IL QUADRATO NON È TONDO

MARCO MANETTI

SOMMARIO. Queste sono dispense per il corso di eccellenza 2015, Sapienza Università di Roma, dove il lettore, se lo vorrà, potrà trovare una dimostrazione della trascendenza di π ed altre interessanti divagazioni matematiche. Rivolto a studenti del secondo anno del corso di laurea in Matematica.

1. Antipasto: irrazionalità di e^n, π^2 e $\sin(n)$

Se avete apprezzato la semplice dimostrazione dell'irrazionalità di e fatta usando uno dei due sviluppi in serie

$$e=\sum_{n\geq 0}\frac{1}{n!}\,,\qquad \frac{1}{e}=\sum_{n\geq 0}\frac{(-1)^n}{n!}\,, \tag{1}$$

dimenticatela: qui non siamo alla mensa universitaria!

Il miglior modo attualmente disponibile per dimostrare non solo l'irrazionalità di e ma anche di tutte le sue potenze intere e^r è mediante i **polinomi di Niven**:

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

dotati della notevole proprietà che tutte le loro derivate, di qualsiasi ordine,

$$f_n^{(0)}(x)=f_n(x),\quad f_n^{(1)}(x)=f_n'(x),\quad f^{(2)}(x)=f''(x),\ \ldots,f_n^{(h)}(x),\ \ldots$$

assumono valori interi per $x=0,1$.

Infatti segue subito dalla formula di Leibniz che $f_n^{(h)}(0)=f_n^{(h)}(1)=0$ per ogni $h<n$. Poi, 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

$$f_n^{(h)}(m)\in\mathbb{Z}\quad\text{per ogni}\quad h\geq n,\ m\in\mathbb{Z}\,.$$

Per uso futuro, notiamo che la stessa proprietà vale per tutti i polinomi del tipo $f_n(x)h(x)$, con $h(x)\in\mathbb{Z}[x]$.

Irrazionalità di e^r e $\log(n)$. Sia r un intero positivo e supponiamo per assurdo che $e^r=a/b$, con a,b interi positivi. Se $g(x)$ è un polinomio di grado $<n$ con la proprietà che $g(x)$ e tutte le sue derivate $g'(x)$, $g''(x)$,..., $g^{(h)}(x)$,... assumono valori interi per $x=0,1$, allora l'integrale definito

$$\int_0^1 br^n e^{rx}g(x)dx$$

è un numero intero. Infatti, integrando per parti si ottiene

$$\int_0^1 br^n e^{rx}g(x)dx=ar^{n-1}g(1)-br^{n-1}g(0)-\int_0^1 br^{n-1}e^{rx}g'(x)dx$$

e la conclusione si ottiene per induzione su n. In particolare, prendendo i polinomi di Niven otteniamo

$$\int_0^1 br^{2n+1}e^{rx}f_n(x)dx\in\mathbb{Z} \tag{2}$$

Date: 14 marzo 2015 (pi day del secolo XXI).

per ogni n. D'altra parte, siccome $e^{rx} \leq e^r$ e $x(1-x) \leq 1$ per ogni $0 \leq x \leq 1$ si ha

$$0 < \int_0^1 br^{2n+1}e^{rx}f_n(x)dx \leq \int_0^1 \frac{br^{2n+1}e^r}{n!}dx = \frac{ar^{2n+1}}{n!},$$

Per n sufficientemente grande si ha però $ar^{2n+1}/n! < 1$ in contraddizione con (2).

Come immediata conseguenza abbiamo anche l'irrazionalità del logaritmo naturale di ogni intero $n > 1$. Infatti, se $\log(n) = \dfrac{a}{b}$, con $a, b > 0$, si avrebbe $e^a = e^{b\log(n)} = n^b$.

Per quanto riguarda i logaritmi in base 10 la situazione è ancora più semplice, infatti per qualunque numero razionale $x > 0$ si ha che $\log_{10}(x) \in \mathbb{Z}$ oppure $\log_{10}(x)$ è irrazionale. Infatti, se $x = a/b$ e $\log_{10}(x) \in \mathbb{Q}$ con a, b interi positivi e senza fattori comuni. Moltiplicando x per un'opportuna potenza di 10 possiamo anche supporre che né a né b siano divisibili per 10. Infine, a meno di scambiare a e b possiamo supporre $\log_{10}(x) \geq 0$. Se $\log_{10}(x) = c/d$, con c, d interi positivi, allora

$$\log_{10}(x^d) = c, \qquad a^d = 10^c b^d,$$

e siccome 10 non divide a si deve avere $c = 0$.

