FORME AUTOMORFE E PUTTANATE ZEN

MAURIZIO MONGE

Questa è una raccolta tutt'altro che sistematica di questioni su serie di Dirichlet, gruppo modulare e forme automorfe. Ringrazio il prof. Rocco Chirivì per il suo interessante e piacevole corso, e Selena Marinelli per il tempo passato risolvendo esercizi che spesso e volentieri degeneravano (quasi sempre per colpa mia) in questioni generali dal sapore supercazzoloso.

1. Raccolta di Koan

Koan 1. *Un giorno un giovane monaco chiese a un maestro Zen se ogni funzione $f : \mathbb{Z} \to \mathbb{C}$ non nulla che sia moltiplicativa (ovvero tale che $f(xy) = f(x)f(y)$ per ogni $x, y \in \mathbb{Z}$), e periodica di periodo M (nel senso che esiste un $M \geq 1$ tale che $f(x) = f(x + M)$ per ogni $x \in \mathbb{Z}$) dovesse essere un carattere di Dirichlet modulo il minimo periodo N.*

Il maestro chiese al monaco cosa fosse un carattere di Dirichlet modulo N, e lo studente rispose che è una funzione moltiplicativa e periodica di periodo N tale che $f(x) = 0$ se e solo se $(x, N) \neq 1$.

Mentre il giovane monaco cercava le parole migliori per finire di spiegare la definizione, il maestro gli spezzò un braccio. In quel momento il monaco fu illuminato.

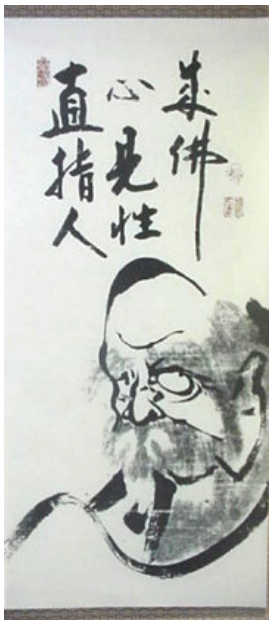


Figura 1: Bodhidarma, Lo Zen punta direttamente al cuore dell'uomo, guarda la tua vera Natura e diventa Buddha! *(opera di Hakuin Ekaku, 1685-1768).*

Interpretazione del koan. Sia N il minimo intero positivo tale che $f(x) = f(x + N)$ per ogni x. Dobbiamo mostrare che $f(y) = 0$ per ogni qual volta $(y, N) \neq 1$, e supponiamo quindi per assurdo che esista un tale y per cui $f(y) \neq 0$.

Possiamo vedere f come definita su $\mathbb{Z}/N\mathbb{Z}$, e se $N = \prod p_i^{e_i}$ è la fattorizzazione di N, abbiamo grazie al teorema cinese del resto che

$$\mathbb{Z}/N\mathbb{Z} \cong \prod \mathbb{Z}/p_i^{e_i}\mathbb{Z},$$

e quindi a y corrisponderà tramite tale isomorfismo un vettore $(y_1, \ldots, y_k)$, in cui la i-esima componente y_i è un elemento di $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$. In particolare, a meno di rimpiazzare y con una sua potenza (nel qual caso avremo ancora che $f(y) \neq 0$) possiamo supporre che le componenti siano tutte 0 o 1, ed inoltre non potranno essere tutte 1 perché altrimenti y sarebbe primo con N.

Poniamo ad esempio che la prima componente sia 0, e osserviamo che se z è l'elemento indicato nel prodotto diretto dal vettore $(0, 1, \ldots, 1)$, allora $zy = y$, e quindi $f(z)f(y) = f(y)$, da cui $f(z) = 1$, dato che $f(y) \neq 0$.

Date: 26 febbraio 2009.

In particolare se u, v sono elementi del prodotto che differiscono solo per la prima componente, allora $zu = zv$, e quindi $f(u) = f(v)$. Ma poniamo ora

$$N' = \prod_{i \geq 2} p_i^{e_i} = N/p_1^{e_1},$$

e osserviamo che due elmenti di $\mathbb{Z}/N\mathbb{Z}$ che differiscono di un multiplo di N', se scritti come vettore tramite il teorema cinese del resto hanno tutte le componenti uguali tranne al più la prima (infatti la loro differenza corrisponde a un vettore della forma $(t, 0, \ldots, 0)$). Ma allora su di essi f assume lo stesso valore, e quindi abbiamo mostrato che di fatto $f(x) = f(x + N')$ per ogni $x \in \mathbb{Z}$, e N non era il minimo periodo. □

Koan 2. *Verso l'anno 1375, un uomo non più giovane desideroso di conoscere la verità si rese conto dopo lunghe meditazioni di non poter proseguire le sue ricerche spirituali senza sapere per quali numeri complessi di valore assoluto* 1 *converga la serie*

$$\sum_{n=1}^{\infty} \frac{\alpha^n}{n},$$

e decise quindi di recarsi da un saggio maestro per avere un consiglio. Il maestro gli chiese se fosse riuscito a risolverlo almeno per gli α *che sono radici dell'unità.*

Non essendoci riuscito, il discepolo passò altri 25 anni conducendo vita da eremita e svolgendo conti. Dopo aver dimostrato la convergenza per ogni radice dell'unità $\neq 1$*, decise di recarsi nuovamente dal maestro, ma entrando nella sua casa si rese conto che ormai egli era morto.*

Uscendo dalla casa del maestro, fece accidentalmente cadere l'antico libro buddhista Functional Analysis*, l'unico libro che il maestro possedeva, e cadendo il libro si aprì al capitolo* Tauberian Theory*. Fu questo il momento in cui l'uomo ricevette l'illuminazione.*

Interpretazione del koan. Per trattare il caso in cui α non è una radice dell'unità ma un qualunque complesso di valore assoluto 1 diverso da 1, abbiamo bisogno del seguente

Teorema (tauberiano di Littlewood)**.** *Sia* $(a_n)_{n \geq 0}$ *una successione reale tale che per ogni* $|x| < 1$ *la serie* $\sum_{n=0}^{\infty} a_n x^n$ *converge, e*

$$\sum_{n=0}^{\infty} a_n x^n \to A, \qquad \text{per } x \nearrow 1.$$

Supponiamo inoltre che $a_n = O(1/n)$*. Allora* $\sum_{n=0}^{\infty} a_n$ *converge e vale* A*.*

La dimostrazione di questo teorema è al di fuori dello scopo di queste note, ma essendo tuttavia esse delle note Zen, eccovi tutti i dettagli (seguendo [Kor04]).

Dimostrazione. Se $(a_n)_{n \geq 0}$ è una successione, indicheremo con $a_n^{(-1)}$ la successiona costituita dalle somme parziali, con $a_n^{(-2)}$ le somme parziali degli $a_n^{(-1)}$, e così via:

$$a_n^{(-1)} = a_0 + a_1 + \cdots + a_n, \qquad a_n^{(-2)} = a_0^{(-1)} + a_1^{(-1)} + \cdots + a_n^{(-1)}.$$

Come prima cosa ci serve il seguente risultato [Kor04, Teo. 6.1], dovuto a Hardy: *sia* $(a_n)_{n \geq 0}$ *una successione reale, e supponiamo che* $a_n^{(-2)}/(n+1)$ *converga (cioè che* $\sum_{n=0}^{\infty} a_n$ *converga secondo Cesàro), e che* $na_n > -C$ *per qualche costante* $C \geq 0$*. Allora* $a_n^{(-1)}$ *converge allo stesso limite.*

Infatti per ogni intero $h > 0$ abbiamo che

$$a_{n+h}^{(-2)} = a_n^{(-2)} + h a_n^{(-1)} + \frac{h(h+1)}{2}\xi, \tag{1}$$

dove ξ è compreso fra il minimo e il massimo degli a_i, per $n+1 \le i \le n+h$. Possiamo inoltre supporre che $a_n^{(-2)}/n$ converga a zero, e supponiamo che $C \ge 1$.

Risolviamo ora la (1) in $a_n^{(-1)}$: dato che $a_n \ge -C/n$, e per ogni ε abbiamo che $|a_n^{(-2)}| < n\varepsilon$ per n sufficientemente grande, otteniamo che per $h \approx 2n\sqrt{\varepsilon/C}$

$$\begin{aligned} a_n^{(-1)} &= \frac{a_{n+h}^{(-2)} - a_n^{(-2)}}{h} - \frac{h+1}{2}\xi \\ &\le \frac{2n+h}{h}\varepsilon + \frac{h+1}{2}\cdot\frac{C}{n+1} < 3\sqrt{C\varepsilon}. \qquad \text{[per } n \text{ grande]} \end{aligned}$$

Per la stima nell'altro senso, basta prendere $h \approx -2n\sqrt{\varepsilon/C}$ e adattare la formula di Taylor discreta (1). In conclusione $a_n^{(-1)} \to 0$ come si desiderava.

