I tre problemi classici dell'antichità

-

l'irrazionalità del numero π di Archimede ed e di Eulero

◆∗◆∗◆∗◆∗◆∗◆ *Prof. Giuseppe Caputo*

I tre problemi della geometria greca che non ammettono soluzione sono:

1. **La quadratura del cerchio**
2. **La duplicazione del cubo**
3. **La trisezione dell'angolo**

Necessari alla comprensione dell'argomento sono i numeri costruibili e i campi numerici, avendo ogni costruzione geometrica uno sfondo algebrico. Cominciamo col definire che cosa si intende per costruzione con riga e compasso anche detta costruzione elementare.

Una costruzione con riga e compasso è costituita dai seguenti passaggi :

- Congiungere due punti con una retta
- Determinare il punto d'intersezione di due rette
- Tracciare una circonferenza noti il centro e il raggio
- Trovare le eventuali intersezioni tra due circonferenze e di una circonferenza con una retta

Un segmento è costruibile con riga e compasso se è il risultato di un processo che utilizzi la costruzione con riga e compasso sopra descritta.

Si dicono noti gli elementi punto, retta, circonferenza predefiniti oppure determinati con i passaggi precedentemente stabiliti. A partire da questi, la geometria euclidea ci insegna che si possono risolvere i seguenti problemi grafici con riga e compasso.

- Su una semiretta si può costruire un segmento di lunghezza uguale a quella di un segmento assegnato appartenente o non appartenente alla semiretta (proprietà del trasporto).

- Data una retta e un punto esterno ad essa , si può tracciare per esso la parallela e la perpendicolare alla retta data.

- Dato un angolo e una semiretta, è possibile costruire un angolo uguale a quello dato avente uno dei lati uguale a quello della semiretta.

- E' possibile bisecare sia segmenti che angoli.

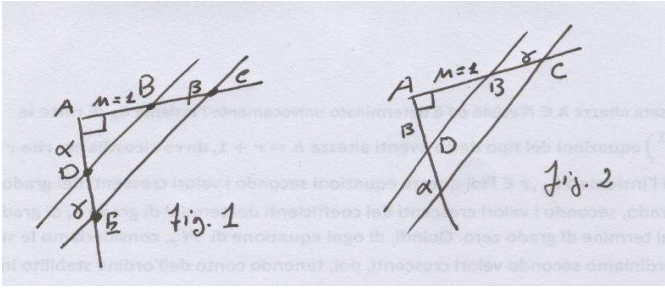
Fissato allora nel piano un segmento di lunghezza unitaria, diremo che un numero reale α è costruibile se è

possibile costruire con riga e compasso un segmento di lunghezza uguale al valore assoluto $|\alpha|$ del numero α.

Proposizione: **I numeri interi sono costruibili.**

Dimostrazione: Se a è un numero intero, detta u= 1 la misura di un segmento unitario, si ha $|a| = |nu| = nu$ = n, $n \in \mathbb{N}$.
Applicando allora n volte la proprietà del trasporto al segmento unitario, si ottiene un segmento di lunghezza $|a| = nu$ = n, per cui il numero intero a risulta costruibile.

Proposizione: **La somma, la differenza, il prodotto e il rapporto di due numeri reali costruibili sono costruibili.**

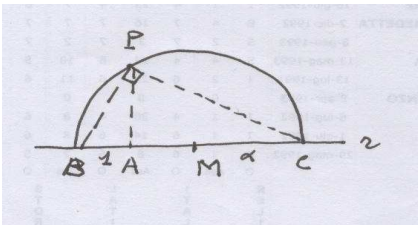
Dimostrazione: La somma di due numeri reali positivi e costruibili è costruibile a partire da un segmento unitario applicando la proprietà del trasporto e così pure per la loro differenza. Dimostriamo allora per il prodotto e per il rapporto. 

Cominciando dal prodotto, ci riferiamo alla fig.1. Costruiti i segmenti AB e BC sulla semiretta di origine A alla quale appartiene il punto B, di modo che $\overline{AB} = 1$e $\overline{BC} = \beta$, consideriamo la semiretta di origine A perpendicolare nel punto A alla prima. Su questa costruiamo il segmento AD di lunghezza $\overline{AD} = \beta$, quindi la retta passante per B e D e la sua parallela per il punto C che incontra nel punto E la perpendicolare in A. Per il teorema di Talete sul fascio di rete parallele intersecanti due trasversali, i segmenti staccati hanno misure direttamente proporzionali, donde si ha la proporzione $\gamma : \alpha = \beta : 1 \Longrightarrow \gamma = \alpha\beta$. Quindi a partire dai numeri costruibili α e β, si è ottenuto il numero γ , prodotto di α e β e misura del segmento costruibile DE, per cuii anch'esso costruibile. Analogamente per il rapporto $\frac{\alpha}{\beta}$ di due numeri reali costruibili α e $\beta \neq 0$, riferendoci alla fig.2, si ha, procedendo similmente a quanto fatto sopra, $\beta : 1 = \alpha : \gamma \Longrightarrow \gamma = \frac{\alpha}{\beta}$, cioè il numero reale γ, rapporto di α e β, risulta costruibile perché misura del segmento costruibile BC.

Corollario: **Tutti i numeri razionali sono costruibili**

Dimostrazione: Poiché un numero razionale $\frac{a}{b}$, $a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\}$ è il rapporto di due interi, quindi di due numeri reali costruibili, per la proposizione precedente è a sua volta costruibile.

Proposizione : **Se un numero reale positivo α è costruibile, allora lo è pure la sua radice quadrata $\sqrt{\alpha}$.**

Dimostrazione: Sulla retta r consideriamo un suo punto A che divide r in due semirette opposte.


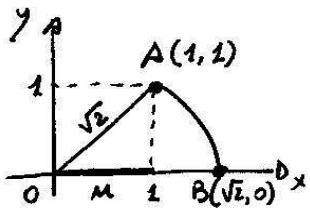
Rispettivamente su queste consideriamo due punti B e C, di modo che $\overline{\overline{AB}} = 1$ e $\overline{\overline{AC}} = \alpha$. Detto M il punto medio del segmento BC, tracciamo la circonferenza di centro M passante per B. La perpendicolare alla retta r nel punto A interseca la circonferenza nel semipiano

superiore nel punto P. Il triangolo APC è rettangolo con angolo retto in P perché inscritto in una semicirconferenza . Applicando il 2° teorema di Euclide a tale triangolo, si ha $\overline{\overline{BA}}:\overline{\overline{AP}} = \overline{\overline{AP}}:\overline{\overline{AC}} \Longrightarrow \overline{\overline{AP}}^2 = \overline{\overline{BA}} \cdot \overline{\overline{AC}} = 1 \cdot \alpha = \alpha \Longrightarrow \overline{\overline{AP}} = \sqrt{\alpha}$, per cui tale numero essendo la lunghezza del segmento costruibile $\overline{\overline{AP}}$, risulta anch'esso costruibile.

<u>Proposizione</u>: $\boldsymbol{b\sqrt{2}, b \in \mathcal{Q}}$ **è costruibile**.

<u>Dimostrazione</u>: Infatti è il prodotto del numeri razionale b costruibile per l'irrazionale $\sqrt{2}$ costruibile, per la proposizione precedente, quindi costruibile per una proposizione precedente.

Riferendoci ad un piano cartesiano $x\hat{O}y$, possiamo supporre inizialmente che sull'asse x sia dato il segmento unitario (che prendiamo come unità) con un estremo nell'origine e l'altro estremo nel punto di coordinate $(1,0)$; sono costruibili con riga e compasso tutti i numeri razionali $\frac{a}{b}$, con $a, b \in \mathbb{Z}$, e $b \neq 0$, che costituiscono un campo numerico chiuso rispetto alle quattro operazioni razionali. Gli irrazionali, che non appartengono al campo $\mathbb{Q}$, geometricamente si possono costruire usando il compasso. Si prende un segmento con un estremo nell'origine, l'altro nel punto di coordinate A(1,1), quindi tracciamo con punta di compasso in O ed apertura OA un arco di circonferenza fino ad intersecare lasse x nel punto $B(\sqrt{2}, 0)$, poiché il segmento OA è la diagonale di un quadrato di lato unitario la cui misura è appunto $\sqrt{2}$, numero irrazionale. Partendo da questo possiamo ottenere, attraverso costruzioni razionali, tutti i numeri del tipo $a + b\sqrt{2}$, con $a, b \in \mathbb{Q}$, che risultano appunto costruibili. La costruzione testé detta prende anche il nome di **<u>estensione 2 – radicale</u>**.



E' facile verificare che numeri di questo tipo, per mezzo delle quattro operazioni, danno ancora numeri siffatti, da cui segue che la classe numerica da essi formata determina un nuovo campo $\mathcal{C}_1$ più vasto del campo $\mathcal{C}_0 = \mathbb{Q} \subset \mathcal{C}_1$ il quale risulta sottocampo di esso perché per $b = 0$ si ottengono tutti i razionali $a \in \mathbb{Q}$; naturalmente $\mathcal{C}_1 \subset \mathbb{R}$, essendo tutti gli elementi di $\mathcal{C}_1$ numeri reali, ma esistendo anche irrazionali come $\sqrt{3} \notin \mathcal{C}_1$.

<u>Definizione</u>: **Un numero $\alpha \in \mathcal{C}_1$ si dice <u>costruibile</u> su $\mathbb{Q}$ se esiste un'estensione 2 - radicale del tipo detto di $\mathbb{Q}$ contenente α.**

<u>Teorema</u>: **Un numero reale è costruibile se e solo se appartiene a un'estensione 2 – radicale di $\mathbb{Q}$.**

<u>Dimostrazione</u>: Se $\alpha \in \mathbb{R}$ è costruibile, allora, come si è visto, è del tipo $\alpha = a + b\sqrt{2}$, dove $a, b \in \mathbb{Q}$, per cui appartiene a un'estensione 2 – radicale di $\mathbb{Q}$.Viceversa se il numero reale α è un'estensione 2 – radicale di $\mathbb{Q}$, allora deve essere del tipo $\alpha = a + b\sqrt{2}$,, $a, b \in \mathbb{Q}$, per cui essendo somma del numero razionale a, costruibile per una proposizione precedente, e del prodotto $b\sqrt{2}$, costruibile per una proposizione precedente, risulta costruibile per la proposizione a pag.2.

Una successiva estensione si può fare a partire dal numero $k = 1 + \sqrt{2}$, il quale è uno dei precedenti ottenuto prendendo $a = b = 1$, quindi considerando l'irrazionale $\sqrt{k}$, che è costruibile similmente a $\sqrt{2}$, quindi considerando il campo C_2 i cui elementi sono i numeri del tipo $p + q\sqrt{k}$, con $p, q \in C_1$. Così facendo si possono costruire successivi campi di numeri costruibili $C_0, C_1, C_2, \cdots$ costituenti una catena rispetto all'inclusione, di sottocampi di $\mathbb{R}$. Osserviamo a questo punto che se C è un campo di questo tipo, l'uso della sola riga non potrà mai consentire un ampliamento di questo. Infatti se (a_1, b_1), (a_2, b_2), sono due punti del piano cartesiano le cui coordinate sono numeri del campo C, la retta passante per questi punti ha equazione $\frac{x-a_1}{a_2-a_1} = \frac{y-b_1}{b_2-b_1} \Rightarrow (b_1 - b_2)x + (a_2 - a_1)y + (a_1 b_2 - a_2 b_1) = 0$, i cui coefficienti sono espressioni razionali formate da numeri di C e perciò appartenenti a C. Se poi consideriamo due rette incidenti nel piano i cui coefficienti sono numeri di C, risolvendo il sistema tra esse si trova che il punto d'intersezione è espresso da frazioni aventi come numeratori e denominatori numeri che sono il risultato di operazioni razionali con i coefficienti delle equazioni delle rette,. Ne risulta che il punto d'incidenza appartiene al campo C. In modo pittoresco si può dire che soltanto con l'uso del compasso si può "uscire" da C. A questo scopo consideriamo un numero $k \in C$ tale che però $\sqrt{k} \notin C$ (nel caso che $\sqrt{k} \in C$, come ad esempio per $k = 4$, non si hanno ampliamenti algebrici, ma si rimane nel campo C) , quindi costruiamoci col compasso $\sqrt{k}$ nello stesso modo con cui abbiamo costruito prima $\sqrt{2}$. Ora tutti i numeri del tipo $a + b\sqrt{k}$, con $a, b \in C$ in particolare razionali, formano un campo C' chiuso rispetto alle quattro operazioni, in quanto operando su una coppia di numeri siffatti, si ottengono ancora tali numeri.

Si ha $C \subset C'$ perché, come detto prima, per $b = 0$ si ha $a \in C$. Quindi, se si parte da un qualsiasi campo C di numeri costruibili che contiene il numero k, usando la riga e una sola volta il compasso, si può costruire $\sqrt{k}$ ed ogni altro numero di C del tipo $a + b\sqrt{k}$, con $a, b \in C$. E' importante notare che tali numeri sono i soli così costruibili, cioè usando una sola volta il compasso, si possono ottenere solo numeri di tale tipo. A tale scopo consideriamo una circonferenza di centro (x_0, y_0) e raggio r, dove $x_0, y_0, r \in C$, la cui equazione è $(x - x_0)^2 + (y - y_0)^2 = r^2 \Rightarrow x^2 + y^2 - 2x_0 x - 2y_0 y + x_0^2 + y_0^2 = 0 \Rightarrow x^2 + y^2 + ax + by + c = 0$, dove $a, b, c \in C$, quindi una retta di equazione $a'x + b'y + c' = 0$, congiungente due punti del piano le cui coordinate appartengono a C, per cui, come già detto, anche $a', b', c' \in C$.

Dal sistema delle due equazioni $\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}$, ricavando la y dalla seconda equazione e sostituendo nella prima, si ottiene l'equazione di 2° grado $Lx^2 + Mx + N = 0$, dove $L, M, N \in C$, le cui due soluzioni $x = \frac{-M \mp \sqrt{M^2 - 4LN}}{2L}$ sono le ascisse dei punti d'intersezione della circonferenza con la retta., mentre le ordinate si ottengono sostituendo tali valori nella 2^a equazione del sistema. Tali soluzioni sono del tipo $p + q\sqrt{k}$, con $p, q, k \in C$. Lo stesso risultato si ha considerando l'intersezione di due circonferenze e quindi il sistema $\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0 \end{cases} \Rightarrow (a - a')x + (b - b')y + (c - c') = 0$ da cui, considerando il sistema $\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ (a - a')x + (b - b')y + (c - c') = 0 \end{cases}$ e procedendo come prima, si ottengono sempre punti le cui coordinate sono numeri del tipo $p + q\sqrt{k}$, con $p, q, k \in C$.

Riassumiamo quanto esposto fino ad ora.

Date inizialmente certe quantità, si possono costruire usando la sola riga tutte le quantità del campo C generate dalle quantità date mediante operazioni razionali. Usando il compasso si può estendere il campo C di quantità costruibili a un campo più vasto contenente il primo, scegliendo un numero non negativo qualsiasi $k \in C$ con il vincolo che $\sqrt{k} \notin C$ (altrimenti si ottiene il campo di partenza), quindi costruendo il campo C' formato dai numeri $a + b\sqrt{k}$, dove $a, b \in C$. C si dice sottocampo di C',in quanto i numeri $a \in C$ si ottengono dai numeri $a + b\sqrt{k} \in C'$ per $b = 0$.

Precisato che le costruzioni geometriche consistono nel tracciare una retta per due punti assegnati,disegnare un cerchio di centro e raggio assegnato,segnare le intersezioni tra due rette o tra due cerchi dati, ogni passaggio di una costruzione geometrica o ci porta ancora a delle quantità appartenenti al campo che già sappiamo costituito da numeri costruibili, oppure, mediante la costruzione di una radice quadrata, si ottiene un nuovo campo più esteso di numeri costruibili. Possiamo allora dare la seguente definizione.

Definizione : Sono **costruibili** tutti e solo i numeri che si possono ottenere con una successione di campi estesi, di modo che alla fine appartengano a un campo C_n, nel senso che, a partire da un campo C_0, definito da quantità qualsiasi assegnate inizialmente (ad esempio il campo razionale $\mathbb{Q}$, qualora venga assegnato all'inizio un solo elemento scelto come unità), preso $k_0 \in C_0$in modo che $\sqrt{k_0} \notin C_0$, si costruisce il campo C_1 dei numeri $a_0 + b_0\sqrt{k_0}$, con $a_0, b_0, k_0 \in C_0$, e così via fino al campo C_n.

E' fondamentale provare che tutti i numeri costruibili sono algebrici, dove, come si vedrà in seguito, un numero reale o complesso è **algebrico** se è radice di un' equazione algebrica di grado $n \geq 1$ a coefficienti interi del tipo $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, dove i coefficienti $a_k \in \mathbb{Z}$ sono numeri interi e $a_n \neq 0$. Un numero reale si dice **trascendente** se non è algebrico.

Teorema : **Tutti i numeri costruibili con riga e compasso sono algebrici.**

Dimostrazione :

Scegliamo inizialmente $C_0 = \mathbb{Q}$ in modo che questo sia il campo generato da un solo segmento ; tutti i numeri costruibili del campo C_1 sono allora del tipo $a + b\sqrt{k}$, con $a, b \in \mathbb{Q}, k \in \mathbb{Q}^+$ e $\sqrt{k} \notin \mathbb{Q}$ e sono radici dell'equazione di 2° grado $x^2 - 2ax + a^2 - b^2k = 0$, come si può facilmente verificare (nel caso che tra i coefficienti dell'equazione vi è almeno una frazione non apparente, allora si può ottenere un'equazione a coefficienti interi equivalente alla data moltiplicando ambo i membri dell'equazione per il m.c.d.).

Il campo $C_1 = \left\{a + b\sqrt{k}, a, b \in \mathbb{Q}, k \in \mathbb{Q}^+, \sqrt{k} \notin \mathbb{Q}\right\}$ così ottenuto ha come sotto campo C_0, essendo $C_0 \subset C_1$. A partire ora da C_1, si può ottenere il campo C_2, i cui numeri sono del tipo $p + q\sqrt{w}$, dove $p, q, w \in C_1, w > 0$ e $\sqrt{w} \notin C_1$ e quindi essi si scrivono come
$p = a + b\sqrt{s},\ q = c + d\sqrt{s},\ w = e + f\sqrt{s}, a, b, c, d, e, f \in \mathbb{Q}, \sqrt{s} \notin \mathbb{Q}, s \in \mathbb{Q}^+$.

Essi sono radici dell'equazione di 2° grado $x^2 - 2px + p^2 - q^2w = 0$, dove tutti i coefficienti appartengono al campo C_1 generato da $\sqrt{s}$. Sostituendo nell'equazione di 2° grado ai coefficienti i valori in funzione dei numeri razionali, si ha:

$$x^2 - 2px + p^2 - q^2w = 0 \Rightarrow x^2 - 2(a + b\sqrt{s})x + (a + b\sqrt{s})^2 - (c + d\sqrt{s})^2(e + f\sqrt{s}) = 0 \Rightarrow$$

$x^2 - 2ax + (a^2 + b^2s - ec^2 - ed^2s - 2cdfs) = \sqrt{s}\,(2bx - 2ab + 2ecd + fc^2 + fd^2s) \Rightarrow$
$x^2 + ux + v = \sqrt{s}\,(rx + t)$, dove sono tutti razionali le quantità
$u = -2a,\ v = a^2 + b^2s - ec^2 - ed^2s - 2cdfs,\ r = 2b,\ t = -2ab + 2ecd + fc^2 + fd^2s$. L'equazione $x^2 + ux + v = \sqrt{s}\,(rx + t)$ è di 2° grado, ma i suoi coefficienti non sono razionali comparendo $\sqrt{s}$, mentre quadrando i due membri si ottiene l'equazione di grado $4 = 2^2$a coefficienti razionali
$(x^2 + ux + v)^2 = s(rx + t)^2$.

In n passi, i numeri del campo C_n risultano radici di un'equazione di grado 2 a coefficienti nel campo C_{n-1} e di grado $\underbrace{2 \cdot \cdots \cdot 2}_{\text{n volte}} = 2^n$a coefficienti razionali, cioè nel campo $C_0 = \mathbb{Q}$. Se ora proviamo che, nell'ipotesi che ciò sia vero per n, allora è vero anche per n+1, in base al principio d'induzione la proposizione risulterà vera per ogni valore di $n \in \mathbb{N}$.