Irrazionalità di π^2. Gli stessi polinomi di Niven trovano posto anche tra gli ingredienti della dimostrazione dell'irrazionalità di π^2. Supponiamo per assurdo che $\pi^2 = \dfrac{a}{b}$, ossia $\dfrac{a}{\pi} = b\pi$, con a, b interi positivi.

Lo stesso ragionamento fatto precedentemente, mediante induzione ed integrazione per parti, mostra stavolta che se $g(x)$ è un polinomio di grado $\leq 2n$ con la proprietà che $g(x)$ e tutte le sue derivate $g'(x)$, $g''(x)$,..., $g^{(h)}(x)$,... assumono valori interi per $x = 0, 1$, allora

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

In particolare si ha dunque

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

in contraddizione, per $n >> 0$, con le stime

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

Irrazionalità di seni e coseni. Con una piccola variazione degli argomenti precedenti, siamo in grado di dimostrare che se β è un numero razionale positivo, allora $\sin^2(\beta)$, $\cos^2(\beta)$ e $\tan^2(x)$ sono irrazionali. Dalle formule

$$\sin^2(\beta) + \cos^2(\beta) = 1, \qquad \cos^2(\beta) - \sin^2(\beta) = \cos(2\beta), \qquad \tan^2(\beta) = \frac{1}{\cos^2(\beta)} - 1$$

si evince che basta dimostrare l'irrazionalità di $\cos(\alpha)$ per ogni numero razionale $\alpha > 0$. Sia dunque $\alpha = a/b$ con a, b interi positivi, e supponiamo per assurdo $\cos(\alpha) = r/s$, con r, s interi, $s > 0$.

Dato un polinomio $f(x)$ di grado n e tale che tutte le sue derivate assumano valori interi per $x = 0, 1$, consideriamo i due integrali

$$A_n = \int_0^1 sa^{n+1}f(x)\sin(\alpha x - \alpha)dx, \qquad B_n = \int_0^1 sa^{n+1}f(x)\cos(\alpha x - \alpha)dx\ .$$

Usando induzione su n e la formula di integrazione per parti si dimostra facilmente che se $f(x)$ è pari, allora $A_n \in \mathbb{Z}$, e se $f(x)$ è dispari, allora $B_n \in \mathbb{Z}$.

La funzione $x(1-x^2)$ ha nell'intervallo $[0, 1]$ un unico punto di massimo in $x_0 = 1/\sqrt{3}$. Lasciamo al lettore il compito di convincersi (vedi Esercizio 7.4) che per $n >> 0$ l'integrale definito

$$\int_0^1 x^n(1-x^2)^n dx$$

è "quasi tutto concentrato" in un intorno di x_0, ossia che per ogni $\epsilon > 0$ si ha

$$\lim_{n\to\infty} \frac{\int_{x_0-\epsilon}^{x_0+\epsilon} x^n(1-x^2)^n dx}{\int_0^1 x^n(1-x^2)^n dx} = 1 \ ,$$

e che per ogni funzione continua $f\colon [0,1] \to \mathbb{R}$ si ha

$$\lim_{n\to\infty} \frac{\int_0^1 x^n(1-x^2)^n f(x) dx}{\int_0^1 x^n(1-x^2)^n dx} = f(x_0) \ .$$

I due numeri $\sin(\alpha/\sqrt{3}-\alpha)$ e $\cos(\alpha/\sqrt{3}-\alpha)$ non sono entrambi nulli; supponiamo per fissare le idee che $h\sin(\alpha/\sqrt{3}-\alpha) > 0$ con $h \in \{-1,1\}$. Allora per $n >> 0$ valgono le disuguaglianze

$$0 < h\int_0^1 x^n(1-x^2)^n \sin(\alpha x - \alpha) dx < \int_0^1 x^n(1-x^2)^n < 1 \ ,$$

$$0 < h\int_0^1 sa^{3n+1} \frac{x^n(1-x^2)^n}{n!} \sin(\alpha x - \alpha) dx < \frac{sa^{3n+1}}{n!}$$

che per n pari e molto grande sono in contraddizione con il fatto che $A_n \in \mathbb{Z}$. Se $\sin(\alpha/\sqrt{3}-\alpha) = 0$ si ripete il ragionamento con n dispari e B_n al posto di A_n.

2. Primo: funzioni simmetriche

Indichiamo con $\mathbb{Z}[x_1,\dots,x_n]$ l'anello dei polinomi in $x_1,\dots,x_n$ a coefficienti interi. Per definizione ogni polinomio è una somma finita di monomi, ossia di espressioni del tipo

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

Di un tale monomio chiameremo **grado** il numero $i_1 + \cdots + i_n$, e chiameremo **peso** il numero $i_1 + 2i_2 + \cdots + ni_n$. Un polinomio in cui tutti i monomi hanno lo steso grado si dice **omogeneo**; un polinomio in cui tutti i monomi hanno lo steso peso si dice **isobaro**.

