$. Inoltre I induce una biiezione quando T è un punto.

I problemi di moduli associati alle curve ellittiche con struttura di N-livello sono problemi di classificazione di tali oggetti. Oltre a classificare le possibili strutture a meno di equivalenza, si intende anche farlo in modo da rappresentare i modi in cui queste possono modulare analiticamente. Per questo uno spazio di moduli deve rappresentare anche le possibili famiglie analitiche di curve ellittiche che vengono di seguito trattate.

Definizione. Sia T una varietà analitica su $\mathbb{C}$. Una *famiglia di curve ellittiche* su T è il dato $(\mathcal{E}, \pi, o)$, dove $\mathcal{E}$ è una varietà analitica, π è una funzione olomorfa suriettiva di rango massimo da $\mathcal{E}$ a T e o una sezione di π, tali che $\big(\mathcal{E}_t, o(t)\big)$ è una curva ellittica $\forall t \in T$.

Osservazione. Se (E, O) è una curva ellittica, per ogni varietà analitica complessa T, la terna $\big(T \times E, \pi_T, (t, O)\big)$ è una famiglia di curve ellittiche, detta la *famiglia banale* su T.

Un esempio non banale, che servirà da modello nel paragrafo successivo, è la seguente famiglia di curve ellittiche su $\mathbb{H}$

$$\big(\mathcal{E}(\infty), \pi_{\mathbb{H}}, (\tau, 0)\big) \;\text{ con }\; \mathcal{E}(\infty) = \{\, (\tau, P) \mid \tau \in \mathbb{H},\ P \in \mathbb{C}/\Lambda_\tau \,\} \ .$$

Osservazione. Si definisce la seguente azione di $\mathbb{Z}^2$ su $\mathbb{H} \times \mathbb{C}$:

$$\mathbb{Z}^2 \times (\mathbb{H} \times \mathbb{C}) \to \mathbb{H} \times \mathbb{C},\ \big((n, m), (\tau, z)\big) \mapsto (\tau, n\tau + m + z) \ .$$

Lo spazio $\mathcal{E}(\infty)$ è il quoziente di $\mathbb{H} \times \mathbb{C}$ modulo l'azione di $\mathbb{Z}^2$.

Osservazione. Dato che l'azione di $\mathbb{Z}^2$ su $\mathbb{H} \times \mathbb{C}$ è propriamente discontinua e libera, è possibile dotare $\mathcal{E}(\infty)$ di un'unica struttura olomorfa tale che la proiezione $\mathbb{H} \times \mathbb{C} \to \mathcal{E}(\infty)$ sia olomorfa.

Definizione. Siano $(\mathcal{E}, \pi, o)$ e $(\mathcal{E}', \pi', o')$ due famiglie di curve ellittiche su T. Queste sono *equivalenti* se esiste un biolomorfismo $\sigma \colon \mathcal{E}' \to \mathcal{E}$ tale che $\pi' = \pi \circ \sigma$ e $o = \sigma \circ o'$.

Definizione. Sia T una varietà analitica su $\mathbb{C}$. Si indica con $Ell(T)$ l'insieme delle classi di equivalenza di famiglie di curve ellittiche su T.

Osservazione. Sia $f\colon S \to T$ una mappa olomorfa e sia $(\mathcal{E}, \pi, o)$ una famiglia di curve ellittiche su T. Esiste un pullback di π lungo f in modo tale che

$$\begin{array}{ccc} f^*\mathcal{E} & \xrightarrow{f^*} & \mathcal{E} \\ {\scriptstyle \pi^*}\downarrow & & \downarrow{\scriptstyle \pi} \\ S & \xrightarrow{f} & T \end{array}$$

sia un diagramma commutativo. Inoltre è possibile scegliere una sezione o^* di π^* che sia compatibile con il diagramma, ovvero tale che $o \circ f = f^* \circ o^*$. In tal caso si ottiene che $(f^*\mathcal{E}, \pi^*, o^*)$ è una famiglia di curve ellittiche su T.

Osservazione. Si osserva che se $(\mathcal{E}', \pi', o')$ è una famiglia equivalente a $(\mathcal{E}, \pi, o)$, allora i due diagrammi

$$\begin{array}{ccc} f^*\mathcal{E} & \longrightarrow & \mathcal{E} \\ {\scriptstyle \pi^*}\downarrow & & \downarrow{\scriptstyle \pi} \\ S & \xrightarrow{f} & T \end{array} \qquad\qquad \begin{array}{ccccc} f^*\mathcal{E}' & \longrightarrow & \mathcal{E}' & \xrightarrow{\sigma} & \mathcal{E} \\ {\scriptstyle (\pi')^*}\downarrow & & {\scriptstyle \pi'}\downarrow & \swarrow{\scriptstyle \pi} & \\ S & \xrightarrow{f} & T & & \end{array}$$

mostrano che π^* e $(\pi')^*$ sono entrambi pullback di π lungo f. Per le proprietà dei pullback esiste un isomorfismo $\sigma^*\colon f^*\mathcal{E}' \to f^*\mathcal{E}$ tale che $(\pi')^* = \pi^* \circ \sigma^*$, dimostrando che $(f^*\mathcal{E}, \pi^*, o^*)$ è equivalente a $(f^*\mathcal{E}', (\pi')^*, (o')^*)$. Allora è possibile considerare f^* come una mappa da $Ell(T)$ a $Ell(S)$.

Osservazione. Sia $(\mathcal{E}, \pi, o)$ una famiglia di curve ellittiche su T e siano $f\colon S \to T$ e $g\colon Z \to S$ due mappe olomorfe. Usando un metodo analogo all'osservazione precedente si ottiene che le famiglie $(g^*f^*\mathcal{E}, \pi^*, o^*)$ e $\big((f \circ g)^*\mathcal{E}, \pi^*, o^*\big)$ definite su Z sono equivalenti.

Le tre osservazioni precedenti dimostrano la seguente Proposizione 5.2.

Proposizione 5.2. *Ell è un problema di moduli.*

Come evidenziato nella Proposizione 5.3, l'esistenza di automorfismi non banali nelle famiglie da classificare rende impossibile l'esistenza di spazi di moduli fini. Per questo motivo si introduce ulteriore struttura alle curve ellittiche, eliminando gli automorfismi non banali. Tali strutture sono dette strutture di livello. Sia N un intero positivo, le strutture di N-livello considerate sono:

$\Gamma(N)$**-strutture:** il dato di due punti P e Q sulla curva ellittica (E, O), dove P e Q sono due generatori di $E[N]$ con Weil-Pairing $e_N(P, Q) = e^{2\pi i/N}$.

Due curve ellittiche con $\Gamma(N)$-struttura (E, O, P, Q) e (E', O', P', Q') sono equivalenti se esiste un'equivalenza tra (E, O) e (E', O') tale che $P \mapsto P', Q \mapsto Q'$.

Le famiglie di curve ellittiche corrispondenti sono $(\mathcal{E}, \pi, o, p, q)$ con $(\mathcal{E}, \pi, o)$ una famiglia di curve ellittiche definita come prima e p, q due sezioni di π tali che $\big(p(t), q(t)\big)$ sia una $\Gamma(N)$-struttura su $\big(\mathcal{E}_t, o(t)\big)$ per ogni $t \in T$.

