Capitolo 8

Irrazionalità e trascendenza di π

In questo capitolo vengono presentate le dimostrazioni dell'irrazionalità e della trascendenza di π. Come abbiamo visto nei capitoli precedenti, nelle attività laboratoriali proposte in questo elaborato la natura di π viene scoperta e narrata ai ragazzi, con l'utilizzo di alcuni artefatti. Non viene naturalmente dimostrata perché tale dimostrazione non è alla portata degli studenti delle scuole secondarie. Il docente che decide di intraprendere un percorso laboratoriale come quello descritto nei precedenti capitoli sarebbe bene avesse comunque un'idea di queste dimostrazioni. Per questo motivo si è scelto di trattarle nei prossimi paragrafi. Per la stesura di questo capitolo si è fatto riferimento alla seguente fonte [25].

8.1 Irrazionalità di π

Per dimostrare l'irrazionalità di π faremo uso dei polinomi di Niven. Richiamiamo quindi la definizione di polinomio per poi passare a quella dei polinomi di Niven.

Definizione 8.1. *Sia $\mathbb{Z}[x_1, ..., x_n]$ l'anello dei polinomi in $x_1, ..., x_n$ a coefficienti interi. Un* ***polinomio*** *è una somma finita di monomi dove un monomio è un'espressione del tipo*

$$ax_1^{i_1} \cdots x_n^{i_n}, \quad a \in \mathbb{Z}, a \neq 0,\ i_1, ..., i_n \geq 0.$$

Di un monomio chiamiamo ***grado*** *il numero $i_1 + \cdots + i_n$, e chiamiamo* ***peso*** *il numero $i_1 + 2i_2 + \cdots + ni_n$.*

Definizione 8.2. *Si chiamano* ***polinomi di Niven*** *i polinomi del tipo*

$$f_n(x) = \frac{x^n(1-x)^n}{n!},\ n \geq 0.$$

Tali polinomi sono dotati della proprietà che tutte le loro derivate, di qualsiasi ordine,

$$f_n^0(x) = f_n(x),\;\; f_n^1(x) = f_n'(x),\;\; f_n^2(x) = f_n''(x),\; ...,\; f_n^{(h)}(x),\; ...$$

assumono valori interi per $x = 0, 1$. Infatti, segue subito dalla formula di Leibniz che $f_n^{(h)}(0) = f_n^{(h)}(1) = 0$, $\forall h < n$. Inoltre, per ogni polinomio a coefficienti interi $g(x) \in \mathbb{Z}[x]$, i coefficienti di $g^{(h)}(x)$ sono tutti divisibili per $h!$. Prendendo $g(x) = x^n(1-x)^n$ si ottiene

$$f_n^{(h)}(m) \in \mathbb{Z} \;\; \forall h \geq n, m \in \mathbb{Z}.$$

Osserviamo anche che la stessa proprietà vale per tutti i polinomi del tipo $f_n(x)h(x)$, con $h(x) \in \mathbb{Z}[x]$. Possiamo ora dimostrare l'irrazionalità di π^2 dalla quale segue l'irrazionalità di π. Infatti, se un numero elevato alla seconda è irrazionale allora anche quel numero deve essere irrazionale.

Teorema 8.3. ***(Irrazionalità di*** π^2***)*** *π^2 è un numero irrazionale.*

Dimostrazione Supponiamo per assurdo che $\pi^2 = \frac{a}{b}$, cioè $\frac{a}{\pi} = b\pi$, con a, b interi positivi. Sia $g(x)$ un polinomio di grado minore o uguale di $2n$ con la proprietà che $g(x)$ e tutte le sue derivate $g'(x), g''(x), ..., g^{(h)}(x), ...$ assumono valori interi per $x = 0, 1$. Osserviamo che per $h \geq 2n$ la derivata $g^{(j)}(x)$ è ovviamente nulla. Allora l'integrale

$$\int_0^1 \pi a^n g(x) \sin(\pi x) dx$$

è un numero intero. Infatti integrando per parti si ha che

$$\int_0^1 \pi a^n g(x) \sin(\pi x) dx = -a^n \int_0^1 g(x)(-\pi \sin(\pi x)) dx =$$