È del tutto chiaro che ogni polinomio si scrive i maniera unica come come somma di polinomi isobari, che il peso della somma è minore od uguale al massimo dei pesi, mentre il peso del prodotto è la somma dei pesi.

Definizione 2.1. Un polinomio $p \in \mathbb{Z}[x_1,\dots,x_n]$ si dice **simmetrico** se

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

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

Ad esempio, in $\mathbb{Z}[x_1,x_2]$ sono simmetrici i polinomi

$$x_1 + x_2, \quad x_1x_2, \quad x_1^2 + x_2^2 = (x_1+x_2)^2 - 2x_1x_2, \quad x_1^2x_2^2, \quad x_1^3x_2 + x_1x_2^3,$$

mentre **non sono** simmetrici i polinomi

$$x_1, \quad x_2, \quad x_1 + 2x_2, \quad x_1^2 - x_2^2, \quad x_1x_2^2 \ .$$

È chiaro che un polinomio è simmetrico se e solo se tutte le sue componenti omogenee sono simmetriche.

Nel seguito indicheremo con Σ_n il gruppo delle permutazioni dell'insieme $\{1,\dots,n\}$.

Esempio 2.2. Dati due interi $0 < k \leq n$, i coefficienti delle potenze di t del polinomio

$$p(t,x_1,\dots,x_n) = \prod_{\sigma\in\Sigma_n} (t^k + x_{\sigma(1)}t^{k-1} + \cdots + x_{\sigma(k)})$$

sono polinomi simmetrici in $x_1,\dots,x_n$. Basta infatti osservare che per ogni permutazione σ si ha $p(t,x_1,\dots,x_n) = p(t,x_{\sigma(1)},\dots,x_{\sigma(n)})$.

Esempio 2.3. Dato che somme e prodotti di polinomi simmetrici sono ancora simmetrici, se $p_1,\ldots,p_m \in \mathbb{Z}[x_1,\ldots,x_n]$ sono simmetrici, allora per ogni $q \in \mathbb{Z}[y_1,\ldots,y_m]$ ne consegue che

$$q(p_1,\ldots,p_m) \in \mathbb{Z}[x_1,\ldots,x_n]$$

è simmetrico.

Definizione 2.4. Per ogni intero positivo n, le **funzioni simmetriche elementari** $\sigma_1,\ldots,\sigma_n \in \mathbb{Z}[x_1,\ldots,x_n]$ sono definite dalla relazione

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

Per meglio dire, i valori delle funzioni simmetriche elementari calcolate su di una n-upla di numeri complessi $(a_1,\ldots,a_n)$ sono i coefficienti del polinomio monico di grado n che ha come radici $-a_1,\ldots,-a_n$. Per $n=3$ le funzioni simmetriche elementari sono

$$\sigma_1 = x_1+x_2+x_3, \quad \sigma_2 = x_1x_2+x_2x_3+x_3x_1, \quad \sigma_3 = x_1x_2x_3.$$

Notiamo 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.

Teorema 2.5. *Ogni polinomio simmetrico a coefficienti interi si può esprimere come un polinomio a coefficienti interi nelle funzioni simmetriche elementari.*

In altri termini, un polinomio $p \in \mathbb{Z}[x_1,\ldots,x_n]$ è simmetrico se e solo se esiste un polinomio $q \in \mathbb{Z}[y_1,\ldots,y_n]$ tale che

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

Dimostrazione. Sia $p \in \mathbb{Z}[x_1,\ldots,x_n]$ simmetrico e sia $p = p_0+\cdots+p_m$ la decomposizione in componenti isobare, con p_i di peso i ed $p_m \neq 0$. Dimostriamo per induzione su m che p è un polinomio nelle funzioni simmetriche elementari.

Ogni monomio di p_m è del tipo $ax_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ con $i_1 \le i_2 \le \cdots \le i_n$; quindi, se poniamo $y_i = x_{n-i+1}x_{n-i+2}\cdots x_n$, si ha

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

Dunque esiste un polinomio $q \in \mathbb{Z}[y_1,\ldots,y_n]$ tale che $p_m(x_1,\ldots,x_n) = q(y_1,\ldots,y_n)$. Il polinomio $p(x_1,\ldots,x_n) - q(\sigma_1,\ldots,\sigma_n)$ è simmetrico di peso $< m$ e si può applicare l'ipotesi induttiva. □

Corollario 2.6. *Consideriamo due polinomi $f,g \in \mathbb{Z}[t]$, con $\deg(g) \le n$ e*

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

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

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

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

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

Dunque $\sigma_i(a\alpha_1,\ldots,a\alpha_n) \in \mathbb{Z}$ per ogni i e, per il Teorema 2.5, la somma $\sum_{i=1}^{m}(a\alpha_i)^p$ si può esprimere come un polinomio a coefficienti interi nelle funzioni simmetriche elementari.