$\Gamma_1(N)$**-strutture:** il dato di un punto P sulla curva ellittica (E, O), dove P ha ordine N.

Due curve ellittiche con $\Gamma_1(N)$-struttura (E, O, P) e (E', O', P') sono equivalenti se esiste un'equivalenza tra (E, O) e (E', O') tale che $P \mapsto P'$.

Le famiglie di curve ellittiche corrispondenti sono $(\mathcal{E}, \pi, o, p)$ con $(\mathcal{E}, \pi, o)$ una famiglia di curve ellittiche definita come prima e p una sezione di π tale che $p(t)$ sia una $\Gamma_1(N)$-struttura su $\big(\mathcal{E}_t, o(t)\big)$ per ogni $t \in T$.

$\Gamma_0(N)$**-strutture:** il dato di un sottogruppo C della curva ellittica (E, O), dove C è un sottogruppo ciclico di ordine N di $E[N]$.

Due curve ellittiche con $\Gamma_0(N)$-struttura (E, O, C) e (E', O', C') sono equivalenti se esiste un'equivalenza tra (E, O) e (E', O') tale che $C \mapsto C'$.

Le famiglie di curve ellittiche corrispondenti sono $(\mathcal{E}, \pi, o, \mathcal{C})$ con $(\mathcal{E}, \pi, o)$ una famiglia di curve ellittiche definita come prima e $\mathcal{C}$ una sottovarietà di $\mathcal{E}$ tale che $\mathcal{E}_t \cap \mathcal{C}$ sia una $\Gamma_0(N)$-struttura su $\big(\mathcal{E}_t, o(t)\big)$ per ogni $t \in T$.

Definizione. I problemi di moduli associati a ciascuna delle strutture sopra descritte sono definiti nel seguente modo:

$$T \mapsto \{ \text{ classi di equivalenza delle famiglie su } T \text{ corrispondenti alla struttura } \}.$$

Verranno denotati Ell_N per le $\Gamma(N)$-strutture, $Ell_{N,1}$ per le $\Gamma_1(N)$-strutture e $Ell_{N,0}$ per le $\Gamma_0(N)$-strutture.

Osservazione. Nel caso in cui $\mathcal{F}$ sia uno dei problemi di moduli *Ell*, Ell_N, $Ell_{N,1}$ o $Ell_{N,0}$ l'oggetto universale $\mathcal{U}$ viene detto *famiglia universale*.

Osservazione. Sia M uno spazio di moduli fine per $\mathcal{F}$. Nel caso in cui T sia un punto e $\mathcal{F}$ sia uno dei problemi di moduli *Ell*, Ell_N, $Ell_{N,1}$ o $Ell_{N,0}$, l'insieme $\mathcal{F}(T)$ può essere considerato come l'iniseme delle classi di equivalenza di curve ellittiche con una determinata struttura di N-livello. Inoltre l'insieme $Hom(T, M)$ è in biiezione con M stesso. Allora si ha la biiezione

$$M \simeq \{ \text{ classi di equivalenza di curve ellittiche con struttura di } N\text{-livello } \}\ .$$

Si ottiene lo stesso risultato anche nel caso di spazi di moduli grezzi.

5.2 "Framings" e rappresentabilità di *Ell*

Un'ulteriore struttura che da rigidità al problema delle curve ellittiche è l'aggiunta di "framings". Data una curva ellittica (E, O), un suo "framing" è una base (come $\mathbb{Z}$-modulo di rango 2) per il gruppo di prima omologia $H_1(E, \mathbb{Z})$.

Osservazione. Quando (E, O) è della forma $(\mathbb{C}/\Lambda, 0)$, la mappa $\omega \mapsto [t \mapsto t\omega]$ induce un isomorfismo canonico $\Lambda \simeq H_1(E, \mathbb{Z})$. Questo implica che dati due "framing" (a, b), (a', b') di una curva ellittica $(\mathbb{C}/\Lambda, 0)$ deve esistere $\gamma \in SL_2(\mathbb{Z})$ tale che

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \gamma \begin{pmatrix} a \\ b \end{pmatrix}\ .$$

Sia $(\mathcal{E}, \pi, o)$ una famiglia di curve ellittiche su T. Ogni famiglia di curve ellittiche è localmente banale ovvero esiste un ricoprimento di aperti semplicemete connessi U di T tali che $\pi^{-1}(U) \simeq U \times \mathcal{E}_t$ per un qualsiasi $t \in U$. Dato che tali U sono semplicemente connessi, esiste un isomorfismo $H_1(\mathcal{E}_t, \mathbb{Z}) \simeq H_1(\pi^{-1}(U), \mathbb{Z})$ indotto da $\mathcal{E}_t \hookrightarrow \pi^{-1}(U)$.

Definizione. Una famiglia $\{\, c(t) \in H_1(\mathcal{E}_t, \mathbb{Z}) \mid t \in T \,\}$ si dice *localmente costante* se ogni coppia $c(t), c(s)$, per $t, s \in U$ per qualche U descritto sopra, è identificata tramite l'isomorfismo indotto dalle inclusioni $\mathcal{E}_t \hookrightarrow \pi^{-1}(U)$ e $\mathcal{E}_s \hookrightarrow \pi^{-1}(U)$.

Una famiglia di curve ellittiche "framed" su T è il dato $(\mathcal{E}, \pi, o, a, b)$ con $(\mathcal{E}, \pi, o)$ una famiglia di curve ellittiche su T e a, b una famiglia di "framings" delle sezioni che sia localmente costante.

Osservazione. Dalla definizione di "framing" si può dedurre che ogni famiglia di curve ellittiche definita su uno spazio semplicemente connesso ammette "framing". Inoltre si può dedurre anche che ogni famiglia di curve ellittiche ammette "framing" localmente.

Si riporta il Teorema 5 che sarà necessario per discutere gli spazi di moduli per *Ell*, Ell_N, $Ell_{N,1}$ e $Ell_{N,0}$. Per una discussione più completa delle curve ellittiche "framed" si veda [5].

Teorema 5. *Il semipiano complesso $\mathbb{H}$ è uno spazio di moduli fine per le curve ellittiche "framed" con la famiglia universale $(\mathcal{E}(\infty), \pi_{\mathbb{H}}, 0, 1, \tau)$. Data una famiglia di curve ellittiche "framed" $(\mathcal{E}, \pi, o, a, b)$ su T, la funzione olomorfa associata a tale famiglia è*

$$T \xrightarrow{\phi} \mathbb{H},\ t \mapsto \frac{\int_{a(t)} \omega_t}{\int_{b(t)} \omega_t}$$

con ω_t un qualsiasi differenziale olomorfo non nullo su $\mathcal{E}_t$.