$$= a^n g(1) + a^n g(0) + a^n \int_0^1 cos(\pi x) g'(x) dx =$$

$$= a^n g(1) + a^n g(0) + \frac{a^n}{\pi} \int_0^1 \pi cos(\pi x) g'(x) dx =$$

$$= a^n g(1) + a^n g(0) - \frac{a^n}{\pi} \int_0^1 sin(\pi x) g''(x) dx =$$

$$= a^n g(1) + a^n g(0) + \frac{a^n}{\pi^2} \int_0^1 (-\pi sin(\pi x)) g''(x) dx =$$

$$= a^n g(1) + a^n g(0) - ba^{n-1} g''(1) - ba^{n-1} g''(0) - ba^n \int_0^1 cos(\pi x) g'''(x) dx.$$

Iterando questo procedimento, al passo $2n + 2$ avremmo una somma algebrica di numeri interi sommata all'integrale

$$a \int_0^1 sin(\pi x) g^{(2n+2)}(x) dx$$

che è uguale a zero dato che $g^{(2n+2)}(x) = 0$. Si può quindi concludere che

$$\int_0^1 \pi a^n g(x) \sin(\pi x) dx \in \mathbb{Z}.$$

In particolare, considerando i polinomi di Niven si ottiene che

$$\int_0^1 \pi a^n f_n(x) \sin(\pi x) dx \in \mathbb{Z}$$

per ogni n.
D'altra parte, dato che $sin(\pi x) \leq 1$ e $x(1-x) \leq 1$ per ogni $0 \leq x \leq 1$ si ha

$$0 < \int_0^1 \frac{\pi a^n}{n!} x^n (1-x)^n \sin(\pi x) dx < \frac{\pi a^n}{n!}.$$

Ma per n sufficientemente grande abbiamo che $\frac{\pi a^n}{n!} < 1$ e quindi

$$0 < \int_0^1 \frac{\pi a^n}{n!} x^n (1-x)^n \sin(\pi x) dx < 1$$

che è in contraddizione con il fatto che $\int_0^1 \frac{\pi a^n}{n!} x^n (1-x)^n \sin(\pi x) dx$ fosse un numero intero.

□

8.2 Funzioni simmetriche

Dopo aver richiamiamo alcune definizioni che caratterizzano i polinomi, passiamo poi alla definizione delle funzioni simmetriche e alla dimostrazione di alcune delle loro proprietà che ci serviranno per dimostrare la trascendenza di π.

Definizione 8.4. *Un polinomio in cui tutti i monomi hanno lo stesso grado si dice **omogeneo**, mentre un polinomio in cui tutti i monomi hanno lo stesso peso si dice **isobaro**.*

Osserviamo che ogni polinomio si scrive in maniera unica come somma di polinomi isobari, inoltre, il peso della somma è minore uguale al massimo dei pesi mentre il peso del prodotto è la somma dei pesi.

Definizione 8.5. *Un polinomio $p \in \mathbb{Z}[x_1, ..., x_n]$ si dice* ***simmetrico*** *se*

$$p(x_1, ..., x_n) = p(x_{\sigma(1)}, ..., x_{\sigma(n)})$$

per ogni permutazione $\sigma : \{1, ..., n\} \to \{1, ..., n\}$.

Un polinomio è simmetrico se e solo se tutte le sue componenti omogenee sono simmetriche.
Indichiamo con Σ_n il gruppo delle permutazioni dell'insieme $\{1, ..., n\}$.

Definizione 8.6. *Per ogni intero positivo n, le* ***funzioni simmetriche elementari*** *$\sigma_1, ..., \sigma_n \in \mathbb{Z}[x_1, ..., x_n]$ sono definite dalla relazione*

$$t^n + \sigma_1(x_1, ..., x_n)t^{n-1} + \cdots + \sigma_n(x_1, ..., x_n) = \prod_{i=1}^{n}(t + x_i).$$

In altre parole, i valori delle funzioni simmetriche elementari calcolate su di una n-upla di numeri complessi $(a_1, ..., a_n)$ sono i coefficienti del polinomio monico di grado n che ha come radici $-a_1, ..., -a_n$.
Osserviamo che σ_i è omogeneo di grado i e tra i suoi monomi $x_{n-i+1} \cdots x_{n-1}x_n$ è l'unico di peso più alto. Il teorema che andremmo a dimostrare ora è noto come il *Teorema fondamentale dei polinomi simmetrici.*

