Sezione Scientifca

La scomponibilità dei numeri naturali in somme di quadrati
(parte prima)

Italo D'Ignazio – Ercole Suppa

Avvertenza: *Questo articolo è stato concepito come una lezione extracurriculare per classi di Liceo scientifico, con lo scopo di introdurre un argomento impegnativo ma attraente, capace di interessare gli studenti o almeno quelli più dotati. Le conoscenze necessarie per la comprensione non vanno oltre l'aritmetica e l'algebra elementari, ma la concatenazione logica delle varie tappe è ardua. Per vincere le difficoltà di questo ordine si è insistito con argomentazioni, considerazioni ed esempi che il lettore esperto giudicherà, probabilmente, inutili lungaggini. Chiediamo venia e invochiamo l'attenuante della buona intenzione: volevamo rendere agevole un cammino impervio!*

§ 1. quadrati e i numeri naturali

Supponiamo di avere un imprecisato numero di mattonelle quadrate e di volerle disporre in modo da formare, con esse, ancora un quadrato. Ciò sarà possibile solo se il numero delle mattonelle è uno dei seguenti:

(1) $1, 4, 9, 16, 25, \ldots$ ossia $1^2, 2^2, 3^2, 4^2, 5^2 \ldots$ (fig. 1)

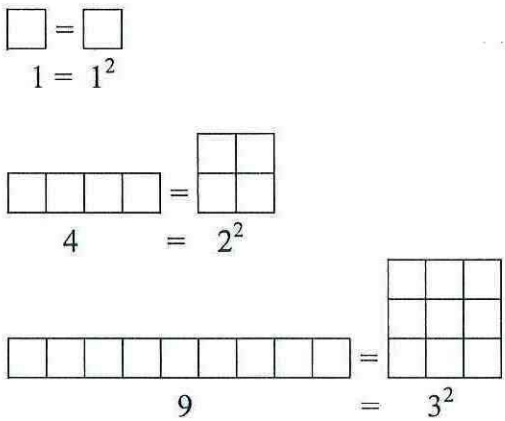


Fig. 1

La successione dei quadrati diviene via via meno "densa", cioè gli intervalli tra quadrati successivi diventano di sempre maggiore ampiezza.

Ciò implica che, al crescere del numero delle mattonelle, diviene via via meno probabile la possibilità di formare con esse un quadrato.

Se il numero delle mattonelle non coincide con uno di quelli della successione (1), può avvenire che, con esse, si possano costruire due quadrati (fig. 2); per esempio, con 13 mattonelle sarebbe possibile costruire un quadrato di $4 = 2^2$ mattonelle ed uno di $9 = 3^2$ mattonelle. Cioè $13 = 2^2 + 3^2$. Analogamente $20 = 2^2 + 4^2, 45 = 3^2 + 6^2$.