Osservazione. L'azione di $SL_2(\mathbb{Z})$ su $\mathbb{H}$ studiata finora induce un'azione di $SL_2(\mathbb{Z})$ su $\mathcal{E}(\infty)$ attraverso i seguenti diagrammi commutativi

$$\begin{array}{ccc} \mathcal{E}(\infty) & \xrightarrow{\tilde{\gamma}} & \mathcal{E}(\infty) \\ {\scriptstyle \pi_{\mathbb{H}}}\downarrow & & \downarrow{\scriptstyle \pi_{\mathbb{H}}} \\ \mathbb{H} & \xrightarrow[\gamma]{} & \mathbb{H} \end{array} \quad \text{con } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})\ .$$

dove $\tilde{\gamma}$ agisce sulle fibre tramite la legge indotta da $\mathbb{H} \times \mathbb{C} \xrightarrow{\tilde{\gamma}} \mathbb{H} \times \mathbb{C},\ (\tau, z) \overset{\tilde{\gamma}}{\mapsto} \left(\gamma\tau, \frac{z}{c\tau + d}\right)$.

Proposizione 5.3. *Ell non ammette spazio di moduli fine.*

Dimostrazione. Si supponga che esista un tale spazio di moduli fine M. Come osservato deve esistere una biiezione

$$M \simeq \{\, \text{classi di equivalenza di curve ellittiche} \,\}\ .$$

Come si deduce dal Capitolo 4, le classi di equivalenza di curve ellittiche sono classificate da $SL_2(\mathbb{Z})\backslash\mathbb{H}$, quindi si può porre $M = SL_2(\mathbb{Z})\backslash\mathbb{H}$.

Sia $(\mathcal{E}, \pi, o)$ una famiglia di curve ellittiche su T e si consideri la famiglia di curve ellittiche $(p^*\mathcal{E}, p^*\pi, p^*o)$ sul rivestimento universale $p\colon \tilde{T} \to T$. Dato che $\tilde{T}$ è semplicemente connesso tale famiglia ammette "framing" (a, b) ed è definita quindi una funzione olomorfa $\phi\colon \tilde{T} \to \mathbb{H}$ per cui $(p^*\mathcal{E}, p^*\pi, p^*o, a, b)$ sia il pullback tramite ϕ della famiglia $(\mathcal{E}(\infty), \pi_{\mathbb{H}}, 0, \tau, 1)$. Si osserva che le curve $\big((p^*\mathcal{E})_{\tilde{t}}, p^*o(t)\big)$, al variare di $\tilde{t} \in p^{-1}(t)$, sono equivalenti alla curva $\big(\mathcal{E}_t, o(t)\big)$, per ogni $t \in T$. Allora i "framings" $\big(a(\tilde{t}), b(\tilde{t})\big)$, al variare di $\tilde{t} \in p^{-1}(t)$, devono essere nella stessa classe di equivalenza modulo $SL_2(\mathbb{Z})$, per ogni $t \in T$, da cui si deduce che $SL_2(\mathbb{Z})\phi(\tilde{t_1}) = SL_2(\mathbb{Z})\phi(\tilde{t_2})$ per ogni coppia $\tilde{t_1}, \tilde{t_2} \in p^{-1}(t)$ per ogni $t \in T$. Complessivamente è possibile definire la mappa olomorfa

$$f\colon T \to SL_2(\mathbb{Z})\backslash\mathbb{H},\ t \mapsto SL_2(\mathbb{Z})\tau,$$

con $SL_2(\mathbb{Z})\tau$ l'unico elemento di $SL_2(\mathbb{Z})\backslash\mathbb{H}$ tale che $\big(\mathcal{E}_t, o(t)\big)$ sia equivalente a $(\mathbb{C}/\Lambda_\tau, 0)$, per cui risulta $\mathcal{E} = f^*\mathcal{U}$.

Se $SL_2(\mathbb{Z})\backslash\mathbb{H}$ fosse spazio di moduli fine per *Ell*, la corrispondenza tra classi di equivalenza di famiglie curve ellittiche su T e funzioni olomorfe tra T e $SL_2(\mathbb{Z})\backslash\mathbb{H}$ dovrebbe essere biunivoca per ogni varietà analitica T. Data una qualsiasi varietà analitica T, osservato che la famiglia banale $\big(T \times \mathbb{C}/\Lambda_\tau, \pi_T, (t, 0)\big)$ rende la funzione associata costante e uguale a $SL_2(\mathbb{Z})\tau$, si ottiene che una famiglia su T che sia associata ad una funzione costante e uguale a $SL_2(\mathbb{Z})\tau$ deve essere equivalente alla famiglia banale $\big(T \times \mathbb{C}/\Lambda_\tau, \pi_T, (t, 0)\big)$.

Si consideri ora l'applicazione $\sigma\colon \mathbb{C} \to \mathbb{C},\ z \mapsto iz$ e si osservi che induce un'applicazione $\sigma\colon \mathbb{C}^* \times \mathbb{C}/\Lambda_i \to \mathbb{C}^* \times \mathbb{C}/\Lambda_i,\ (z, P) \to (iz, iP)$. Si consideri la famiglia di curve ellittiche

$$\begin{array}{c} \frac{\mathbb{C}^* \times \mathbb{C}/\Lambda_i}{\langle\sigma\rangle} \\ \Big\downarrow \pi_{\mathbb{C}^*} \\ \frac{\mathbb{C}^*}{\langle\sigma\rangle} \end{array}$$

in cui ogni sezione $\pi_{C^*}^{-1}(z)$ è equivalente a $\mathbb{C}/\Lambda_i$. Tale famiglia non è banale dato che le fibre sono tutte equivalenti ma non coincidenti. □

Osservazione. La curva ellittica $\mathbb{C}/\Lambda_i$ è una delle possibili curve in cui l'anello degli endomorfismi non è costituito solo dalle mappe moltiplicazione per N, ma contiene ulteriori automorfismi non banali, come ad esempio la moltiplicazione per i. Si dice che tali tori hanno *moltiplicazione complessa*.

Teorema 6. *$SL_2(\mathbb{Z})\backslash\mathbb{H}$ è lo spazio di moduli grezzo per Ell.*

Dimostrazione. In effetti la discussione iniziale nella dimostrazione della Proposizione 5.3 è sufficiente a definire la trasformazione naturale cercata. Inoltre è stato osservato nel Capitolo 4 come $SL_2(\mathbb{Z})\backslash\mathbb{H}$ classifica le curve ellittiche a meno di equivalenza. □

5.3 Rappresentabilità di $\boldsymbol{Ell_N}$, $\boldsymbol{Ell_{N,1}}$ e $\boldsymbol{Ell_{N,0}}$

Non sempre gli spazi trattati nei primi capitoli sono adeguati allo scopo di essere spazi di moduli fini per i problemi di moduli *Ell*, Ell_N, $Ell_{N,1}$ e $Ell_{N,0}$. Si è già visto l'esempio di

Ell e $SL_2(\mathbb{Z})\backslash\mathbb{H}$ nel paragrafo precedente e si vedrà ora l'esempio di $Ell_{N,0}$ e $Y_0(N)$. Dati due risultati generali di [6] che garantiscono l'esistenza di spazi di moduli fini per Ell_N e $Ell_{N,1}$ in un contesto più generale, si mostra esplicitamente che $Y(N)$ e $Y_1(N)$ sono gli spazi di moduli fini per Ell_N e $Ell_{N,1}$ rispettivamente.