Teorema 8.7. *Ogni polinomio simmetrico a coefficienti interi si può esprimere come un polinomio a coefficienti interi nelle funzioni simmetriche elementari.*

Questo teorema significa che un polinomio $p \in \mathbb{Z}[x_1, ..., x_n]$ è simmetrico se e solo se esiste un polinomio $q \in \mathbb{Z}[y_1, ..., y_n]$ tale che

$$p(x_1, ..., x_n) = q(\sigma_1, ..., \sigma_n).$$

Dimostrazione Sia $p \in \mathbb{Z}[x_1, ..., x_n]$ simmetrico e sia $p = p_0 + \cdots + p_m$ la decomposizione in componenti isobare, con p_i di peso i e $p_m \neq 0$. Dimostriamo che p è un polinomio nelle funzioni simmetriche elementari. Procediamo per induzione su m.
Se $m = 0$ allora p_0 è costante dato che è un polinomio di grado zero e quindi è scritto nelle funzioni simmetriche elementari. Supponiamo l'affermazione vera per $m - 1$, cioè p_{m-1} si può scrivere nelle funzioni simmetriche elementari e dimostriamolo per p_m.
Ogni monomio di p_m è del tipo $ax_1^{i_1}x_2^{i_2} \cdots x_n^{i_n}$ con $i_1 \leq i_2 \leq \cdots \leq i_n$; quindi, se poniamo $y_i = x_{n-i+1}x_{n-i+2} \cdots x_n$, si ha

$$ax_1^{i_1}x_2^{i_2} \cdots x_n^{i_n} = ay_1^{b_1} \cdots y_n^{b_n}, \quad b_n = i_1, b_{n-1} = i_2 - i_1, ...$$

Dunque esiste un polinomio $q \in \mathbb{Z}[y_1, ..., y_n]$ tale che $p_m(x_1, ..., x_n) = q(y_1, ..., y_n)$. Il polinomio $p(x_1, ..., x_n) - q(\sigma_1, ..., \sigma_n)$ è simmetrico di peso minore di m e quindi per ipotesi induttiva p si può scrivere come polinomio nelle funzioni simmetriche elementari.

□

Corollario 8.8. *Consideriamo due polinomi $f, g \in \mathbb{Z}[t]$, con $deg(g) \leq n$ e*

$$f(t) = a(t-\alpha_1)\cdots(t-\alpha_m), \quad a \neq 0, m > 0, \alpha_i \in \mathbb{C}.$$

Allora, per ogni intero $p \geq 0$, si ha:

$$\sum_{i=1}^{m}(a\alpha_i)^p \in \mathbb{Z},$$

$$\frac{a^{n-p}}{p!}\sum_{i=1}^{m} g^{(p)}(\alpha_i) \in \mathbb{Z}.$$

Dimostrazione Osserviamo che i numeri complessi $a\alpha_1, ..., a\alpha_n$ sono le radici, contate con molteplicità, del polinomio monico a coefficienti interi

$$a^{m-1} f\left(\frac{t}{a}\right). \tag{8.1}$$

Dato che il polinomio 8.1 ha coefficienti interi allora tutte le funzioni simmetriche elementari calcolate in essi risultano essere intere

$$\sigma_i(a\alpha_1, ..., a\alpha_n) \in \mathbb{Z} \quad \textit{per ognii}.$$

Risulta quindi intero anche il valore in esse del polinomio $x_1^p + \cdots + x_n^p$ da cui segue la prima equazione. Dimostriamo ora la seconda condizione. Consideriamo il caso $g = t^q$ con $q \leq n$. Se $p > q$ siamo a posto dato che $g^{(p)} = 0$ se invece, $p \leq q$ abbiamo che

$$\frac{a^{n-p}}{p!}\sum_{i=1}^{m} g^{(p)}(\alpha_i) = \frac{a^{n-p}}{p!}\sum_{i=1}^{m} q(q-1)\cdots(q-(p-1))(\alpha_i)^{q-p} =$$

$$= \frac{a^{n-p}}{p!}\sum_{i=1}^{m}\frac{q!}{(q-p)!}(\alpha_i)^{q-p} = a^{n-q}\binom{q}{p}\sum_{i=1}^{m}(a\alpha_i)^{q-p}$$

che è un intero dato che $\sum_{i=1}^{m}(a\alpha_i)^{q-p} \in \mathbb{Z}$.