Supponiamo quindi che il numero reale $x \in C_n$, per cui deve avere la forma $x = \mu + \zeta\sqrt{\chi}$, con $\mu, \zeta, \chi \in C_{n-1}$ e $\sqrt{\chi} \notin C_{n-1}, \chi > 0$, di modo che l'estensione algebrica sia effettiva, e soddisfi l'equazione di 2° grado $x^2 - 2\mu x + \mu^2 - \zeta^2\chi = 0$ a coefficienti in C_{n-1}, quindi soddisfi pure un'equazione di grado 2^n a coefficienti razionali. Costruiamoci il numero $\omega = x + y\sqrt{z}$, dove $x, y, z \in C_n$ e $\sqrt{z}, \notin C_n$, che appartenendo al campo C_{n+1}, deve soddisfare a un'equazione di grado 2 a coefficienti nel campo C_n, di grado 2^2 a coefficienti nel campo C_{n-1}, di grado 2^{n+1} a coefficienti nel campo razionale $C_0 = \mathbb{Q}$. Il teorema è così completamente provato.

<u>Corollario</u>: **Un numero trascendente non è costruibile.**

<u>Dimostrazione</u>: Se per assurdo lo fosse, dovrebbe essere per la proposizione precedente algebrico, contro l'ipotesi.

<u>Osservazione</u>: Come si vedrà tra breve, **<u>il teorema non è invertibile</u>**, esistendo numeri algebrici che non sono costruibili con riga e compasso. Tutti i numeri razionali sono algebrici e costruibili; per quanto riguarda i numeri irrazionali, ci sono tra essi numeri costruibili come $\sqrt{2}$ e numeri non costruibili come $\sqrt[3]{2}$. A questo scopo dimostriamo le seguenti proposizioni. La prima prova che $\sqrt[3]{2}$ non è razionale.

<u>Proposizione</u>: Il numero reale $\sqrt[3]{2}$ è irrazionale.

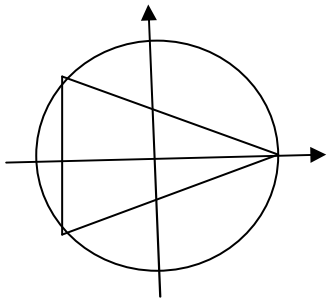
<u>Dimostrazione</u>: Se per assurdo $\sqrt[3]{2}$ fosse razionale, allora dovrebbe esistere una coppia di interi $a, b \in \mathbb{Z}, b \neq 0, (a, b) = 1$ tale che sia esprimibile con la frazione ridotta ai minimi termini $\frac{a}{b} = \sqrt[3]{2} \Longrightarrow a^3 = 2b^3$. Da ciò segue che comparendo 2 nella scomposizione in fattori primi di a^3, deve esserci pure in quella di a, per cui risultando a pari, è esprimibile come $a = 2k, k \in \mathbb{Z}$. Sostituendo si ha $8k^3 = 2b^3 \Rightarrow b^3 = 4k^3 = 2t, t = 2k^3$, per cui, avendo b^3 nella scomposizione in fattori primi il numero 2, anche b lo ha, donde b è pari. In conclusione, risultando sia a che b pari, entrambi sono divisibili per 2, il che implica $(a, b) \neq 1$, contro l'ipotesi.

<u>Proposizione</u>: Il numero reale $\sqrt[3]{2}$ è algebrico.

<u>Dimostrazione</u>: Infatti $\sqrt[3]{2}$ è l'unica radice reale dell'equazione cubica $x^3 - 2 = 0$, avente le radici (considerando $\sqrt[3]{2}$ come numero complesso):

$$\sqrt[3]{2} \in \mathbb{C} \Rightarrow \left[2^{\frac{1}{3}}, \frac{0+2k\pi}{3}\right]_{k=0,1,2} = \left[\sqrt[3]{2}, k \cdot \frac{2}{3}\pi\right]_{k=0,1,2} \Rightarrow$$

$$\begin{cases} k = 0 \Rightarrow \left[\sqrt[3]{2}, 0\right] = \sqrt[3]{2}(\cos 0 + i \sin 0) = \sqrt[3]{2} \\ k = 1 \Rightarrow \left[\sqrt[3]{2}, \frac{2}{3}\pi\right] = \sqrt[3]{2}\left(\cos\frac{2}{3}\pi + i \sin\frac{2}{3}\pi\right) = \sqrt[3]{2}\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) \\ k = 2 \Rightarrow \left[\sqrt[3]{2}, \frac{4}{3}\pi\right] = \sqrt[3]{2}\left(\cos\frac{4}{3}\pi + i \sin\frac{4}{3}\pi\right) = \sqrt[3]{2}\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) \end{cases}$$



<u>Proposizione</u>: Il numero reale $\sqrt[3]{2}$ non è costruibile con riga e compasso.

<u>Dimostrazione</u>: Se per assurdo $x = \sqrt[3]{2}$ fosse costruibile, allora $x \in \mathcal{C}_k$ campo opportuno ottenuto con ampliamenti algebrici successivi del campo razionale mediante l'aggiunta di radici quadrate. Per una proposizione precedente Il numero reale $\sqrt[3]{2}$ è irrazionale, per cui $x \notin \mathcal{C}_0 = \mathbb{Q}$, implicando ciò che $k > 0$ è un numero intero positivo. Tra tutti i possibili $k \in \mathbb{N}$ per cui si ha $x \in \mathcal{C}_k$ scegliamo il minimo; detto ciò, x deve avere la forma $x = p + q\sqrt{w}$, dove $p, q, w \in \mathcal{C}_{k-1}$, inoltre $\sqrt{w} \notin \mathcal{C}_{k-1}$.

Per la proposizione precedente x è algebrico, soddisfacendo l'equazione cubica $x^3 - 2 = 0$, che ha una sola radice reale e le altre due complesse coniugate, quindi $p + q\sqrt{w}$, con $p, q, w \in \mathcal{C}_{k-1}$, $\sqrt{w} \notin \mathcal{C}_{k-1}$, è radice di tale equazione. Ci proponiamo di provare che anche il numero reale $p - q\sqrt{w}$, con p e q diversi da 0, è radice dell'equazione $x^3 - 2 = 0$, il che conduce ad un assurdo perché la radice reale di tale equazione è unica. Si ha $x \in \mathcal{C}_k \Rightarrow x^3 \in \mathcal{C}_k \Rightarrow x^3 - 2 \in \mathcal{C}_k$, si ha

$x^3 - 2 = \left(p + q\sqrt{w}\right)^3 - 2 = (p^3 + 3pq^2w - 2) + (3p^2q + q^3w)\sqrt{w} = a + b\sqrt{w}$ con $a, b \in \mathcal{C}_{k-1}$, inoltre poniamo

$y = p - q\sqrt{w} \Rightarrow y^3 - 2 = \left(p - q\sqrt{w}\right)^3 - 2 = (p^3 + 3pq^2w - 2) - (3p^2q + q^3w)\sqrt{w} = a - b\sqrt{w}$. Poiché $p + q\sqrt{w}$ è radice dell'equazione $x^3 - 2 = 0$, deve aversi $a + b\sqrt{w} = 0$, con $a = b = 0$ poichè altrimenti, se $b \neq 0$, da tale uguaglianza segue $\sqrt{w} = -\frac{a}{b} \Rightarrow \sqrt{w} \in \mathcal{C}_{k-1}$, assurdo in quanto $a, b \in \mathcal{C}_{k-1}$, ed anche $a = 0$, un volta posto $b = 0$,

Ma da $y^2 - 2 = a - b\sqrt{w} = 0$, segue che $y = p - q\sqrt{w}$ è radice dell'equazione cubica, anche distinta da $x = p + q\sqrt{w}$, perché se fosse $x = y$, si avrebbe

$p + q\sqrt{w} = p - q\sqrt{w} \Rightarrow 2q\sqrt{w} = 0 \Rightarrow q = 0 \Rightarrow x = p \in \mathcal{C}_{k-1}$, contro il fatto che $x \in \mathcal{C}_k$.

L'esistenza dei numeri trascendenti fu dimostrata nel 1844 da Joseph Liouville, mentre nel 1873 Charles Hermite dimostrò la trascendenza del numero di Eulero e. Un anno dopo Georg Cantor dimostrò che i numeri trascendenti non sono numerabili e nel 1882 fu Ferdinand von Lindemann

che, basandosi sulla precedente dimostrazione di Hermite , dimostrò che π è un numero trascendente. Una conseguenza immediata è:

<u>Proposizione</u> : Il numero π non è costruibile.

<u>Dimostrazione</u>: Se fosse costruibile, per una proposizione precedente sarebbe algebrico, mentre per il teorema di Lindemann è trascendente.

<u>Corollario</u> : Il numero π non appartiene ad alcun campo algebrico costruibile con riga e compasso.

<u>Dimostrazione</u>: Se per assurdo $\exists k \in \mathbb{N}$ tale che $\pi \in C_k$, π sarebbe costruibile contro la proposizione precedente.

<u>Proposizione</u>: Il numero $\sqrt{\pi}$ non è algebrico, quindi è trascendente.

<u>Dimostrazione</u>: Se per assurdo fosse algebrico, dovrebbe esistere un polinomio di grado $n \in \mathbb{N}$ a coefficienti interi $a_0, a_1, \cdots, a_{n-1}, a_n$, $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, di cui $\sqrt{\pi}$ è una radice.

Ciò significa che $P(\pi) = a_0(\sqrt{\pi})^n + a_1(\sqrt{\pi})^{n-1} + \cdots + a_{n-1}\sqrt{\pi} + a_n = 0$, con $a_0, a_1, \cdots, a_n$ $n+1$ coefficienti interi.Supposto che $n = 2h, h \in \mathbb{N}$ sia un numero pari (analogamente si dimostra se $n = 2h+1, h \in \mathbb{N}$ è dispari), raggruppando le potenze di ordine pari e dispari, si ha:

$$a_0(\sqrt{\pi})^{2h} + a_1(\sqrt{\pi})^{2h-1} + a_2(\sqrt{\pi})^{2h-2} + \cdots + a_{n-2}(\sqrt{\pi})^2 + a_{n-1}\sqrt{\pi} + a_n = 0 \Longrightarrow$$

$$\left[a_0(\sqrt{\pi})^{2h} + a_2(\sqrt{\pi})^{2h-2} + \cdots + a_{n-2}(\sqrt{\pi})^2 + a_n\right] + \left[a_1(\sqrt{\pi})^{2h-1} + a_3(\sqrt{\pi})^{2h-3} + \cdots + a_{n-1}\sqrt{\pi}\right] =$$

$$\left\{a_0\left[(\sqrt{\pi})^2\right]^h + a_2\left[(\sqrt{\pi})^2\right]^{h-1} + \cdots + a_{n-1}(\sqrt{\pi})^2 + a_n\right\} + \sqrt{\pi}\left[a_1(\sqrt{\pi})^{2h-2} + a_3(\sqrt{\pi})^{2h-4} + \cdots + a_{n-1}\right] =$$

$$[a_0\pi^h + a_2\pi^{h-1} + \cdots + a_{n-2}\pi + a_n] + \sqrt{\pi}[a_1\pi^{h-1} + a_3\pi^{h-2} + \cdots + a_{n-1}] = A(\pi) + B(\pi)\sqrt{\pi} = 0\,,$$

Da ciò consegue che $A(\pi) + B(\pi)\sqrt{\pi} = 0$, dove $A(\pi)$ e $B(\pi)$ sono espressioni razionali intere in π a coefficienti interi. Da questa uguaglianza si ricava che $A(\pi) = -B(\pi)\sqrt{\pi}$, da cui quadrando ambo i membri segue $A^2(\pi) = B^2(\pi)\pi \Longrightarrow A^2(\pi) - B^2(\pi)\pi = 0$, ovvero π essendo radice del polinomio $A^2(x) - B^2(x)x$ a coefficienti interi risulta algebrico, assurdo essendo π trascendente.

E' possibile dimostrare la trascendenza di $\sqrt{\pi}$ in un altro modo; premettiamo le seguenti proposizioni.

<u>Proposizione</u>: α è un numero algebrico, se e solo se anche lo è la sua potenza ad esponente intero positivo $\alpha^k, k \in \mathbb{N}$.

<u>Dimostrazione</u>: Poiché si dimostra che i numeri algebrici costituiscono un campo rispetto alla somma e al prodotto di numeri algebrici, le potenze dei numeri algebrici appartengono al campo per cui sono numeri algebrici. Viceversa se una potenza α^k è un numero algebrico, necessariamente lo è pure la base α della potenza. Infatti se per assurdo α fosse trascendente, allora in base alla proposizione successiva lo sarebbe pure la sua potenza α^k , contro l'ipotesi.

Proposizione: : α è un numero trascendente, se e solo se anche lo è la sua potenza ad esponente intero positivo $\alpha^k, k \in \mathbb{N}$..

Dimostrazione: La condizione è necessaria. Infatti se α è un numero trascendente, supposto per assurdo che α^k fosse algebrico, allora dovrebbe esistere un opportuno polinomio di grado $n \in \mathbb{N}$ a coefficienti interi $a_0, a_1, \cdots, a_{n-1}, a_n$, $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, tale che $x = \alpha^k$ è radice, ovvero

$P(\alpha^k) = a_0\alpha^{kn} + a_1\alpha^{k(n-1)} + \cdots + a_{n-1}\alpha^k + a_n = 0$. Ma allora il polinomio di grado kn

$P_1(x) = a_0x^{kn} + a_1x^{k(n-1)} + \cdots + a_{n-1}x^k + a_n$ ha la radice $x = \alpha$, per cui sarebbe algebrico, contro l'ipotesi. Viceversa se α^k è trascendente, se per assurdo α fosse algebrico, allora per la proposizione precedente lo sarebbe anche α, contro l'ipotesi.

Proviamo quindi che:

Proposizione: α è trascendente $\Longrightarrow \sqrt[k]{\alpha}$, $\mathrm{k} \in \mathbb{N}$ è trascendente.

Dimostrazione: Se per assurdo $\sqrt[k]{\alpha}$ fosse algebrico, allora anche la sua potenza $\left(\sqrt[k]{\alpha}\right)^k = \alpha$ dovrebbe esserlo per la proposizione precedente, per cui α sarebbe algebrico, contro l'ipotesi.

Corollario: Il numero $\sqrt{\pi}$ non è algebrico, quindi è trascendente.

Dimostrazione: Per $\alpha = \pi$ e $k = 2$ dalla proposizione precedente.

Proposizione: Il numero $\sqrt{\pi}$ non è costruibile.

Dimostrazione: Se per assurdo fosse costruibile, sarebbe algebrico per il teorema pag.3, contro la proposizione precedente.

Veniamo ora finalmente il problema della quadratura del cerchio.

Esso consiste,come già si è detto, nel determinare un quadrato di lato incognito x la cui area $A = x^2$ è uguale a quella di un cerchio di raggio unitario. In sostanza l'assunto equivale a determinare la radice positiva dell'equazione $x^2 = \pi$, ovvero $x = \sqrt{\pi}$. Il problema non ha soluzione utilizzando una costruzione con riga e compasso.

Teorema: Il problema della quadratura del cerchio non è risolvibile con riga e compasso.

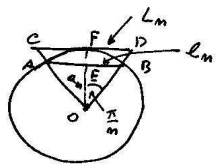
Dimostrazione: Se per assurdo il problema fosse risolvibile, allora l'equazione $x^2 - \pi = 0$ dovrebbe avere la radice $\sqrt{\pi}$ costruibile, contro la proposizione precedente.

Prima di vedere il 2° problema della duplicazione del cubo, diciamo ancora qualche cosa su π.

Sappiamo dalla geometria che la lunghezza di una circonferenza di raggio assegnato r può essere definita come il limite di una successione i cui termini sono i perimetri dei poligoni regolari inscritti o circoscritti con un numero crescente di lati. In particolare, se r = 1, la lunghezza della circonferenza così definita si indica con 2π, per cui π risulta essere la misura della lunghezza della

semicirconferenza di raggio unitario. [1]Così facendo, implicitamente presupponiamo che tale limite esista finito e sia un numero reale, giustificando tale assunto con la sua evidenza geometrica.

[1] Più precisamente, se rispettivamente p_n e P_n denotano il perimetro del poligono regolare di n lati inscritto e circoscritto, si ha che la successione $\{p_n\}$ è monotona strettamente crescente limitata superiormente da 2π, mentre la successione $\{P_n\}$ è monotona strettamente decrescente limitata inferiormente da 2π. Per un teorema sui limiti delle successioni monotone si ha che 2π è il limite di entrambe le due successioni, mentre per ogni $n \in \mathbb{N}$ fissato, rispettivamente p_n e P_n ne forniscono un'approssimazione per difetto e per eccesso. Se $\overline{CD} = L_n$ è la misura del lato del poligono regolare circoscritto di n lati P_n, $\overline{AB} = l_n$ il lato del poligono regolare inscritto di n lati, $\overline{OE} = a_n$ l'apotema del poligono inscritto(raggio della circonferenza inscritta nel poligono inscritto) $\overline{OF} = r$ apotema del poligono circoscritto, si ha la misura in radianti $\widehat{AOB} = \frac{2\pi}{n}$ in quanto la regolarità del poligono implica che tutti gli angoli al centro sottesi dai rispettivi lati sono uguali, donde $\widehat{AOE} = \frac{\pi}{n}$. Allora $\overline{OE} = a_n = r\cos\frac{\pi}{n}$, $\overline{AE} = \frac{1}{2}l_n = r\sin\frac{\pi}{n}$, $\overline{CF} = \frac{1}{2}L_n = r\tan\frac{\pi}{n}$, da cui $l_n = 2r\sin\frac{\pi}{n}$, $L_n = 2r\tan\frac{\pi}{n}$ e quindi $p_n = nl_n = 2rn\sin\frac{\pi}{n}$, $P_n = nL_n = 2nr\tan\frac{\pi}{n}$ Si ricava allora che $\lim_{n\to\infty} p_n = \lim_{n\to\infty} 2nr\sin\frac{\pi}{n} = 2\pi r\lim_{n\to\infty}\frac{\sin\frac{\pi}{n}}{\frac{\pi}{n}} = 2\pi r\lim_{\frac{\pi}{n}\to 0^+}\frac{\sin\frac{\pi}{n}}{\frac{\pi}{n}} = 2\pi r$ e $\lim_{n\to\infty} P_n = \lim_{n\to\infty} 2nr\tan\frac{\pi}{n} = 2\pi r\lim_{n\to\infty}\frac{\tan\frac{\pi}{n}}{\frac{\pi}{n}} = 2\pi r\lim_{\frac{\pi}{n}\to 0^+}\frac{\tan\frac{\pi}{n}}{\frac{\pi}{n}} = 2\pi r$. Posto $r = 1$, da queste relazioni si ricava che $\frac{1}{2}\lim_{n\to\infty} p_n = \frac{1}{2}\lim_{n\to\infty} P_n = \pi$



. Naturalmente <u>si può definire π come l'area di un cerchio di raggio unitario</u>.Consideriamo allora rispettivamente le aree del poligono regolare di n lati inscritto e circoscritto $s_n = nS(AOB) = \frac{1}{2}nr^2\sin\frac{2\pi}{n} = \frac{1}{2}nr^2 2\sin\frac{\pi}{n}\cos\frac{\pi}{n} = \frac{1}{2}p_n a_n$,

$S_n = nS(COD) = \frac{1}{2}nCD\cdot\overline{OF} = \frac{1}{2}nL_n r = \frac{1}{2}n2r\tan\frac{\pi}{n}r = nr^2\tan\frac{\pi}{n} = \frac{1}{2}P_n r$. Si ha quindi $\begin{cases} s_n = \frac{1}{2}nr^2\sin\frac{2\pi}{n} \\ S_n = nr^2\tan\frac{\pi}{n} \end{cases}$, da cui

$\lim_{n\to\infty} s_n = \lim_{n\to\infty}\frac{1}{2}nr^2\sin\frac{2\pi}{n} = \pi r^2\lim_{\frac{2\pi}{n}\to 0}\frac{\sin\frac{2\pi}{n}}{\frac{2\pi}{n}} = \pi r^2$ e $\lim_{n\to\infty} S_n = \lim_{n\to\infty} nr^2\tan\frac{\pi}{n} = \pi r^2\lim_{\frac{\pi}{n}\to 0}\frac{\tan\frac{\pi}{n}}{\frac{\pi}{n}} = \pi r^2$. Posto $r = 1$, da queste relazioni si ricava che $\lim_{n\to\infty} s_n = \lim_{n\to\infty} S_n = \pi$.Consideriamo ora, sempre per $r = 1$, $\frac{2\pi}{n} = \theta$, le aree dei poligonl inscritti di n lati e di $2n$ lati, rispettivamente date da $s_n = \frac{1}{2}n\sin\theta \Rightarrow \sin\theta = \frac{2s_n}{n}$ e

$s_{2n} = \frac{1}{2}\cdot 2n\sin\frac{\theta}{2} = n\sin\frac{\theta}{2} = n\sqrt{\frac{1-\cos\theta}{2}} = \frac{n}{\sqrt{2}}\sqrt{1-\cos\theta} = \frac{n}{\sqrt{2}}\sqrt{1-\sqrt{1-\sin^2\theta}} = \frac{n}{\sqrt{2}}\sqrt{1-\sqrt{1-\frac{4s_n^2}{n^2}}}$. Posto $n = 2^k \Rightarrow 2n = 2^{k+1}$ si ha

$s_{2^{k+1}} = 2^{k-\frac{1}{2}}\sqrt{1-\sqrt{1-4^{1-k}s_{2^k}^2}}$, da cui posto $s_{2^k} = f_k$, $s_{2^{k+1}} = f_{k+1}$ si ottiene $f_{k+1} = 2^{k-\frac{1}{2}}\sqrt{1-\sqrt{1-4^{1-k}f_k^2}}$. Ora la successione $\{f_k\}_{k\in\mathbb{N}}$ di aree di poligoni inscritti nel cerchio di raggio unitario al crescere del numero dei lati, è strettamente crescente e limitata da 4, area del quadrato circoscritto al cerchio, quindi convergente all'area del cerchio, per cui si ha $\lim_{k\to\infty} f_k = \pi$. Poiché per $k = 2$ si ha

$f_2 = s_4 = \frac{1}{2}\cdot 4\sin\frac{2\pi}{4} = 2$, segue applicando la formula ricorsiva $f_3 = 2^{2-\frac{1}{2}}\sqrt{1-\sqrt{1-4^{1-2}f_2^2}} = 2\sqrt{2}$, $f_4 \approx 3.06$, $f_5 \approx 3.12$.