Per la seconda basta considerare il caso $g = t^q$ con $q \le n$. Se $p > q$ vale $g^{(p)} = 0$, mentre se $p \le q$ si ha

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

□

3. Secondo: numeri algebrici e trascendenti

Definizione 3.1. Un **numero algebrico** è un numero complesso che 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**.

Più precisamente, un numero $\alpha \in \mathbb{C}$ è algebrico se e solo se esistono un intero positivo n ed $n+1$ numeri razionali $a_0, a_1, \ldots, a_n$ tali che

$$a_n \neq 0, \qquad a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0. \tag{3}$$

Ogni numero razionale $x = p/q$ è algebrico poiché è radice del polinomio $qx - p$. Il numero $\sqrt{2}$ è algebrico poiché è radice del polinomio $x^2 - 2$. L'unità immaginaria i è un numero algebrico poiché è radice del polinomio $x^2 + 1$.

Notiamo immediatamente che se α è un numero algebrico diverso da 0, allora anche α^{-1} è algebrico: basta dividere (3) per α^n.

Ovviamente, nella definizione di numero algebrico non è restrittivo supporre che il polinomio $f(t)$ sia monico, ossia del tipo $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_n$. Alternativamente, moltiplicando per un denominatore comune, non è restrittivo supporre che il polinomio $f(t)$ sia a coefficienti interi.

Lemma 3.2. *Un numero complesso α è algebrico se e solo se può essere esteso ad una successione finita $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ 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 un prodotto di polinomi di primo grado. □

Lemma 3.3. *Siano $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, $n \geq 2$, 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 ogni $i \neq j$.

Dimostrazione. Per ipotesi le funzioni simmetriche elementari $\sigma_i(\alpha_1, \ldots, \alpha_n)$ sono numeri razionali in quanto coincidono, a meno del segno, con i coefficienti del polinomio $f(t)$. Ogni coefficiente dei polinomi

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

è un polinomio simmetrico a coefficienti interi in $\alpha_1, \ldots, \alpha_n$ ed è quindi esprimibile come un polinonio a coefficienti interi nelle funzioni simmetriche elementari. Dunque $g(t), h(t) \in \mathbb{Q}[t]$. □

Teorema 3.4. *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 $\alpha_1, \alpha_2, \ldots, \alpha_n$ e $\beta_1, \beta_2, \ldots, \beta_m$ tali che $\alpha = \alpha_1$, $\beta = \beta_1$,

$$f_1(t) = \prod_{i=1}^{n}(t - \alpha_i) \in \mathbb{Q}[t], \qquad f_2(t) = \prod_{i=1}^{m}(t - \beta_i) \in \mathbb{Q}[t]\ .$$

basta adesso applicare il lemma precedente al polinomio $f(t) = f_1(t)f_2(t)$. □

Nota: è possibile dimostrare il Teorema 3.4 anche senza l'aiuto del teorema fondamentale dell'algebra; in tal caso sono però necessarie alcune nozioni non banali di algebra lineare e teoria dei campi (vedi il corso di Algebra 2).

L'insieme dei numeri algebrici si indica solitamente con $\overline{\mathbb{Q}}$. Possiamo riformulare il Teorema 3.4 dicendo che $\overline{\mathbb{Q}}$ è un sottocampo di $\mathbb{C}$.

È facilissimo dimostrare in maniera non costruttiva l'esistenza di numeri trascendenti: per ogni intero $n > 0$ indichiamo con $S_n \subset \mathbb{R}$ l'insieme (finito) dei numeri reali che sono radice di un polinomio di grado $\leq n$ i cui coefficienti sono numeri interi di modulo $\leq n$. Possiamo quindi trovare due successioni $a_n, b_n \in \mathbb{R}$ tali che

$$a_n \leq a_{n+1} < b_{n+1} \leq b_n, \qquad [a_n, b_n] \cap S_n = \emptyset,$$

per ogni n; di conseguenza $\lim a_n \notin \cup S_n$ e quindi non è algebrico.

Più difficile è dimostrare che determinati numeri sono trascendenti. Storicamente il primo numero reale del quale è stata dimostrata la trascendenza è il numero di Liouville

$$l = \sum_{n=1}^{+\infty} \frac{1}{10^{n!}} = 0,110001000000000000000010000000\ldots .$$

Definizione 3.5. 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.