Osservazione. Come è stato osservato nel paragrafo precedente, se M è spazio di moduli fine o grezzo per uno dei problemi di moduli Ell_N, $Ell_{N,1}$ o $Ell_{N,0}$ si ha la corrispondenza

$$M \simeq \{ \text{ classi di equivalenza di curve ellittiche con struttura di } N\text{-livello } \} \ .$$

Si danno allora le Proposizioni 5.6, 5.7, 5.4 che mostrano che, se esistono degli spazi di moduli per Ell_N, $Ell_{N,1}$, $Ell_{N,0}$, questi devono essere $Y(N)$, $Y_1(N)$, $Y_0(N)$ rispettivamente.

Le dimostrazioni delle Proposizioni 5.6, 5.7, 5.4 sono molto simili tra loro, ma si riportano tutte e tre dato che in ognuna ci sono alcuni dettagli specifici che dipendono dalla definizione dei sottogruppi di congruenza considerati.

Proposizione 5.4. *La curva modulare $Y_0(N)$ classifica a meno di equivalenza le curve ellittiche con $\Gamma_0(N)$-struttura.*

Dimostrazione. Sia (E, O, C) una curva ellittica con $\Gamma_0(N)$-struttura. Per quanto visto nel Capitolo 4 esiste un $\tau \in \mathbb{H}$ tale che (E, O) sia equivalente a $(\mathbb{C}/\Lambda_\tau, 0)$. Allora (E, O, C) è equivalente a $\big(\mathbb{C}/\Lambda_\tau, 0, \langle Q \rangle\big)$ per un qualche $Q = \frac{c\tau+d}{N} + \Lambda_\tau \in \mathbb{C}/\Lambda_\tau$, dato che C è ciclico. Poiché l'ordine di Q deve essere esattamente N, si deduce che $MCD(c, d, N) = 1$. Procedendo come nel Capitolo 1 si ottiene che esiste $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Allora, usando i risultati del Paragrafo 4.1, si ottiene che $\mathbb{C}/\Lambda_\tau$ è equivalente a $\mathbb{C}/\Lambda_{\gamma\tau}$ e l'immagine di Q sotto l'equivalenza è $\frac{1}{N} + \Lambda_{\gamma\tau}$. Complessivamente, quindi, si ottiene che ogni curva ellittica con $\Gamma_0(N)$-struttura è equivalente a una qualche $\big(\mathbb{C}/\Lambda_\tau, 0, \langle \frac{1}{N} + \Lambda_\tau \rangle\big)$.

Si considerino ora $\big(\mathbb{C}/\Lambda_\tau, 0, \langle \frac{1}{N} + \Lambda_\tau \rangle\big)$ e $\big(\mathbb{C}/\Lambda_{\tau'}, 0, \langle \frac{1}{N} + \Lambda_{\tau'} \rangle\big)$. Si vuole dimostrare che queste sono equivalenti se e solo se $\tau' \in \Gamma_0(N)\tau$.

Se $\tau' = \gamma\tau$ con $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, si ha come prima che $\big(\mathbb{C}/\Lambda_\tau, 0\big)$ è equivalente a $\big(\mathbb{C}/\Lambda_{\tau'}, 0\big)$ e l'immagine di $\frac{1}{N} + \Lambda_\tau$ in $\mathbb{C}/\Lambda_{\tau'}$ è $\frac{c\tau'+d}{N} + \Lambda_{\tau'}$. Ora, dato che si ha $\gamma \in \Gamma_0(N)$, si ha che $c \equiv 0 \mod N$, da cui si ottiene che l'immagine di $\frac{1}{N} + \Lambda_\tau$ in $\mathbb{C}/\Lambda_{\tau'}$ è $\frac{d}{N} + \Lambda_{\tau'}$ per qualche d coprimo con N. Allora si ottiene che $\langle \frac{d}{N} + \Lambda_{\tau'} \rangle = \langle \frac{1}{N} + \Lambda_{\tau'} \rangle$, dimostrando che $\big(\mathbb{C}/\Lambda_\tau, 0, \langle \frac{1}{N} + \Lambda_\tau \rangle\big)$ e $\big(\mathbb{C}/\Lambda_{\tau'}, 0, \langle \frac{1}{N} + \Lambda_{\tau'} \rangle\big)$ sono equivalenti.

Se $\big(\mathbb{C}/\Lambda_\tau, 0, \langle \frac{1}{N} + \Lambda_\tau \rangle\big)$ e $\big(\mathbb{C}/\Lambda_{\tau'}, 0, \langle \frac{1}{N} + \Lambda_{\tau'} \rangle\big)$ sono equivalenti, deve esistere $m \in \mathbb{C}$ tale che $m\Lambda_\tau = \Lambda_{\tau'}$ e $m\big(\frac{1}{N} + \Lambda_\tau\big) = \big(\frac{d}{N} + \Lambda_{\tau'}\big)$ per qualche d coprimo con N. La prima delle due condizioni mostra che

$$\text{esiste } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \text{ tale che } \begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$$

da cui si ottiene in particolare che $m = c\tau' + d$. Applicando questo risultato alla seconda condizione, si ottiene che $\frac{c\tau'+d}{N} + \Lambda_{\tau'} = \frac{d}{N} + \Lambda_{\tau'}$, da cui si deduce che $c \equiv 0 \mod N$, ovvero che $\gamma \in \Gamma_0(N)$. È stato ottenuto che $\tau = \gamma\tau'$ con $\gamma \in \Gamma_0(N)$ come si voleva. □

Prima di proseguire con le Proposizioni 5.6 e 5.7 sulla classificazione delle curve con $\Gamma(N)$-struttura e $\Gamma_1(N)$-struttura, si dimostrano la Proposizione 5.5 e il Teorema 7 sugli spazi di moduli per $Ell_{N,0}$.

Proposizione 5.5. *$Ell_{N,0}$ non ammette spazio di moduli fine per ogni intero positivo N.*

Dimostrazione. Si supponga che esista un tale spazio di moduli fine che si indica con M. Allora la Proposizione 5.4 dimostra che si può porre $M = Y_0(N)$. Procedendo come nel caso di *Ell*, sia data $(\mathcal{E}, \pi, o, \mathcal{C})$ una famiglia di curve ellittiche su T. Si consideri la famiglia $(p^*\mathcal{E}, p^*\pi, p^*o, p^*\mathcal{C})$ sul rivestimento universale $p\colon \tilde{T} \to T$. Dato che $\tilde{T}$ è semplicemente connesso, tale famiglia ammette "framing" (a, b) ed è quindi definita una funzione olomorfa $\phi\colon \tilde{T} \to \mathbb{H}$ per cui $(p^*\mathcal{E}, p^*\pi, p^*o, a, b)$ sia il pullback di $(\mathcal{E}(\infty), \pi_{\mathbb{H}}, 0, \tau, 1)$ lungo ϕ. Si osserva che le curve con $\Gamma_0(N)$-struttura $\big((p^*\mathcal{E})_{\tilde{t}}, p^*o(\tilde{t}), p^*\mathcal{C} \cap (p^*\mathcal{E})_{\tilde{t}}\big)$, al variare di $\tilde{t} \in p^{-1}(t)$, sono equivalenti alla curva con $\Gamma_0(N)$-struttura $\big(\mathcal{E}_t, o(t), \mathcal{E}_t \cap \mathcal{C}\big)$. Allora i "framings" $\big(a(\tilde{t}), b(\tilde{t})\big)$, al variare di $\tilde{t} \in p^{-1}(t)$, devono essere nella stessa classe di equivalenza modulo $\Gamma_0(N)$, per ogni $t \in T$, da cui si deduce che $\Gamma_0(N)\phi(\tilde{t_1}) = \Gamma_0(N)\phi(\tilde{t_2})$ per ogni coppia $\tilde{t_1}, \tilde{t_2} \in p^{-1}(t)$ per ogni $t \in T$. Complessivamente è possibile definire la mappa olomorfa