Nel Bulletin of American Mathematical Society del 1947 (a pag.509 I.III, 1947, 6) era riportato il seguente articolo" A simple proof that π is irrational" di Ivan Niven riguardante , come dice il titolo, una semplice dimostrazione che π è un numero irrazionale. La dimostrazione viene riportata

in un libro di esercizi di Analisi Matematica del prof. Enrico Giusti ed è, come dire, piuttosto sintetica.[2]

[2] Ancor più è la dimostrazione riportata nel libro "δ La matematica- Problemi e teoremi" a cura Claudio Bartocci e Piergiorgio Odi8freddi- Ed. Einaudi- nell'articolo di Jonathan Borwein "La vita di pi greco" che qui riporto per soddisfare la "curiosità" del lettore. Supponiamo che $\pi = \frac{a}{b}$ sia il quoziente di due interi positivi a e b. Definiamo i polinomi

$f(x) = \frac{x^n(a-bx)^n}{n!}$ e $F(x) = f(x) - f''(x) + f^{(4)}(x) - \dots + (-1)^n f^{(2n)}(x)$, specificando in seguito l'intero positivo n. Dal momento che $n!f(x)$ ha coefficienti interi e che i suoi termini in x hanno grado minimo n, $f(x)$ e le sue derivate $f^{(k)}(x)$ assumono valori interi per $x = 0$ e anche per $x = \pi = \frac{a}{b}$, dal momento che $f(x) = f\left(\frac{a}{b} - x\right)$. Usando gli elementi di base del calcolo infinitesimale otteniamo $\frac{d}{dx}[F'(x)\sin x - F(x)\cos x] =$

$F''(x)\sin x - F(x)\sin x = f(x)\sin x$ e $\int_0^\pi f(x)\sin x dx = [F'(x)\sin x - F(x)\cos x]_0^\pi = F(\pi) + F(0)$. Ora $F(\pi) + F(0)$ è un numero intero, poiché $f^{(k)}(0)$ e $f^{(k)}(\pi)$ sono interi. Ma per $0 < x < \pi$, $0 < f(x)\sin x < \frac{\pi^n a^n}{n!}$ e quindi l'integrale $\int_0^\pi f(x)\sin x dx$ è"positivo ma arbitrariamente piccolo"per n sufficientemente grande. L'eguaglianza $\int_0^\pi f(x)\sin x dx = F(\pi) + F(0)$ è quindi falsa, e quindi lo è anche la nostra assunzione che π sia razionale.

Credo di fare un'azione meritoria dal punto di vista didattico, riportando la dimostrazione e giustificando ogni implicazione con tutti i passaggi matematici. Vedremo più avanti (corollario pag.26) che la conoscenza che π è un numero trascendente implica immediatamente che è irrazionale e ciò vale pure per il numero e. Ma a differenza di quest'ultimo, la dimostrazione del 1882 di Lindemann che π è trascendente è piuttosto complicata, per cui la tralasciamo, dimostrando solo che il numero di Eulero è trascendente (pag. 18). Dimostrazione comunque relativamente laboriosa.

Le conoscenze necessarie sono quelle dell'ultimo anno del liceo scientifico con approfondimenti, ma alla fine, come il lettore potrà constatare, la dimostrazione è piuttosto lunga e per niente "semplice".Come dire il termine semplice è sempre relativo!

<u>Teorema</u>: Il numero π è irrazionale.

<u>Dimostrazione</u>; Ragioniamo per assurdo supponendo che π sia un numero razionale.

Allora devono esistere due interi positivi a e b, con $b \neq 0$, eventualmente supponendo (ma ciò non è necessario ai fini della dimostrazione) che il loro massimo comun divisore sia 1 di modo che la frazione $\frac{a}{b} = \pi$ sia ridotta ai minimi termini.

Consideriamo quindi il polinomio della variabile reale x avente grado $2n \in \mathbb{N}$,

$$P(x) = \frac{x^n(a-bx)^n}{n!}$$

Il quale si annulla per $x = 0, x = \frac{a}{b} = \pi$.

Per considerazioni che faremo in seguito, conviene sviluppare Il termine $(a - bx)^n$ con la formula del binomio di Newton. Si ha:

$$(a-bx)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}(-b)^k x^k$$
$$= \binom{n}{0} a^n - \binom{n}{1} a^{n-1} bx + \binom{n}{2} a^{n-2} b^2 x^2 + \cdots + \binom{n}{n-1} a(-b)^{n-1} x^{n-1}$$
$$+ \binom{n}{n} (-b)^n x^n$$

da cui segue che

$$\frac{x^n(a-bx)^n}{n!} = \frac{1}{n!}\binom{n}{0} a^n x^n - \frac{1}{n!}\binom{n}{1} a^{n-1} bx^{n+1} + \frac{1}{n!}\binom{n}{2} a^{n-2} b^2 x^{n+2} + \cdots +$$
$$\frac{(-1)^{n-1}}{n!}\binom{n}{n-1} ab^{n-1} x^{2n-1} + \frac{(-1)^n}{n!}\binom{n}{n} b^n x^{2n}$$
.

Se si pone $a_k = \frac{(-1)^k}{n!}\binom{n}{k} a^{n-k} b^k$, $k = 0, \cdots, n$, si ha l'espressione del polinomio

$P(x) = a_0 x^n + a_1 x^{n+1} + \cdots + a_{n-1} x^{2n-1} + a_n x^{2n}$. Avremmo potuto subito scrivere tale espressione di $P(x)$, ma non avremmo in tal caso potuto specificare i coefficienti a_k. C'è da dire però che ai fini della dimostrazione tale specifica non è necessaria.

Derivando l'espressione di $P(x)$, si ha:

$$P(x)' = na_0 x^{n-1} + (n+1)a_1 x^n + \cdots + (2n-1)a_{n-1} x^{2n-2} + 2na_n x^{2n-1};$$

$$P(x)'' = n(n-1)a_0 x^{n-2} + (n+1)\mathrm{n}a_1 x^{n-1} + \cdots + (2n-1)(2n-2)a_{n-1} x^{2n-3} +$$

$$+2n(2n-1)a_n x^{2n-2};$$

.....

$$P(x)^{(n-1)} = n(n-1)\cdot\cdots\cdot 2a_0 x + (n+1)n\cdot\cdots\cdot 3a_1 x^2 + \cdots + (2n-1)(2n-2)\cdot\cdots\cdot$$

$$(2n-(n-1))a_{n-1} x^{2n-1-(n-1)} + 2n\cdot\cdots\cdot(n-2)(n-1)a_n x^{2n-(n-1)} =$$

$$n(n-1)\cdot\cdots\cdot 2a_0 x + (n+1)n\cdot\cdots\cdot 3a_1 x^2 + \cdots + (2n-1)\cdot\cdots\cdot(n+1)a_{n-1} x^n +$$

$$+2n\cdot\cdots\cdot(n-1)a_n x^{n+1};$$

$$P(x)^{(n)} = n(n-1)\cdot\cdots\cdot 2\cdot 1\cdot a_0 + (n+1)n\cdot\cdots\cdot 2a_1 x + \cdots + (2n-1)\cdot\cdots\cdot$$

$$(2n-n)a_{n-1} x^{2n-1-n} + 2n\cdot\cdots\cdot(n-1)na_n x^{2n-n} =$$

$$n!\,a_0 + (n+1)!\,a_1 x + \cdots + \frac{(2n-1)!}{n!} a_{n-1} x^{n-1} + \frac{(2n)!}{n!} a_n x^n \;;$$

Possiamo quindi scrivere il polinomio $P(x)$ e le sue derivate successive fino all'ordine n nel modo seguente:

$$P(x) = a_{0,0}x^n + a_{0,1}x^{n+1} + \cdots + a_{0,n-1}x^{2n-1} + a_{0,n}x^{2n}$$
$$P'(x) = a_{0,1}x^{n-1} + a_{1,1}x^n + \cdots + a_{n-1,1}x^{2n-2} + a_{n,1}x^{2n-1}$$
$$P''(x) = a_{0,2}x^{n-2} + a_{1,2}x^{n-1} + \cdots + a_{n-1,2}x^{2n-3} + a_{n,2}x^{2n-2}$$

……

$$P^{(n-1)}(x) = a_{0,n-1}x + a_{1,n-1}x^2 + \cdots + a_{n-1,n-1}x^n + a_{n,n-1}x^{n+1}$$
$$P^{(n)}(x) = a_{0,n} + a_{1,n}x + \cdots + a_{n-1,n}x^{n-1} + a_{n,n}x^n$$

$$P^{(n+1)}(x) = a_{1,n} + a_{2,n}x \cdots + na_{n,n}x^{n-1}$$

……

$$P^{(2n)}(x) = n!\,a_{n,n}$$

Osserviamo che per $x = 0$ si ha $P(0) = P'(0) = \cdots = P^{(n-1)}(0) = 0$, annullandosi per $x = 0$ il polinomio con tutte le sue derivate fino alla n-1-ma,mentre le derivate di ordine da n a 2n assumono valori interi, avendosi $P^{(n+1)}(0) = a_{1,n}, \cdots P^{(2n)}(0) = n!\,a_{n,n}$.

Inoltre i coefficienti $a_{i,j}$ $(i,j = 1,\cdots,n)$ sono valori interi potendosi effettuare delle semplificazioni nelle frazioni contenenti i fattoriali $^{(*)}$

Posto $P(x) = P^{(0)}(x)$, consideriamo il polinomio

$$Q(x) = P(x) - P''(x) + P^{(4)}(x) - \cdots + (-1)^n P^{(2n)}(x) = \sum_{k=0}^{n} (-1)^k P^{(2k)}(x)$$

Per quanto abbiamo detto prima, si ha $Q(0) = \sum_{k=0}^{n}(-1)^k P^{(2k)}(0)$ è un numero intero, cioè il valore che il polinomio Q(x) assume per x = 0 è un intero.

Notiamo che si ha:

$$P\left(\frac{a}{b} - x\right) = \frac{\left(\frac{a}{b} - x\right)^n \left[a - b\left(\frac{a}{b} - x\right)\right]^n}{n!} = \frac{\frac{\left(\frac{a}{b} - x\right)^n b^n x^n}{b^n}}{n!} = P(x)$$

Inoltre da $P(x) = P\left(\frac{a}{b} - x\right)$ segue, derivando successivamente , $P'(x) = -P'\left(\frac{a}{b} - x\right)$,

$P''(x) = P''\left(\frac{a}{b} - x\right), P'''(x) = -P'''\left(\frac{a}{b} - x\right), \cdots, P^{(k)}(x) = (-1)^k P^{(k)}\left(\frac{a}{b} - x\right)$, per cui in particolare $P^{(2k)}(x) = P^{(2k)}\left(\frac{a}{b} - x\right)$ per $k = 0,1,\cdots,n$, donde per x = 0 si ha $P(0) = P\left(\frac{a}{b}\right)$,

$P^{(2k)}(0) = P^{(2k)}\left(\frac{a}{b}\right)$ e quindi

$Q(0) = \sum_{k=0}^{n}(-1)^k P^{(2k)}(0) = \sum_{k=0}^{n}(-1)^k P^{(2k)}\left(\frac{a}{b}\right) = Q\left(\frac{a}{b}\right) = Q(\pi)$.

L'eguaglianza $Q(\pi) = Q(0)$ stabilisce che il polinomio $Q(x)$ assume lo stesso valore intero per

x = 0 e per x = π.

Derivando il polinomio Q(x), si ha:

$Q'(x) = P'(x) - P'''(x) + P^{(5)}(x) - \cdots + (-1)^n P^{(2n+1)}(x) = P'(x) - P'''(x) + P^{(5)}(x) - \cdots + (-1)^{n-1} P^{(2n)}(x)$

, poiché $P^{(2n+1)}(x) \equiv 0$

$$Q''(x) = P''(x) - P^{(4)}(x) + P^{(6)}(x) - \cdots + (-1)^{n-1} P^{(2n+1)}(x)$$
$$= P''(x) - P^{(4)}(x) + P^{(6)}(x) - \cdots + (-1)^n P^{(2n)}(x) = P(x) - Q(x)$$

(*)Ad esempio $\frac{(2n)!}{n!}a_n = \frac{2n\cdots n!}{n!}\frac{(-1)^n}{n!}\binom{n}{n}b^n = \frac{2n\cdots(n+1)}{n!}(-1)^n b^n = \frac{2n(2n-1)(2n-2)(2n-3)(2n-4)\cdots(n+1)}{n(n-1)(n-2)\cdots 2\cdot 1}(-1)^n b^n = \frac{(2n-1)\cdot 2\cdot(n-1)(2n-3)\cdot 2\cdot(n-2)\cdot\cdots\cdot(n+1)}{(n-1)(n-2)\cdot\cdots\cdot 3}(-1)^n b^n$

Da ciò segue

$Q''(x) = P(x) - Q(x) \Rightarrow P(x) = Q''(x) + Q(x) \Rightarrow$

$P(x)\sin x = \left(Q''(x) + Q(x)\right)\sin x =$
$Q''(x)\sin x + Q(x)\sin x = Q''(x)\sin x + Q'(x)\cos x - Q'(x)\cos x + Q(x)\sin x =$

$(Q''(x)\sin x + Q'(x)\cos x) - (Q'(x)\cos x - Q(x)\sin x) = (Q'(x)\sin x)' - (Q(x)\cos x)' =$

$(Q'(x)\sin x - Q(x)\cos x)'$.

Allora dall'uguaglianza $P(x)\sin x = \frac{d}{dx}[Q'(x)\sin x - Q(x)\cos x]$, integrando ambo i membri tra

0 e π, si ha:

$\int_0^{\pi} P(x)\sin x\,dx = [Q'(x)\sin x - Q(x)\cos x]_0^{\pi} = Q'(\pi)\sin\pi - Q(\pi)\cos\pi - Q'(0)\sin 0 + Q(0)\cos 0 = Q(\pi) + Q(0) = 2Q(\pi)$

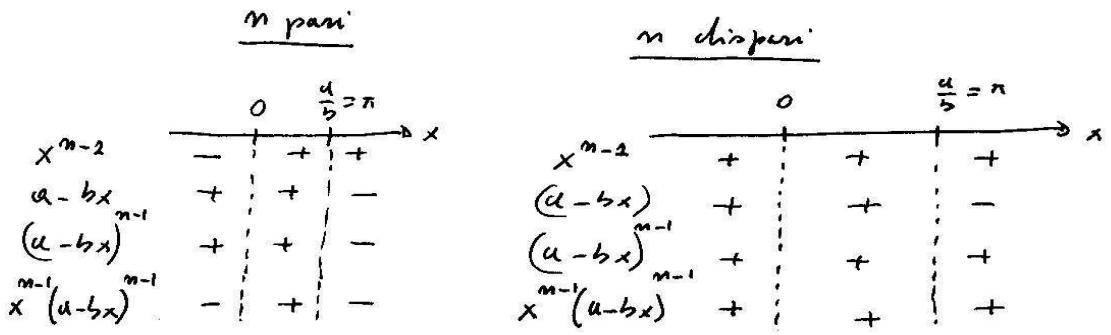
, che essendo un numero intero, fa sì che anche l'integrale definito è un numero intero.

Per conoscere gli eventuali estremi del polinomio $P(x) = \frac{x^n(a-bx)^n}{n!}$, calcoliamo la sua derivata prima. Si ha:

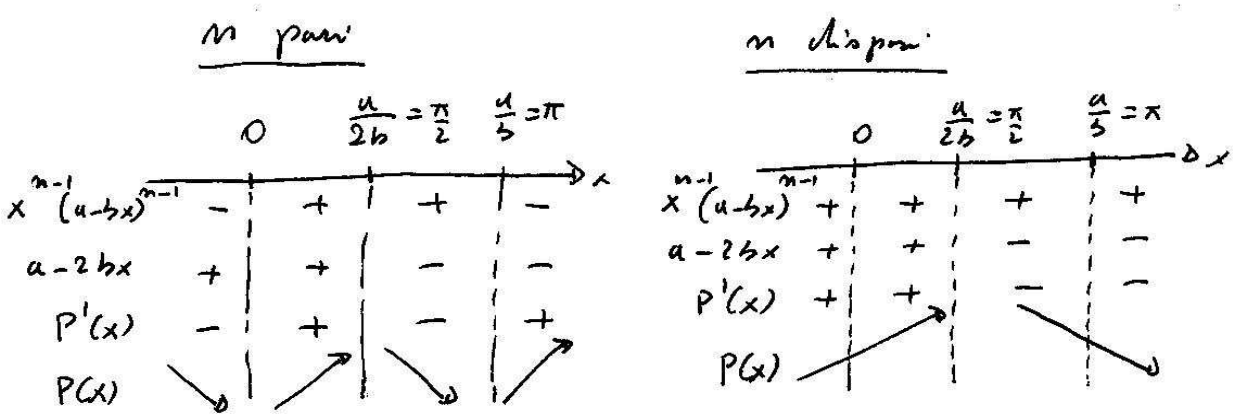
$$P'(x) = \frac{1}{n!}[nx^{n-1}(a-bx)^n + x^n n(a-bx)^{n-1}(-b)] = \frac{nx^{n-1}(a-bx)^n - nbx^n(a-bx)^{n-1}}{n!}$$
$$= \frac{nx^{n-1}(a-bx)^{n-1}(a-bx-bx)}{n!} = \frac{x^{n-1}(a-bx)^{n-1}(a-2bx)}{(n-1)!}$$

$$P'(x) = 0 \Rightarrow x = 0 \ \vee \ a - bx = 0 \ \vee \ a - 2bx = 0 \Rightarrow x = 0 \ \vee \ x = \frac{a}{b} = \pi \ \vee \ x = \frac{a}{2b} = \frac{\pi}{2}$$

A questo punto notiamo che il prodotto $x^{n-1}(a-bx)^{n-1}$ per $0 < x < \frac{a}{b} = \pi$ è sempre positivo sia per n pari che per n dispari, come risulta dal seguente specchietto:



Allora poiché $a - bx \geq 0 \Leftrightarrow x \leq \frac{a}{2b}$, segue la crescenza e la decrescenza del polinomio P(x) riassunta nel seguente specchietto:



Quindi $\forall x \in \mathbb{N}\ x = \frac{a}{2b} = \frac{\pi}{2}$ è punto di massimo relativo per P(x) , che assume il valore

$$P\left(\frac{\pi}{2}\right) = \frac{\left(\frac{\pi}{2}\right)^n \left(a - b\frac{a}{2b}\right)^n}{n!} = \frac{\frac{\pi^n}{2^n}\frac{a^n}{2^n}}{n!} = \frac{\pi^n a^n}{4^n n!}$$

Ora il prodotto $P(x)\sin x$ nell'intervallo $(0,\pi)$ raggiunge il suo valore massimo per $x=\frac{\pi}{2}$ in quanto entrambi i fattori del prodotto sono massimi in tale punto e tale massimo vale appunto

$P\left(\frac{\pi}{2}\right)\sin\frac{\pi}{2}=\frac{\pi^n a^n}{4^n n!}$. (**)Poiché quindi nell'intervallo $\left[0,\frac{\pi}{2}\right]$ la funzione $P(x)\sin x$ assume agli estremi rispettivamente i valori 0 e $\frac{\pi}{2}$ ed ha il massimo per $x=\frac{\pi}{2}$, deve valere la diseguaglianza doppia $0<P(x)\sin x<\frac{\pi^n a^n}{4^n n!}$. Ricordando allora una proprietà dell' integrale definito (***)si ha:

(**) D'altra parte, affinché la funzione $P(x)\sin x$abbia un estremo, necessariamente deve essere $(P(x)\sin x)'=P'(x)\sin x+P(x)\cos x=0\Rightarrow P'(x)+P(x)\cot x=0$, che è un'equazione differenziale lineare omogenea del 1° ordine che, posto $y(x)=P(x)$, possiamo scrivere nel modo seguente $y'+y\cot x=0$ da risolvere nell'intervallo $(0,\pi)$. Poiché $e^{\int\cot x dx}\neq 0$, si ha

$e^{\int\cot x dx}(y'+y\cot x)=0\Rightarrow y'e^{\int\cot x dx}+y\cot x e^{\int\cot x dx}=0\Rightarrow\left(ye^{\int\cot x dx}\right)'=0\Rightarrow ye^{\int\cot x dx}+c=0\Rightarrow y=ce^{-\int\cot x dx}=ce^{-\int\frac{\cos x}{\sin x}dx}=ce^{-\int\frac{d(\sin x)}{\sin x}}=ce^{-\ln\sin x}=\frac{c}{e^{\ln\sin x}}=\frac{c}{\sin x}$

,con c costante arbitraria, è l'integrale generale. Imponendo la condizione iniziale $x=\frac{\pi}{2}$, si ottiene $y\left(\frac{\pi}{2}\right)=c$.