Esempio 3.6. Un numero algebrico è razionale se e solo se ha grado 1; i numeri algebrici i e $\sqrt{2}$ hanno grado 2.

Lemma 3.7. *Sia $x \in \mathbb{R}$ un numero algebrico di grado d. Allora esiste un numero reale positivo M tale che per ogni coppia di numeri interi p, q, con $q > M$ vale*

$$x = \frac{p}{q} \quad \textit{oppure} \quad \left| x - \frac{p}{q} \right| > \frac{1}{q^{d+1}} .$$

Dimostrazione. Sia $h(t)$ un polinomio di grado d a coefficienti interi tale che $h(x) = 0$ e sia $\delta > 0$ tale che $h(t)$ non abbia radici nell'intervallo $[x - \delta, x + \delta]$ diverse da x. Indichiamo con m il massimo della funzione continua $|h'(t)|$ nell'intervallo $[x - \delta, x + \delta]$ e definiamo

$$M = \max\left(m, \sqrt[d+1]{\frac{1}{\delta}} \right).$$

Dunque, se $q > M$ si ha in particolare

$$q^{d+1} > M^{d+1} \geq \frac{1}{\delta}, \qquad \frac{1}{q^{d+1}} < \delta$$

e se $x = p/q$ oppure $|x - \frac{p}{q}| > \delta$ il risultato è banalmente vero. Se $|x - \frac{p}{q}| \leq \delta$ e $x \neq p/q$, allora per il teorema del valor medio esiste $\xi \in [x - \delta, x + \delta]$ tale che

$$0 \neq h\left(\frac{p}{q}\right) = h\left(\frac{p}{q}\right) - h(x) = h'(\xi)\left(\frac{p}{q} - x\right).$$

Moltiplicando per q^d e prendendo il valore assoluto

$$\left| q^d h\left(\frac{p}{q}\right) \right| = q^d |h'(\xi)| \left| \frac{p}{q} - x \right| \leq q^d m \left| \frac{p}{q} - x \right|.$$

D'altra parte $q^d h\left(\frac{p}{q}\right)$ è un intero non nullo e quindi il suo valore assoluto è ≥ 1, e quindi

$$1 \leq \left| q^d h\left(\frac{p}{q}\right) \right| \leq q^d m \left| \frac{p}{q} - x \right|$$

da cui deduciamo

$$\left| \frac{p}{q} - x \right| \geq \frac{1}{q^d m} \geq \frac{1}{q^d M} \geq \frac{1}{q^{d+1}}.$$

□

Teorema 3.8. *Il numero di Liouville $l = \sum_n \frac{1}{10^{n!}}$ è trascendente.*

Dimostrazione. Sia $N > 0$ e scriviamo

$$l = \sum_{n=1}^{+\infty} \frac{1}{10^{n!}} = \frac{p}{10^{N!}} + \sum_{n=N+1}^{+\infty} \frac{1}{10^{n!}}$$

per un opportuno numero intero p. Si verifica facilmente che

$$\left| l - \frac{p}{10^{N!}} \right| = \sum_{n=N+1}^{+\infty} \frac{1}{10^{n!}} = \frac{1}{10^{(N!)N}} \sum_{n=N+1}^{+\infty} \frac{1}{10^{n!-(N!)N}} < \frac{1}{(10^{N!})^N} \ .$$

Se l fosse algebrico di grado d, per $N > d$ e sufficientemente grande otteniamo una stima che contraddice il Lemma 3.7. □

4. Contorno: stime preliminari

Per dimostrare la trascendenza dei numeri e e π avremo bisogno di alcune disuguaglianze meno banali di quelle usate nella dimostrazione dell'irrazionaltà di e^r.

Dato un polinomio $f(x) \in \mathbb{C}[x]$, $f(x) = \sum a_i x^i$, denotiamo come al solito con $f^{(p)}(x)$ la sua derivata p-esima e con $\tilde{f}(x) = \sum |a_i| x^i$. Si noti che

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

Lemma 4.1. *Dati $f, g \in \mathbb{C}[x]$, per ogni numero reale $a \geq 0$ vale*

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

Dimostrazione. Banale conseguenza della disuguaglianza triangolare $|z+w| \leq |z|+|w|$, $z, w \in \mathbb{C}$, (dettagli per esercizio). □

Ricordiamo che una serie di numeri complessi $\sum_{n=0}^{\infty} a_n$ si dice assolutamente convergente se $\sum_{n=0}^{\infty} |a_n| < +\infty$. Chiaramente se $a_n = b_n + ic_n$, con $b_n, c_n \in \mathbb{R}$ e $\sum_{n=0}^{\infty} a_n$ è assulutamente convergente, allora pure le serie $\sum_{n=0}^{\infty} b_n$ e $\sum_{n=0}^{\infty} c_n$ cono assulutamente convergenti e si può definire

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

Ad esempio, la serie esponenziale

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

è assolutamente convergente per ogni $z \in \mathbb{C}$. Come nel caso delle serie reali si possono fare somme e prodotti di Cauchy di serie assolutamente convergenti senza rischio alcuno.