Abbiamo ora bisogno di un risultato di Kamarata [Kor04, Teo. 11.1], che permette di passare dalla convergenza secondo Abel a quella secondo Cesàro: *supponiamo che* $\sum s_n x^n$ *converga per* $|x| < 1$, *e che*

$$f(x) = (1-x)\sum_{n=0}^{\infty} s_n x^n \to A, \qquad \textit{per } x \nearrow 1. \tag{2}$$

Se gli s_n *soddisfano la condizione tauberiana* $s_n \ge -C$ *per ogni* n, *abbiamo che*

$$\frac{1}{N}s_N^{(-1)} = \frac{1}{N}\sum_{n\le N} s_n \to A, \qquad \textit{per } N \to \infty. \tag{3}$$

A meno di sommare C agli s_n, possiamo supporre che essi soddisfino $s_n \ge 0$ per ogni n. Dalla (2) abbiamo che per ogni intero $k > 0$

$$(1-x)\sum_{n=0}^{\infty} s_n x^{kn} = \frac{1-x}{1-x^k} f(x^k) \to \frac{A}{k} = A\int_0^1 t^k \frac{\mathrm{d}t}{t}, \qquad \text{per } x \nearrow 1.$$

Quindi dato un polinomio $P(t) = \sum_{k=1}^m b_k t^k$, abbiamo

$$(1-x)\sum_{n=0}^{\infty} s_n P(x^n) \to A\sum_{k=1}^{m}\frac{b_k}{k} = A\int_0^1 P(t)\frac{\mathrm{d}t}{t}, \qquad \text{per } x \nearrow 1. \tag{4}$$

Purtroppo non possiamo scrivere la somma parziale $s_N^{(-1)}$ come $\sum_{n=0}^{\infty} s_n P(x^n)$ per qualche polinomio P, ma se prendiamo l'indicatrice $g(y)$ dell'intervallo $[1/e, 1]$ e $x = e^{-1/N}$, otteniamo che

$$s_N^{(-1)} = \sum_{n\le N} s_n = \sum_{n=0}^{\infty} s_n g(x^n).$$

Mostreremo che nella (4) è possibile rimpiazzare P con g, ovvero

$$\lim_{x\nearrow 1}(1-x)\sum_{n=0}^{\infty} s_n g(x^n) = A\int_0^1 g(t)\frac{\mathrm{d}t}{t} = A. \tag{5}$$

Da essa segue immediatamente la tesi, perché ponendo $x = e^{-1/N}$ otteniamo

$$\lim_{N\to\infty}\frac{1}{N}s_n^{(-1)} = \lim_{N\to\infty}\left(1-e^{-1/N}\right)\sum_{n=0}^{\infty} s_n g(e^{-n/N}) = A.$$

Per dimostrare la (5) ci basta mostrare che il *lim sup* è $\le A$, similarmente si può procedere per il *lim inf*. Per un qualunque $\varepsilon > 0$, possiamo costruire un polinomio P con costante nullo tale che $P \ge g$, e

$$\int_0^1 \left(P(t) - g(t)\right)\frac{\mathrm{d}t}{t} < \varepsilon,$$

e dato che $s_n \geq 0$ abbiamo che

$$\begin{aligned}\limsup_{x\nearrow 1}(1-x)\sum_{n=0}^{\infty} s_n g(x^n) \\ &\leq \limsup_{x\nearrow 1}(1-x)\sum_{n=0}^{\infty} s_n P(x^n) \\ &= A\int_0^1 P(t)\frac{\mathrm{d}t}{t} \leq A(1+\varepsilon).\end{aligned}$$

Per costuire un polinomio con le proprietà richieste, basta prendere un maggiorante continuo $h(t)$ di $g(t)$ che coincide con $g(t)$ tranne che nell'intervallo $[1/e-\varepsilon, 1/e]$ in cui è lineare, approssimare $h(t)/t+\varepsilon$ a meno di ε grazie al teorema di Weierstrass con un polinomio $P(t)/t$, e stimare l'errore:

$$\int_0^1 \frac{P(t)-h(t)}{t}\mathrm{d}t \leq 2\varepsilon, \quad \int_{1/e-\varepsilon}^{1/e} \frac{h(t)-g(t)}{t}\mathrm{d}t \leq \frac{\varepsilon}{1/e-\varepsilon} < 6\varepsilon.$$

Possiamo ora dare la dimostrazione del teorema di Littlewood [Kor04, Remark 11.2, Cor. 5.2]: dato che la $\sum_{n=0}^{\infty} a_n$ è sommabile secondo Abel, abbiamo che

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = (1-x)\sum_{n=0}^{\infty} s_n x^n \to A \qquad \text{per } x \nearrow 1,$$

dove abbiamo posto $s_n = a_n^{(-1)} = \sum_{k=0}^{n} a_n$.

Osserviamo che

$$\begin{aligned}|s_n - f(x)| &= \left|\sum_{n=1}^{N} a_n(1-x^n) - \sum_{n=N+1}^{\infty} a_n x^n\right| \\ &\leq (1-x)\sum_{n=1}^{N}|na_n| + \frac{1}{N(1-x)}\sup_{n\geq N+1}|na_n|,\end{aligned}$$

in cui se poniamo $x = 1-1/N$ otteniamo

$$|s_n - f(1-1/N)| \leq \frac{1}{N}\sum_{n=1}^{N}|na_n| + \sup_{n\geq N+1}|na_n|,$$

e quindi siccome gli $|na_n|$ sono limitati e $f(x)$ ha limite per $x \nearrow 1$ per ipotesi, abbiamo che anche gli s_n devono essere limitati. Quindi per la (2) la somma $\sum_{n=0}^{\infty} a_n$ è sommabile secondo Cesàro e ha limite A, e applicando il teorema di Hardy abbiamo che $\sum_{n=0}^{\infty} a_n = A$. □

Osserviamo che anche se originalmente inteso per essere applicato a serie reali, il teorema di Littlewood funziona altrettanto bene se gli a_n sono complessi.

Se ora poniamo $a_n = \alpha^n/n$, abbiamo che

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \frac{\alpha^n}{n} x^n$$

è una serie di potenze con raggio di convergenza 1.

Inoltre se $\alpha \neq 1$ essa ha limite per $x \nearrow 1$ dato che la sua derivata è

$$f'(x) = \sum_{n=0}^{\infty} \alpha^n x^{n-1} = \frac{\alpha}{1-x\alpha}$$

che per ogni $\alpha \neq 1$ è ben definita e olomorfa in un intorno di 1. Possiamo quindi applicare il teorema tauberiano, e abbiamo la convergenza.

Metodo alternativo. Esiste in realtà un metodo molto più facile di dimostrare la convergenza che non passa attraverso il teorema tauberiano di Liouville, ma utilizza il seguente [Kno56, §5.5, Teo. 4]

Figura 2: Hui Neng, il sesto patriarca, mentra fa essiccare dei Sutra (Liáng Kăi, XII-XIII secolo).

Teorema (Abel-Dedekind-Dirichlet)**.** *Sia data una successione $(a_n)_{n\geq 0}$, di numeri complessi poniamo, tale che le somme parziali $a_n^{(-1)} = \sum_{k=0}^{n} a_k$ sono limitate, e sia $(b_n)_{n\geq 0}$ una successione tale che $b_n \to 0$ e inoltre ha* variazione limitata*, nel senso che*

$$\sum_{k=0}^{\infty} \big|b_{k+1} - b_k\big| < \infty.$$

Allora la serie $\sum_{k=0}^{\infty} a_k b_k$ converge.

Ad esempio, qualunque successione reale monotona tendente a 0 soddisfa le ipotesi richieste alla successione $(b_n)_{n\geq 0}$.

La dimostrazione di questo teorema è immediata, il lettore che si senta seccato per aver letto l'intera dimostrazione del teorema tauberiano quando c'è un metodo molto più facile si consoli pensando che io l'ho addirittura texata, quella dimostrazione.

Dimostrazione. Infatti il termine n-esimo si può scrivere come

$$\begin{aligned}\sum_{k=0}^{n} a_k b_k &= \left(\sum_{j=0}^{n} a_j\right)\cdot b_n + \sum_{k=0}^{n-1}\left(\sum_{j=0}^{k} a_j\right)\cdot\big(b_k - b_{k+1}\big)\\ &= a_n^{(-1)}\cdot b_n + \sum_{k=0}^{n-1} a_k^{(-1)}\cdot\big(b_k - b_{k+1}\big),\end{aligned}$$

e quindi come somma di una parte che tende a 0 più la somma dei primi n termini della serie

$$\sum_{k=0}^{\infty} a_k^{(-1)}\cdot\big(b_k - b_{k+1}\big),$$

che converge assolutamente dato che ogni termine è minore di $C|b_k - b_{k+1}|$ per qualche costante fissata C. □

Questo teorema ci dà immediatamente la convergenza, ponendo $a_n = \alpha^{n+1}$ e $b_n = 1/(n+1)$, poiché ci basta infatti verificare che

$$\left|\sum_{k=0}^{n} \alpha^{k+1}\right| = \left|\frac{\alpha(1-\alpha^{n+1})}{1-\alpha}\right| \leq \left|\frac{\alpha 2}{1-\alpha}\right|, \qquad \text{per ogni } n \geq 0. \qquad \square$$

Koan 3. *Si narra che in un villaggio della Cina medievale fosse un giorno giunto un santone indiano, che trasmise i suoi insegnamenti alla popolazione locale. Quando iniziò ad essere conosciuto ed amato dagli abitanti del villaggio, si mise a proporre a tutte le persone che incontrava il problema di dimostrare che*

$$\sum \frac{1}{n-1} = 1,$$

dove la somma è su tutti gli n che sono un potenza intera non banale $n = a^b$ con $a, b > 1$. Le persone a cui lui propose il problema raccoglievano la sfida, e

incominciarono a passare il loro tempo cercando di risolverlo, trascurando i campi, la cura delle cose, dei bambini e i commerci, tanto che giunse una grave carestia. Gli abitanti sprofondarono in una pesante miseria, dalla quale non si seppero sollevare perché anziché lavorare continuavano a pensare al problema.