Essendo d'altraparte $y\left(\frac{\pi}{2}\right)=\frac{\pi^n a^n}{4^n n!}$, segue il valore della costante $c=\frac{\pi^n a^n}{4^n n!}$ e l'integrale particolare $y=\frac{\pi^n a^n}{4^n n!}\frac{1}{\sin x}$ passante per il punto $\left(\frac{\pi}{2},\frac{\pi^n a^n}{4^n n!}\right)$.

(***) Se f(x) e g(x) sono due funzioni reali di una variabile reale x definite nell'intervallo chiuso e limitato [a,b] ed ivi continue, con $f(x)\leq g(x),\forall x\in[a,b]$, allora si ha anche per gli integrali definiti sull'intervallo [a,b] la diseguaglianza $\int_a^b f(x)dx\leq\int_a^b g(x)dx$. Infatti dall'ipotesi segue che, posto $h(x)=g(x)-f(x)$, si ha $h(x)\geq 0,\forall x\in[a,b]$. Suddiviso arbitrariamente l'intervallo [a,b] in intervallino parziali $I_k=[x_{k-1},x_k]$ di ampiezza $h_k=x_k-x_{k-1}$, dove $k=1,\cdots,n$, scegliamo rispettivamente in ogni intervallino $I_k$in modo arbitrario dei punti ξ_k. Poiché $h(x)\geq 0,\forall x\in[a,b]$, deve in particolare aversi $\forall k=1,\cdots,n$,

$h(\xi_k)\geq 0\Rightarrow h(\xi_k)h_k\geq 0\Rightarrow\sum_{k=1}^n h(\xi_k)h_k\geq 0\Rightarrow\lim_{\delta\to 0}\sum_{k=1}^n h(\xi_k)h_k\geq 0\Rightarrow\int_a^b h(x)dx\Rightarrow\int_a^b[g(x)-f(x)]dx\geq 0\Rightarrow\int_a^b g(x)dx\geq\int_a^b f(x)dx.$

$$0<\int_0^\pi P(x)\sin x\,dx<\int_0^\pi\frac{\pi^n a^n}{4^n n!}dx\Rightarrow 0<\int_0^\pi P(x)\sin x\,dx<\frac{\pi^n a^n}{4^n n!}.$$

A questo punto consideriamo la successione numerica a termini positivi $\left\{\frac{\pi^n a^n}{4^n n!}\right\}_{n\in\mathbb{N}}$ che si può scrivere come $\left\{\frac{\pi\left(\frac{\pi a}{4}\right)^n}{n!}\right\}_{n\in\mathbb{N}}$ e quindi posto $\alpha=\frac{\pi a}{4}$, diviene $\{\beta_n\}_{n\in\mathbb{N}}=\left\{\frac{\pi\alpha^n}{n!}\right\}_{n\in\mathbb{N}}$. Per studiare il carattere della successione $\{\beta_n\}_{n\in\mathbb{N}}$, consideriamo il rapporto $\frac{\beta_{n+1}}{\beta_n}=\frac{\frac{\pi\alpha^{n+1}}{(n+1)!}}{\frac{\pi\alpha^n}{n!}}=\frac{\alpha}{n+1}$, quindi essendo possibile determinare un opportuno indice $\nu>0$ tale che per $n>\nu$ risulti $\alpha<n+1$, si ha $0<\frac{\alpha}{n+1}<1\Rightarrow 0<\frac{\beta_{n+1}}{\beta_n}<1\Rightarrow\beta_{n+1}<\beta_n\Rightarrow\{\beta_n\}_{n\in\mathbb{N}}$ è una successione a termini

positivi strettamente decrescente il cui massimo $\beta_1 = \frac{\pi^2 a}{4}$ è l'estremo superiore e 0 l'estremo inferiore. Essendo quindi limitata e strettamente monotona decrescente, la successione deve convergere a un limite λ. Dall'uguaglianza $\frac{\beta_{n+1}}{\beta_n} = \frac{\alpha}{n+1}$, segue

$\beta_{n+1} = \frac{\alpha}{n+1}\beta_n \Rightarrow \lim_{n\to\infty}\beta_{n+1} = \lim_{n\to\infty}\frac{\alpha}{n+1}\beta_n = \lim_{n\to\infty}\frac{\alpha}{n+1}\lim_{n\to\infty}\beta_n \Rightarrow \lambda = \lim_{n\to\infty}\frac{\alpha}{n+1}\cdot\lambda =$

$0\cdot\lambda = 0$, cioè $\lambda = \lim_{n\to\infty}\beta_{n+1} = \lim_{n\to\infty}\frac{\pi^{n+1}a^n}{4^n n!} = 0$ per cui la successione $\left\{\frac{\pi^n a^n}{4^n n!}\right\}_{n\in\mathbb{N}}$ è infinitesima. Allora dalla definizione di limite, per $\epsilon = 1$ segue che è possibile determinare in corrispondenza di ϵ un indice $\nu > 0$ tale che per $n > \nu$ risulti $\frac{\pi^n a^n}{4^n n!} < 1$ implicando ciò che

$0 < \int_0^\pi P(x)\sin x\, dx < 1$.

Siamo giunti all'assurdo poiché abbiamo detto a pag.4 che l'integrale $\int_0^\pi P(x)\sin x\, dx$ è un numero intero. Poiché ciò contraddice l'ipotesi, ne consegue che non essendo possibile esprimere il numero π con una frazione, esso è un numero irrazionale.

Passiamo ora al 2° problema, ovvero la duplicazione del cubo.

Duplicazione del cubo

Dato un cubo di lato unitario $l = 1$ e di volume $V = l^3 = 1$, costruire utilizzando riga e compasso un cubo di lato incognito x avente volume $V' = x^3$ doppio del precedente, cioè tale che $V' = 2V \Longrightarrow$
$x^3 = 2 \Rightarrow x^3 - 2 = 0$.

<u>Teorema</u>: **Il problema della duplicazione del cubo non ha soluzione**.

<u>Dimostrazione</u>:

Infatti per la proposizione pag.7 , la costruzione del lato x del cubo non può avvenire con l'utilizzo della riga e del compasso, perché ciò implicherebbe che $\sqrt[3]{2}$ sia un numero costruibile.

A questo punto però bisogna dire che tutti e tre i problemi dipendono algebricamente dalle equazioni cubiche. Vediamo di chiarire questo aspetto cominciando a notare una proprietà dell'equazione di 3° grado a cui seguirà un importante teorema di legame.

La proprietà che ora vogliamo evidenziare, è una proprietà che vale per una generica equazione algebrica di grado n $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$. Allora si ha, applicando il teorema fondamentale dell'algebra e il criterio di divisibilità n volte, che se $x_1, x_2, \cdots, x_n$ sono le radici reali o complesse coniugate dell'equazione, vale la scomposizione

$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = a_0(x - x_1)(x - x_2) \cdot \cdots \cdot (x - x_n)$ da cui, svolgendo i calcoli e applicando il principio d'identità dei polinomi, seguono le notevoli relazioni tra le radici e i coefficienti di un'equazione algebrica

$$\begin{cases} x_1 + x_2 + \cdot \cdots + x_n = -\frac{a_1}{a_0} \\ x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \frac{a_2}{a_0} \\ x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n = -\frac{a_3}{a_0} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_1x_2 \cdot \cdots \cdot x_n = (-1)^n \frac{a_n}{a_0} \end{cases}$$

in base alle quali la somma dei prodotti ad h ad h delle radici di un'equazione algebrica di grado n è uguale al quoziente di a_h per a_0 o al suo opposto secondo che h è pari o dispari. E' bene comunque ricordare che un'equazione algebrica a coefficienti reali ha sempre un numero pari di radici complesse e quindi se è di grado dispari ammette almeno una radice reale.

Consideriamo quindi l'equazione cubica $x^3 + ax^2 + bx + c = 0$, a coefficienti razionali $a, b, c \in \mathbb{Q}$, aventi le radici x_1, x_2, x_3. Si ha

$x^3 + ax^2 + bx + c = (x - x_1)(x - x_2)(x - x_3) = (x - x_1)[x^3 - (x_2 + x_3)x + x_2x_3] =$

$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3$, da cui applicando il principio d'identità dei polinomi segue

$$\begin{cases} -a = x_1 + x_2 + x_3 \\ b = x_1x_2 + x_1x_3 + x_2x_3 \\ -c = x_1x_2x_3 \end{cases}$$

<u>Teorema</u>: Se l'equazione cubica a coefficienti razionali $x^3 + ax^2 + bx + c = 0$ non ammette radici razionali, allora nessuna delle sue radici è un numero costruibile partendo dal campo razionale $C_0 = \mathbb{Q}$

<u>Dimostrazione</u>: Se per assurdo x_1 fosse una radice costruibile, allora dovrebbe $\exists k \in \mathbb{N}$ tale che $x_1 \in \mathcal{C}_k$, ultimo campo della catena di campi estesi $\mathcal{C}_0, \mathcal{C}_1, \cdots, \mathcal{C}_k$, con k più piccolo intero positivo per cui ciò accada (poiché x_1 non è per ipotesi radice razionale della cubica,allora $x_1 \notin \mathcal{C}_0 = \mathbb{Q}$, donde $k > 0$). Avendosi allora $x_1 \in \mathcal{C}_k$, segue che è del tipo $x_1 = p + q\sqrt{w}$, dove $p, q, w \in \mathcal{C}_{k-1}$ e $\sqrt{w} \notin \mathcal{C}_{k-1}$, inoltre per quanto visto precedentemente pure $x_2 = p - q\sqrt{w}$ è radice dell'equazione, dove dovendo essere $q \neq 0$, segue $x_1 \neq x_2$ e $x_1 + x_2 = 2p$. Poiché $x_1 + x_2 + x_3 = -a \Longrightarrow x_3 = -a - x_1 - x_2 = -a - 2p$, nell'espressione della terza radice x_3 non compare il termine dell'espressione 2 – radicale $\sqrt{w}$, per cui deve aversi $x_3 \in \mathcal{C}_{k-1}$, contro il fatto che k è il minimo intero positivo tale che un campo $\mathcal{C}_k$ contenga una radice dell'equazione cubica data. Ciò prova l'asserto.

Il teorema dimostrato implica che:

<u>Teorema</u> :Una costruzione con solo riga e compasso è impossibile se l'equivalente algebrico del problema è la soluzione di un'equazione cubica priva di radici razionali.

<u>Osservazione</u> : Ciò dimostra subito che il problema della duplicazione del cubo è impossibile da risolvere con una costruzione che prevede l'uso della sola riga e del compasso.

Vediamo quindi il terzo problema della trisezione dell'angolo, però prima di affrontarlo conviene considerare una <u>relazione trigonometrica tra un angolo e la sua terza parte</u>. La formula di De Moivre sulla potenza di un numero complesso stabilisce che dato il numero complesso $z = x + iy = [\rho, \varphi] = \rho(\cos\varphi + i\sin\varphi)$,dove $\rho = \sqrt{x^2 + y^2}$, si ha $z^n = [\rho, \varphi]^n = [\rho^n, n\varphi] = \rho^n(\cos n\varphi + i\sin n\varphi)$. Posto $\rho = 1$ e $n = 3$, di modo che l'affissa del numero complesso appartenga al cerchio di raggio unitario con centro l'origine, si ha in particolare che

$z^3 = (\cos\varphi + i\sin\varphi)^3 = \cos 3\varphi + i\sin 3\varphi \Longrightarrow \cos^3\varphi + 3\cos^2\varphi\, i\sin\varphi + 3\cos\varphi\, i^2\sin^2\varphi + i3\sin3\varphi = \cos3\varphi + i\sin3\varphi \Longrightarrow \cos3\varphi + 3i\cos2\varphi\sin\varphi - 3\cos\varphi\sin2\varphi - i\sin3\varphi = \cos3\varphi + i\sin3\varphi \Longrightarrow \cos3\varphi - 3\cos\varphi\sin2\varphi + i3\cos2\varphi\sin\varphi - \sin3\varphi = \cos3\varphi + i\sin3\varphi$, da cui eguagliando le parti reali e le immaginarie segie

$$\begin{cases} cos^3\varphi - 3\cos\varphi sin^2\varphi = \cos 3\varphi \\ 3cos^2\varphi\sin\varphi - sin^3\varphi = sin\, 3\varphi \end{cases} \Longrightarrow \begin{cases} \cos 3\varphi = cos^3\varphi - 3\cos\varphi(1 - cos^2\varphi) = 4cos^3\varphi - 3cos\,\varphi \\ \sin 3\varphi = 3(1 - sin^2\varphi)\sin\varphi - sin^3\varphi = -4sin^3\varphi + 3\sin\varphi \end{cases}$$

Da queste formule per $\varphi = \frac{\theta}{3}$ si ottiene una relazione che lega $\cos\frac{\theta}{3}$ con $cos\,\theta$

$$\cos\theta = 4cos^3\frac{\theta}{3} - 3cos\frac{\theta}{3}$$

Trisezione dell'angolo

Il problema consiste nel dividere un angolo assegnato in tre parti uguali e in generale non è risolvibile con l'uso della sola riga e del compasso. Dobbiamo quindi provare che non esiste un metodo che possa essere usato per trisecare ogni angolo, esistendo però casi particolari come gli angoli di 90° e 180° trisecabili rispettivamente in angoli di 30° e 60° e così pure l'angolo di 270° di cui 90° è la sua terza parte.. Consideriamo quindi un generico angolo θ che vogliamo trisecare e sia $\cos\theta = a$ il suo coseno. Essendo $\frac{\theta}{3}$ la trisezione di θ, la determinazione di $\cos\frac{\theta}{3} = x$, comporta quella di $\frac{\theta}{3} = \arccos x \Longrightarrow \theta = 3\arccos x$. Dalla relazione trigonometrica trovata sopra,sostituendo e raggruppando i termini, si ha l'equazione cubica

$$4x^3 - 3x - a = 0$$

Questo comporta che il problema della trisezione dell'angolo è equivalente al problema algebrico del determinare una soluzione costruibile dell'equazione cubica precedente. Per far vedere che ciò non è in generale possibile, <u>consideriamo ad esempio l'angolo $\theta = 60°$.</u>

Si ha che $a = \cos 60° = \frac{1}{2}$, per cui l'equazione diviene $8x^3 - 6x - 1 = 0$, la quale , posto $x = \frac{v}{2}$, si riduce alla $v^3 - 3v - 1 = 0$.

In base al teorema precedente è sufficiente provare che tale equazione non ammette radici razionali. Ragioniamo per assurdo, supponendo che esista una radice razionale $v = \frac{r}{s}$, con r ed s

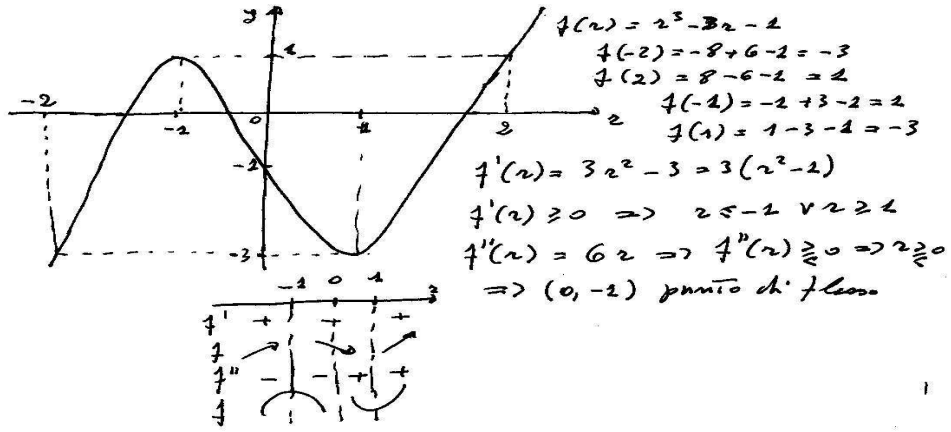
interi primi tra loro (non hanno divisori comuni tranne l'unità) diversi entrambi dall'unità. Sostituendo si ha

$r^3 - 3s^2r - s^3 = 0$ e le relazioni tra interi $\begin{cases} s^3 = r(r^2 - 3s^2) \\ r^3 = s^2(s + 3r) \end{cases}$. Dalla prima si deduce si ricava che r è un fattore di s^3, cioè $r/_s$ (leggi r divide s); ora, avendo ogni numero intero un'unica scomposizione in fattori primi, si ha

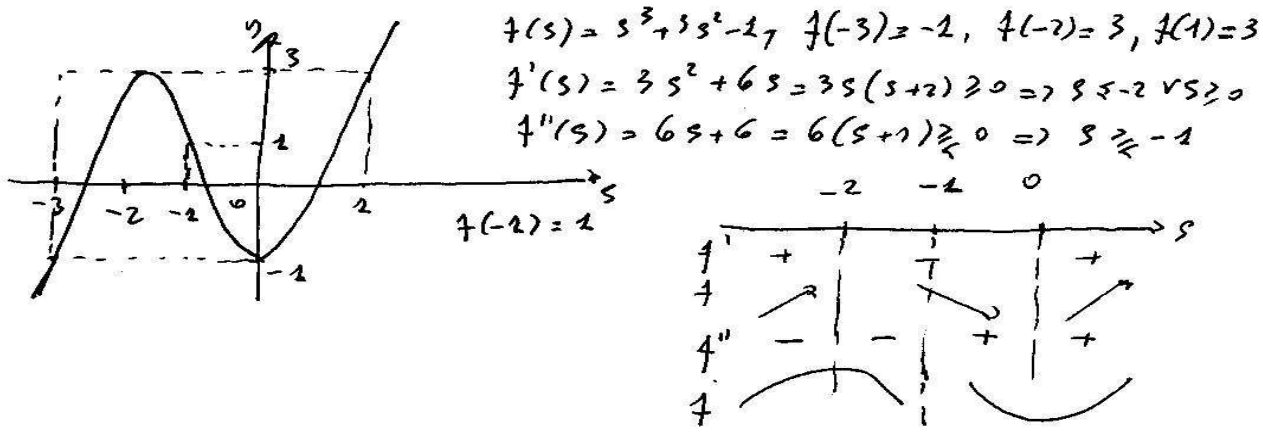
$s = s_1^{\alpha_1} \cdot \dots \cdot s_p^{\alpha_p} \Longrightarrow s^3 = s_1^{3\alpha_1} \cdot \dots \cdot s_p^{3\alpha_p}$ e $r = r_1^{\beta_1} \cdot \dots \cdot r_q^{\beta_q}$, per cui tra i fattori della scomposizione di r deve esistere almeno uno di essi r_i, $(i = 1, \dots, q)$ tale che $r_i/_{s^3}$.