$$f\colon T \to Y_0(N),\ t \mapsto \Gamma_0(N)\tau,$$

con $\Gamma_0(N)\tau$ l'unico elemento di $Y_0(N)$ tale che $\big(\mathcal{E}_t, o(t), \mathcal{E}_t \cap \mathcal{C}\big)$ sia equivalente al rappresentante $\big(\mathbb{C}/\Lambda_\tau, 0, \langle \frac{1}{N} + \Lambda_\tau \rangle\big)$, per cui risulta $\mathcal{E} = f^*\mathcal{U}$. Da questa costruzione si deduce che se la mappa f risulta costante, la famiglia considerata è una famiglia banale.

Come nella dimostrazione della Proposizione 5.3 si consideri $\sigma\colon \mathbb{C} \to \mathbb{C},\ z \mapsto iz$ e si osservi che induce $\sigma\colon \mathbb{C}^* \times \mathbb{C}/\Lambda_i \to \mathbb{C}^* \times \mathbb{C}/\Lambda_i,\ (z, P) \to (iz, iP)$. Si osserva che il sottogruppo ciclico $\langle \frac{1+i}{N} + \Lambda_\tau \rangle$ di ordine N è preservato da σ. Si considera allora la famiglia di curve ellittiche con $\Gamma_0(N)$-struttura

$$\begin{array}{c} \frac{\mathbb{C}^* \times \mathbb{C}/\Lambda_i}{\langle\sigma\rangle} \\ \big\downarrow \pi_{\mathbb{C}^*} \\ \frac{\mathbb{C}^*}{\langle\sigma\rangle} \end{array}$$

con $\mathcal{C} = \langle \frac{1+i}{N} + \Lambda_\tau \rangle \times \mathbb{C}^*/\langle\sigma\rangle$. Ogni fibra $\pi^{-1}_{C^*}(z)$ è equivalente a $\mathbb{C}/\Lambda_i$ e il sottogruppo $\mathcal{C} \cap \pi^{-1}_{C^*}(z)$ viene mappato dall'equivalenza in $\langle \frac{1+i}{N} + \Lambda_\tau \rangle$ per ogni $z \in \mathbb{C}^*/\langle\sigma\rangle$. Tale famiglia non è banale dato che le fibre sono tutte equivalenti ma non coincidenti. □

Teorema 7. *$Y_0(N)$ è spazio di moduli grezzo per $Ell_{N,0}$ per ogni intero positivo N.*

Dimostrazione. La discussione iniziale della dimostrazione della Proposizione 5.5 è sufficiente a definire la trasformazione naturale cercata. Inoltre la Proposizione 5.4 mostra che $Y_0(N)$ classifica le curve ellittiche con $\Gamma_0(N)$-struttura a meno di equivalenza. □

Proposizione 5.6. *La curva modulare $Y(N)$ classifica a meno di equivalenza le curve ellittiche con $\Gamma(N)$-struttura.*

Dimostrazione. Sia (E, O, P, Q) una curva ellittica con $\Gamma_1(N)$-struttura. Procedendo come nel caso precedente, si ottiene che (E, O) è equivalente a $\big(\mathbb{C}/\Lambda_\tau, 0\big)$ e le immagini dei punti P e Q sono $\frac{a\tau+b}{N} + \Lambda_\tau$ e $\frac{c\tau+d}{N} + \Lambda_\tau$. Si osserva che, dalla Proposizione 4.6, si ottiene che $\frac{a\tau+b}{N} + \Lambda_\tau$ e $\frac{c\tau+d}{N} + \Lambda_\tau$ hanno ancora Weil-Pairing $e^{2\pi i/N}$, da cui si deduce che

$\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Allora, usando i risultati del Paragrafo 4.1, si ottiene che $\mathbb{C}/\Lambda_\tau$ è equivalente a $\mathbb{C}/\Lambda_{\gamma\tau}$ e le immagini di P e Q sotto l'equivalenza sono $\frac{\gamma\tau}{N} + \Lambda_{\gamma\tau}$ e $\frac{1}{N} + \Lambda_{\gamma\tau}$. Si è ottenuto che ogni curva ellittica con $\Gamma(N)$-struttura è equivalente ad una curva ellittica con $\Gamma(N)$-struttura del tipo $\big(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau, \frac{\tau}{N} + \Lambda_\tau\big)$.

Si considerino ora $\big(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau, \frac{\tau}{N} + \Lambda_\tau\big)$ e $\big(\mathbb{C}/\Lambda_{\tau'}, 0, \frac{1}{N} + \Lambda_{\tau'}, \frac{\tau'}{N} + \Lambda_{\tau'}\big)$. Si vuole dimostrare che questi sono equivalenti se e solo se $\tau' \in \Gamma(N)\tau$.

Se $\tau' = \gamma\tau$ con $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(N)$, si ha come prima che $\big(\mathbb{C}/\Lambda_\tau, 0\big)$ è equivalente a $\big(\mathbb{C}/\Lambda_{\tau'}, 0\big)$ e le immagini di $\frac{1}{N} + \Lambda_\tau$ e $\frac{\tau}{N} + \Lambda_\tau$ in $\mathbb{C}/\Lambda_{\tau'}$ sono $\frac{a\tau'+b}{N} + \Lambda_{\tau'}$ e $\frac{c\tau'+d}{N} + \Lambda_{\tau'}$. Ora, dato che si ha $\gamma \in \Gamma(N)$, si ha che le immagini di $\frac{\tau}{N} + \Lambda_\tau$ e $\frac{1}{N} + \Lambda_\tau$ in $\mathbb{C}/\Lambda_{\tau'}$ sono $\frac{1}{N} + \Lambda_{\tau'}$ e $\frac{\tau'}{N} + \Lambda_{\tau'}$, dimostrando che $\big(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau, \frac{\tau}{N} + \Lambda_\tau\big)$ e $\big(\mathbb{C}/\Lambda_{\tau'}, 0, \frac{1}{N} + \Lambda_{\tau'}, \frac{\tau'}{N} + \Lambda_{\tau'}\big)$ sono equivalenti.