□

8.3 Numeri algebrici e trascendenti

In questo paragrafo vengono richiamate le definizioni di numero algebrico e trascendente. Vengono inoltre illustrate alcune delle proprietà che caratterizzano questi numeri per concludere con una piccola discussione sull'esistenza dei numeri trascendenti.

Definizione 8.9. *Un numero complesso viene detto* ***algebrico*** *se è radice di un polinomio non nullo a coefficienti razionali $f(t) \in \mathbb{Q}[t]$. Un numero complesso che non è algebrico viene detto* ***trascendente****.*

In altre parole, un numero $\alpha \in \mathbb{C}$ è algebrico se e solo se esistono un intero positivo n e $n+1$ numeri razionali $a_0, a_1, ..., a_n$ tali che

$$a_n \neq 0, \quad a_0 + a_1\alpha + ... + a_n\alpha^n = 0. \tag{8.2}$$

Osserviamo che ogni numero razionale $x = \frac{p}{q}$ è algebrico dato che è radice del polinomio $qx - p$.
Inoltre, se α è un numero algebrico diverso da 0, allora anche α^{-1} è algebrico infatti dividendo la 8.2 per α^n si ottiene

$$a_0(\alpha^{-1})^n + a_1(\alpha^{-1})^{n-1} + \cdots + a_{n-1}\alpha^{-1} + a_n.$$

Nella definizione di numero algebrico non è restrittivo supporre che il polinomio $f(t)$ sia monico, cioè $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_n$. In alternativa, non è restrittivo nemmeno supporre che il polinomio $f(t)$ sia a coefficienti interi infatti basta moltiplicare per un denominatore comune.

Definizione 8.10. *Il* ***grado*** *di un numero algebrico $\alpha \in \mathbb{C}$ è il più piccolo intero positivo d tale che x è radice di un polinomio di grado d a coefficienti interi.*

Lemma 8.11. *Un numero complesso α è algebrico se e solo se può essere esteso ad una successione finita $\alpha = \alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{C}$ tale che*

$$f(t) = \prod_{i=1}^{n}(t - \alpha_i) \in \mathbb{Q}[t].$$

Dimostrazione Per il teorema fondamentale dell'algebra ogni polinomio a coefficienti complessi si scrive come prodotto di polinomi di primo grado.

□

Lemma 8.12. *Siano $\alpha_1, ..., \alpha_n \in \mathbb{C}$, $n \geq 2$, numeri complessi non necessariamente distinti tali che*

$$f(t) = \prod_{i=1}^{n}(t - \alpha_i) \in \mathbb{Q}[t].$$

Allora i numeri $\alpha_i + \alpha_j$ e $\alpha_i\alpha_j$ sono algebrici per $i \neq j$.

Dimostrazione Per ipotesi le funzioni simmetriche elementari $\sigma_i(\alpha_1, ..., \alpha_n)$ sono numeri razionali dato che coincidono, a meno del segno, con i coefficienti di $f(t)$. Consideriamo i polinomi

$$g(t) = \prod_{i \neq j}(t - \alpha_i - \alpha_j),$$

$$h(t) = \prod_{i \neq j}(t - \alpha_i \alpha_j).$$

Ogni coefficiente di $g(t)$ e $h(t)$ è un polinomio simmetrico a coefficienti interi in $\alpha_1, ..., \alpha_n$ ed è quindi esprimibile come un polinomio a coefficienti interi nelle funzioni simmetriche elementari. Dunque $g(t), h(t) \in \mathbb{Q}[t]$ e di conseguenza $\alpha_i + \alpha_j$ e $\alpha_i \alpha_j$ sono algebrici per ogni $i \neq j$.

□

Teorema 8.13. *Somme e prodotti di numeri algebrici sono ancora numeri algebrici.*

Dimostrazione Siano α, β due numeri algebrici. Per il teorema fondamentale dell'algebra esistono due successioni $\alpha_1, \alpha_2, ..., \alpha_n$ e $\beta_1, \beta_2, ..., \beta_m$ tali che $\alpha = \alpha_1$, $\beta = \beta_1$ e

$$f_1(t) = \prod_{i=1}^{n}(t - \alpha_i) \in \mathbb{Q}[t],$$

$$f_2(t) = \prod_{i=1}^{m}(t - \beta_i) \in \mathbb{Q}[t].$$

Applicando il lemma precedente al polinomio $f(t) = f_1(t) f_2(t)$ si ottiene quindi la conclusione.