Quindi pure r_i è uno dei fattori primi della scomposizione di s, ossia deve esistere un unico fattore primo s_j,$(j = 1, \dots, p)$ tale che $r_i = s_j$. Questo comporta che s ed r hanno un divisore comune, contro l'ipotesi che essi, essendo relativamente primi, non hanno divisori comuni. Nel caso che $s = 1$ $r \neq 1$, si ha $v = r$ e l'equazione diviene $r^3 - 3r - 1 = 0$ che non ha radici intere così pure nel caso che R=1, $s \neq 1$ in cui l'equazione si riduce a $s^3 + 3s^2 - 1 = 0$ (*)

(*) Infatti lo studio della funzione lo esclude



Nell'altro caso si ha



Nel caso infine che entrambi sono in valore assoluto uguali all'unità, il rapporto $\frac{r}{s}$ si riduce a $v = \mp 1$ che non è radice dell'equazione$v^3 - 3v - 1 = 0$. Il . Quindi il problema della trisezione dell'angolo non ha soluzioni in generale usando una costruzione geometrica che preveda l'uso della sola riga e del compasso.

<u>Nota</u>: Similmente a come fatto per l'angolo di 60°, **non è possibile costruire un angolo di 20° con riga e compasso.** Infatti come detto nel caso di 60°, costruire un angolo di ampiezza θ equivale a costruire un segmento di lunghezza $\cos\theta$, per cui in base all'identità trigonometrica di pag.19, che scriviamo però come $\cos 3\theta = 4cos^3\theta - 3cos\,\theta$, per $\theta = 20°$ si ottiene

$\frac{1}{2} = 4cos^3 20° - 3cos\,20° \Longrightarrow cos^3 20° - \frac{3}{4}\cos 20° - \frac{1}{8} = 0$. Questo significa che $\cos 20°$è radice del polinomio a coefficienti razionali $P(x) = x^3 - \frac{3}{4}x - \frac{1}{8}$ che, similmente a quanto visto a pag.19, noi ha radici razionali., per cui è il polinomio minimo del numero reale $\cos 20°$ sull'insieme dei razionali, donde per il teorema pag.3 tale numero non è costruibile non appartenendo a un'estensione 2 – radicale di $\mathbb{Q}$.

Da ciò segue pure che non è possibile costruire con riga e compasso un ennagono regolare (9 lati) i cui angoli al centro sono di 40° perché, dividendo uno di questi si costruirebbe con riga e compasso un angolo di 20°, che per quanto prima detto non è costruibile.

Nel 1748 il matematico svizzero Leonhard Euler , italianizzato Eulero (1707-1783), pubblicò la sua "Introductio in analisi infinitorum" in cui il numero e (del suo cognome) , così come altri numeri reali, viene introdotto come somma di una serie fattoriale. È necessario quindi introdurre brevemente il concetto di serie numerica.

Se $a_1, a_2, \cdots, a_n, \cdots$ è una successione di numeri reali o complessi, definiamo induttivamente da essa la successione $s_1, s_2, \cdots, s_n, \cdots$ delle <u>somme parziali</u> o <u>ridotte</u> della serie nel modo seguente:

$$\begin{cases} s_1 = a_1 \\ s_2 = a_1 + a_2 \\ \cdots\cdots\cdots\cdots \\ s_n = a_1 + a_2 + \cdots + a_n \\ \cdots\cdots\cdots\cdots \end{cases}$$

L'operazione che associa ai termini della successione $\{a_n\}$ i termini della successione delle sue somme parziali $\{s_n\}$, si chiama <u>serie</u> e si indica convenzionalmente col simbolo (privo di significato algebrico, trattandosi di somme d'infiniti termini, ma molto intuitivo)

$$a_1 + a_2 + \cdots + a_n + \cdots = \sum_{n=1}^{\infty} a_n$$

Dove a_n prende il nome di <u>termine generale</u> della serie o <u>termine n-mo</u>.

La serie si dice <u>convergente</u> se risulta convergente la successione delle sue somme parziali $\{s_n\}$ e al suo limite $\lim_{n\to\infty} s_n = s$ si dà il nome di <u>somma della serie</u> per cui si scrive $\sum_{n=1}^{\infty} a_n = s$.

In questo modo il simbolo s ha il duplice significato di indicare la serie e rappresentare la sua somma, in quanto l'uguaglianza $a_1 + a_2 + \cdots + a_n + \cdots = s$ esprime il contenuto delle due proposizioni

$a_1 + a_2 + \cdots + a_n = s_n$ e $\lim_{n\to\infty} s_n = s$.

Si dice poi che la serie è <u>divergente</u> o <u>indeterminata</u> se lo è rispettivamente la successione delle sue somme parziali. Di conseguenza il <u>carattere</u> di una serie è la sua proprietà di essere convergente, divergente, indeterminata.

Abbiamo detto che data una serie $\sum_{n=1}^{\infty} a_n$, la successione delle sue somme parziali $\{s_n\}$ è essenziale per stabilirne il carattere, ma anche viceversa ad ogni data successione $\{a_n\}$, è possibile associare la particolare serie $b_1 + b_2 + \cdots + b_n$ in cui ogni termine è la differenza col precedente, per cui $b_1 = a_1, b_2 = a_2 - a_1$ $, \cdots, b_n = a_n - a_{n-1}, \cdots$, di modo che il termine n-mo della successione delle somme parziali risulti

$$s_n = b_1 + b_2 + \cdots + b_n = a_1 + (a_2 - a_1) + \cdots + (a_n - a_{n-1}) = a_n.$$

In questo modo, una qualsiasi successione numerica può pensarsi come la successione delle somme parziali di una serie e quindi lo studio delle serie è equivalente a quello delle successioni.

Notiamo che una condizione necessaria (ma non sufficiente) affinché una serie converga è che la successione dei suoi termini sia infinitesima, Infatti, poiché $s_n - s_{n-1} = a_n$, passando al limite

l'uguaglianza si ha $\lim_{n\to\infty} s_n - \lim_{n\to\infty} s_{n-1} = \lim_{n\to\infty} a_n \Rightarrow s - s = \lim_{n\to\infty} a_n \Rightarrow \lim_{n\to\infty} a_n = 0$.

Per quanto diremo tra breve conviene osservare che, se una serie ha somma un numero s, cioè $\sum_{n=1}^{\infty} a_n = s$, allora la serie $b\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} b a_n$, ottenuta moltiplicando ogni termine a_n per il numero b, ha come somma $b \cdot s$, perché per una proprietà dei limiti delle successioni si ha

$$\lim_{n\to\infty} s_n = s \Rightarrow \lim_{n\to\infty} b s_n = bs$$

Ritornando al numero e di Eulero, consideriamo la serie fattoriale

$1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \cdots$ la cui somma parziale n-ma è $s_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}$

La successione delle somme parziali $\{s_n\}$ è monotona strettamente crescente avendosi

$s_{n+1} = s_n + \frac{1}{(n+1)!} \Rightarrow s_n < s_{n+1}$, poiché $\frac{1}{(n+1)!} > 0$, $\forall n \in \mathbb{N}$. La successione è limitata da 3 in quanto si ha $\forall n \in \mathbb{N}$. $s_n < 3$; infatti $\forall n \geq 2$ $, \frac{1}{n!} = \frac{1}{2} \cdot \frac{1}{3} \cdot \dots \cdot \frac{1}{n} < \frac{1}{2} \cdot \frac{1}{2} \cdot \dots \cdot \frac{1}{2} = \frac{1}{2^{n-1}}$ per cui

$$s_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{n!} < 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \dots + \frac{1}{2^{n-1}} = 1 + \frac{1 - \left(\frac{1}{2}\right)^n}{1 - \frac{1}{2}} =$$

$1 + 2\left[1 - \left(\frac{1}{2}\right)^n\right] = 3 - \left(\frac{1}{2}\right)^{n-1} < 3$, essendo la somma $1 + \frac{1}{2} + \frac{1}{2^2} + \dots + \frac{1}{2^{n-1}}$ degli n termini

Di una progressione geometrica di ragione $\frac{1}{2}$. Per il teorema delle successioni monotone limitate, esiste il limite della successione $\{s_n\}$ ed è uguale al suo estremo superiore, cioè si ha

$$\lim_{n \to \infty} s_n = \sup_{n \in \mathbb{N}} s_n = e. \quad (*)$$

(*) D'altra parte sviluppando col binomio di Newton,

$$\left(1 + \frac{1}{n}\right)^n = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{n^k} = 1 + 1 + \frac{1}{2!}\left(1 - \frac{1}{n}\right) + \dots + \frac{1}{k!}\left(1 - \frac{1}{n}\right) \cdot \dots \cdot \left(1 - \frac{k-1}{n}\right) + \dots + \frac{1}{n!}\left(1 - \frac{1}{n}\right) \cdot \dots \cdot \left(1 - \frac{n-1}{n}\right)$$

da cui passando al limite, si ha

$$\lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n = \lim_{n \to \infty} \sum_{k=0}^{n} \binom{n}{k} \frac{1}{n^k} = 1 + \frac{1}{2!} + \dots + \frac{1}{k!} + \dots + \frac{1}{n!} + \dots = e,$$ poiché in dettaglio

$$\left(1 + \frac{1}{n}\right)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{1-k} \left(\frac{1}{n}\right)^k = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{n^k} = \binom{n}{0} \frac{1}{n^0} + \binom{n}{1} \frac{1}{n} + \binom{n}{2} \frac{1}{n^2} + \binom{n}{3} \frac{1}{n^3} + \dots + \binom{n}{k} \frac{1}{n^k} + \dots + \binom{n}{n} \frac{1}{n^n}$$

$$\begin{aligned}
&= 1 \cdot \frac{1}{1} + n \cdot \frac{1}{n} + \frac{n(n-1)}{2!} \frac{1}{n^2} + \frac{n(n-1)(n-2)}{3!} \frac{1}{n^3} + \dots + \frac{n(n-1)(n-2) \cdot \dots \cdot (n-k+1)}{k!} \frac{1}{n^k} + \dots \\
&\quad + \frac{n(n-1)(n-2) \cdot \dots \cdot (n-n+1)}{n!} \frac{1}{n^n} \\
&= 1 + 1 + \frac{1}{2!} \frac{n-1}{n} + \frac{1}{3!} \frac{(n-1)(n-2)}{n^2} + \dots + \frac{1}{k!} \frac{(n-1)(n-2) \cdot \dots \cdot (n-k+1)}{n^{k-1}} + \dots \\
&\quad + \frac{1}{n!} \frac{(n-1)(n-2) \cdot \dots \cdot (n-n+1)}{n^{n-1}} \\
&= 1 + 1 + \frac{1}{2!}\left(1 - \frac{1}{n}\right) + \frac{1}{3!}\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) + \dots + \frac{1}{k!}\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) \cdot \dots \cdot \left(1 - \frac{k-1}{n}\right) + \dots \\
&\quad + \frac{1}{n!}\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) \cdot \dots \cdot \left(1 - \frac{n-1}{n}\right)
\end{aligned}$$

Volendo dimostrare rigorosamente che $\lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n = e$, cominciamo ad osservare che

$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{(n+1)n!}{k!(n-k)!(n-k+1)} \cdot \frac{n-k+1}{n+1} = \frac{(n+1)!}{k!(n+1-k)} \cdot \frac{n+1-k}{n+1} = \binom{n+1}{k}\left(1 - \frac{k}{n+1}\right)$. Inoltre $\forall h \in [-1, +\infty)$, $\forall n \in \mathbb{N}$ si ha $(1+h)^n \geq 1 + nh$. Infatti per $n = 1$ la proposizione è vera avendosi $1 + h \geq 1 + h$; supposta la

proposizione vera per n, proviamo che è vera per $n+1$. Si ha:
$(1+h)^{n+1} = (1+h)(1+h)^n \geq (1+h)(1+nh) = 1+(n+1)h+nh^2 \geq 1(n+1)h$. Allora per il principio d'induzione la proposizione è vera per ogni $n \in \mathbb{N}$.

Posto $h = -\frac{1}{n+1}$, si ha $h > -1$ (poichè $n > 0 \Rightarrow n+1 > 1 \Rightarrow \frac{1}{n+1} < 1 \Rightarrow -\frac{1}{n+1} > -1$) per cui è applicabile la formula per $k \in \mathbb{N}$, $1+kh \leq (1+h)^k \Rightarrow 1-\frac{k}{n+1} \leq \left(1-\frac{1}{n+1}\right)^k = \left(\frac{n}{n+1}\right)^k$. Consideriamo la successione $\left\{\left(1+\frac{1}{n}\right)^n\right\}_{n\in\mathbb{N}} = \{a_n\}_{n\in\mathbb{N}}$; , si ha

$a_n = \left(1+\frac{1}{n}\right)^n = \sum_{k=0}^{n}\binom{n}{k}\frac{1}{n^k} = \sum_{k=0}^{n}\binom{n+1}{k}\left(1-\frac{k}{n+1}\right)\frac{1}{n^k} \leq \sum_{k=0}^{n}\binom{n+1}{k}\left(\frac{n}{n+1}\right)^k\frac{1}{n^k} = \sum_{k=0}^{n}\binom{n+1}{k}\frac{1}{(n+1)^k} < \sum_{k=0}^{n}\binom{n+1}{k}\frac{1}{(n+1)^k} + \frac{1}{(n+1)^{n+1}} = \sum_{k=0}^{n+1}\binom{n+1}{k}\frac{1}{(n+1)^k} = a_{n+1}$

. Allora essendo $a_n < a_{n+1}$, la successione $\{a_n\}_{n\in\mathbb{N}}$ è strettamente crescente. La successione è pure limitata superiormente (ovviamente lo è pure inferiormente dal suo valore minimo 2, per cui è limitata). Infatti da $\underbrace{n(n-1)\cdot\cdots\cdot(n-k+1)}_{k\,volte} < \underbrace{n\cdot n\cdot\cdots\cdot n}_{k\,volte} < n^k \Rightarrow \frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{n^k} < 1$ segue che

$\binom{n}{k}\frac{1}{n^k} = \frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{k!}\frac{1}{n^k} = \frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{n^k}\frac{1}{k!} < \frac{1}{k!}$ e dunque $a_n = \left(1+\frac{1}{n}\right)^n = \sum_{k=0}^{n}\binom{n}{k}\frac{1}{n^k} = \sum_{k=0}^{n}\frac{1}{k!} < \sum_{k=0}^{\infty}\frac{1}{k!} = e$. Per un teorema sulle successioni monotone crescenti, la successione $\{a_n\}_{n\in\mathbb{N}}$ ha come limite il suo estremo superiore. (*) $L = sup_{n\in\mathbb{N}}\, a_n$, per cui deve essere $\lim_{n\to\infty} a_n = L \leq e$, essendo e un maggiorante della successione. Per provare che e è il minimo dei maggioranti della successione, da cui $L = e$, osserviamo che, essendo la successione strettamente crescente, per $m < n$ si ha:

$L \sum_{k=0}^{m}\frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{n^k}\cdot\frac{1}{k!} < \sum_{k=0}^{n}\frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{n^k}\cdot\frac{1}{k!} = \sum_{k=0}^{n}\binom{n}{k}\frac{1}{n^k} = \left(1+\frac{1}{n}\right)^n = a_n$. Poiché per $k = 0,1,\cdots,m$, $\lim_{n\to\infty}\frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{n^k} = 1$, avendo il numeratore k fattori per cui è un polinomio di grado k, il termine $\sum_{k=0}^{m}\frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{n^k}\cdot\frac{1}{k!}$ per ogni $m < n$ fissato, è il termine generico della successione $\left\{\sum_{k=0}^{m}\frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{n^k}\cdot\frac{1}{k!}\right\}_{n\in\mathbb{N}}$ avente limite

$\lim_{n\to\infty}\sum_{k=0}^{m}\frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{n^k}\cdot\frac{1}{k!} = \sum_{k=0}^{m}\frac{1}{k!}\cdot\lim_{n\to\infty}\frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{n^k} = \sum_{k=0}^{m}\frac{1}{k!}\cdot 1 = \sum_{k=0}^{m}\frac{1}{k!}$. Quindi la successione $\{b_n\}_{n\in\mathbb{N}} = \left\{\sum_{k=0}^{m}\frac{n(n-1)\cdot\cdots\cdot(n-k+1)}{n^k}\cdot\frac{1}{k!}\right\}$ avente limite $\lim_{n\to\infty} b_n = \sum_{k=0}^{m}\frac{1}{k!}$ è maggiorata dalla successione $\{a_n\}_{n\in\mathbb{N}}$ avente limite L, donde, in base a un teorema sui limiti delle successioni (**) e tenendo presente che $\lim_{m\to\infty}\sum_{k=0}^{m}\frac{1}{k!} = \sum_{k=0}^{\infty}\frac{1}{k!} = e$, si ha $\lim_{n\to\infty} b_n \leq \lim_{n\to\infty} a_n \Rightarrow \sum_{k=0}^{m}\frac{1}{k!} \leq L \Rightarrow e \leq L$. Poiché sopra si è visto che $L \leq e$, valendo contemporaneamente le due diseguaglianze, si conclude che $L = e$ e ciò conclude la dimostrazione.

(*)Il teorema richiamato è il seguente. Ogni successione monotona è regolare ed è convergente se è limitata, avendosi nel caso che $\{a_n\}$è crescente, lim $a_n = sup\{a_n\}$, mentre nel caso che $\{a_n\}$è decrescente, lim $a_n = inf\{a_n\}$.

Proviamo solo la prima implicazione. Se $\{a_n\}$ è limitata ed è crescente, posto $L = sup\{a_n\}$, per le proprietà dell'estremo superiore si ha $\forall\epsilon > 0, \exists\nu > 0: L-\epsilon < a_n \leq L$. D'altra parte per $n > \nu$, essendo $\{a_n\}$ crescente, si ha: $L-\epsilon < a_\nu \leq a_n \leq L < L+\epsilon \Rightarrow a_n \in (L-\epsilon, L+\epsilon) \Rightarrow |a_n - L| < \epsilon \Rightarrow \lim a_n = L$. Se poi $\{a_n\}$ non è limitata superiormente, allora $sup\{a_n\} = +\infty$ e quindi $\forall k > 0, \exists\nu > 0: a_\nu > k$; allora poichè $\{a_n\}$ è crescente, $\forall n > \nu$, $a_n \geq a_\nu > k \Rightarrow$ lim $a_n = +\infty = sup\{a_n\}$,.

(**) Il teorema richiamato è il seguente. Se $\{a_n\}$ e $\{b_n\}$ sono due successioni convergenti ai limiti lim $a_n = a$ e iim $b_n = b$, allora si ha $a < b \Rightarrow a_n < b_n$definitivamente (cioè da un certo indice in poi).

Viceversa $a_n < b_n$definitivamente$\Rightarrow a \leq b$. Proviamo la prima implicazione. Stante l'ipotesi, fissato $\epsilon < 0, \exists\, \nu_1 > 0$: $n > \nu_1$, $a - \epsilon < a_n < a + \epsilon \Rightarrow -a_n > -a - \epsilon$, d'altra parte pure in corrispondenza dell'ϵ fissato $\exists\, \nu_2 > 0 : n > \nu_2$, $b - \epsilon < b_n < b + \epsilon$. Posto $\nu = \max\ \{\nu_1, \nu_2\}$, si ha per $n > \nu$, $\begin{cases} b_n > b - \epsilon \\ -a_n > -a - \epsilon \end{cases} \Rightarrow b_n - a_n > b - a - 2\epsilon$. Scelto allora $\epsilon = \frac{b-a}{2}$, si ha per $n > \nu$, $b_n - a_n > 0 \Rightarrow a_n < b_n$.

Viceversa proviamo la seconda implicazione$a_n < b_n$definitivamente$\Rightarrow a \leq b$. Infatti se per assurdo fosse $a > b$, allora per la prima implicazione dovrebbe essere $a_n > b_n$ definitivamente, contro l'ipotesi.

La serie fattoriale $\sum_{n=1}^{\infty} \frac{1}{n!} = e$ permette il calcolo di e con una qualsiasi approssimazione si voglia.

Ad esempio la somma della serie fino a $\frac{1}{12!}$ è $s_{12} = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{12!} = 2.71828183$.