Se $\big(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau, \frac{\tau}{N} + \Lambda_\tau\big)$ e $\big(\mathbb{C}/\Lambda_{\tau'}, 0, \frac{1}{N} + \Lambda_{\tau'}, \frac{\tau'}{N} + \Lambda_{\tau'}\big)$ sono equivalenti, deve esistere $m \in \mathbb{C}$ tale che $m\Lambda_\tau = \Lambda_{\tau'}$, $m\big(\frac{\tau}{N} + \Lambda_\tau\big) = \big(\frac{\tau'}{N} + \Lambda_{\tau'}\big)$ e $m\big(\frac{1}{N} + \Lambda_\tau\big) = \big(\frac{1}{N} + \Lambda_{\tau'}\big)$. La prima delle tre condizioni mostra che

$$\text{esiste } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \text{ tale che } \begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$$

da cui si ottiene in particolare che $m = c\tau' + d$. Applicando questo risultato alla seconda condizione, si ottiene che $\frac{a\tau'+b}{N} + \Lambda_{\tau'} = \frac{\tau'}{N} + \Lambda_{\tau'}$, da cui si deduce che $a \equiv 1, b \equiv 0 \mod N$. Applicandolo invece alla terza condizione, si ottiene che $\frac{c\tau'+d}{N} + \Lambda_{\tau'} = \frac{1}{N} + \Lambda_{\tau'}$, da cui si deduce che $c \equiv 1, d \equiv 0 \mod N$. Complessivamente è stato ottenuto che $\tau = \gamma\tau'$ con $\gamma \in \Gamma(N)$ come si voleva. □

Proposizione 5.7. *La curva modulare $Y_1(N)$ classifica a meno di equivalenza le curve ellittiche con $\Gamma_1(N)$-struttura.*

Dimostrazione. Sia (E, O, P) una curva ellittica con $\Gamma_1(N)$-struttura. Per quanto visto nel Capitolo 4 esiste un $\tau \in \mathbb{H}$ tale che (E, O) sia equivalente a $\big(\mathbb{C}/\Lambda_\tau, 0\big)$. Allora (E, O, P) è equivalente a $\big(\mathbb{C}/\Lambda_\tau, 0, Q\big)$, per un qualche $Q = \frac{c\tau+d}{N} + \Lambda_\tau \in \mathbb{C}/\Lambda_\tau$. Poiché l'ordine di Q deve essere esattamente N, si deduce che $MCD(c, d, N) = 1$. Procedendo come nel Capitolo 1, si ottiene che esiste $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Allora, usando i risultati del Paragrafo 4.1, si ottiene che $\mathbb{C}/\Lambda_\tau$ è equivalente a $\mathbb{C}/\Lambda_{\gamma\tau}$ e l'immagine di Q sotto l'equivalenza è $\frac{1}{N} + \Lambda_{\gamma\tau}$. Si è ottenuto che ogni curva ellittica con $\Gamma_1(N)$-struttura è equivalente ad una curva ellittica con $\Gamma_1(N)$-struttura del tipo $\big(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau\big)$.

Si considerino ora $\big(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau\big)$ e $\big(\mathbb{C}/\Lambda_{\tau'}, 0, \frac{1}{N} + \Lambda_{\tau'}\big)$. Si vuole dimostrare che questi sono equivalenti se e solo se $\tau' \in \Gamma_1(N)\tau$.

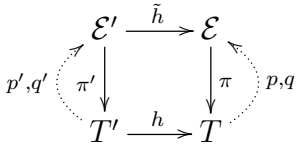
Se $\tau' = \gamma\tau$ con $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$, si ha come prima che $\big(\mathbb{C}/\Lambda_\tau, 0\big)$ è equivalente a $\big(\mathbb{C}/\Lambda_{\tau'}, 0\big)$ e l'immagine di $\frac{1}{N} + \Lambda_\tau$ in $\mathbb{C}/\Lambda_{\tau'}$ è $\frac{c\tau'+d}{N} + \Lambda_{\tau'}$. Ora, dato che si ha $\gamma \in \Gamma_1(N)$, si ha che $c \equiv 0, d \equiv 1 \mod N$, da cui si ottiene che l'immagine di $\frac{1}{N} + \Lambda_\tau$ in $\mathbb{C}/\Lambda_{\tau'}$ è $\frac{1}{N} + \Lambda_{\tau'}$, dimostrando che $\big(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau\big)$ e $\big(\mathbb{C}/\Lambda_{\tau'}, 0, \frac{1}{N} + \Lambda_{\tau'}\big)$ sono equivalenti.

Se $\big(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau\big)$ e $\big(\mathbb{C}/\Lambda_{\tau'}, 0, \frac{1}{N} + \Lambda_{\tau'}\big)$ sono equivalenti, deve esistere $m \in \mathbb{C}$ tale che $m\Lambda_\tau = \Lambda_{\tau'}$ e $m\big(\frac{1}{N} + \Lambda_\tau\big) = \big(\frac{1}{N} + \Lambda_{\tau'}\big)$. La prima delle due condizioni mostra che

$$\text{esiste } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \text{ tale che } \begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$$

da cui si ottiene in particolare che $m = c\tau' + d$. Applicando questo risultato alla seconda condizione, si ottiene che $\frac{c\tau'+d}{N} + \Lambda_{\tau'} = \frac{1}{N} + \Lambda_{\tau'}$, da cui si deduce che $c \equiv 0, d \equiv 1 \mod N$, ovvero che $\gamma \in \Gamma_1(N)$. È stato ottenuto che $\tau = \gamma\tau'$ con $\gamma \in \Gamma_1(N)$ come si voleva. □

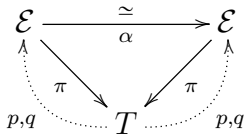
Proposizione 5.8. *Si ponga $N > 2$ e sia $(\mathcal{E}, \pi, o, p, q)$ una famiglia di curve ellittiche con $\Gamma(N)$-struttura su una varietà analitica T. Non esistono equivalenze non banali di $(\mathcal{E}, \pi, o, p, q)$ con sé stessa. Equivalentemente, dato il diagramma commutativo*



la mappa $\tilde{h}$ è univocamente determinata da h.

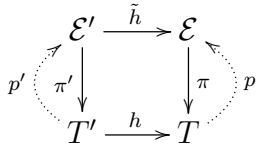
Dimostrazione. Si dimostra prima che una curva ellittica con $\Gamma(N)$-struttura è equivalente a sé stessa solo tramite l'identità. Per quanto visto nella dimostrazione della Proposizione 5.6, si può considerare il problema restringendosi alle curve ellittiche con $\Gamma(N)$-struttura del tipo $\left(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau, \frac{\tau}{N} + \Lambda_\tau\right)$. Due curve di questo tipo, associate a τ e τ', sono equivalenti se e solo se $\tau' = \gamma\tau$ per qualche $\gamma \in \Gamma(N)$, quindi le possibili equivalenze di $\left(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau, \frac{\tau}{N} + \Lambda_\tau\right)$ con sé stessa sono determinate da $\Gamma(N)_\tau$. Come osservato nel Paragrafo 2.1 un elemento di $SL_2(\mathbb{Z})$ ammette punto fisso solo se ha ordine finito. Essendo che dalla Proposizione 1.9 il sottogruppo di congruenza $\Gamma(N)$ è privo di torsione per $N > 2$, non esistono elementi di $\Gamma(N)$ di ordine finito distinti dall'identità. Complessivamente si ha $\Gamma(N)_\tau \subseteq \{ \mathbb{1} \}$, quindi l'unica equivalenza di $\left(\mathbb{C}/\Lambda_\tau, 0, \frac{1}{N} + \Lambda_\tau, \frac{\tau}{N} + \Lambda_\tau\right)$ in sé è l'identità.