□

Dimostrare l'esistenza dei numeri trascendenti è semplice. Una dimostrazione dell'esistenza dei numeri trascendenti fu data da G. F. Cantor nel 1874. Essa si basa sul fatto che la cardinalità dell'insieme dei numeri reali è strettamente maggiore di quella dell'insieme dei numeri reali algebrici. Infatti si può dimostrare che l'insieme dei numeri algebrici è numerabile ma i numeri reali hanno la potenza del continuo, perciò non solo esistono numeri reali non algebrici (numeri trascendenti), ma essi costituiscono un insieme avente la potenza del continuo. [24]
Complicato è invece dimostrare che un determinato numero è trascendente. Nei prossimi paragrafi vedremo la dimostrazione della trascendenza di π.

8.4 Alcune stime

Per dimostrare la trascendenza di π dobbiamo prima dimostrare alcune disuguaglianze.
Consideriamo $f(x) \in \mathbb{C}[x]$, $f(x) = \sum a_i x^i$. Denotiamo con $f^{(p)}(x)$ la sua derivata p-esima e con $\tilde{f}(x) = \sum |a_i| x^i$. Osserviamo che

$$\tilde{f}^{(p)}(0) = p!|a_p| = |f^{(p)}(0)|.$$

Lemma 8.14. *Siano $f, g \in \mathbb{C}[x]$, allora per ogni numero reale $a \geq 0$ vale*

$$0 \leq \widetilde{fg}(a) \leq \tilde{f}(a)\tilde{g}(a).$$

Dimostrazione Conseguenza della disuguaglianza triangolare $|z+w| \leq |z| + |w|$ $z, w \in \mathbb{C}$. Infatti dati $f(x) = \sum_{i=1}^{n} b_i x^i$ e $\sum_{j=1}^{m} c_j x^j$, abbiamo che

$$\widetilde{fg}(a) = \sum_{h=0}^{n+m} \mid \sum_{i+j=h} b_i c_j \mid a^h \leq \sum_{h=0}^{n+m} \sum_{i+j=h} \mid b_i c_j \mid a^h = \tilde{f}(a)\tilde{g}(a).$$

□

Richiamiamo che una serie di numeri complessi $\sum_{n=0}^{\infty} a_n$ si dice assolutamente convergente se $\sum_{n=0}^{\infty} |a_n| < +\infty$. Se $a_n = b_n + ic_n$, con $b_n, c_n \in \mathbb{R}$ e $\sum_{n=0}^{\infty} a_n$ è assolutamente convergente, allora anche le serie $\sum_{n=0}^{\infty} b_n$ e $\sum_{n=0}^{\infty} c_n$ sono assolutamente convergenti e si può scrivere

$$\sum_{n=0}^{\infty} a_n = \sum_{n=0}^{\infty} b_n + i \sum_{n=0}^{\infty} c_n \in \mathbb{C}.$$

La serie esponenziale

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

è assolutamente convergente per ogni $z \in \mathbb{C}$.
Si può dimostrare anche che $e^{z+w} = e^z e^w$ per ogni $z, w \in \mathbb{C}$ ed in particolare, per ogni $r, \theta \in \mathbb{R}$, si ha $e^{r+i\theta} = e^r e^{i\theta}$. [1] Inoltre,

$$e^{i\theta} = \sum_{n=o}^{\infty} i^n \frac{\theta^n}{n!} = \sum_{m=0}^{\infty} (-1)^m \frac{\theta^{2m}}{(2m)!} + i \sum_{m=0}^{\infty} (-1)^m \frac{\theta^{2m+1}}{(2m+1)!}$$

e confrontando con gli sviluppi in serie del seno e del coseno ricaviamo la formula

$$e^{i\theta} = \cos\theta + i \sin\theta.$$

Ad ogni polinomio $f \in \mathbb{C}[x]$ associamo la funzione complessa $I_f : \mathbb{C} \to \mathbb{C}$

$$I_f(z) = e^z \sum_{h=0}^{\infty} f^{(h)}(0) - \sum_{h=0}^{\infty} f^{(h)}(z), \quad z \in \mathbb{C}.$$

Notiamo che nella definizione di I_f le sommatorie sono di fatto finite in quanto $f^{(h)} = 0$ se $h > deg(f)$.