Allo stesso modo del caso reale si dimostra 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 $e^{r+i\theta} = e^r e^{i\theta}$. Inoltre,

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

e confrontando con i ben noti sviluppi in serie di seno e coseno ricaviamo la formula

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

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

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

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

Osservazione 4.2. Se $f(x) \in \mathbb{R}[x]$, allora la restrizione di I_f all'asse reale è la soluzione del problema di Cauchy

$$I_f'(t) = I_f(t) + f(t), \qquad I_f(0) = 0,$$

che si risolve nel modo standard:

$$I_f(t) = \int_0^t f(s)e^{t-s}ds\ . \tag{4}$$

Chi segue il corso di Variabile Complessa scoprirà presto che la formula integrale (4) ha perfettamente senso anche per $t \in \mathbb{C}$, dove l'integrale è fatto lungo un qualsiasi cammino che congiunge 0 e t nel piano di Gauss.

Lemma 4.3. *Nella notazioni precedenti, per ogni $z \in \mathbb{C}$ vale*

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

Dimostrazione. Sviluppando l'esponenziale in serie ed usando gli sviluppi di Taylor

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

otteniamo

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

Ponendo $q = n-1-p$ si ottiene

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

e per la disuguaglianza triangolare

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

□

Lemma 4.4. *Sia $f \in \mathbb{C}[x]$, allora esistono due costanti C, D, dipendenti da f, tali che,*

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

per ogni $p > 0$.

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

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

se $\alpha_1, \ldots, \alpha_m$ sono le radici complesse di $f(x)$ basta prendere

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

□

Lemma 4.5. *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. Basta osservare che, scrivendo

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

si ha

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

Se $m \in \mathbb{Z}$ e $f(m) = 0$ il polinomio $(x-m)$ divide $f(x)$, dunque $(x-m)^p$ divide $g(x)$ e $g^{(h)}(m) = 0$ per ogni $h < p$. Basta adesso osservare che, siccome $g(x) \in \mathbb{Z}[x]$, il polinomio $g^{(h)}(x)$ è divisibile per $h!$, per ogni $h > 0$.

□

5. Dolce: la trascendenza di e e π

Supponiamo che π sia algebrico, allora anche $\theta_1 = i\pi$ è algebrico ed è radice di un polinomio monico $q(x) \in \mathbb{Q}[x]$ di grado $d > 0$. Scriviamo

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

e consideriamo i 2^d numeri complessi, contati con molteplicità,

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

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

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

Per il teorema delle funzioni simmetriche il polinomio $\hat{f}$ ha coefficienti razionali. Se indichiamo con $\alpha_1, \ldots, \alpha_n$, $1 \leq n \leq 2^d$, i numeri $a_1\theta_1 + \cdots + a_d\theta_d$ diversi da 0 e $q = 2^d - n$. Siccome $e^0 + e^{\theta_1} = 1 + e^{i\pi} = 0$, la relazione

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

diventa

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

Esiste 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 un primo $p >> 0$, consideriamo i polinomi

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

ed il numero complesso

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

Abbiamo visto che esistono due costanti $C, D > 0$, indipendenti da p tali che

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

Scriviamo $-J$ per esteso:

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

Abbiamo dimostrato 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 $p!$. Ne consegue che $J/(p-1)!$ è un intero non nullo e questo è in contraddizione con il fatto che $DC^p/(p-1)!$ tende a zero per p che tende ad infinito.

La trascendenza di e si dimostra in modo simile. Supponiamo per assurdo che e sia algebrico di grado n, allora si ha una relazione

$$a_1e + a_2e^2 + \cdots + a_ne^n = q, \qquad q, a_1, \ldots, a_n \in \mathbb{Z}, \quad q \neq 0\ .$$

Stavolta consideriamo un primo $p >> 0$, il polinomio (detto di **Hermite**)

$$g(x) = x^{p-1}(x-1)^p(x-2)^p\cdots(x-n)^p$$

ed il numero complesso

$$J = a_1I_g(1) + \cdots + a_nI_g(n).$$

Come sopra esistono due costanti C, D indipendenti da p tali che $|J| \leq DC^p$. D'altra parte si ha

$$J = \sum_{i=1}^{n} a_ie^i \sum_{j=0}^{\infty} g^{(j)}(0) - \sum_{i=1}^{n} a_i \sum_{j=0}^{\infty} g^{(j)}(i) = q\sum_{j=0}^{\infty} g^{(j)}(0) - \sum_{i=1}^{n} a_i \sum_{j=0}^{\infty} g^{(j)}(i)$$

Gli stessi ragionamenti fatti sopra mostrano che la prima sommatoria è un numero intero divisibile per $(p-1)!$ ma non per $p!$, mentre

$$\sum_{j=0}^{\infty} g^{(j)}(i) = \sum_{j=p}^{\infty} g^{(j)}(i)$$

è divisibile per $p!$ per ogni $i = 1, \ldots, n$. Come sopra si deduce che $J/(p-1)!$ è un intero non nullo.