Informato dell'accaduto, l'imperatore incaricò l'abate di un monastero Shaolin di prendersi cura del problema. Il saggio abate si recò nel villaggio e si unì devotamente agli altri fedeli che si recavano dal santone, desideroso anch'egli di conoscere la carismatica figura. Infine, quando ebbe trovato il santone e fu al suo cospetto, lo ammazzò di botte.

Interpretazione del koan. Osserviamo che la somma può essere vista come una somma su tutti gli $n = a^b$, per $a, b > 1$ dove a non è una potenza non banale di nessun altro intero

$$\sum_{\substack{a,b\geq 2\\ a \text{ non pot.}}} \frac{1}{a^b - 1}.$$

In particolare possiamo espandere

$$\frac{1}{a^b-1} = \frac{1}{a^b} + \frac{1}{a^{2b}} + \frac{1}{a^{3b}} + \cdots + \frac{1}{a^{ib}} + \ldots,$$

e osserviamo che espandendo ogni addendo $1/(a^b-1)$ il contributo al termine $1/a^k$ è dato da tutti i modi in cui è possibile ottenere $1/a^k$ come $1/a^{ib}$ per $b > 1$, ed è quindi il numero di divisori > 1 di k, $\delta(k)$ poniamo.

La somma può quindi essere scritta come

$$\sum_{\substack{a,k\geq 2\\ a \text{ non pot.}}} \delta(k)\frac{1}{a^k},$$

e osserviamo che se scriviamo

$$\sum_{n\geq 2}\left(\frac{1}{n^2} + \frac{1}{n^3} + \frac{1}{n^4} + \ldots\right)$$

anche in questo modo otteniamo ogni termine $1/a^k$ precisamente $\delta(k)$ volte. Raggruppando le serie geometriche abbiamo che la nostra somma vale

$$\sum_{n\geq 2}\frac{1}{n(n-1)} = \sum_{n\geq 2}\left(\frac{1}{n-1} - \frac{1}{n}\right),$$

che è uguale a 1 dato che la somma dei primi n termini della serie è precisamente $1 - 1/n$ e tende a 1 per $n \to \infty$. □

Koan 4. *Un giorno il maestro di un monastero Zen si ritrovò a dover scegliere il suo successore, e dichiarò che avrebbe scelto colui che avrebbe saputo stupirlo.*

Quello che era considerato il migliore dei suoi studenti gli mostrò come si calcolava la cardinalità di $SL_n(\mathbb{Z}/N\mathbb{Z})$. Successivamente, un altro suo studente altrettanto bravo dimostrò che l'omomorfismo $SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/N\mathbb{Z})$ dato dalla riduzione modulo N è surgettivo. Nessuno degli altri studenti si fece avanti, perché nessuno pensava di poter fare di meglio, ma il maestro ancora non era soddisfatto.

Il giorno dopo il garzone della cucina, che era da tutti considerato il più ignorante e neppure degno di sedere accanto agli altri studenti, andò dal maestro e gli mostrò quant'era bravo nel colpire le mosche con il catarro. Il maestro fu esterrefatto, e lo nominò suo sucessore.

Interpretazione del koan. Per calcolare la cardinalità di $SL_n(\mathbb{Z}/N\mathbb{Z})$ ci basta saperlo fare per $SL_n(\mathbb{Z}/p^e\mathbb{Z})$, e mettere tutto insieme con il teorema cinese del resto. Per fare questo osserviamo che la successione

$$0 \longrightarrow SL_n(\mathbb{Z}/p^e\mathbb{Z}) \longrightarrow GL_n(\mathbb{Z}/p^e\mathbb{Z}) \xrightarrow{\det} \mathbb{Z}/p^e\mathbb{Z}^\times \longrightarrow 0$$

è esatta, visto che per definizione $SL_n(\mathbb{Z}/p^e\mathbb{Z})$ è il *ker* della mappa *det*, la quale è a sua volta chiaramente surgettiva (basta prendere una matrice diagonale con un elemento x sulla diagonale e gli altri 1).

Per calcolare la cardinalità di $GL_n(\mathbb{Z}/p^e\mathbb{Z})$ osserviamo ogni matrice ridotta modulo p deve ancora avere determinante $\neq 0$, e ogni matrice in $GL_n(\mathbb{Z}/p\mathbb{Z})$ è l'immagine di altre $p^{(e-1)n^2}$ in $GL_n(\mathbb{Z}/p^e\mathbb{Z})$. D'altra parte la cardinalità di $GL_n(\mathbb{Z}/p\mathbb{Z})$ si ottiene contando il numero di basi dello spazio vettoriale $\mathbb{Z}/p\mathbb{Z}^n$, e nella scelta di una tale base il primo vettore si può scegliere in $p^n - 1$ modi, il secondo non deve stare nello spazio generato dal primo e ho $p^n - p$ possibilità, ho poi $p^n - p^2$ possibilità per il terzo, e così via, e quindi ottengo

$$\begin{aligned}\#GL_n(\mathbb{Z}/p\mathbb{Z}) &= (p^n-1)(p^n-p)\dots(p^n-p^{n-1}) \\ &= p^{n(n-1)/2}(p^n-1)(p^{n-1}-1)\dots(p^2-1)(p-1).\end{aligned}$$

Di conseguenza, avendo $\mathbb{Z}/p^e\mathbb{Z}^\times$ precisamente $p^{e-1}(p-1)$ elementi abbiamo che

$$\#SL_n(\mathbb{Z}/p^e\mathbb{Z}) = p^{(e-1)(n^2-1)+n(n-1)/2}(p^n-1)(p^{n-1}-1)\dots(p^2-1),$$

e la cardinalità di $SL_n(\mathbb{Z}/N\mathbb{Z})$ si ottiene scrivendo $N = \prod p_i^{e_i}$, come prodotto delle cardinalità degli $SL_n(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$.

Per mostrare che l'omomorfismo

$$SL_n(\mathbb{Z}) \xrightarrow{\text{mod } N} SL_n(\mathbb{Z}/N\mathbb{Z})$$

è surgettivo, prendiamo una matrice $\bar{A} \in SL_n(\mathbb{Z}/N\mathbb{Z})$, e una qualunque sua controimmagine A in $M_{n\times n}(\mathbb{Z})$ (che non avrà determinante 1, però). Per il teorema dei divisori elementari, la matrice A si può scrivere come

$$A = E_1 \cdot D \cdot E_2,$$

dove $E_1, E_2 \in SL_n(\mathbb{Z})$, e D è diagonale (il teorema ci dice anche che possiamo fare sì che gli elementi $d_1, \dots, d_n$ sulla diagonale siano tali che $d_i | d_{i+1}$, ma questo non ci servirà).

Ci basta quindi trovare una matrice $D' \in SL_n(\mathbb{Z})$ che coincida con D modulo N, e dato che $\det D \equiv 1 \pmod N$, basta mostrare che è possibile fare questo per ogni matrice 2×2 della forma

$$D = \begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix}, \qquad aa' \equiv 1 \pmod N.$$

Possiamo inoltre supporre che a, a' siano elementi coprimi in $\mathbb{Z}$, a meno di sommare un multiplo di N a uno di essi (infatti $a' + tN \equiv 1 \pmod a$ per qualche $t \in \mathbb{Z}$).

Prendiamo quindi una matrice della forma

$$D' = \begin{pmatrix} a + kN & N \\ \ell N & a' + k'N \end{pmatrix},$$

e imponiamo che

$$(a + kN)(a' + k'N) - \ell N^2 = 1. \tag{6}$$

Dato che $aa' = 1 + rN$ per qualche r, ci basta scegliere k, k' in modo che

$$ka' + k'a = -r$$

perché la (6) sia verificata modulo N^2, e scegliendo un ℓ opportuno possiamo fare sì che sia vera in $\mathbb{Z}$. □

Koan 5. *Un giorno un erudito filoso si recò a far visita ad un maestro Zen, il quale lo accolse di buon grado. Il filosofo iniziò a raccontare al maestro tutte le sue conoscenze delle discipline Zen, mostrando di sapere a menadito i più insignificanti dettagli della disciplina, come anche tutte le tradizioni buddhiste. Diede lungamente sfoggio di conoscenza delle pratiche meditative e spirituali, e infine dopo alcune ore tacque, desideroso di udire una qualche risposta o commento da parte del maestro Zen.*

Rispose il maestro:

- *È giusto tutto ciò che avete detto, e inoltre ogni sottogruppo discreto* Γ *di un gruppo topologico di Hausdorff* G *agisce in modo discontinuo sullo spazio dei laterali* G/K *con la topologia quoziente, per ogni sottogruppo compatto* K*.*
- *Eeeeeeeh?????!?*
- *Puppa!*

Figura 3: Dipinto giapponese di Linji Yixuan, conosciuto in Giappone come Rinzai Gigen (?-866).

Interpretazione del koan. Ci servirà il seguente fatto di teoria dei gruppi topologici: per ogni intorno dell'identità U, esiste un intorno V tale che $V \cdot V \subseteq U$ ed è simmetrico, cioè $V = V^{-1}$. Infatti la moltiplicazione è una funzione continua $G \times G \to G$, e la topologia di $G \times G$ ha come base gli aperti della forma $W_1 \times W_2$. L'immagine inversa di U per questa mappa conterrà quindi sicuramente un intorno di $(e, e) \in G \times G$ della forma $W_1 \times W_2$, e ci basta porre $V = W_1 \cap W_2$. Per ottenere la seconda asserzione, possiamo rimpiazzare eventualmente V con $V \cap V^{-1}$.