Osservazione 8.15. *Se $f(x) \in \mathbb{R}[x]$, allora la restrizione di I_f all'asse reale è la soluzione del problema di Cauchy*

$$I'_f(t) = I_f(t) + f(t), \quad I_f(0) = 0,$$

che si risolvono nel modo standard

$$I_f(t) = \int_0^t f(s)e^{t-s}ds. \tag{8.3}$$

Lemma 8.16. *Per ogni $z \in \mathbb{C}$ vale*

$$|I_f(z)| \leq |z|e^{|z|}\tilde{f}(|z|).$$

Dimostrazione Utilizzando lo sviluppo di Taylor

$$f^{(p)}(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!} f^{(p+n)}(0)$$

e sviluppando l'esponenziale si ottiene

$$I_f(z) = \sum_{n,p=0}^{\infty} \frac{z^n}{n!} f^{(p)}(0) - \sum_{n,p=0}^{\infty} \frac{z^n}{n!} f^{(p+n)}(0) = \sum_{n=0}^{\infty} \frac{z^n}{n!} \sum_{p=0}^{n-1} f^{(p)}(0).$$

Ponendo $q = n - 1 - p$ quest'ultima diventa

$$I_f(z) = z \sum_{p,q=0}^{\infty} \frac{z^p z^q}{(p+q+1)!} f^{(p)}(0)$$

che per la disuguaglianza triangolare risulta

$$|I_f(z)| \leq |z| \sum_{p,q=0}^{\infty} \frac{|z^p||z^q|}{(p+q+1)!} |f^{(p)}(0)| \leq |z| \sum_{p,q=0}^{\infty} \frac{|z^q|}{q!} \frac{|z|^p}{p!} \tilde{f}^{(p)}(0) = |z|e^{|z|}\tilde{f}(|z|).$$

□

Lemma 8.17. *Sia $f \in \mathbb{C}[x]$, allora esistono due costanti C,D dipendenti da f, tali che,*

$$z \in \mathbb{C}, f(z) = 0 \Rightarrow |I_{x^{p-1}f(x)^p}(z)| \leq DC^p,$$

per ogni $p > 0$.

Dimostrazione Definiamo $g(x) = x^{p-1}f(x)^p \in \mathbb{C}[x]$. Allora

$$\tilde{g}(|z|) \leq |z|^{p-1}\tilde{f}(|z|)^p,$$
$$|z|e^{|z|}\tilde{g}(|z|) \leq |z|^p e^{|z|}\tilde{f}(|z|)^p.$$

Quindi date $\alpha_1, ..., \alpha_m$ radici complesse di $f(x)$ per avere la conclusione basta prendere

$$C = \max(|\alpha_1|\tilde{f}(|\alpha_1|), ..., |\alpha_m|\tilde{f}(|\alpha_m|))$$
$$D = \max(e^{|\alpha_1|}, ..., e^{|\alpha_m|}).$$

□

Lemma 8.18. *Siano $f \in \mathbb{Z}[x]$ con $f(0) \neq 0$, p un numero primo sufficientemente grande (rispetto ai coefficienti di f) e $g(x) = x^{p-1}f(x)^p$. Allora l'intero*

$$\sum_{h\geq 0} g^{(h)}(0)$$

è divisibile per $(p-1)!$ ma non per $p!$. Se $m \in \mathbb{Z}$ e $f(m) = 0$, allora

$$\sum_{h\geq 0} g^{(h)}(m)$$

è divisibile per $p!$.