La trascendenza di e e la trascendenza di π sono casi particolari del seguente teorema la cui dimostrazione, sebbene simile alle precedenti (ma decisamente meno elementare), è omessa e rimandata ai testi specializzati, come ad esempio [1, 7].

Teorema 5.1 (Lindemann-Weierstrass 1885)**.** *Siano $\alpha_1, \ldots, \alpha_n$ numeri algebrici distinti. Allora i numeri $e^{\alpha_1}, \ldots, e^{\alpha_n}$ sono linearmente indipendenti su $\overline{\mathbb{Q}}$.*

Come immediata conseguenza si ha la trascendenza di $\log(n+1), \cos(n), \sin(n)$ per ogni intero $n > 0$.

6. Limoncello: brevissimi cenni storico-folkloristici

Il pi greco è anche conosciuto come costante di Archimede, costante di Ludolph, costante Ludolphina, numero di Ludolph. Se infatti fu Archimede, con il suo metodo di esaustione, a dare circa 2.500 anni fa la prima stima precisa di π (arrivando alle prime due cifre), Ludolph van Ceulen, matematico tedesco del XVI secolo, spese la maggior parte della sua vita calcolando il valore di pi greco usando essenzialmente i suoi stessi metodi. Riuscì ad arrivare a 35 cifre decimali e se le fece incidere sulla tomba. Le 35 cifre calcolate a mano da Ludolph van Ceulen nel XVIII secolo e le 126 trovate dal matematico sloveno Jurij Vega nel XIX, impallidiscono di fronte alle 572 cifre calcolate a mano nel 1873 dal matematico dilettante inglese William Shanks. Shanks, che morì nel 1882, aveva l'hobby di calcolare costanti matematiche: ogni mattina, calcolava una nuova cifra, e passava poi il pomeriggio a controllare l'esattezza del risultato. Nel 1873 raggiunse le 707 cifre di π Greco, ma solo le prime 527 erano giuste.

La prima volta che fu usato il simbolo π per indicare il rapporto tra la circonferenza di un cerchio e il suo diametro è nel lavoro di un matematico, William Jones, intitolato Synopsis Palmariorum Matheseos o New Introduction to the Mathematics. La lettera greca compare nella frase"1/2 Periphery (π)", a proposito di un cerchio con raggio unitario, e Jones scelse proprio π perché era la prima nella parola greca corrispondente a periphery. Successivamente, la lettera greca non fu più usata da nessuno a questo scopo, finché non comparve nella Mechanica di Eulero, che era un big della matematica e che lanciò il pi greco in tutto il mondo occidentale [6].

La teoria dei numeri trascendenti ha avuto inizio con una memoria di Liouville del 1844, nella quale l'autore dimostrò che esisteva una classe, piuttosto ampia, di numeri che non erano radici

di equazioni algebriche a coefficienti interi. I problemi legati all'irrazionalità erano incece già ampiamente studiati e risale infatti al 1744 la dimostrazione di Eulero dell'irrazionalità di e ed al 1761 la dimostrazione di Lambert dell'irrazionalità di π. La dimostrazione dell'irrazionalità di π di queste note è tratta da [5].

Nel 1874 Cantor introdusse il concetto di infinito numerabile e questo portò quasi immediatamente alla constatazione che "quasi tutti" i numeri sono trascendenti: come già osservato, l'insieme dei numeri algebrici è una unione numerabile di insiemi finiti e quindi è un insieme numerabile, mentre l'insieme dei numeri reali non è numerabile.

La dimostrazione della trascendenza di e compare in una memoria di Hermite del 1873 che è stata fonte di ispirazione per molti anni a seguire. Nel 1882 Lindemann [4] riusci ad estendere il lavoro di Hermite per dimostrare la trascendenza di π e, di conseguenza, a chiudere definitivamente l'antico problema della quadratura del cerchio con riga e compasso.

La prova della trascendenza di π qui riportata segue sostanzialmente la semplificazione di Gordan [3] della dimostrazione di Lindemann.