Mostriamo ora che Γ deve essere chiuso in G. Essendo Γ discreto possiamo prendere un intorno U di e in G tale che $U \cap \Gamma = \{e\}$, e sia V un intorno simmetrico dell'identità tale che $V \cdot V \subseteq U$.

Se ora $x \in G$ è un qualunque elemento di G, è facile vedere che xV è un intorno di x che incontra Γ in al più un punto. Supponiamo infatti che

$$\gamma_1 = xv_1, \qquad \gamma_2 = xv_2,$$

con $\gamma_1, \gamma_2 \in \Gamma$ distinti, e $v_1, v_2 \in V$. Allora $\gamma_1 v_1^{-1} = x = \gamma_2 v_2^{-1}$, e quindi

$$\gamma_2^{-1}\gamma_1 = v_2^{-1}v_1 \qquad \in V^{-1} \cdot V \subseteq U,$$

ma d'altra parte U incontra Γ solo nell'identità, e quindi γ_1 era uguale a γ_2.

Quindi xV contiene al più un elemento di Γ, e se $x \notin \Gamma$ possiamo facilmente passare ad un intorno di x che non ne contiene nessuno, essendo G di Hausdorff. Quindi Γ è chiuso in G.

Mostriamo ora che il risultato è vero se $K = \{e\}$. Siano $K_1, K_2 \subset G$ compatti, dobbiamo verificare che $\gamma K_1 \cap K_2 \neq \emptyset$ solo per una quantità finita di $\gamma \in \Gamma$. Sia

$$Q = \Gamma \cap (K_2 \cdot K_1^{-1}),$$

che è l'insieme costituito degli elementi $\gamma \in \Gamma$ che si possono scrivere come $k_2 k_1^{-1}$ per qualche $k_1 \in K_1$ e $k_2 \in K_2$. Il particolare $\gamma \in Q$ se e solo se $\gamma K_1 \cap K_2 \neq \emptyset$.

Osserviamo che $K_2 \cdot K_1^{-1}$ è l'immagine di $K_2 \times K_1$ tramite la mappa di moltiplicazione composta con l'inversione sulla seconda coordinata, e in particolare essendo $K_2 \times K_1$ prodotto di compatti e tale mappa continua, la sua immagine $K_2 \cdot K_1^{-1}$ è ancora compatta.

Siccome Γ è chiuso, Q è un chiuso in $K_2 \cdot K_1^{-1}$ e quindi compatto. Inoltre la topologia indotta su Γ dalla topologia di G è la topologia discreta. Quindi Q è finito, essendo compatto e discreto al tempo stesso.

Consideriamo ora il caso in cui K non sia banale, e siano $\bar{K}_1, \bar{K}_2$ dei compatti di G/K. Sia $\pi : G \to G/K$ la proiezione, ci basta dimostrare che le controimmagini $K_1 = \pi^{-1}(\bar{K}_1), K_2 = \pi^{-1}(\bar{K}_2)$ sono compatte, perché avremmo allora che

$$\gamma K_1 \cap K_2 \neq \emptyset \;\Leftrightarrow\; \gamma \bar{K}_1 \cap \bar{K}_2 \neq \emptyset$$

solo per un numero finito di $\gamma \in \Gamma$.

Prendiamo quindi un $\bar{F}$ compatto in G/K, e sia $F = \pi^{-1}(F)$. Sia dato un ricoprimento aperto $(U_\alpha)_{\alpha \in A}$ di F, e sia xK un laterale di K contenuto in F. Ogni punto $y \in xK$ sta dentro qualche U_α, e sia V_y un intorno dell'identità tale che $V_y y \subset U_\alpha$ per qualche $\alpha \in A$. Sia W_y intorno simmetrico dell'identità tale che $W_y \cdot W_y \subset V_y$.

Al variare di y in xK gli $W_y y$ ricoprono xK, ed essendo xK compatto esso sarà ricoperto da un numero finito di essi, $W_{y_i} y_i$ poniamo. Inoltre ciascuno dei $V_{y_i} y_i \supseteq W_{y_i} W_{y_i} y_i$ è per costruzione a sua volta contenuto in un qualche U_α, in U_{α_i} poniamo.

Quindi se W è l'intersezione dei W_{y_i}, che è un aperto essendo i W_{y_i} in numero finito, abbiamo che

$$W \cdot xK \subseteq W \cdot \bigcup_i W_{y_i} y_i \subseteq \bigcup_i W_{y_i} W_{y_i} y_i \subseteq \bigcup_i V_{y_i} y_i \subseteq \bigcup_i U_{\alpha_i}.$$

Siccome la proiezione π è aperta, abbiamo mostrato che una collezione finita di U_α contiene di fatto l'immagine inversa dell'intorno aperto $\pi(W)$ in G/K di $\pi(x) \in \bar{F}$. Essendo a sua volta $\bar{F}$ compatto, abbiamo che una finitudine di tali collezioni finite è quindi sufficiente a ricoprire tutto F. □

Koan 6. *Un giorno un uomo desideroso di intraprendere la via dello spirito ad ogni costo si presentò ad un monastero Zen. L'abate del monastero gli chiese cosa volesse, ed egli rispose che sarebbe stato disposto a qualunque sacrificio pur di conoscere la dimostrazione dell'equazione funzionale della $\zeta(s)$ e della continuazione analitica della $\Gamma(s)$.*

Gli rispose il maestro:

- *Certo, come no. Ho fiducia nella tua abilità con le parole, ma sapresti far loro seguire dei fatti di esse degni?*

Non sapendo cosa rispondere, l'uomo si amputò un braccio e lo offrì all'abate del monastero come prova della sua determinazione perché lo accettassero fra i discepoli. Rispose l'abate:

- *Oh, scusa, devi sapere che sono un po' sordo, è da un po' che continuano a passare testimoni di Geova e non so come fare a mandarli via. Non avevo capito che volevi solo diventare un nuovo discepolo. Benvenuto!*

Interpretazione del koan. Incominciamo con qualche fatto generale sulla $\Gamma(s)$. Essa è definita come

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} \mathrm{d}t,$$

e dalla definizione si verififa immediatamente che $\Gamma(1) = 1$, e inoltre dato che

$$\int_0^\infty e^{-t} t^{s-1} \mathrm{d}t = \left[-e^{-t} t^{s-1}\right]_0^\infty - \int_0^\infty (-e^{-t})(s-1) t^{s-2} \mathrm{d}t$$

possiamo osservare che $\Gamma(s) = (s-1)\Gamma(s-1)$, e abbiamo quindi che $\Gamma(n) = (n-1)!$ per ogni n intero positivo.

L'integrale con cui è stata definita la $\Gamma(s)$ converge per $\Re(s) > 0$. Per definire un'estensione meromorfa dimostreremo che vale l'equazione

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s} \tag{7}$$

per $0 < \Re(s) < 1$. Abbiamo infatti che

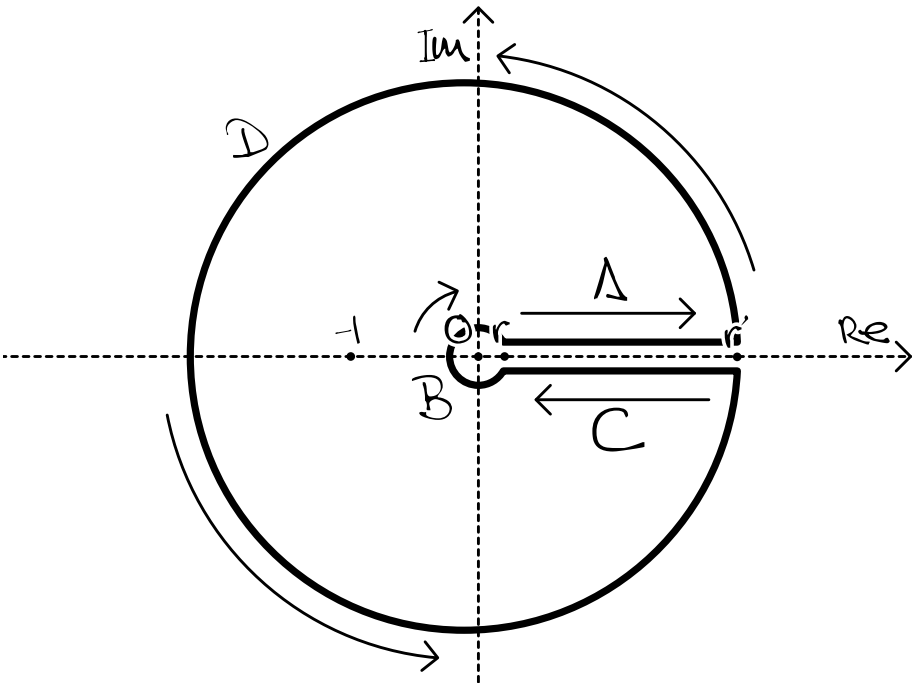
$$\begin{aligned}
\Gamma(s)\Gamma(1-s) &= \iint e^{-t-u} t^{s-1} u^{-s} \mathrm{d}t\mathrm{d}u \\
&= \iint e^{-uv-u} (uv)^{s-1} u^{-s} u \mathrm{d}v\mathrm{d}u \quad [\text{ponendo } t = uv] \\
&= \iint e^{-u(1+v)} v^{s-1} \mathrm{d}v\mathrm{d}u \\
&= \iint e^{-\frac{w}{1+v}(1+v)} v^{s-1} \frac{1}{1+v} \mathrm{d}w\mathrm{d}v \quad [\text{scambiando e per } u = \frac{w}{1+v}] \\
&= \iint e^{-w} \frac{v^{s-1}}{1+v} \mathrm{d}w\mathrm{d}v = \int_0^\infty \frac{v^{s-1}}{1+v} \mathrm{d}v.
\end{aligned}$$

Per calcolare questo integrale, sia

$$🧘(v) = \frac{(-v)^{s-1}}{1+v}$$

dove poniamo $(-v)^{s-1} = e^{(s-1)\log(-v)}$ prendendo il ramo principale del logaritmo, nel senso che $\log(-v)$ è reale per v reale negativo (e quindi la sua parte immaginaria su su un complesso della forma $1 - i\varepsilon$ vale circa π, e su uno della forma $1 + i\varepsilon$ circa $-\pi$, per $\varepsilon > 0$ piccolo).