Detto $r_n = s - s_n$ il <u>resto parziale</u> della serie, nel nostro caso si ha:

$$r_{12} = e - s_{12} = \frac{1}{13!} + \frac{1}{14!} + \frac{1}{15!} + \cdots = \frac{1}{13!} + \frac{1}{14 \cdot 13!} + \frac{1}{15 \cdot 14 \cdot 13!} + \cdots = \frac{1}{13!}\left(1 + \frac{1}{14} + \frac{1}{14 \cdot 15} + \cdots\right) <$$
$$\frac{1}{13!}\left(1 + \frac{1}{13} + \frac{1}{13^2} + \cdots\right) = \frac{1}{13!}\frac{1}{1 - \frac{1}{13}} = \frac{1}{13!}\frac{13}{12} = \frac{1}{12 \cdot 12!} = \frac{1}{5748019200} = 0.173972974 \cdot 10^{-9}$$

, in quanto la serie geometrica $1 + \frac{1}{13} + \frac{1}{13^2} + \cdots + \frac{1}{13^n} + \cdots$ di ragione $q = \frac{1}{13} < 1$ converge a $\frac{1}{1 - \frac{1}{13}}$

poiché la sua somma parziale n-ma è $\sigma_n = 1 + \frac{1}{13} + \frac{1}{13^2} + \cdots + \frac{1}{13^n} = \frac{1 - \left(\frac{1}{13}\right)^n}{1 - \frac{1}{13}}$, per cui

$$\lim_{n \to \infty} \sigma_n = \frac{1}{1 - \frac{1}{13}} = \frac{13}{12}.$$

Ora, essendo $s = s_n + r_n$, si ha nel nostro caso
$e = s_{12} + r_{12} = 2.71828183 + r_{12} = 0.000000000173$, che non può influenzare la nona cifra della stima approssimata di e perché, anche ammettendo che l'ultima cifra del valore scritto sopra non sia esatta, si ha $e = 2.7182818$, con otto cifre esatte. D'altra parte, per valutare l'errore che si commette se si sostituisce al numero e il valore approssimato della somma n-ma S_n della serie fattoriale, consideriamo il resto n.m – mo di questa

$$r_{n,m} = S_{n+m} - S_n = \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots + \frac{1}{(n+m)!} = \frac{1}{(n+1)!}\left[1 + \frac{1}{n+2} + \cdots + \frac{1}{(n+2)\cdots(n+m)}\right] \leq$$
$$\frac{1}{(n+1)!}\left[1 + \frac{1}{n+2} + \frac{1}{(n+2)^2} + \cdots + \frac{1}{(n+2)^{m-1}}\right] \leq \frac{1}{(n+1)!}\frac{1}{1 - \frac{1}{n+2}} = \frac{1}{(n+1)!}\frac{n+2}{n+1}$$

, in quanto $\underbrace{(n+2)\cdots(n+m)}_{m-1 \text{ volte}} > \underbrace{(n+2)\cdots(n+2)}_{m-1 \text{ volte}} = (n+2)^{m-1} \Rightarrow \frac{1}{(n+2)\cdots(n+m)} < \frac{1}{(n+2)^{m-1}}$. Passando al limite per $m \to \infty$ la diseguaglianza

$S_{n+m} - S_n \leq \frac{1}{(n+1)!}\frac{n+2}{n+1} \Rightarrow \lim_{m\to\infty} S_{n+m} - \lim_{m\to\infty} S_n = e - S_n \leq \lim_{m\to\infty} \frac{1}{(n+1)!}\cdot\frac{n+2}{n+1} = \frac{1}{(n+1)!}\cdot$
$\frac{n+2}{n+1} = \frac{1}{n!}\cdot\frac{n+2}{(n+1)^2} < \frac{1}{n!}\cdot\frac{1}{n}$

, poiché $n^2 + 2n < n^2 + 2n + 1 \Rightarrow n(n+1) < (n+1)^2 \Rightarrow \frac{n+2}{(n+1)^2} < \frac{1}{n}$. La diseguaglianza $\mathcal{E} = e - S_n < \frac{1}{n!n}$ esprime la maggiorazione dell'errore $\mathcal{E} > 0$ che si commette approssimando e con la somma n – ma della serie fattoriale.

Detto ciò sulle approssimazioni di e, esiste sempre la possibilità che tale numero possa essere esprimibile con il rapporto di due opportuni interi, ovvero essere un numero razionale.

La seguente dimostrazione per assurdo, prova che ciò non è possibile e che quindi e è un numero irrazionale A tal proposito si veda pure il corollario al teorema sulla trascendenza di e a pag.40

Siano p e q due numeri interi positivi primi tra loro di modo che $q \neq 0$, $q \neq 1$ e quindi $q \geq 2$ e risulti irriducibile la frazione $\frac{p}{q} = e$. Moltiplicando per $q!$ tutti i termini della serie

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{(q-2)!} + \frac{1}{(q-1)!} + \frac{1}{q!} + \frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \cdots$$

e tenendo presente che $eq! = \frac{p}{q}q! = \frac{p}{q}q(q-1)! = p(q-1)(q-2)\cdot\cdots\cdot 3\cdot 2\cdot 1$, si ha:

$$p(q-1)(q-2)\cdot\cdots\cdot 3\cdot 2\cdot 1 = q! + q! + \frac{q!}{2!} + \frac{q!}{3!} + \cdots + \frac{q!}{(q-2)!} + \frac{q!}{(q-1)!} + \frac{q!}{q!} + \frac{q!}{(q+1)!} +$$

$$+ \frac{q!}{(q+2)!} + \cdots = q! + q! + q(q-1)(q-2)\cdot\cdots\cdot 4\cdot 3 + q(q-1)(q-2)\cdot\cdots\cdot 5\cdot 4 + \cdots +$$

$$\frac{q(q-1)(q-2)!}{(q-2)!} + \frac{q(q-1)!}{(q-1)!} + 1 + \frac{q!}{(q+1)q!} + \frac{q!}{(q+2)(q+1)q!} + \cdots =$$

$$[q! + q! + q(q-1)(q-2)\cdot\cdots\cdot 4\cdot 3 + q(q-1)(q-2)\cdot\cdots\cdot 5\cdot 4 + \cdots + q(q-1) + q + 1] +$$

$$\frac{1}{q+1} + \frac{1}{(q+2)(q+1)} + \cdots$$

Ora il termine iniziale della catena di uguaglianze $p(q-1)(q-2)\cdot\cdots\cdot 3\cdot 2\cdot 1$è evidentemente un intero, essendo il prodotto di interi, e così pure il termine alla fine in parentesi quadre, mentre il termine $\frac{1}{q+1} + \frac{1}{(q+2)(q+1)} + \cdots$non è un intero. Infatti, avendosi $q \geq 2$, questo termine risulta essere una serie a termini positivi, maggiorata dalla serie geometrica di ragione $\frac{1}{3} < 1$

$\frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \cdots$ convergente a $s = \lim_{n\to\infty} s_n = \lim_{n\to\infty} \frac{1}{3}\frac{1-\left(\frac{1}{3}\right)^n}{1-\frac{1}{3}} = \frac{1}{3}\frac{1}{1-\frac{1}{3}} = \frac{1}{2}$, in quanto per ciascun termine si ha rispettivamente $\frac{1}{q+1} \leq \frac{1}{3}$, $\frac{1}{(q+2)(q+1)} \leq \frac{1}{3}\cdot\frac{1}{3} = \frac{1}{3^2}, \ldots$

Allora tale serie $\frac{1}{q+1}+\frac{1}{(q+2)(q+1)}+\cdots$, risulta essere convergente (il teorema è una facile estensione del teorema del confronto delle successioni) per cui se s' **è la sua somma**, deve aversi $s' \leq s$, donde la quantità

$[q!+q!+q(q-1)(q-2)\cdot\cdots\cdot 4\cdot 3+q(q-1)(q-2)\cdot\cdots\cdot 5\cdot 4+\cdots+q(q-1)+q+1]+$

$\frac{1}{q+1}+\frac{1}{(q+2)(q+1)}+\cdots$ essendo la somma di un intero (il termine in parentesi quadre) più un numero positivo $s' \leq \frac{1}{2}$, non è un intero. Questo contraddice l'uguaglianza

$$\begin{aligned} p(q-1)(q-2)\cdot\cdots\cdot 3\cdot 2\cdot 1 \\ &= [q!+q!+q(q-1)(q-2)\cdot\cdots\cdot 4\cdot 3+q(q-1)(q-2)\cdot\cdots\cdot 5\cdot 4+\cdots \\ &+q(q-1)+q+1]+\frac{1}{q+1}+\frac{1}{(q+2)(q+1)}+\cdots \end{aligned}$$

da cui l'assurdo.

Forse però è sicuramente più semplice ragionare così per dimostrare l'irrazionalità di e. Se per assurdo fosse esprimibile attraverso la frazione ridotta ai minimi termini $\frac{p}{q}$, con p e q relativamente primi, tenendo conto della maggiorazione dell'errore della pagina precedente $0<\mathcal{E}=e-S_n<\frac{1}{n!n}$, si ha $0<\frac{p}{q}-S_q=\frac{p}{q}-1-\frac{1}{1!}-\frac{1}{2!}-\cdots-\frac{1}{q!}<\frac{1}{q!q}\Rightarrow q!\left(\frac{p}{q}-S_q\right)<\frac{1}{q}$, dove il membro a sinistra di quest'ultima diseguaglianza è un intero positivo, mentre i termine a destra non è un intero, assurdo.

Adesso che abbiamo visto nei dettagli le due dimostrazioni dell'irrazionalità di π ed e, vi getto nel più totale sconforto dicendo che esse sono praticamente inutili se si sa che questi due numeri sono trascendenti.

Andiamo per ordine riprendendo i concetti già detti di numero algebrico e trascendente.

<u>Definizione</u>: Un numero x reale o complesso è <u>algebrico</u> se soddisfa un'equazione algebrica di grado

n$\in\mathbb{N}$ della forma $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$, dove i coefficienti $a_k\in\mathbb{Z}$ sono numeri interi e $a_{n\neq 0}$. Questo equivale ad affermare che affinché il numero x sia algebrico, occorre che sia una radice di un opportuno polinomio irriducibile di grado n determinato a n + 1 coefficienti interi primi tra loro (il loro M.C.D. è 1).A tal proposito ricordiamo che un polinomio si dice <u>irriducibile</u> se gli unici suoi divisori sono il polinomio unitario 1 e sé stesso [(1)].In generale allora se $\mathbb{R}$ è il campo dei numeri reali e il suo sottocampo proprio $\mathbb{Q}$ dei numeri razionali (tra cui ci sono gli interi $\mathbb{Z}$), si dice che un numero reale è <u>algebrico</u> rispetto a $\mathbb{Q}$, se è radice di una equazione algebrica $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ a coefficienti in $\mathbb{Q}$, $a_k\in\mathbb{Q}$ .Si osservi che ogni numero reale algebrico è radice di un'equazione algebrica a coefficienti interi e primi tra loro, irriducibile nell'anello dei polinomi a coefficienti in $\mathbb{Q}$ (invero se tra i coefficienti a_k ci sono frazioni, basta moltiplicare tutti i termini per il m.c.m. dei denominatori per ottenere solo coefficienti interi, quindi dividere tutti i termini per il M.C.D. di essi nel caso che non risultino relativamente primi). Da ciò si deduce che l'insieme dei numeri algebrici è l'insieme di tutte le radici delle equazioni a coefficienti interi primi tra loro irriducibili nell'anello dei polinomi nell'indeterminata x (variabile)a coefficienti in $\mathbb{Q}$.

È importante notare che <u>ogni numero algebrico è radice di una sola equazione del tipo detto</u>.

Ragionando per assurdo, se il numero reale $a \in \mathbb{R}$ fosse radice di due equazioni algebriche distinte $f(x) = 0, g(x) = 0$, irriducibili sull'anello dei polinomi a coefficienti nel campo razionale, dove i coefficienti sono interi primi tra loro,per il criterio di divisibilità entrambi i polinomi $f(x)$ e $g(x)$ sarebbero divisibili per il polinomio di 1°grado $(x - a)$. Ha senso allora considerare il polinomio di grado non nullo $D(x)$ a coefficienti in $\mathbb{Q}$, M.C.D. dei due polinomi $f(x)$ e $g(x)$,il quale deve avere grado minore di quello dei due polinomi. Da ciò segue che almeno uno dei due polinomi $f(x)$ o $g(x)$ è riducibile sull'anello, contro l'ipotesi.

(*) Un polinomio si dice <u>riducibile</u> se risulta fattorizzabile nel prodotto di due opportuni polinomi non invertibili. Ricordato che un <u>anello</u> è una struttura algebrica con le due operazioni di somma e prodotto, di cui rispetto alla somma è un gruppo abeliano, rispetto al prodotto vale la proprietà associativa, infine vale la proprietà di legame tra le due operazioni, ovvero la proprietà distributiva della prodotto rispetto alla somma, $\mathbb{Z}(+,\cdot)$ è un anello commutativo unitario, contenendo 1 elemento neutro rispetto al prodotto e vale la proprietà commutativa del prodotto. Orbene, l'esposizione rigorosa dal punto di vista algebrico dell'anello dei polinomi definiti su un anello esula dalla nostra trattazione che è quella dell'analisi infinitesimale, però occorre notare delle sottigliezze. Un **<u>campo</u>** è un anello avente la struttura moltiplicativa, meno l'elemento neutro 0 della somma, di gruppo abeliano; ad esempio sono campi sia il corpo dei numeri razionali $Q(+,\cdot)$ che quello dei numeri reali $\mathbb{R}(+,\cdot)$. Consideriamo quindi il polinomio $P(x) = kx + k, k \in Q - \{0\}$, avente il coefficiente sia del termine di 1°grado che di grado zero uguale al numero razionale k, per cui k stesso può essere considerato polinomio di grado zero e il polinomio $P(x)$ come polinomio dell'anello dei polinomi sul campo razionale. In quest'ottica il polinomio k è invertibile in quanto esiste k^{-1} tale che $k^{-1} \cdot k = 1$, e nella fattorizzazione $P(x) = k(x+1)$, il polinomio $x + 1$ non è invertibile, ma il polinomio k è invertibile. Ne consegue allora che il polinomio $P(x)$ è irriducibile sul campo $Q(+,\cdot)$ perché nella sua scomposizione c'è un elemento invertibile. Se invece consideriamo il polinomio $P(x)$ sull'anello $\mathbb{Z}(+,\cdot)$, allora $k \in \mathbb{Z}$ e, non esistendo in $\mathbb{Z}$ l'inverso k^{-1}, la fattorizzazione $P(x) = k(x+1)$ non è banale non essendo invertibili i suoi fattori, per cui $P(x)$è riducibile in $\mathbb{Z}(+,\cdot)$. Certamente però se il polinomio ha i coefficienti appartenenti ad un campo, come può essere $\mathbb{Q}(+,\cdot)$ o $\mathbb{R}(+,\cdot)$, allora, se il polinomio è riducibile, i suoi fattori hanno grado inferiore e non sono costanti, come nel caso di $x^2 - 1 = (x-1)(x^2 + x + 1)$.

<u>Nota</u>: Occorre notare che, dato un numero algebrico, se si sopprime l'ipotesi che i coefficienti siano primi tra loro e che il polinomio stesso sia irriducibile, possono esistere più (infiniti) polinomi di grado differente o anche dello stesso grado che lo ammettono come radice. Ad esempio il numero 2 è l'unica radice del polinomio di primo grado $x - 2$, ma anche del polinomio $kx - 2k$, con k intero non nullo, o la radice positiva del polinomio di secondo grado $x^2 - 4$ o anche del polinomio $kx^2 - 4k, k \in \mathbb{Z} - \{0\}$, o la radice reale del polinomio di terzo grado $x^3 - 8$, ecc. Le soluzioni $\mp i$ della equazione $x^2 + 1 = 0$ sono numeri algebrici. E' immediato provare che se a e b sono numeri reali algebrici, allora anche il numero complesso $z = a + ib$ è un numero algebrico.

Il concetto di numero algebrico è una naturale estensione di quella di numero razionale corrispondente al caso particolare di numeri algebrici relativi a polinomi di grado n = 1 del tipo $ax - b$, con a e b interi e $a \neq 0$, le cui radici sono appunto le frazioni $\frac{b}{a}$, significando ciò che <u>tutti i numeri razionali sono algebrici.</u>

Il viceversa però non vale perché ci sono numeri irrazionali che sono algebrici, come nel caso di $\sqrt{2}$ che è un numero algebrico, essendo radice dell'equazione a coefficienti interi $x^2 - 2 = 0$, ma che non è razionale.

Infatti, se per assurdo lo fosse dovrebbero esistere due opportuni interi positivi primi tra loro a e b (l'ipotesi che $(a, b) = 1$, cioè che il loro M.C.D. sia 1, esclude che b possa essere nullo), tali che $\frac{a}{b} = \sqrt{2}$.

Elevando al quadrato ambo i membri , si ha $\frac{a^2}{b^2} = 2 \Rightarrow a^2 = 2b^2$, da cui, tenendo presente che la scomposizione in fattori primi di un numero intero è unica, dal fatto che a^2è un numero pari, nella sua scomposizione in fattori deve comparire almeno una volta il numero 2, per cui anche nella scomposizione di a deve comparire almeno una volta il numero 2, donde anche il numero a è pari e si può scrivere come $a = 2k, k \in \mathbb{Z}$. Ne consegue che $a^2 = 2b^2 \Rightarrow 4k^2 = 2b^2 \Rightarrow b^2 = 2k^2$, da

cui, essendo b^2 un numero pari, anche b è un numero pari. Siamo giunti alla conclusione che entrambi gli interi a e b sono pari, contro l'ipotesi che essi sono relativamente primi.

Riprendendo il nostro discorso su i numeri algebrici, ogni radice di un'equazione a coefficienti interi di qualsiasi grado è un numero algebrico, indipendentemente dal fatto che esso possa o meno essere espresso attraverso radicali ed esso può essere sia razionale che irrazionale come si è già detto. In generale si può dire che i numeri irrazionali definibili tramite radicali e operazioni con numeri interi sono algebrici. E' importante ricordare però che, come conseguenza della teoria di Galois, a partire dall'equazione di 5° grado, non tutte le soluzioni possono essere espresse tramite radicali. Ma quanti sono i numeri algebrici? G. Cantor ha dimostrato che l'insieme di tutti i numeri algebrici è numerabile (vedi i miei appunti sul sito della scuola sulle potenze di insiemi). Infatti consideriamo l'applicazione H dall'anello dei polinomi di grado n all'insieme $\mathbb{N}$ dei numeri naturali che associa ad ogni polinomio di grado n del tipo $P_n(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ l'intero positivo (detto sua <u>altezza</u>) $\mathbf{h} = |a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0| + n$, $h > 1$,ottenuto prendendo i valori assoluti dei coefficienti del polinomio e sommando alla fine il grado del polinomio (si dice <u>rango</u> dell'equazione il numero intero positivo $r = |a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0| + n - 1$, da cui segue $r = h - 1$ e $r > 0$).

L'applicazione H è ben posta in quanto per ogni fissato polinomio sono univocamente determinati il suo grado e i suoi coefficienti, donde l'immagine $H(P_n)$ = h è unica. Viceversa per ogni fissato valore di h esiste soltanto un numero finito di equazioni del tipo $\mathbf{h} = |a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0| + n$ di altezza h, per cui l'applicazione H non è iniettiva. Ognuna di tali equazioni può al più avere n radici distinte, da cui si ricava che può esistere soltanto un numero finito di numeri algebrici le cui equazioni corrispondenti abbiano altezza h. Questo permette di ordinare tutti i numeri algebrici in una successione in ordine crescente di altezza . Allo scopo di provare ciò, ci proponiamo di determinare il numero dei vettori $(|a_0|, |a_1|, \cdots, |a_n|)$, con le n + 1 componenti non tutte contemporaneamente nulle $|a_i| \geq 0$, $(i = 0,1,2, \cdots, n)$, che siano soluzioni dell'equazione $|a_0| + |a_1| + \cdots + |a_n| = s$, con s intero positivo.

Posto x_k, $(k = 1,2, \ldots, r), r \in \mathbb{N}$, in sostituzione dei termini $|a_i|$ e l'intero n al posto di s, l'equazione precedente diviene $x_1 + x_2 + \cdots + x_r = n$, con $r < n$, per cui il problema equivale alla ricerca del numero di vettori interi non negativi $(x_1, x_2, \ldots, x_r)$. Inizialmente mettiamoci nel caso particolare che sia $x_k > 0 \; \forall k \in \{1,2, \ldots, r\}$, donde il problema è quello di determinare il numero delle soluzioni intere positive dell'equazione $x_1 + x_2 + \cdots + x_r = n$.

Ciò si può visualizzare calcolando i modi con cui si possono distribuire n palline indistinguibili in n urne, mettendo x_1 palline nella prima urna, $x_2$nella seconda,..., x_r palline nell'r-ma urna. Si sono ripartite le n palline iniziali in r gruppi nel modo seguente: tra le n palline iniziali vi sono n – 1 spazi tra palline adiacenti, tra questi ne scegliamo r – 1 come punti di divisione, ottenendo r gruppi di palline da mettere nelle r urne. A questo punto notiamo che il numero dei modi con cui si possono

scegliere gli r – 1 punti di divisione tra n - 1 palline (la prima è esclusa) è dato dalle combinazioni semplici di n – 1 oggetti presi a r – 1 a r – 1 alla volta, cioè $C_{n-1,r-1} = \binom{n-1}{r-1}$.