Sia data ora una famiglia di curve ellittiche con $\Gamma(N)$-struttura $(\mathcal{E}, \pi, o, p, q)$ su T. Si considera il diagramma commutativo



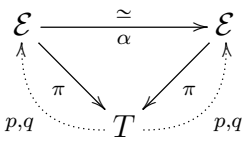
Tale condizione si verifica solo se le restrizioni $\alpha_t \colon \mathcal{E}_t \simeq \mathcal{E}_t$ inducono l'identità su $\mathcal{E}_t[N]$. Allora, per quanto visto sopra, α_t deve essere l'identità per ogni $t \in T$, per cui α deve essere l'identità di $\mathcal{E}$. □

Proposizione 5.9. *Si ponga $N > 3$ e sia $(\mathcal{E}, \pi, o, p)$ una famiglia di curve ellittiche con $\Gamma_1(N)$-struttura su una varietà analitica T. Non esistono equivalenze non banali di $(\mathcal{E}, \pi, o, p)$ con sé stessa. Equivalentemente, dato il diagramma commutativo*



la mappa $\tilde{h}$ è univocamente determinata da h.

Dimostrazione. Procedendo in modo analogo a prima e sfruttando la Proposizione 1.10, si ottiene che una curva ellittica con $\Gamma_1(N)$-struttura è equivalente a sé stessa solo tramite l'identità. Sia data ora una famiglia di curve ellittiche con $\Gamma_1(N)$-struttura $(\mathcal{E}, \pi, o, p)$ su T. Si considera il diagramma commutativo



Tale condizione si verifica solo se le restrizioni $\alpha_t \colon \mathcal{E}_t \simeq \mathcal{E}_t$ rispettano la $\Gamma_1(N)$-struttura. Allora, per quanto detto sopra, α_t deve essere l'identità su tutte le fibre, per cui α deve essere l'identità di $\mathcal{E}$. □

Come già detto nell'introduzione di questo paragrafo, si citano due risultati di [6] che garantiscono l'esistenza di spazi di moduli fini per Ell_N e $Ell_{N,1}$. L'argomento è trattato nella generalità della teoria degli schemi la cui trattazione non è inclusa tra gli obiettivi di questa tesi.

Teorema 8. *Per $N > 2$ il problema di moduli definito sulla categoria $\big(Ell/\mathbb{Z}[1/N]\big)$*

$$E/S \mapsto \big\{ \textit{S-gruppo-schema isomorfismi } (\mathbb{Z}/N\mathbb{Z})^2 \simeq E[N] \big\}$$

è rappresentabile da una curva liscia affine su $\mathbb{Z}[1/N]$.

Teorema 9. *Per $N > 3$ il problema di moduli definito sulla categoria $\big(Ell/\mathbb{Z}[1/N]\big)$*

$$E/S \mapsto \{ \textit{S-gruppo-schema omomorfismi } (\mathbb{Z}/N\mathbb{Z}) \to E[N] \}$$

è rappresentabile da una curva liscia affine su $\mathbb{Z}[1/N]$.

Osservazione. In [6] i problemi di moduli sono definiti sulla categoria delle curve ellittiche (che corrispondono a quelle che in questa tesi sono dette famiglie di curve ellittiche) denotata (*Ell*). Viene però mostrato che è equivalente considerare opportuni problemi di moduli sulla categoria degli schemi che, opportunamente ristretta, corrisponde alla categoria delle varietà analitiche trattata in questa tesi. I problemi di moduli presentati nei Teoremi 8 e 9 sono equivalenti ai problemi di moduli Ell_N e $Ell_{N,1}$ rispettivamente.

Definizione. Sia Γ un sottogruppo di congruenza. Sia $\Gamma \ltimes \mathbb{Z}^2$ il prodotto semidiretto definito dalla seguente azione di Γ su $\mathbb{Z}^2$

$$(n, m) \overset{\gamma}{\mapsto} (n, m)\gamma \ .$$

Si definisce un'azione di $\Gamma \ltimes \mathbb{Z}^2$ su $\mathbb{H} \times \mathbb{C}$ tramite

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} n \\ m \end{pmatrix} \right)(\tau, z) = \left(\frac{a\tau + b}{c\tau + d}, \frac{n + m\tau + z}{c\tau + d} \right) .$$

Si pone

$$\mathcal{E}(\Gamma) = \frac{\mathbb{H} \times \mathbb{C}}{\Gamma \ltimes \mathbb{Z}^2} \ .$$

Notazione. Se $\Gamma = \Gamma(N), \Gamma_1(N)$, lo spazio $\mathcal{E}(\Gamma)$ si denota $\mathcal{E}(N), \mathcal{E}_1(N)$ rispettivamente.

Osservazione. È già stato osservato nel Paragrafo 5.2 che l'azione di $SL_2(\mathbb{Z})$ su $\mathbb{H}$ si traduce in un'azione di $SL_2(\mathbb{Z})$ su $\mathcal{E}(\infty)$. Lo spazio $\mathcal{E}(\Gamma)$ sopra definito corrisponde al quoziente $\Gamma\backslash\mathcal{E}(\infty)$. Se inoltre l'azione di Γ su $\mathcal{E}(\infty)$ è libera allora è possibile dotare $\mathcal{E}(\Gamma)$ di un'unica struttura olomorfa tale che la proiezione $\mathcal{E}(\infty) \to \mathcal{E}(\Gamma)$ sia olomorfa.

Osservazione. Posto $N > 2$ l'azione di $\Gamma(N)$ su $\mathcal{E}(\infty)$ è libera. Infatti l'azione di ogni elemento di $\Gamma(N)$ su $\mathbb{H}$ è sollevata ad un'unica azione su $\mathcal{E}(\infty)$ per la Proposizione 5.8 e l'azione di $\Gamma(N)$ su $\mathbb{H}$ è libera. Allora $\mathcal{E}(N)$ ha una struttura di varietà complessa e si può osservare che il seguente diagramma

$$\begin{array}{ccc} \mathcal{E}(\infty) & \longrightarrow & \mathcal{E}(N) \\ \downarrow & & \downarrow \\ \mathbb{H} & \longrightarrow & Y(N) \end{array}$$

è un diagramma di pullback.