Se consideriamo il seguente percorso di integrazione



per il teorema dei residui abbiamo che

$$\int_A \text{🧘} + \int_B \text{🧘} + \int_C \text{🧘} + \int_D \text{🧘} = 2\pi i \text{Res}(\text{🧘}, -1),$$

essendo -1 l'unico polo (v^{s-1} è olomorfa).

Inolte il residuo in -1 è 1, dato che secondo la nostra valutazione di v^{s-1} in -1 essa vale 1.

Abbiamo che $\text{🧘}(v) = O(v^{s-2})$ per $v \to \infty$, mentre $\text{🧘}(v) = O(v^{s-1})$ per $v \to 0$. Quindi se facciamo tendere i raggi r, r' che definiscono i percorsi B, D a 0 e ∞ rispettivamente, abbiamo che gli integrali su questi domini tendono a 0.

D'altra parte avvicinando A, C all'asse reale (e portandoli a coincidere, pur di usare la valutazione giusta del logaritmo), abbiamo che da una parte $\log(-v) = \log v - i\pi$ sul dominio A, mentre sul dominio C il logaritmo vale $\log v + i\pi$.

Quindi

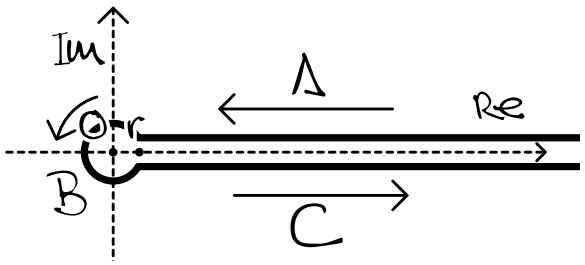
$$\begin{aligned}
\int_A \text{🧘} + \int_C \text{🧘} &= \int_0^\infty \frac{e^{(s-1)[\log(v)-i\pi]}}{1+v}\mathrm{d}v - \int_0^\infty \frac{e^{(s-1)[\log(v)+i\pi]}}{1+v}\mathrm{d}v \\
&= \left[e^{-(s-1)i\pi} - e^{(s-1)i\pi}\right] \int_0^\infty \frac{v^{s-1}}{1+v}\mathrm{d}v \\
&= 2i\sin(\pi(1-s)) \int_0^\infty \frac{v^{s-1}}{1+v}\mathrm{d}v \\
&= 2i\sin(\pi s) \int_0^\infty \frac{v^{s-1}}{1+v}\mathrm{d}v.
\end{aligned}$$

Siccome questa quantità vale $2\pi i$ grazie al teorema dei residui, abbiamo che

$$\int_0^\infty \frac{v^{s-1}}{1+v}\mathrm{d}v = \frac{\pi}{\sin(\pi s)},$$

e ci siamo. Per ultieriori informazioni sulla funzione $\Gamma(s)$ si veda [Art64].

Consideriamo ora il seguente percorso di integrazione



detto *contorno di Henkel* e che indicheremo $\mathcal{H}$, e integriamo su di esso la funzione

$$\text{☯}_n(v) = (-v)^{s-1}e^{-nv},$$

dipendente dal parametro intero $n \geq 1$, sempre definendo $(-v)^{s-1} = e^{(s-1)log(-v)}$ e prendendo il ramo principale del logaritmo.

Osserviamo che anche in questo caso $\text{☯}_n(v) = O(v^{s-1})$ per $v \to 0$, e quindi se mandiamo a 0 il raggio r del dominio B l'integrale va a 0.

D'altro canto abbiamo ragionando come sopra che

$$\begin{aligned}\int_A \text{☯}_n + \int_C \text{☯}_n &= -\int_0^\infty \left(e^{(s-1)[\log(v)-i\pi]}\right) e^{-nv}\mathrm{d}v + \int_0^\infty \left(e^{(s-1)[\log(v)+i\pi]}\right) e^{-nv}\mathrm{d}v \\ &= \left[e^{(s-1)i\pi} - e^{-(s-1)i\pi}\right] \int_0^\infty v^{s-1}e^{-nv}\mathrm{d}v \\ &= 2i\sin(\pi(s-1)) \int_0^\infty n^{1-s}u^{s-1}e^{-u}n^{-1}\mathrm{d}u \qquad [\text{ponendo } v = n^{-1}u] \\ &= -2i\sin(\pi s)\frac{\Gamma(s)}{n^s}.\end{aligned}$$

In particolare abbiamo applicando la (7) che

$$\frac{1}{n^s} = -\frac{\Gamma(1-s)}{2\pi i}\int_{\mathcal{H}} \text{☯}_n,$$

e quindi se indichiamo con

$$\text{🕉}(v) = \frac{(-v)^{s-1}}{e^v - 1} = \sum_{n=1}^\infty (-v)^{s-1}e^{-nv} = \sum_{n=1}^\infty \text{☯}_n(v)$$

abbiamo ottenuto che

$$\zeta(s) = -\frac{\Gamma(1-s)}{2\pi i}\int_{\mathcal{H}} \text{🕉}(v)\mathrm{d}v. \tag{8}$$

La prima dimostrazione di Riemann dell'equazione funzionale procede ora così: la funzione 🕉(v) ha dei poli nei complessi della forma $2\pi in$ per tutti gli $n \in \mathbb{Z}$, ma se d'altra parte prendiamo dei raggi di integrazione r sempre più grandi della forma $r = 2\pi i(n + \frac{1}{2})$ abbiamo che sul dominio B la parte $1/(e^v - 1)$ è limitata (infatti questa funzione è periodica di periodo $2\pi i$ e scoppia solo attorno ai suoi poli), mentre la parte $(-v)^{s-1}$ va a 0 più velocemente di $1/v$ se $s < 0$.

Quindi

$$\int_B \text{🕉}(v)\mathrm{d}v \to 0 \qquad \text{per } r = 2\pi i\left(n + \frac{1}{2}\right),\ n \to \infty.$$

Di conseguenza possiamo calcolare l'integrale su $\mathcal{H}$ calcolando i residui di 🕉(v):

$$\int_{\mathcal{H}} \text{🕉}(v)\mathrm{d}v = -2\pi i \sum_{n\neq 0} \mathrm{Res}(\text{🕉}, 2\pi in). \tag{9}$$

Calcoliamo insieme il residuo in $2\pi in$ e $-2\pi in$, per n positivo:

$$\begin{aligned}\mathrm{Res}(\text{🕉}, 2\pi in) + \mathrm{Res}(\text{🕉}, -2\pi in) &= (-2\pi in)^{s-1} + (2\pi in)^{s-1} \\ &= e^{(s-1)[log(2\pi n)+i\frac{\pi}{2}]} + (2\pi)^{s-1}e^{(s-1)[log(2\pi n)-i\frac{\pi}{2}]} \\ &= (2\pi n)^{s-1}\cdot\left[e^{\pi i(s-1)/2} + e^{-\pi i(s-1)/2}\right] \\ &= (2\pi n)^{s-1}\cdot 2\cos\left(\frac{\pi(s-1)}{2}\right) \\ &= 2^s\pi^{s-1}\sin\left(\frac{\pi s}{2}\right)\frac{1}{n^{1-s}}.\end{aligned}$$

Sommando su tutti gli $n \in \mathbb{N}$, abbiamo grazie alla (9) che

$$\int_{\mathcal{H}} \text{🕉}(v)\mathrm{d}v = -i2^{s+1}\pi^s\sin\left(\frac{\pi s}{2}\right)\zeta(s-1),$$

che sostituendo nella (8) ci dice che

$$\zeta(s) = 2^s\pi^{s-1}\sin\left(\frac{\pi s}{2}\right)\Gamma(1-s)\zeta(1-s). \tag{10}$$

Abbiamo quindi ottenuto la versione 'asimmetrica' dell'equazione funzionale della $\zeta(s)$, si veda [Tit86, Cap. 2] per ulteriori dettagli e svariate altre dimostrazioni dell'equazione funzionale.

La (8) ci permette anche di calcolare il valore della $\zeta(s)$ negli interi negativi: infatti dato che

$$\frac{t}{e^t-1}=\sum_{k=0}^{\infty}B_k\frac{t^k}{k!},$$

abbiamo che se s è un intero negativo $s=1-n$ per qualche $n\in N$, allora

$$\text{ॐ}(v)=(-1)^{-n}\sum_{k=0}^{\infty}B_k\frac{t^{k-n-1}}{k!},$$

e in particolare e il coefficiente del termine di grado -1 è precisamente $(-1)^nB^n/n!$.