Analizziamo ora il caso più generale in cui $x_k \geq 0\ \forall k \in \{1,2,\dots,r\}$delle soluzioni non negative dell'equazione $x_1 + x_2 + \cdots + x_r = n$. Sommando l'unità ad ogni x_k r volte, otteniamo $(x_1 + 1) + (x_2 + 1) + \cdots + (x_r + 1) = n + r$, per cui posto $y_k = x_k + 1$, il numero delle soluzioni non negative dell' equazione $x_1 + x_2 + \cdots + x_r = n$ è uguale al numero delle soluzioni positive dell'equazione $y_1 + y_2 + \cdots + y_r = n + r$, cioè $C_{n+r-1,r-1} = \binom{n+r-1}{r-1}$.

Ritornando al nostro caso $|a_0| + |a_1| + \cdots + |a_n| = s$, il numero delle soluzioni dell'equazione, uguale al numero delle n + 1 – ple componenti del vettore $(|a_0|, |a_1|, \cdots, |a_n|)$ è

$\binom{s + (n+1) - 1}{(n+1) - 1} = \binom{s+n}{n}$ e ciò implica che se $h = n + |a_0| + |a_1| + \cdots + |a_n|$, il numero dei vettori $(n, |a_0|, |a_1|, \cdots, |a_n|)$ aventi n + 2 componenti è $\binom{h + (n+2) - 1}{(n+2) - 1} = \binom{h+n+1}{n+1}$.
Fissato allora il numero positivo $h = n + |a_0| + |a_1| + \cdots + |a_n|$ detto altezza del polinomio, esistono in corrispondenza $\binom{h+n+1}{n+1}$ equazioni $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$, per ognuna delle quali è individuato un numero algebrico $x \in \mathbb{C}$ soluzione di essa.

Al numero h si può quindi associare l'insieme S_h costituito dai $\binom{h+n+1}{n+1}$ numeri algebrici soluzioni delle rispettive equazioni. La successione $\{S_h\}_{h\in\mathbb{N}}$ è quindi costituita da insiemi finiti, ciascuno di cardinalità $|S_h| = \binom{h+n+1}{n+1}$, pertanto l'unione $\bigcup_{h\in\mathbb{N}} S_h$ è l'unione numerabile di insiemi finiti, che risulta numerabile per un noto teorema (vedi appunti sulle potenze di insiemi).

<u>Nota</u>: Il risultato precedente, oltre a determinare il numero delle soluzioni intere non negative di un'equazione del tipo $x_1 + x_2 + \cdots + x_r = n$, ha diverse applicazioni; vediamone una.

Un investitore ha un capitale di 20000 euro e decide di frazionarlo in quattro possibili investimenti, investendo una parte intera in migliaia di euro in ciascun investimento. Si vuole sapere il numero delle possibili strategie qual'ora si utilizzi l'intero capitale oppure solo una parte a scelta di esso.

Se n = 20 in migliaia di euro è il capitale e r = 4 il numero delle possibili strategie d'investimento, per $k = 1,2,3,4$ siano x_k le possibili ripartizioni della somma, allora il numero degli investimenti è dato dalle soluzioni intere non negative dell'equazione $x_1 + x_2 + x_3 + x_4 = 20$. Tale numero è

$\binom{n+r-1}{r-1} = \binom{20+4-1}{4-1} = \binom{23}{3} = 1771$ corrispondente alle strategie possibili d'investimento.

Se invece si vuole investire solo una parte della somma, indicata con x_5 la somma da trattenere, una strategia è un vettore di interi $(x_1, x_2, x_3, x_4, x_5)$ tale che $x_1 + x_2 + x_3 + x_4 + x_5 = 20$, da cui si deduce che le possibili strategie sono $\binom{20+5-1}{5-1} = \binom{24}{4} = 10626$.

Siamo ora in grado di provare che l'insieme dei numeri algebrici è numerabile.

Per ogni fissata altezza $h \in \mathbb{N}$ esiste ed è determinato univocamente l'insieme S_h di tutte le $\binom{h+n+1}{n+1}$ equazioni del tipo detto aventi altezza $h = r + 1$, dove ricordiamo che r è il rango. Ordiniamo l'insieme $\mathcal{H}_r$, $r \in \mathbb{N}$ di queste equazioni secondo i valori crescenti del grado n e, a parità di grado, secondo i valori crescenti dei coefficienti dei termini di grado n, di grado n – 1, ecc., fino al termine di grado zero. Quindi, di ogni equazione di $\mathcal{H}_r$, consideriamo le sue radici reali e le ordiniamo secondo valori crescenti, poi, tenendo conto dell'ordine stabilito in $\mathcal{H}_r$, otteniamo che tutte le radici di equazioni di altezza h e rango r risultano ordinate.

Facciamo ora seguire alle radici ordinate delle equazioni di rango 1 dell'insieme $\mathcal{H}_1$, le radici ordinate delle equazioni di rango 2 del'insieme $\mathcal{H}_2$, e così via.

In questo modo l'insieme dei numeri algebrici risulta ordinato secondo un indice crescente e la corrispondenza biunivoca, così costruita, con i numeri naturali assicura la numerabilità dell'insieme $\mathcal{A}$ dei numeri algebrici il cui insieme ha quindi cardinalità $|\mathcal{A}| = \aleph_0 = |\mathbb{N}|$ (leggi aleph con zero). In sostanza l'insieme dei numeri algebrici è numerabile perché è numerabile l'insieme dei polinomi a coefficienti interi o razionali e gli zeri di ciascun polinomio sono in numero finito, per cui essendo l'insieme di tutte le radici unione di una famiglia numerabile, di insiemi finiti, è a sua volta numerabile. Poiché l'insieme $\mathbb{R}$ dei numeri reali ha la potenza del continuo, superiore a quella del numerabile, (vedi il mio articolo sulla potenza degli insiemi), i numeri algebrici sono relativamente "pochi" rispetto a tutti gli altri numeri reali, e ciò risponde al nostro interrogativo di pag.12.

E'naturale allora definire un numero <u>trascendente</u> rispetto al campo $\mathbb{Q}$ dei razionali un numero reale che non è algebrico rispetto a $\mathbb{Q}$, perché, come disse Eulero, essi trascendono il potere dei metodi algebrici. Ovviamente l'insieme dei numeri algebrici non è numerabile ed ha la potenza del continuo.

Si prova in Algebra che l'insieme dei numeri algebrici forma un campo $\mathcal{A}(+,\cdot)$ numerico, sottocampo di $\mathbb{R}(+,\cdot)$. Se consideriamo l'anello dei polinomi sul campo $\mathcal{A}(+,\cdot)$, per cui i coefficienti dei polinomi sono numeri algebrici, allora le radici delle equazioni sono ancora numeri algebrici e il campo $\mathcal{A}(+,\cdot)$ è algebricamente chiuso, essendo il più piccolo campo algebricamente chiuso contenente il campo razionale, chiusura algebrica di questo. Non mi soffermo su questo.

L'esistenza dei numeri trascendenti fu dimostrata nel 1844 da Joseph Liouville, mentre nel 1873 Charles Hermite dimostrò la trascendenza del numero di Eulero e. Un anno dopo Georg Cantor dimostrò che i numeri trascendenti non sono numerabili e nel 1882 fu Ferdinand von Lindemann che, basandosi sulla precedente dimostrazione di Hermite , dimostrò che π è un numero trascendente. Una conseguenza immediata è che Il numero π non è costruibile, come si è già visto, e che non è possibile quadrare il cerchio con riga e compasso. La scoperta dei numeri trascendenti permise quindi di dimostrare l'impossibilità dei tre famosi problemi dell'antichità di cui si è detto.

In seguito alla dimostrazione della trascendenza di e da parte di Hermite, David Hilbert (1862-1943) ne fornì una versione semplificata che adesso vediamo. Premettiamo la seguente utile proposizione.

<u>Proposizione</u>:Se P(x) e un polinomio di grado n, sia $F(x) = P(x) + P'(x) + \cdots + P^n(x)$ il polinomio che si ottiene sommando il polinomio $P(x)$ con tutte le sue derivate fino all'ordine n-mo, si ha $F(a) = e^a F(0) - e^a \int_0^a e^{-x} P(x) dx$.

<u>Dimostrazione</u>: Integrando successivamente per parti, si ha:

$$\int e^{-x} P(x) dx = \int P(x) d(-e^{-x}) = -e^{-x} P(x) - \int -e^{-x} P'(x) dx =$$

$$-e^{-x} P(x) + \int e^{-x} P'(x) dx = -e^{-x} P(x) - e^{-x} P'(x) + \int e^{-x} P''(x) dx =$$

$$-e^{-x} P(x) - e^{-x} P'^{(x)} - \cdots - e^{-x} P^{(n)}(x)$$
$$+ \int e^{-x} P^{(n+1)}(x) dx = -e^{-x}(P(x) + P'(x) + \cdots + P^n(x)) = -e^{-x} F(x) + c$$

Da cui segue $\int_0^a e^{-x} P(x) dx = [-e^{-x} F(x)]_0^a = -e^{-a} F(a) + e^0 F(0) = -\frac{1}{e} F(a) + F0)$ e quindi l'asserto $F(a) = e^a F(0) - e^a \int_0^a e^{-x} P(x) dx$.

Possiamo finalmente dimostrare che :

<u>Proposizione</u>: Il numero e è trascendente.

<u>Dimostrazione</u>: Ragioniamo per assurdo. Se e non fosse trascendente, allora dovrebbe essere algebrico per cui dovrebbe esistere un opportuno polinomio irriducibile di grado m a coefficienti interi $a_0, a_1, \cdots, a_m$, $A(x) = a_0 + a_1 x + \cdots + a_m x^m$, dove $a_0 \neq 0$, tale che e sia una sua radice, per cui deve risultare $A(e) = a_0 + a_1 e + \cdots + a_m e^m = 0$.

Sostituendo nella proposizione precedente
$F(a) = e^a F(0) - e^a \int_0^a e^{-x} P(x) dx$, valida per un qualsiasi polinomio $P(x)$, i valori $a = 0,1,\cdots,m$, si ha:

$$\begin{cases} F(0) = e^0F(0) - e^0\int_0^0 e^{-x}P(x)dx = F(0) \\ F(1) = eF(0) - e\int_0^1 e^{-x}P(x)dx \\ F(2) = e^2F(0) - e^2\int_0^2 e^{-x}P(x)dx \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ F(m) = e^mF(0) - e^m\int_0^m e^{-x}P(x)dx \end{cases}$$

Donde $a_0F(0) + a_1F(1) + \cdots + a_mF(m) = \quad a_0F(0) + a_1eF(0) - a_1e\int_0^1 e^{-x}P(x)dx$

$$\begin{aligned} a_2e^2F(0) - a_2e^2\int_0^2 e^{-x}P(x)dx + \cdots + a_me^mF(0) - a_me^m\int_0^m e^{-x}P(x)dx \\ = F(0)(a_0 + a_1e + a_2e^2 + \cdots + a_me^m) \\ -\left(a_0e^0\int_0^0 e^{-x}P(x)dx + a_1e\int_0^1 e^{-x}P(x)dx + \cdots + a_me^m\int_0^m e^{-x}P(x)dx\right) \\ = F(0)\cdot 0 - \sum_{i=0}^{m} a_ie^i\int_0^i e^{-x}P(x)dx = -\sum_{i=0}^{m} a_ie^i\int_0^i e^{-x}P(x)dx \end{aligned}$$

Se ora p è un numero primo maggiore di m ed a_0, consideriamo il polinomio

$$P(x) = \frac{1}{(p-1)!}x^{p-1}(x-1)^p(x-2)^p\cdot\dots\cdot(x-m)^p$$

avente grado $p - 1 + mp = (m+1)p - 1$, che, posto $Q_1(x) = (x-1)^p(x-2)^p\cdot\dots\cdot(x-m)^p$, polinomio di grado mp avente le radici multiple di ordine p i numeri interi $1, 2, \cdots, m$, si scrive

$$P(x) = \frac{1}{(p-1)!}x^{p-1}\cdot Q_1(x)$$

Osservato che il termine noto del polinomio $Q_1(x)$ si ottiene moltiplicando tra loro tutti i termini noti degli m fattori di primo grado elevati alla p, si ha $[(-1)^p(-2)^p\cdot\dots\cdot(-m)^p] = [(-1)(-2)\cdot\dots\cdot(-m)]^p =$

$[(-1)^m\cdot 1\cdot 2\cdot\dots\cdot m]^p = [(-1)^m\cdot m!]^p = (-1)^{mp}(m!)^p$, da cui l'espressione in funzione dei coefficienti

$Q_1(x) = (-1)^{mp}(m!)^p + q_1x + q_2x^2 + \cdots + q_{m-1}x^{mp-1} + x^{mp}$.

Calcoliamo quindi le derivate successive di $Q_1(x)$.

Si ha:

$$\begin{cases} Q_1(x) = (-1)^{mp}(m!)^p + q_1 x + q_2 x^2 + \cdots + q_{m-1}x^{mp-1} + x^{mp} \\ Q_1'(x) = q_1 + 2q_2 + 3q_3 x^2 + \cdots + (p-1)q_{p-1}x^{p-2} + \cdots + (mp-1)q_{mp-1}x^{mp-2} + mp\,x^{mp-1} \\ Q_1''(x) = 2q_2 + 3\cdot 2q_3 x + \cdots + (p-1)(p-2)q_{p-1}x^{p-3} + \cdots + (mp-1)(mp-2)q_{mp-1}x^{mp-3} + mp(mp-1)x^{mp-2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ Q_1^{(p-1)}(x) = (p-1)!\,q_{p-1} + p!\,q_p x + \cdots + mp(mp-1)\cdot\cdots\cdot[mp-(p-2)]x^{mp-(p-1)} = \\ = (p-1)!\,q_{p-1} + p!\,q_p x + \cdots + mp(mp-1)\cdot\cdots\cdot[(m-1)p+2]x^{(m-1)p+1} \end{cases}$$

Le quali calcolate per $x = 0$ danno

$$\begin{cases} Q_1(0) = (-1)^{mp}(m!)^p \\ Q_1'(0) = q_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ Q_1^{(p-1)}(0) = (p-1)!\,q_{p-1} \end{cases}$$

Fatto ciò, calcoliamo le derivate del polinomio

$$P(x) = \frac{1}{(p-1)!}x^{p-1}\cdot Q_1(x)$$

avendo notato che

$$P(0) = \frac{1}{(p-1)!}\cdot 0\cdot Q_1(0) = 0$$

Si ha per la derivata prima

$$P'(x) = \frac{d}{dx}\left[\frac{1}{(p-1)!}x^{p-1}\cdot Q_1(x)\right] = \frac{x^{p-2}}{(p-1)!}\left(xQ_1'(x) + (p-1)Q_1(x)\right) = \frac{x^{p-2}}{(p-1)!}Q_2(x)$$

dove $Q_2(x) = xQ_1'(x) + (p-1)Q_1(x) \Rightarrow Q_2(0) = (p-1)Q_1(0) = (p-1)(-1)^{mp}(m!)^p$, da cui si ottiene

$P'(0) = 0\cdot Q_2(0) = 0.$

Per la derivata seconda

$$P''(x) = \frac{d}{dx}P'(x) = \frac{d}{dx}\left[\frac{x^{p-2}}{(p-1)!}Q_2(x)\right] = \frac{x^{p-3}}{(p-1)!}[xQ_2'(x) + (p-2)Q_2(x)] = \frac{x^{p-3}}{(p-1)!}Q_3(x),$$

dove $Q_3(x) = xQ_2'(x) + (p-2)Q_2(x) \Rightarrow Q_3(0) = (p-2)Q_2(0) = (p-1)(p-2)(-1)^{mp}(m!)^p$, donde

$P''(0) = 0\cdot Q_3(0) = 0$. Derivando successivamente fino all'ordine $p-2$, si ha:

$P^{(p-2)}(x) = \frac{x^{p-(p-1)}}{(p-1)!}Q_{p-1}(x) = \frac{x}{(p-1)!}Q_{p-1}(x)$, dove $Q_{p-1}(x) = xQ_{p-2}'(x) + [p-(p-2)]Q_{p-2}(x) =$

$xQ_{p-2}'(x) + 2Q_{p-2}(x) \Rightarrow Q_{p-1}(0) = 2Q_{p-2}(0) = (p-1)(p-2)\cdot\cdots\cdot 2\cdot(-1)^{mp}(m!)^p =$

$(p-1)!\,(-1)^{mp}(m!)^p$, donde $P^{(p-2)}(0) = 0\cdot Q_{p-1}(0) = 0$.

Riassumendo si ha: $P(0) = 0, P'(0) = 0, \cdots, P^{(p-1)}(0) = 0.$

Per le derivate successive a partire dalla $(p-1)$ – ma invece: $P^{(p-1)}(x) = \frac{x^{p-p}}{(p-1)!} Q_p(x) = \frac{Q_p(x)}{(p-1)!}$, polinomio di grado $(m+1)p - 1 - (p-1) = mp$, essendo $P(x)$ di grado $(m+1)p - 1$, dove

$$Q_p(x) = xQ'_{p-1}(x) + [p-(p-1)]Q_{p-1}(x) = xQ'_{p-1}(x) + Q_{p-1}(x) \Rightarrow Q_p(0) = 0 + Q_{p-1}(0) =$$

$(p-1)!\,(-1)^{mp}(m!)^p$, da cui si ricava che $P^{(p-1)}(0) = \frac{Q_p(0)}{(p-1)!} = (-1)^{mp}(m!)^p$.

Osserviamo che tale quantità non è divisibile per p perché, essendo p primo e maggiore di m, lo è pure di $m-1, m-2, \cdots, 2, 1$, per cui p non divide nessuno di essi e di conseguenza non divide il loro prodotto $m! = m(m-1)(m-2)\cdot\cdots\cdot 2\cdot 1$. Allora p non divide neppure la potenza $(m!)^p = m^p(m-1)^p(m-2)^p\cdot\cdots\cdot 2^p\cdot 1^p$.

Da ciò segue che $P^{(p-1)}(0)$ non è divisibile per p. Per la derivata p – ma invece:

$$P^{(p)}(x) = \frac{d}{dx}P^{(p-1)}(x) = \frac{d}{dx}\frac{Q_p(x)}{(p-1)!} = \frac{Q'_p(x)}{(p-1)!} = \frac{1}{(p-1)!}\frac{d}{dx}\left[xQ'_{p-1}(x) + Q_{p-1}(x)\right] =$$

$$\begin{aligned}
\frac{1}{(p-1)!}\left(xQ''_{p-1}(x) + Q'_{p-1}(x) + Q'_{p-1}(x)\right) &= \frac{1}{(p-1)!}\left(xQ''_{p-1}(x) + 2Q'_{p-1}(x)\right) \\
&= \frac{1}{(p-1)!}\left(xQ''_{p-1}(x) + 2\frac{d}{dx}\left[xQ'_{p-2}(x) + Q_{p-2}(x)\right]\right) \\
&= \frac{1}{(p-1)!}\left(xQ''_{p-1}(x) + 2xQ''_{p-2}(x) + 2Q'_{p-2}(x) + Q'_{p-2}(x)\right) \\
&= \frac{1}{(p-1)!}\left(xQ''_{p-1}(x) + 2xQ''_{p-2}(x) + 4Q'_{p-2}(x)\right) \\
&= \frac{1}{(p-1)!}\left(xQ''_{p-1}(x) + 2xQ''_{p-2}(x) + 4\frac{d}{dx}\left[xQ'_{p-3}(x) + Q_{p-3}(x)\right]\right) \\
&= \frac{1}{(p-1)!}\left(xQ''_{p-1}(x) + 2xQ''_{p-2}(x) + 4xQ''_{p-3}(x) + 4Q'_{p-3}(x) + 4Q'_{p-3}(x)\right) \\
&= \frac{1}{(p-1)!}\left(xQ''_{p-1}(x) + 2xQ''_{p-2}(x) + 4xQ''_{p-3}(x) + 8Q'_{p-3}(x)\right) \\
&= \frac{1}{(p-1)!}\left(2^0xQ''_{p-1}(x) + 2^1xQ''_{p-2}(x) + 2^2xQ''_{p-3}(x) + \cdots + 2^{p-2}xQ''_2(x) + 2^{p-1}Q'_1(x)\right) \\
&= \frac{1}{(p-1)!}\left(2^0xQ''_{p-1}(x) + 2^1xQ''_{p-2}(x) + 2^2xQ''_{p-3}(x) + \cdots + 2^{p-2}xQ''_2(x)\right. \\
&\left. + 2^{p-1}\frac{d}{dx}\left[(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^p\right]\right) = \quad (*)
\end{aligned}$$

$$\frac{x}{(p-1)!}\sum_{k=1}^{p-1}2^{k-1}Q''_{p-k}(x)+\frac{2^{p-1}}{(p-1)!}\frac{\mathrm{d}}{\mathrm{dx}}[(\mathrm{x}-1)(\mathrm{x}-2)\cdot\cdots\cdot(\mathrm{x}-\mathrm{m})]^{\mathrm{p}}$$

$$=\frac{x}{(p-1)!}\sum_{k=1}^{p-1}2^{k-1}Q''_{p-k}(x)+\frac{2^{p-1}}{(p-1)!}\cdot p[(\mathrm{x}-1)(\mathrm{x}-2)\cdot\cdots\cdot(\mathrm{x}-\mathrm{m})]^{\mathrm{p}-1}$$

$$\cdot\frac{\mathrm{d}}{\mathrm{dx}}[(\mathrm{x}-1)(\mathrm{x}-2)\cdot\cdots\cdot(\mathrm{x}-\mathrm{m})]$$

$$=\frac{x}{(p-1)!}\sum_{k=1}^{p-1}2^{k-1}Q''_{p-k}(x)+\frac{2^{p-1}}{(p-1)!}\cdot p[(-1)^m m!+s_1x+s_2x^2+\cdots+s_{m-1}x^{m-1}+x^m]^{p-1}$$

$$\cdot[s_1+2s_2x+\cdots+mx^{m-1}]$$

che per $x = 0$ dà $\mathbf{P}^{(p)}(0)=\frac{2^{p-1}}{(p-1)!}p(-1)^m m!$ quantità divisibile per p.