Dimostrazione Riscriviamo $g(x)$ come

$$g(x) = f(0)^p x^{p-1} + a_p x^p + a_{p+1}x^{p+1} + \cdots$$

Allora

$$\sum_{h\geq 0} g^{(h)}(0) = f(0)^p(p-1)! + \sum_{h\geq p} h!a_h$$

dalla quale segue che $\sum_{h\geq 0} g^{(h)}(0)$ è divisibile per $(p-1)!$ ma non per $p!$ dato che per l'uguaglianza qui sopra il primo termine della somma non è divisibile per p. Siano ora $m \in \mathbb{Z}$ e $f(m) = 0$ allora il polinomio $(x-m)$ divide $f(x)$ e quindi $(x-m)^p$ divide $g(x)$ e $g^{(h)}(m) = 0$ per ogni $h < p$. Dato che $g(x) \in \mathbb{Z}[x]$, il polinomio $g^{(h)}(x)$ è divisibile per $h!$ per ogni $h > 0$ da cui segue la seconda affermazione.

□

8.5 Trascendenza di π

Possiamo dimostrare ora che π è un numero trascendente.

Teorema 8.19. *(**trascendenza di** π) π è un numero trascendente*

Dimostrazione Supponiamo per assurdo che π sia algebrico. Allora anche $\theta_1 = i\pi$ è algebrico, cioé è radice di un polinomio monico $q(x) \in \mathbb{Q}[x]$ di grado $d > 0$ tale che

$$q(x) = \prod_{i=1}^{d}(x-\theta_i), \quad \theta_i \in \mathbb{C}.$$

Consideriamo i 2^d numeri complessi, contati con molteplicità,

$$a_1\theta_1 + \cdots + a_d\theta_d, \quad a_i \in \{0,1\}.$$

Essi sono a loro volta radici del polinomio di grado 2^d.

$$\hat{f}(x) = \prod_{a_1,\dots,a_d=0,1} (x - a_1\theta_1 - \cdots - a_d\theta_d).$$

Per il teorema delle funzioni simmetriche (8.7) il polinomio $\hat{f}(x)$ ha coefficienti razionali. Indichiamo con $\alpha_1, \dots, \alpha_n, 1 \leq n \leq 2^d$, i numeri $a_1\theta_1 + \cdots + a_d\theta_d$ diversi da 0 e $q = 2^d - n$. Dato che, per la formula di Eulero, $e^0 + e^{\theta_1} = 1 + e^{i\pi} = 0$, la relazione

$$(e^0 + e^{\theta_1}) \cdots (e^0 + e^{\theta_d}) = 0$$

e si può riscrivere

$$q + e^{\alpha_1} + \cdots + e^{\alpha_n} = 0.$$

Esiste quindi un intero $a > 0$ tale che

$$f(x) = a\frac{\hat{f}(x)}{x^q} = a(x - \alpha_1) \cdots (x - \alpha_n) \in \mathbb{Z}[x].$$

Fissato ora un primo p sufficientemente grande, consideriamo i polinomi

$$h(x) = x^{p-1}f(x)^p,$$

$$g(x) = a^{np}h(x) = x^{p-1}(a^n f(x))^p$$

e il numero complesso

$$J = I_g(\alpha_1) + \cdots + I_g(\alpha_n).$$

Per il lemma 8.17 sappiamo che esistono due costanti $C, D > 0$, indipendenti da p tali che

$$|J| \leq DC^p.$$

Scriviamo quindi $-J$ per esteso

$$-J = \sum_{i=1}^{n}\sum_{j=0}^{\infty} g^{(j)}(\alpha_i) - \sum_{i=1}^{n} e^{\alpha_i} \sum_{j=0}^{\infty} g^{(j)}(0) = q\sum_{j=0}^{\infty} g^{(j)}(0) + \sum_{j=0}^{\infty}\sum_{i=1}^{n} g^{(j)}(\alpha_i).$$

Dal lemma 8.18 segue che $q\sum_{j=0}^{\infty} g^{(j)}(0)$ è un intero divisibile per $(p-1)!$ ma non per $p!$. Inoltre, $g^{(j)}(\alpha_i) = 0$ se $j < p$ e quindi

$$\sum_{j=0}^{\infty}\sum_{i=1}^{n} g^{(j)}(\alpha_i) = \sum_{j=p}^{\infty}\sum_{i=1}^{n} a^{np}h^{(j)}(\alpha_i)$$

è un intero divisibile per $p!$. Segue quindi che

$$\frac{J}{(p-1)!}$$

è un intero non nullo e questo è in contraddizione con il fatto che

$$\frac{DC^p}{(p-1)!}$$

tende a 0 per p che tende all'infinito.

$\square$