Ma se s è un intero la ॐ(v) è meromorfa e l'integrale su $\mathcal{H}$ equivale a $2\pi i\mathrm{Res}(\text{ॐ},0)$, e sostiuendo nella (8), e tenendo conto che $\Gamma(n)=(n-1)!$, abbiamo

$$\zeta(1-n)=(-1)^{n+1}\frac{B_n}{n}$$

(In realtà $B_n=0$ se n è dispari ≥ 3, e otteniamo gli zeri 'banali' della $\zeta(s)$ sugli interi negativi pari).

Infine, applicando l'equazione funzionale (10) per $s=1-n$ otteniamo che per n pari

$$\zeta(n)=(-1)^{n/2+1}2^{n-1}\pi^n\frac{B_n}{n!}$$

(visto che infatti $\sin(\pi(1-n)/2)=\cos(-\pi n/2)=(-1)^{n/2}$).

Si veda [Was97, Cap. 4] per il calcolo di valori speciali per le $L(s,\chi)$. □

Koan 7. *Un discepolo di Buddha si recò un giorno in viaggio fra le montagne, deciso a fare vita contemplativa dedicandosi completamente alla meditazione e alla ricerca dell'illuminazione.*

Quando dopo molti anni decise di tornare in India, dovette attraversare un passo montuoso dove si narrava che vivesse una creatura mostruosa con busto da amazzone, corpo da leone, ali da aquila, e che si cibava dei viaggiatori incauti che di là passavano.

Appena fu visto dalla sfinge, essa gli scaglio addosso un pesante masso. Ma lo studio del discepolo era stato tanto profondo al punto da acquisire poteri soprannaturali, e facendo appello alla sua natura ordinò al masso di fermarsi e cadere a terra.

La sfinge estrasse allora il pesante arco e gli scagliò una freccia. Ma tale era stato l'acuirsi dei sensi dello studioso che nel momento in cui percepì la freccia avvicinarsi egli si voltò, afferrandola cui denti. Prese la freccia fra le dita, e la scagliò alla sfinge con un movimento aggraziato e preciso, ferendola alla gamba.

Messa alle strette, la sfinge gli propose di dimostrare che

$$\prod_{n\geq 1}(1+q^{2n-1}z)(1+q^{2n-1}z^{-1})(1-q^{2n})=\sum_{\ell\in\mathbb{Z}}q^{\ell^2}z^{\ell}.$$

Non sappiamo cosa rispose l'illuminato, ma sappiamo che quando l'ebbe udito la sfinge perdette completamente la ragione e in preda alla disperazione si gettò da una rupe.

Interpretazione del koan. Richard Borcherds, che alcuni sospettano essere la reincarnazione dello studioso della storia, diede questa dimostrazione [Cam94, §13.3] dell'identità (del prodotto triplo di Jacobi).

Se rimpiazziamo q con $q^{1/2}$ e spostiamo a destra l'ultimo fattore del prodotto, l'identità prende la forma

$$\prod_{n\geq 1}(1+q^{n-1/2}z)(1+q^{n-1/2}z^{-1}) = \left(\sum_{\ell\in\mathbb{Z}} q^{\ell^2/2}z^\ell\right)\left(\prod_{n\geq 1}(1-q^n)^{-1}\right). \qquad (11)$$

Chiameremo *livello* un numero della forma $n+\frac{1}{2}$, dove $n\in\mathbb{Z}$. Uno *stato* è una collezione di livelli che contiene tutti i livelli negativi tranne al più una quantità finita, e una quantità finita di livelli positivi. Lo stato che contiene tutti i livelli negativi e nessuno positivo è detto *vuoto* e lo indicheremo con V. Dato uno stato S, definiamo la sua *energia* come

$$\sum_{\ell\in S,\ell>0}\ell - \sum_{\ell\notin S,\ell<0}\ell = \sum_{\ell\in S\triangle V}|\ell|,$$

indicando con $A\triangle B$ la differenza simmetrica $(A\setminus B)\cup(B\setminus A)$ per ogni coppia di insiemi A, B. Il *numero di particelle* di S è invece definito come

$$\#\{\ell\in S,\ell>0\} - \#\{\ell\notin S,\ell<0\} = \#(S\setminus V) - \#(V\setminus S).$$

Nonostante non sia necessario per la dimostrazione, diamo qualche informazione in più per dar e senso a questa notazione. Dirac mostrò che gli elettroni relativistici possono avere energia negativa oltre che positiva. Siccome essi tendono a saltare a un livello di energia minore se possibile, Dirac ipotizzò che nel vuoto tutti i livelli energetici negativi fossero occupati. Gli elettroni nei livelli energetici negativi non possono essere rilevati. Se un elettrone acquisisce abbastanza energia per saltare a un livello positivo, allora esso diventa 'visibile', e il 'buco' lasciato dietro si comporta come una particella con la stessa massa ma carica opposta di quella dell'elettrone (pochi anni più tardi, furono scoperti i positroni che soddisfano precisamente queste proprietà). Se il vuoto si considera senza nessuna particella e con energia zero, allora l'energia e il numero di particelle di un qualunque stato devono essere relativi al vuoto, dando luogo alle definizioni che abbiamo dato.

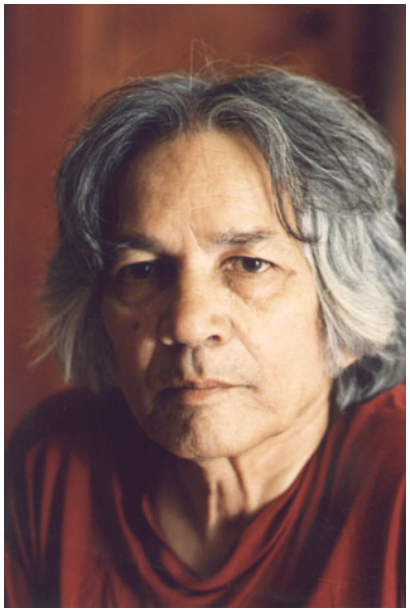


Figura 4: U. G. Krishnamurti, *My teaching, if that is the word you want to use, has no copyright. You are free to reproduce, distribute, interpret, misinterpret, distort, garble, do what you like, even claim authorship, without my consent or the permission of anybody.*

Mostreremo ora che il coefficiente di $q^m z^\ell$ in entrambi i membri della (11) è uguale al numero di stati di energia m e con numero di particelle ℓ.

Per il primo membro la dimostrazione è immediata. Un termine nell'espansione si ottiene selezionando $q^{n-1/2}z$ o $q^{n-1/2}z^{-1}$ da un numero finito di fattori. Questi corrispondono alla presenza di un elettrone nel livello positivo $n-\frac{1}{2}$ (che contribuisce $n-\frac{1}{2}$ all'energia e 1 al numero di particelle), o un buco nel livello negativo $-(n-\frac{1}{2})$ (che contribuisce $n-\frac{1}{2}$ all'energia e -1 al numero di particelle). Di conseguenza il coefficiente di $q^m z^\ell$ nel primo membro è come stabilito.

Per quanto riguarda il secondo membro, consideriamo per iniziare gli stati con numero di particelle 0. Ogni tale stato si ottiene in modo unico dal vuoto spostando

gli elettroni che si trovano nei k livelli negativi superiori in alto di $n_1, n_2, \ldots, n_k$, poniamo, con $n_1 \geq n_2 \geq \cdots \geq n_k$ (la monotonia equivale a richiedere che nell'operazione gli elettroni non si scavalchino). L'energia dello stato così ottenuto è quindi $n_1 + n_2 + \cdots + n_k$. Di conseguenza, il numero di stati con energia m e numero di particelle 0 è uguale al numero $p(m)$ di partizioni dell'intero m, ed è anche il coefficiente di q^m in $\Phi(q) = \prod_{n\geq 1}(1-q^n)^{-1}$.

Consideriamo ora gli stati con un numero positivo di particelle ℓ. Esiste un unico *stato base* con ℓ particelle, in cui sono occupati tutti i livelli negativi e i primi ℓ livelli positivi. L'energia di questo stato è $\frac{1}{2} + \frac{3}{2} + \cdots + \frac{2\ell-1}{2} = \frac{\ell^2}{2}$, e il suo numero di particelle ℓ. Qualunque altro stato con numero di particelle ℓ si ottiene da questo facendo 'saltare' gli elettroni come sopra, e quindi il numero di tali stati con energia m è $p(m - \frac{\ell^2}{2})$, essendo $\frac{\ell^2}{2}$ l'energia dello stato base, e questo è anche il coefficiente di $q^m z^\ell$ in $q^{\ell^2/2} z^\ell \Phi(q)$, come richiesto.

Similarmente si tratta il caso con un numero di particelle negativo (o alternativamente basta verificare che la (11) resta invariata rimpiazzando z con z^{-1}). □

Koan 8. *Un discepolo chiese un giorno ad un maestro Zen su cosa bisognasse meditare per raggiungere l'illuminazione. Il maestro gli rispose che non c'è un argomento in particolare, ma che ad esempio poteva meditare sul problema di stabilire se ogni sottogruppo normale di $SL_2(\mathbb{Z})$ di indice finito sia un sottogruppo di congruenza.*

Il discepolo decise che quello era un buon soggetto per la meditazione, e si dedicò lungamente e con grande dedizione ad esso.

Dopo alcuni anni, torno dal maestro, chiedendogli:

- *Maestro, ho meditato lungamente sull'argomento che mi avevate proposto, ma non sono giusto a nessuna conclusione.*
- *Che esperienza puoi trarre dalle tue meditazioni?*
- *Che la matematica non ha nessun senso, non serve a niente e che non è neppure in grado di soddisfare il nostro desiderio di spiegare la realtà.*
- *Ce ne hai messo ad arrivarci, che ci posso fare io se tu sei un po' lento?*

Udendo queste parole, il discepolo fu illuminato.