Teorema 10. *Si fissi un intero $N > 2$. La curva modulare $Y(N)$ è spazio di moduli fine per Ell_N con la famiglia universale $\big(\mathcal{E}(N), \Pi, O, P, Q\big)$ dove Π è indotta dalla proiezione naturale di $\mathbb{H} \times \mathbb{C}$ su $\mathbb{H}$, O è indotta da $\tau \mapsto 0$, P e Q sono indotte da $\tau \mapsto 1/N$ e $\tau \mapsto \tau/N$ rispettivamente.*

Dimostrazione. Sia $(\mathcal{E}, \pi, o, p, q)$ una famiglia di curve ellittiche con $\Gamma(N)$-struttura su T. Localmente su T esiste un "framing" (a, b), allora, per il Teorema 5, è possibile definire localmente $\phi\colon T \to \mathbb{H}$ in modo da avere il diagramma

$$\begin{array}{ccccc} \mathcal{E} & \xrightarrow{\tilde{\phi}} & \mathcal{E}(\infty) & \longrightarrow & \mathcal{E}(N) \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi_{\mathbb{H}}} & & \downarrow{\scriptstyle\Pi} \\ T & \xrightarrow[\phi]{} & \mathbb{H} & \longrightarrow & Y(N) \\ & \searrow^{\varphi} & & \nearrow & \end{array}$$

A questo punto si osserva che il "framing" (a, b) viene trasportato nel "framing" canonico $(1, \phi)$ che viene poi trasportato nella $\Gamma(N)$-struttura $(1/N, \phi/N)$. Anche la $\Gamma(N)$-struttura (p, q) viene trasportata in una $\Gamma(N)$-struttura su $\mathcal{E}(N)$ (che si denoterà ancora (p, q) per semplicità). Allora esiste una $\tilde{\gamma} \in SL_2(\mathbb{Z}/N\mathbb{Z})$ tale che $(1/N, \phi/N) = \tilde{\gamma}(p, q)$. Si ricorda che, dalla Proposizione 1.4, la proiezione $\lambda_N\colon SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ è suriettiva per cui esiste $\gamma \in SL_2(\mathbb{Z})$ tale che $\gamma \equiv \tilde{\gamma} \mod N$. Allora è possibile scegliere un "framing" (a, b) in modo che $(1/N, \phi/N) = (p, q)$, e questa scelta è unica a meno di $\ker \lambda_N = \Gamma(N)$. Complessivamente è stata trovata un'unica $\varphi\colon T \to Y(N)$ tale che il seguente sia un diagramma di pullback

$$\begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{E}(N) \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\Pi} \\ T & \xrightarrow[\varphi]{} & Y(N) \end{array}$$

e tale che la $\Gamma(N)$-struttura venga rispettata. □

Osservazione. Posto $N > 3$ l'azione di $\Gamma_1(N)/\Gamma(N)$ su $\mathcal{E}(N)$, indotta dall'azione di $\Gamma_1(N)$ su $\mathcal{E}(\infty)$ è libera. Infatti l'azione di ogni elemento di $\Gamma_1(N)$ su $\mathbb{H}$ è sollevata ad un'unica azione su $\mathcal{E}(\infty)$ per la Proposizione 5.9 e l'azione di $\Gamma_1(N)$ su $\mathbb{H}$ è libera, dimostrando che l'azione di $\Gamma_1(N)$ su $\mathcal{E}(\infty)$ è libera. Quindi l'azione di $\Gamma_1(N)/\Gamma(N)$ su $\Gamma(N)\backslash\mathcal{E}(\infty) = \mathcal{E}(N)$ deve essere libera come si voleva. Allora $\mathcal{E}_1(N)$, che corrisponde a $\big(\Gamma_1(N)/\Gamma(N)\big)\backslash\mathcal{E}(N)$, ha una struttura di varietà complessa e si può osservare che il seguente diagramma

$$\begin{array}{ccc} \mathcal{E}(N) & \longrightarrow & \mathcal{E}_1(N) \\ \downarrow & & \downarrow \\ Y(N) & \longrightarrow & Y_1(N) \end{array}$$

è un diagramma di pullback.

Teorema 11. *Si fissi un intero $N > 3$. La curva modulare $Y_1(N)$ è spazio di moduli fine per $Ell_{N,1}$ con la famiglia universale $\big(\mathcal{E}_1(N), \Pi, O, P\big)$ dove Π è indotta dalla proiezione naturale $\pi_{\mathbb{H}}\colon \mathbb{H}\times\mathbb{C} \to \mathbb{H}$, O è indotta da $\tau \mapsto 0$ e P è indotta da $\tau \mapsto 1/N$.*

Dimostrazione. Sia $(\mathcal{E}, \pi, o, p)$ una famiglia di curve ellittiche con $\Gamma_1(N)$-struttura. Avendo che $p(t)$ è un elemento di ordine esattamente N in $\mathcal{E}_t[N]$ per ogni $t \in T$ è possibile estendere la $\Gamma_1(N)$-struttura p ad una $\Gamma(N)$-struttura (p, q). Allora per il Teorema 10 esiste, per ogni scelta di q, un'unica funzione olomorfa $\varphi\colon T \to Y(N)$ in modo da avere il diagramma

$$\begin{array}{ccccc} \mathcal{E} & \xrightarrow{\tilde{\varphi}} & \mathcal{E}(N) & \longrightarrow & \mathcal{E}_1(N) \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi_{\mathbb{H}}} & & \downarrow{\scriptstyle\Pi} \\ T & \xrightarrow[\varphi]{} & Y(N) & \longrightarrow & Y_1(N) \\ & \searrow^{\psi} & & & \nearrow \end{array}$$

Si osserva che la $\Gamma(N)$-struttura (p, q) viene trasportata nella $\Gamma(N)$-struttura canonica $(1/N, \varphi/N)$ che viene poi trasportata nella $\Gamma_1(N)$-struttura $1/N$. La scelta di q è unica a meno di azioni di matrici $\tilde{\gamma} \in SL_2(\mathbb{Z}/N\mathbb{Z})$ che preservano $1/N$ in $\mathcal{E}(N)_\varphi[N]$, ovvero matrici della forma $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. Il gruppo di tali matrici è l'immagine di $\Gamma_1(N)$ tramite λ_N ed è quindi isomorfo a $\Gamma_1(N)/\Gamma(N)$ per il Primo Teorema di Isomorfismo. Complessivamente è stata trovata un'unica $\psi\colon T \to Y_1(N)$ tale che il seguente sia un diagramma di pullback

$$\begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{E}_1(N) \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\Pi} \\ T & \xrightarrow[\psi]{} & Y_1(N) \end{array}$$

e tale che la $\Gamma_1(N)$-struttura venga rispettata. □

Bibliografia

[1] D. Arapura. *Abelian Varieties and Moduli*. 2012. URL: https://www.math.purdue.edu/~arapura/preprints/abelian.pdf.

[2] B. Conrad. *Modular Curves*. Course Handouts for graduate course 248B Stanford University. URL: https://virtualmath1.stanford.edu/~conrad/248BPage/.

[3] K. Conrad. $SL_2(\mathbb{Z})$. Expository papers. URL: https://kconrad.math.uconn.edu/blurbs/grouptheory/SL(2,Z).pdf.

[4] F. Diamond, J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics. Springer New York. 2005.

[5] R. Hain. *Lectures on Moduli Spaces of Elliptic Curves*. 2008. URL: https://doi.org/10.48550/arXiv.0812.1803.

[6] N. M. Katz, B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Annals of Mathematics Studies. Princeton University Press. 1985.

[7] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Mathematics. Springer New York. 1993.

[8] D. Loeffler. *Modular Curves* . Lecture Notes. 2014. URL: https://warwick.ac.uk/fac/sci/maths/people/staff/david_loeffler/teaching/modularcurves.

[9] R. Miranda. *Algebraic Curves and Riemann Surfaces*. Graduate Studies in Mathematics. American Mathematical Society. 1995.

[10] T. Miyake. *Modular Forms*. Springer Monographs in Mathematics. Springer Berlin. 1989.

[11] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York. 2009.