(*) Alternativamente si può continuare nel modo seguente

$$\frac{x}{(p-1)!}\sum_{k=1}^{p-1}2^{k-1}Q''_{p-k}(x)+\frac{2^{p-1}}{(p-1)!}$$

$$(p(x-1)^{p-1}(x-2)^p\cdot\cdots\cdot(x-m)^p+p(x-1)^p(x-2)^{p-1}\cdot\cdots\cdot(x-m)^p+\cdots+p(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^{p-1})=$$

$$=\frac{x}{(p-1)!}\sum_{k=1}^{p-1}2^{k-1}Q''_{p-k}(x)+\frac{2^{p-1}}{(p-1)!}p\,[(x-1)\cdot\cdots\cdot(x-m)]^{p-1}[(x-2)\cdot\cdots\cdot(x-m)+(x-1)(x-3)\cdot\cdots\cdot(x-m)+\cdots$$

$$+(x-1)(x-2)\cdot\cdots\cdot(x-m+1)]=\mathrm{P}^{(p)}(0)=\frac{2^{p-1}}{(p-1)!}p[(-1)^m\cdot m!]^{p-1}[\ldots\ldots]$$

La quale è una quantità divisibile per p.

D'altra parte, dall'espressione del polinomio $P(x)=\frac{1}{(p-1)!}x^{p-1}(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^p$, derivando p – 1 volte il fattore x^{p-1} e almeno una volta uno dei fattori $(x-h)^p$ con $h=1,2,\cdots,m$, **si ottiene almeno la derivata** $\mathbf{p-1}$ **– ma** $\frac{d^{p-1}}{dx^{p-1}}x^{p-1}\cdot\frac{d}{dx}(x-h)^p=(p-1)!p(x-h)^{p-1}$, che è una quantità divisibile per p. (**)

(**) Un altro modo di procedere è il seguente che usa la formula di Leibniz (dimostrabile per induzione) per il calcolo della derivata n – ma $D^{(n)}(f_1\cdot f_2)=\sum_{k=0}^{n}\binom{n}{k}f_1^{(n-k)}f_2^{(k)}$. Applicando la formula si ha:

$$\mathrm{P}^{(p)}(x)=\frac{\mathrm{d}^p}{\mathrm{dx}^p}\left[\frac{1}{(p-1)!}x^{p-1}(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^p\right]=\frac{1}{(p-1)!}\sum_{k=0}^{p}\binom{p}{k}[x^{p-1}]^{(p-k)}[(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^p]^{(k)}=$$

$$\frac{1}{(p-1)!}\left\{\binom{p}{0}[x^{p-1}]^{(p)}[(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^p]+\binom{p}{1}[x^{p-1}]^{(p-1)}[(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^p]'\right\}$$

$$+\frac{1}{(p-1)!}\sum_{k=2}^{p}\binom{p}{k}[x^{p-1}]^{(p-k)}[(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^p]^{(k)}=$$

$$\frac{1}{(p-1)!}\{1\cdot 0\cdot[(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^p]+p(p-1)!$$

$$\cdot[p(x-1)^{p-1}(x-2)^p\cdot\cdots\cdot(x-m)^p+\cdots+p(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^{p-1}]\}+$$

$$\frac{1}{(p-1)!}\sum_{k=2}^{p}\binom{p}{k}[x^{p-1}]^{(p-k)}[(x-1)^p(x-2)^p\cdot\cdots\cdot(x-m)^p]^{(k)}=$$

$$\frac{1}{(p-1)!}\{p^p(p-1)![(x-1)(x-2)\cdot\ldots\cdot(x-m)]^{p-1}\cdot[(x-2)\cdot\ldots\cdot(x-m)+\ldots+(x-1)\cdot\ldots\cdot(x-m+1)]\}+$$

$$\frac{1}{(p-1)!}\sum_{k=1}^{p}\binom{p}{k}[x^{p-1}]^{(p-k)}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(k)}=$$

$$=p^p[(x-1)(x-2)\cdot\ldots\cdot(x-m)]^{p-1}\cdot[(x-2)\cdot\ldots\cdot(x-m)+\ldots+(x-1)\cdot\ldots\cdot(x-m+1)]+\frac{1}{(p-1)!}\sum_{k=1}^{p}\binom{p}{k}[x^{p-1}]^{(p-k)}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(k)}$$

.

Per $x = 0$ si annulla la sommatoria contenendo prodotti in cui compare la x, da cui segue

$P^{(p)}(0) = p^p\left[(-1)^{m(p-1)}(m!)^{p-1}[(-1)^{m-1}m! + \cdots + (-1)^{m-1}(m-1)!]\right]$, quantità divisibile per p.

Derivando fino alla derivata alla derivata n – ma e calcolando per $x = 0$, si ottengono tutte quantità divisibili per p Per la derivata n – ma si ha:

$$P^{(n)}(x) = \frac{d^n}{dx^n}\left[\frac{1}{(p-1)!}x^{p-1}(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p\right] = \frac{1}{(p-1)!}\sum_{k=0}^{n}\binom{n}{k}[x^{p-1}]^{(n-k)}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(k)} =$$

$$\frac{1}{(p-1)!}\sum_{k=0}^{n-p}\binom{n}{k}[x^{p-1}]^{(n-k)}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(k)} + \frac{1}{(p-1)!}\sum_{k=n-p+1}^{n}\binom{n}{k}[x^{p-1}]^{(n-k)}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(k)} =$$

$$\frac{1}{(p-1)!}\left\{\binom{n}{0}[x^{p-1}]^{(n)}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p] + \ldots + \binom{n}{n-p}[x^{p-1}]^{(p)}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(n-p)}\right\}+$$

$$\frac{1}{(p-1)!}\left\{\binom{n}{n-p+1}[x^{p-1}]^{(p-1)}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(n-p+1)} + \binom{n}{n-p+2}[x^{p-1}]^{(p-2)}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(n-p+2)} + \ldots + \binom{n}{n}x^{p-1}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(n)}\right\} =$$

$$\frac{1}{(p-1)!}\left\{\binom{n}{n-p+1}(p-1)![(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(n-p+1)} + \binom{n}{n-p+2}(p-1)!x[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(n-p+2)} + \ldots + \binom{n}{n}x^{p-1}[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]^{(n)}\right\}$$

che per $x = 0$ dà

$$P^{(n)}(0) = \frac{1}{(p-1)!}\binom{n}{n-p+1}(p-1)!\frac{d^{n-p+1}}{dx^{n-p+1}}\{[(x-1)^p(x-2)^p\cdot\ldots\cdot(x-m)^p]\}_{x=0} =$$

$$\binom{n}{n-p+1}\frac{d^{n-p+1}}{dx^{n-p+1}}\{[(x-1)(x-2)\cdot\ldots\cdot(x-m)]^p\}_{x=0} = \binom{n}{n-p+1}p\cdot\frac{d^{n-p}}{dx^{n-p}}\{[(x-1)(x-2)\cdot\ldots\cdot(x-m)]^{p-1}\}_{x=0}$$

quantità divisibile per p.

Riassumendo si ha $P(0) = P'(0) = \cdots = P^{(p-2)}(0) = 0$, perché derivando meno di p-1 volte, resterà sempre qualche potenza di x che si annulla per $x = 0$. Se invece si deriva esattamente p – 1 volte e si pone x = 0, l'unico termine non nullo sarà quello che si ottiene derivando p – 1 volte il fattore x^{p-1}, conseguendo che la quantità $P^{(p-1)}(0) = (-1)^{mp}(m!)^p$ non è divisibile per p. Tutte le altre derivate $P^{(p)}(0), P^{(p+1)}(0), \cdots, P^{(n)}(0)$, che si ottengono derivando p – 1 volte il fattore x^{p-1}e almeno una volta uno degli altri fattori, sono divisibili per p, per cui anche la loro somma $A = P^{(p)}(0) + (0) + \cdots + P^{(n)}(0)$ lo è.

Poiché si è posto $F(x) = P(x) + P'(x) + \cdots + P^{(p-2)}(x) + P^{(p-1)}(x) + P^{(p)}(x) + \cdots + P^{(n)}(x)$, per $x = 0$ si ricava che

$F(0) = P(0) + P'(0) + \cdots + P^{(p-2)}(0) + P^{(p-1)}(0) + P^{(p)}(0) + \cdots + P^{(n)}(0) = (-1)^{mp}(m!)^p + A$, con A quantità divisibile per p.

Con ragionamento simile (ciò andrebbe provato cominciando da $F(1) = P(1) + P'(1) + \cdots + P^n(1)$ e provando che ogni addendo della somma è divisibile per p), si dimostra che le quantità $F(1), F(2), \cdots, F(m)$ sono tutte divisibili per p. osserviamo il il primo membro dell'eguaglianza di pag.16

1. $$a_0F(0) + a_1F(1) + \cdots + a_mF(m) = -\sum_{i=0}^{m} a_i e^i \int_0^i e^{-x}P(x)dx \ .$$

La quantità $a_1F(1) + \cdots + a_mF(m)$essendo la somma di prodotti di interi divisibili per p, è un intero divisibile per p, mentre il termine $a_0F(0) = a_0((-1)^{mp}(m!)^p + A) = a_0(-1)^{mp}(m!)^p + a_0A$

è un intero non divisibile per p perché somma rispettivamente di un intero non divisibile per p e di un intero divisibile per p. Ne consegue che $a_0F(0)$è un intero non nullo e quindi pure $a_0F(0) + a_1F(1) + \cdots + a_mF(m)$è un intero non nullo, comportando ciò

$|a_0F(0) + a_1F(1) + \cdots + a_mF(m)| \geq 1.$

Analizziamo ora il secondo membro della 1.cercandone una maggiorazione del modulo . Supponendo che $0 \leq x \leq m$, si ha: $\begin{cases} x-1 < x \leq m \\ x-2 < x \leq m \\ \dots\dots\dots\dots\dots\dots \\ x-m < x \leq m \end{cases}$

$$|P(x)| = \frac{1}{(p-1)!}|x^{p-1}(x-1)^p(x-2)^p \cdot \cdots \cdot (x-m)^p| \leq \frac{1}{(p-1)!}|m^{p-1} \cdot m^p \cdot m^p \cdot \cdots \cdot m^p| = \frac{1}{(p-1)!}m^{p-1+mp} = \frac{m^{(m+1)p-1}}{(p-1)!}$$

, da cui moltiplicando per e^{-x}

(si tenga presente che

$e^{-x} > 0, \forall x \in \mathbb{R}$, quindi la proprietà dell'integrale definito $f(x) \leq g(x), \forall x \in [a,b] \Rightarrow \int_a^b f(x)dx \leq \int_a^b g(x)dx$ e $\left|\int_a^b f(x)dx\right| \leq \int_a^b |f(x)|dx$),

segue per $i = 0, 1, \cdots, m$

$$|P(x)|e^{-x} = |P(x)e^{-x}| \leq \frac{m^{(m+1)p-1}}{(p-1)!}e^{-x} \Rightarrow \left|\int_0^i P(x)e^{-x}dx\right| \leq \int_0^i |P(x)e^{-x}|\,dx$$
$$\leq \int_0^i \frac{m^{(m+1)p-1}}{(p-1)!}e^{-x}dx = \frac{m^{(m+1)p-1}}{(p-1)!}\int_0^i e^{-x}dx \leq \frac{m^{(m+1)p-1}}{(p-1)!}$$

in quanto $\int_0^i e^{-x}dx = -[e^{-x}]_0^i = -\left(\frac{1}{e^i} - 1\right) = 1 - \frac{1}{e^i} < 1$, poiché $0 < \frac{1}{e^i} < 1$

Quindi $|P(x)|e^{-x} \leq \frac{m^{(m+1)p-1}}{(p-1)!}$ ed inoltre vale pure la maggiorazione

$|\sum_{i=0}^{m} a_i e^i| \leq \sum_{i=0}^{m}|a_i e^i| = \sum_{i=0}^{m}|a_i|\,|e^i| = \sum_{i=0}^{m}|a_i|e^i \leq \sum_{i=0}^{m}|a_i|e^m = e^m\sum_{i=0}^{m}|a_i| = Me^m$, con $M = \sum_{i=0}^{m}|a_i|$

da cui si ottiene in definitiva

$$\left|-\sum_{i=0}^{m} a_i e^i \int_0^1 P(x)e^{-x}dx\right| = \left|\sum_{i=0}^{m} a_i e^i \int_0^1 P(x)e^{-x}dx\right| = \left|\sum_{i=0}^{m} a_i e^i\right| \left|\int_0^1 P(x)e^{-x}dx\right| \leq Me^m \frac{m^{(m+1)p-1}}{(p-1)!}$$

Allora dalla 1. $a_0F(0) + a_1F(1) + \cdots + a_mF(m) = -\sum_{i=0}^{m} a_i e^i \int_0^i e^{-x}P(x)dx$ segue:

$$1 \leq \left|\sum_{k=0}^{m} a_k F(k)\right| = \left|-\sum_{i=0}^{m} a_i e^i \int_0^i P(x)\, e^{-x}dx\right| \leq Me^m \frac{m^{(m+1)p-1}}{(p-1)!}$$

Consideriamo ora la successione della variabile intera positiva p

$$\left\{\frac{m^{(m+1)p-1}}{(p-1)!}\right\}_{p\in\mathbb{N}} = \left\{\frac{Me^m}{m}\frac{m^{(m+1)p}}{(p-1)!}\right\}_{p\in\mathbb{N}} = \left\{\frac{Me^m}{m}\frac{[m^{m+1}]^p}{(p-1)!}\right\}_{p\in\mathbb{N}} = \left\{\frac{Me^m}{m}\frac{\alpha^p}{(p-1)!}\right\}_{p\in\mathbb{N}} = \left\{\mu\frac{\alpha^p}{p!}\right\}_{p\in\mathbb{N}}$$

dove si è posto $\mu = \frac{Me^m}{m}$ e $\alpha = m^{m+1}$. (*)

(*)<u>Nota</u> : Essendo p numero primo, la successione $\left\{\mu\frac{\alpha^p}{p!}\right\}_{p\in\mathbb{N}}$ ha senso in quanto i numeri primi sono infiniti, anzi , essendo l'insieme dei numeri primi un sottoinsieme infinito dei numeri naturali, la sua potenza è quella del numerabile. Infatti, se per assurdo esistesse solo un numero finito n di numeri primi, siano essi $p_1, p_2, \cdots, p_n$, il numero intero maggiore di 1 $p_1p_2\cdot\cdots\cdot p_n + 1$,ottenuto moltiplicando tra loro $p_1, p_2, \cdots, p_n$ e sommando il risultato con l'unità, è distinto dai precedenti e non può essere primo per l'ipotesi dell'assurdo. Indicato con d un suo divisore primo, questo necessariamente deve essere tra gli n numeri primi possibili $p_1, p_2, \cdots, p_n$, per cui divide il loro prodotto $p_1p_2\cdot\cdots\cdot p_n$ oltre che $p_1p_2\cdot\cdots\cdot p_n + 1$. Poiché il divisore di due numeri interi divide pure la loro differenza,si ha che d deve dividere $p_1p_2\cdot\cdots\cdot p_n + 1 - p_1p_2\cdot\cdots\cdot p_n = 1$, assurdo perché dovrebbe aversi $1 = d\cdot t$ con $t \in \mathbb{N}$, ovvero t e d entrambi interi maggiori di 1. (Si ha $c/a \wedge c/b \Rightarrow c/(a-b)$, perché $c/a \Rightarrow a = c\cdot t$, $t \in \mathbb{N}$, $c/b \Rightarrow b = c\cdot u$, $u \in \mathbb{N}$, donde $a - b = c\cdot t - c\cdot u = c(t-u) = c\cdot s$, $s = (t-u) \in \mathbb{Z}$ cioè $c/(a-b)$).

A pag. 7 abbiamo già una successione simile. Consideriamo il rapporto tra il generico termine p+1 - mo della successione e il suo antecedente p - mo

$$\frac{\mu\frac{\alpha^{p+1}}{(p+1)!}}{\mu\frac{\alpha^p}{p!}} = \frac{\alpha^{p+1}}{\alpha^p}\frac{p!}{(p+1)!} = \frac{\alpha}{p+1} > 0$$

La successione $\left\{\frac{\alpha}{p+1}\right\}_{p\in\mathbb{N}}$ è infinitesima essendo $\lim_{p\to\infty}\frac{\alpha}{p+1} = 0$, per cui fissato $\epsilon = 1$, è possibile determinare in corrispondenza un indice $\nu > 0$ tale che $\forall p > \nu$ risulti $0 < \frac{\alpha}{p+1} < 1$ che implica

$\frac{\mu\frac{\alpha^{p+1}}{(p+1)!}}{\mu\frac{\alpha^p}{p!}} < 1 \Rightarrow \mu\frac{\alpha^{p+1}}{(p+1)!} < \mu\frac{\alpha^p}{p!}$. Questo significa che la successione a termini positivi $\left\{\mu\frac{\alpha^p}{p!}\right\}_{p\in\mathbb{N}}$

è monotona strettamente decrescente inferiormente limitata da 0 e quindi convergente a 0 , cioè

$\lim_{p\to\infty}\mu\frac{\alpha^p}{p!}=0$. Che $\lambda=0$ sia appunto $inf\left\{\mu\frac{\alpha^p}{p!}\right\}_{p\in\mathbb{N}}$ si può dedurre dal fatto che posto $\lambda=\lim_{p\to\infty}\mu\frac{\alpha^p}{p!}$

$$\frac{\mu\frac{\alpha^{p+1}}{(p+1)!}}{\mu\frac{\alpha^p}{p!}}=\frac{\alpha}{p+1}\Rightarrow\mu\frac{\alpha^{p+1}}{(p+1)!}=\frac{\alpha}{p+1}\cdot\mu\frac{\alpha^p}{p!}\Rightarrow\lim_{p\to\infty}\mu\frac{\alpha^{p+1}}{(p+1)!}=\lim_{p\to\infty}\left[\frac{\alpha}{p+1}\cdot\mu\frac{\alpha^p}{p!}\right]$$

$$=\lim_{p\to\infty}\frac{\alpha}{p+1}\cdot\lim_{p\to\infty}\mu\frac{\alpha^p}{p!}\Rightarrow\lambda=\lim_{p\to\infty}\frac{\alpha}{p+1}\cdot\lambda=0\cdot\lambda=0$$

cioè $\lim_{p\to\infty}\mu\frac{\alpha^p}{p!}=0$.

Ritornando alla diseguaglianza $1\leq\left|-\sum_{i=0}^{m}a_ie^i\int_0^1P(x)e^{-x}dx\right|\leq Me^m\frac{m^{(m+1)p-1}}{(p-1)!}$, per quanto visto la successione $\left\{\frac{m^{(m+1)p-1}}{(p-1)!}\right\}$ è infinitesima, per cui in corrispondenza di $\epsilon=1$, è possibile determinare un opportuno indice $\nu>0$ tale che per ogni $p>\nu$ si abbia

$$Me^m\frac{m^{(m+1)p-1}}{(p-1)!}<1$$

Ma questo implica che

$$1\leq\left|-\sum_{i=0}^{m}a_ie^i\int_0^1P(x)e^{-x}dx\right|<1$$

$1<1$, assurdo.

<u>Corollario</u>: Il numero e è irrazionale.

<u>Dimostrazione</u>: Se per assurdo il numero e fosse razionale, allora dovrebbe essere algebrico, contro l'ipotesi.

◆◆◆◆◆◆◆