Interpretazione del koan. Mostreremo ora come sia possibile costruire un sottogruppo normale di indice finito di $SL_2(\mathbb{Z})$ che non può essere un sottogruppo di congruenza.

E' possibile costruire un omomorfismo surgettivo $\varphi : SL_2(\mathbb{Z}) \to A_6$ nel seguente modo: una presentazione di $PSL_2(\mathbb{Z})$ (che è un quoziente di $SL_2(\mathbb{Z})$) è data dal gruppo libero generato da a, b modulo le relazioni $a^2 = b^3 = 1$, ci basta quindi definire le immagini di a, b ad elementi di ordine $2, 3$. Prendiamo $\varphi(a) = \alpha, \varphi(b) = \beta$, dove

$$\alpha = (12)(3546), \qquad \beta = (123),$$

dobbiamo dimostrare che essi generano tutto A_6.

Una dimostrazione sintetica di questo fatto è la seguente: $\alpha^2 = (34)(56)$, quindi α^2 e β ristrette agli elementi $1, 2, 3, 4$ generano tutte le permutazioni. Inoltre essi agiscono sulla componente disgiunta $5, 6$, e sia $\tau = (56)$. Siccome sia α^2 che β sono permutazioni pari, abbiamo che su $1, \ldots, 6$ le permutazioni da essi generate sono tutte e sole quelle della forma $\tau^{\varepsilon(\sigma)}\sigma$, dove σ è un elemento che sposta soltanto $1, 2, 3, 4$ e $\varepsilon(\sigma)$ il suo segno.

Sia ora γ un qualunque elemento di A_6. E' facile vedere che possiamo costruire un elemento in termini di α e β che manda gli elementi $\gamma^{-1}(5), \gamma^{-1}(6)$ in $5, 6$, ad esempio mandando a posto come prima cosa $\gamma^{-1}(6)$ (il gruppo generato da α, β è ovviamente transitivo), e poi usando il fatto che $\beta^3\alpha\beta\alpha\beta = (13542)$.

Ora l'elemento δ che abbiamo ottenuto differisce da γ solo per un elemento $\gamma^{-1}\delta$ che è una permutazione pari di $1, 2, 3, 4$, e come abbiamo visto sopra queste appartengono tutte al gruppo generato.

Mostriamo ora che $\ker(\varphi)$ non può essere un sottogruppo di congruenza di $SL_2(\mathbb{Z})$, seguendo la traccia in [Rag04], [Rag05]. Per fare questo ci serve il

Teorema (Jordan-Hölder)**.** *Sia G un gruppo finito. Una successione di sottogruppi*

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_{r-1} \rhd H_r = 1$$

è detta serie di composizione *se H_{i+1} è un sottogruppo normale massimale di H_i, per $i = 0, \ldots, r-1$, e quindi i quozienti H_i/H_{i+1}, detti* fattori di composizione*, sono semplici e non banali.*

Abbiamo che se sono date due distinte serie di composizione, allora esse hanno la stessa lunghezza, e fattori di composizione coincidono a meno di permutazione.

Anche se questo teorema dovesse risultarvi ovvio, siccome ho avuto la malsana idea di scrivere delle dispense Zen non posso risparmiare la dimostrazione:

Dimostrazione. La dimostrazione procede per induzione sull'ordine di G, e se G è semplice il risultato è banalmente vero. Supponiamo quindi di avere due serie di composizione

$$G \rhd H \rhd H_1 \rhd \cdots \rhd H_r = 1, \qquad G \rhd K \rhd K_1 \rhd \cdots \rhd K_s = 1,$$

e osserviamo che se $H_1 \neq K_1$ la tesi segue immediatamente grazie all'impotesi induttiva.

Supponiamo quindi $H \neq K$, e osserviamo che essendo H, K distinti e massimali si deve forzatamente avere $HK = G$. Sia $L = H \cap K$, e osserviamo che per il secondo teorema di omomorfismo abbiamo che $G/H \cong K/L$ e $G/K \cong H/L$ (no, la dimostrazione di questo non la metto neppure in queste dispense Zen, andatevi a vedere un libro di algebra o qualche pergamena Buddhista).

Sia ora $L \rhd L_1 \rhd \cdots \rhd L_t = 1$ una qualunque serie di composizione per L, e osserviamo ora che le due serie di composizione

$$G \rhd H \rhd H_1 \rhd \cdots \rhd H_r = 1, \qquad G \rhd H \rhd L \rhd L_1 \rhd \cdots \rhd L_t = 1,$$

hanno la stessa lunghezza e gli stessi fattori di composizione a meno di permutazione, applicando l'ipotesi induttiva su H. Analogamente abbiamo lo stesso per le serie

$$G \rhd K \rhd K_1 \rhd \cdots \rhd K_s = 1, \qquad G \rhd K \rhd L \rhd L_1 \rhd \cdots \rhd L_t = 1,$$

e siccome abbiamo visto che i quozienti che compaiono in $G \rhd K \rhd L$ sono gli stessi che compaiono in $G \rhd K \rhd L$, la tesi segue. □

Supponiamo che il kernel di $\varphi : SL_2(\mathbb{Z}) \to A_6$ esso contenga un qualche $\Gamma(N)$, che è anche il kernel della mappa naturale surgettiva $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$. Avremmo allora che A_6 è un quoziente di $SL_2(\mathbb{Z}/N\mathbb{Z})$, il quale, se la fattorizzazione di N è $\prod p_i^{e_i}$, è a sua volta isomorfo a $\prod SL_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$.

Applicando Jordan-Hölder alla nostra situazione, abbiamo che A_6 deve essere un quoziente di $SL_2(\mathbb{Z}/p^e\mathbb{Z})$ per $p = p_i, e = e_i$ per qualche i. Osserviamo ora che il kernel della mappa $SL_2(\mathbb{Z}/p^e\mathbb{Z}) \to SL_2(\mathbb{Z}/p\mathbb{Z})$ di riduzione modulo p è un p-gruppo, e quindi sempre per Jordan-Hölder A_6 o è un quoziente di $SL_2(\mathbb{Z}/p\mathbb{Z})$ o è un p-gruppo, ma quest'ultima possibilità è assurda (un p-gruppo ha addirittura sottogruppi normali di ogni ordine). Infine, $SL_2(\mathbb{Z}/p\mathbb{Z})$ ha il sottogruppo normale di ordine due $\{\pm Id\}$, e quindi A_6 deve essere un quoziente di $SL_2(\mathbb{Z}/p\mathbb{Z})/\{\pm Id\} \cong PSL_2(\mathbb{Z}/p\mathbb{Z})$.

Ma eccetto che per $PSL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$ e $PSL_2(\mathbb{Z}/3\mathbb{Z}) \cong A_4$, il gruppo $PSL_2(\mathbb{Z}/p\mathbb{Z})$ è semplice e ha ordine $(p-1)p(p+1)$, e dovrebbe quindi essere isomorfo ad A_6, ma

questo è impossibile avendo A_6 ordine 360 (lo so, una dimostrazione della semplicità di $PSL_2(\mathbb{Z}/p\mathbb{Z})$ tolte le eccezioni sopra dette gioverebbe sicuramente all'aspirante illuminato, se ne farà forse oggetto di un futuro koan).

Caso di $SL_n(\mathbb{Z})$. Può essere interessante sapere che per $n \geq 3$, un risultato *difficile* di Bass-Lazard-Serre [BLS64], e, indipendentemente, Mennicke, [Men65] dice che per $n \geq 3$ invece *tutti* i sottogruppi normali di indice finito sono sottogruppi di congruenza. Il problema è stato studiato anche per altri gruppi classici e su anelli diversi da $\mathbb{Z}$, ad esempio da Bass-Milnor-Serre [BMS67]. □

Koan 9. *Chiese un giorno un discepolo al suo maestro:*

- *Maestro, perché non ci insegnate che le somme di Gauss sono dei prodotti scalari di un carattere moltiplicativo modulo N con i vettori di una base dello spazio delle funzioni periodiche di periodo N da $\mathbb{Z}$ in $\mathbb{C}$?*
- *Perché non sareste in grado di concepirne l'importanza se noi vi dessimo direttamente questa informazione anziché lasciarvi il piacere di arrivarci attraverso sudati conti.*
- *Ma maestro, ci sono altri fatti importanti che farei bene a sapere ma non mi avete mai detto?*
- *Ma no, figurati! Tranquillo! Hai la mia parola.*

Interpretazione del koan. Definiamo sulle funzioni da $\mathbb{Z} \to \mathbb{C}$ periodiche di periodo N il prodotto scalare hermitiano

$$\langle \alpha, \beta \rangle = \frac{1}{N} \sum_{a \pmod N} \alpha(a)\overline{\beta(a)}.$$

Se definiamo η_m come la funzione su $\mathbb{Z}$ a valori complessi

$$\eta_m(a) = e^{-2\pi i m a/N},$$

possiamo osservare che $\langle \eta_m, \eta_n \rangle$ vale 1 se $m \equiv n \pmod N$ e 0 altrimenti, come è possibile verificare facilmente a mano (e infatti le η_m sono i 'veri' caratteri del gruppo ciclico $\mathbb{Z}/N\mathbb{Z}$, e il prodotto scalare appena introdotto è precisamente il prodotto scalare definito sui caratteri).