7. Caffè: esercizi

7.1. Usare gli sviluppi in serie (1) per dimostrare che $1, e, e^{-1}$ sono linearmente indipendenti su $\mathbb{Q}$ o, equivalentemente, che e non è radice di un polinomio di secondo grado a coefficienti interi.

7.2. Dimostrare che $e^{\sqrt{2}}$ è irrazionale (sugg.: sviluppo in serie di $e^{\sqrt{2}} + e^{-\sqrt{2}}$).

7.3. Dimostrare l'irrazionalità di $\sin(1)$ e $\cos(1)$ usando gli sviluppi in serie

$$\sin(1) = \sum_{n\geq 0} \frac{(-1)^n}{(2n+1)!}, \qquad \cos(1) = \sum_{n\geq 0} \frac{(-1)^n}{(2n)!} \ .$$

7.4. Usare la concavità per $x \geq 0$ della funzione $x - x^3$ per dimostrare che

$$\int_0^1 x^n (1-x^2)^n dx \geq \frac{1}{n+1} \left(\frac{2}{3\sqrt{3}}\right)^n \ .$$

Usare il teorema della media integrale per dimostrare che per ogni funzione continua $f\colon [0,1] \to \mathbb{R}$ si ha

$$\lim_{n\to\infty} \frac{\int_0^1 x^n (1-x^2)^n f(x) dx}{\int_0^1 x^n (1-x^2)^n dx} = f(x_0) \ .$$

7.5. Il calcolo dei valori approssimati di π può essere fatto mediante lo sviluppo in serie dell'arcotangente

$$\arctan(x) = \int_0^x \frac{1}{1+t^2} dt = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots$$

da cui segue

$$\frac{\pi}{4} = \arctan(1) = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} \ .$$

Tuttavia le serie converge abbastanza lentamente. Per avere stime più rapide di possono considerare i polinomi

$$g_n(x) = \frac{x^{4n}(1-x)^{4n}}{4^n} = x^{4n} \left(\frac{1-x}{\sqrt{2}}\right)^{4n}, \qquad n > 0.$$

Siccome $g_n(i) = g_n(-i) = (-1)^n$ ne segue che $g_n(x) - (-1)^n$ è divisibile per $1 + x^2$ in $\mathbb{Q}[x]$ e vale

$$\frac{\pi}{4} = \arctan(1) = \int_0^1 \frac{1 - (-1)^n g_n(x)}{1+x^2} dx + (-1)^n \int_0^1 \frac{x^{4n}(1-x)^{4n}}{4^n(1+x^2)} dx \ .$$

In conclusione, $\int_0^1 \frac{1-(-1)^n g_n(x)}{1+x^2} dx$ è un numero razionale che approssima $\pi/4$ con un errore inferiore a 4^{-5n}.

7.6. Indichiamo come al solito con $\sigma_1, \ldots, \sigma_n \in \mathbb{Z}[x_1, \ldots, x_n]$ le funzioni simmetriche elementari. Provare che se $q \in \mathbb{Z}[y_1, \ldots, y_n]$ e $q(\sigma_1, \ldots, \sigma_n) \equiv 0$, allora anche il polinomio q è identicamente nullo.

7.7. Quali sono i gradi dei numero algebrici $\sqrt{2}+\sqrt{3}$ e $\sqrt{2}+\sqrt{3}+\sqrt{5}$?

7.8. Usare la costruzione dell'Esempio 2.2 per dedurre che:

(1) ogni polinomio monico in $\overline{\mathbb{Q}}[t]$ divide un polinomio monico in $\mathbb{Q}[t]$;
(2) il campo $\overline{\mathbb{Q}}$ è algebricamente chiuso.

7.9. Dedurre dal teorema di Lindemann-Weierstrass che per ogni successione periodica c_n di numeri algebrici (ossia esiste $k > 0$ tale $c_{n+k} = c_n$) e non tutti nulli, il numero

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

è trascendente (sugg.: matrice di Vandermonde delle radici k-esime di 1).

Riferimenti bibliografici

[1] A. Baker: *Trascendental number theory.* Cambridge University Press (1975).
[2] L. Colzani: *La quadratura del cerchio e dell'iperbole.* (si trova in rete).
[3] P. Gordan: *Transcendenz von e und π.* Math. Ann. **43** (1893), 222-224.
[4] F. Lindemann: *Ueber die zhal π.* Math. Ann. **20** (1882), 2013-225.
[5] I. Niven: *Irrational numbers.* The Mathematical Association of America (1956).
[6] S. Pisani: http://www.wired.it/attualita/tech/2015/03/13/pi-greco-day-cose-da-sapere/
[7] M. Ram Murty and Perusottam Rath: *Trascendental numbers.* Springer (2014).