Abbiamo allora che $\tau(\chi)/N = \langle \chi, \eta_1 \rangle$ per ogni carattere di Dirichlet χ primitivo modulo N, e la formula

$$\sum_{a \bmod N} \chi(a) e^{2\pi i m a/N} = \chi(m)\tau(\chi)$$

diventa

$$\langle \chi, \eta_m \rangle = \chi(m)\langle \chi, \eta_1 \rangle. \tag{12}$$

Alla vista di questo fatto, diventa molto facile dimostrare che $|\tau(\chi)| = \sqrt{n}$. Infatti se $x = \langle \chi, \eta_1 \rangle$, i prodotti scalari $\langle \chi, \eta_m \rangle$ sono tutti della forma $\alpha_m x$ per una qualche radice dell'unità α_m nel caso in cui $(m, N) = 1$, e 0 altrimenti. Quindi

$$\chi = \sum_{m \bmod N} \langle \chi, \eta_m \rangle \cdot \eta_m = \sum_{\substack{m \bmod N \\ (m,N)=1}} \alpha_m x \cdot \eta_m,$$

da cui

$$\langle \chi, \chi \rangle = \sum_{\substack{m \bmod N \\ (m,N)=1}} x^2 = \varphi(N)|x|^2.$$

Ma d'altra parte applicando la definizione abbiamo chiaramente che

$$\langle \chi, \chi \rangle = \varphi(N)/N,$$

da cui $|x| = 1/\sqrt{N}$, e di conseguenza $|\tau(\chi)| = \sqrt{N}$.

Un'altra conseguenza della (12) è la seguente: se rimpiazziamo nella somma m con $-m$, e scriviamo

$$\langle \chi, \eta_{-m} \rangle = \overline{\chi(-m)} \langle \chi, \eta_1 \rangle = \chi(-1) \langle \chi, \eta_1 \rangle \cdot \overline{\chi(m)},$$

abbiamo che

$$\chi = \chi(-1) \langle \chi, \eta_1 \rangle \sum_{m \bmod N} \overline{\chi(m)} \eta_{-m},$$

un identità fra funzioni da $\mathbb{Z} \to \mathbb{C}$.

Facendo la somma $\sum_{n \geq 1} f(n)/n$ in entrambi i membri otteniamo

$$L(1, \chi) = -\chi(-1) \langle \chi, \eta_1 \rangle \sum_{m \bmod N} \overline{\chi(m)} \log(1 - e^{2\pi i m/N}) \tag{13}$$

$$= -\frac{\chi(-1)\tau(\chi)}{N} \sum_{m \bmod N} \overline{\chi(m)} \log(1 - e^{2\pi i m/N}) \tag{14}$$

nella notazione classica.

Ora, se $\log(x)$ è il ramo principale del logaritmo, abbiamo che da una parte

$$\log(1 - e^{2\pi i m/N}) + \log(1 - e^{-2\pi i m/N}) = \log\left[(1 - e^{2\pi i m/N})\overline{(1 - e^{2\pi i m/N})}\right]$$
$$= \log\left|1 - e^{2\pi i m/N}\right|^2 = 2\log\left|1 - e^{2\pi i m/N}\right|,$$

mentre dall'altra

$$\log(1 - e^{2\pi i m/N}) - \log(1 - e^{-2\pi i m/N}) = \log\left(\frac{1 - e^{2\pi i m/N}}{1 - e^{-2\pi i m/N}}\right)$$
$$= \log(-e^{2\pi i m/N}) = 2\pi i m/N - \pi i = \frac{\pi i}{N}(2m - N),$$

grazie al fatto che il prodotto di due complessi con parte reale positiva non fa il giro oltre l'asse reale negativo e quindi $\log(x) + \log(y) = \log(xy)$ per due tali x, y se si prende il ramo principale del logaritmo.

Se prendiamo la (14) e sommiamo insieme i termini in m e $-m$ per $0 < m < N/2$, abbiamo quindi grazie alle espansioni che abbiamo appena dato che

$$L(1, \chi) = \begin{cases} -\dfrac{\tau(\chi)}{N} \displaystyle\sum_{m \bmod N} \overline{\chi(m)} \log\left|1 - e^{2\pi i m/N}\right| & \text{se } \chi(-1) = 1, \\ \dfrac{\pi i \tau(\chi)}{N^2} \displaystyle\sum_{m=1}^{N} \overline{\chi(m)} m & \text{se } \chi(-1) = -1. \end{cases}$$

□

Koan 10. *Verso l'anno 1256, un saggio e anziamo maestro di scuola coreano si faceva carico dell'istruzione dei giovani, ai quali insegnava severamente l'arte dei numeri. Da sempre egli aveva rifiutato che si introducesse alcun precetto religioso nei suoi insegnamenti, considerando tali discipline come un vizio della gente da poco, che poteva soltanto distrarre le giovani menti dal vero apprendimento.*

Grandemente temuto era dai bambini della sua scuola, ai quali era solito infliggere pesanti punizioni fisiche.

Un giorno in cui la sua mente era concentrata sullo stabilire se $PSL_2(\mathbb{Z})$ sia il prodotto libero $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$, problema a cui aveva dedicato la vita senza esser mai giunto ad alcuna conclusione, fu disturbato da due dei suoi scolari che schiamazzavano:

- *Qual è la somma dei numeri razionali a/b e c/d?*

L'anziano maestro, seccato, prese il suo bastone, e si diresse verso i bambini, convinto che una congrua dose di legnate avrebbe sia giovato all'educazione dei ragazzi, sia li avrebbe aiutati a comprendere la risposta alla loro domanda.

• *Ignorante! - Urlò uno di essi - Ovviamente è* $\frac{a+c}{b+d}$ *!!!*

Udendo queste parole, l'aziano maestro fu illuminato.

Interpretazione del koan. È ben noto che $PSL_2(\mathbb{Z})$ è generato dalle proiezioni di

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

Se poniamo $a = S$ e $b = ST$, possiamo verificare facilmente che $a^2 = b^3 = 1$, e siccome essi generano $PSL_2(\mathbb{Z})$ ci basta mostrare che essi non hanno relazioni. Ma nel gruppo finitamente presentato generato da a, b con $a^2 = b^3 = 1$ ogni elemento può essere scritto in termini di a, b con a che compare alla prima potenza e b alla prima o alla seconda. Quindi se $\ell = ab$ e $r = ab^2$ (ℓ, r stanno per *left* e *right*) ogni elemento si scrive in modo unico come nella forma $a^e \ell r r \ell \dots r r \ell r \ell \ell a^f$, con $e, f \in \{0, 1\}$, e in mezzo ad a^e e a^f una qualunque successione finita di ℓ e r. Ci basta quindi mostrare che una qualunque successione finita di ℓ, r è diversa da 1 per mostrare che a, b non hanno relazioni.

Ma abbiamo (a meno del segno essendo in $PSL_2(\mathbb{Z})$) che

$$\ell = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad r = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

e consideriamo le frazioni di Farey consecutive iniziali $1/0$ e $0/1$, che scriviamo come matrice $\begin{pmatrix} 1 \ / \ 0 \\ 0 \ / \ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Se ora trasformiamo una coppia di frazioni di Farey scrite in minimi termini a/b e c/d in una matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, abbiamo che la matrice ℓM è la matrice corrispondente alla coppia di frazioni consecutive $(a+c)/(b+d)$ e c/d, mentre rM corrisponde alla coppia di a/b e $(a+c)/(b+d)$.

Quindi partire dall'identità e moltiplicare a sinistra successivamente per ℓ o r corrisponde a partire dalle frazioni di Farey $1/0$ e $0/1$, e passare ad ogni passo dalla coppia a/b,c/d alla coppia di frazioni di Farey interna sinistra o destra, ed è quindi chiaro che ℓ, r non possono soddisfare relazioni.

ℓ, r generano il cosiddetto *monoide diadico*, che codifica la posizione di un nodo nell'albero binario (detto di Stern-Brocott) che abbiamo costruito con le coppie di frazioni di Farey. □

RIFERIMENTI BIBLIOGRAFICI

[Art64] E. Artin, *The Gamma Function*, Holt, Rinehart and Winston, 1964.

[BLS64] H. Bass, M. Lazard, and J.P. Serre, *Sous-groupes d'indice fini dans SL (n, Z)*, Bull. Amer. Math. Soc **70** (1964), 385–392.

[BMS67] H. Bass, J. Milnor, and J.P. Serre, *Solution of the congruence subgroup problem for* $SL_n (n \geq 3)$ *and* $Sp_{2n} (n \geq 2)$, Publications Mathématiques de l'IHÉS **33** (1967), 59–137.

[Cam94] P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, 1994.

[Kno56] K. Knopp, *Infinite Sequences and Series*, Courier Dover Publications, 1956.

[Kor04] J. Korevaar, *Tauberian Theory: A Century of Developments*, Springer, 2004.

[Men65] J. Mennicke, *Finite factor groups of the unimodular group*, Ann. Math **81** (1965), no. 1, 31–37.

[Rag04] M.S. Raghunathan, *The congruence subgroup problem*, Proceedings Mathematical Sciences **114** (2004), no. 4, 299–308.

[Rag05] ———, *Erratum*, Proceedings Mathematical Sciences **115** (2005), no. 3, 369–369.

[Tit86] E.C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford University Press, 1986.

[Was97] L.C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1997.

SCUOLA NORMALE SUPERIORE DI PISA - PIAZZA DEI CAVALIERI, 7 - 56126 PISA

E-mail address: maurizio.monge@gmail.com