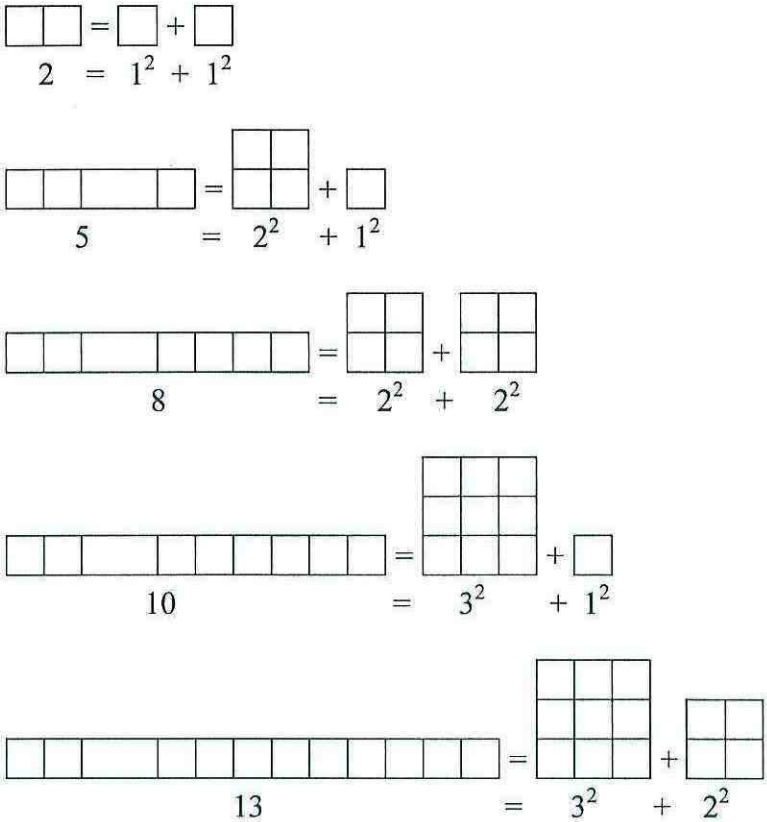


Fig. 2

Tuttavia, anche a far ricorso a due quadrati, non c'è certezza di poter risolvere in ogni caso il problema. Per esempio se le mattonelle sono 6, isoli quadrati di cui possiamo disporre sono quelli formati o da una sola mattonella o da quattro; e con due soli addendi comunque scelti tra 1 e 4

non riusciamo ad ottenere come somma 6 (infatti: $1 + 1 = 2$, $1 + 4 = 5$, $4 + 4 = 8$); occorre far ricorso ad un terzo addendo: $6 = 4 + 1 + 1 = 2^2 + 1^2 + 1^2$ (fig. 3).

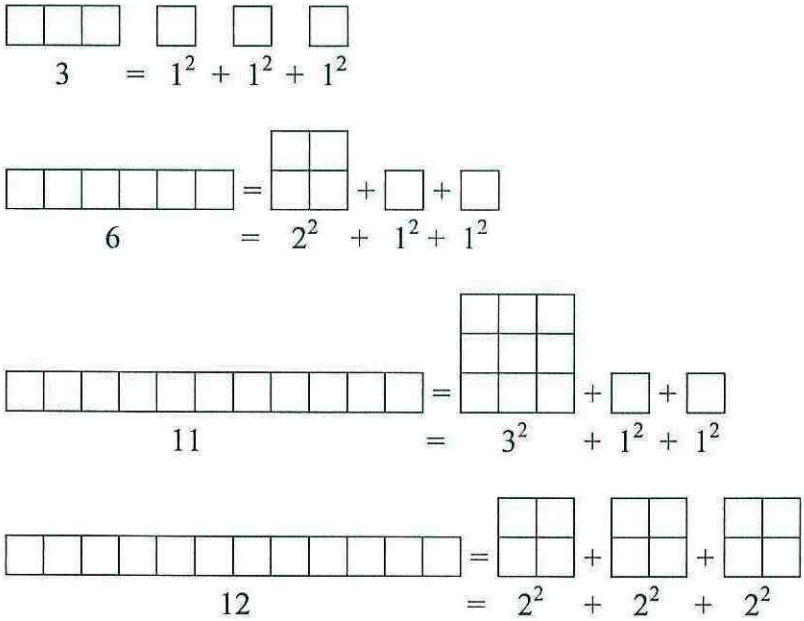


Fig. 3

Per il numero successivo a 6, cioè per il 7, neanche tre addendi sono sufficienti, ne necessita un quarto: $7 = 4 + 1 + 1 + 1 = 2^2 + 1^2 + 1^2$ (fig. 4).

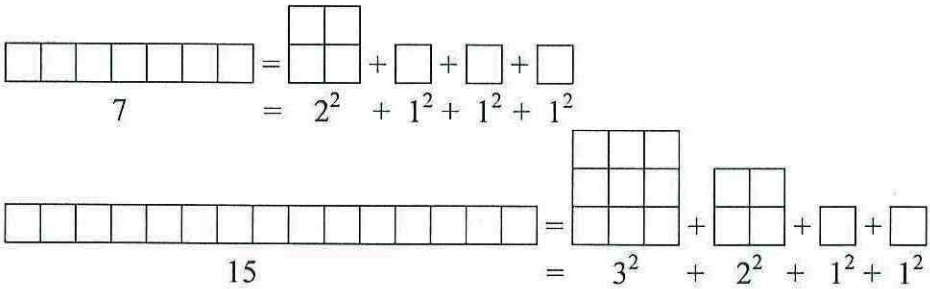


Fig. 4

A questo punto però, accade un fatto a prima vista sorprendente.

Sembrerebbe naturale aspettarsi di incontrare qualche numero per il quale neanche quattro quadrati sono sufficienti; e poi dei numeri via via più grandi per i quali sia necessario un sempre maggior numero di quadrati. Invece, no! Procedendo per tentativi si constata che *qualunque sia il numero delle nostre mattonelle è sempre possibile formare con esse un numero di quadrati non superiore a quattro.*

Esaminando i numeri naturali da 0 a 200, si trova che tra essi ci sono 15 quadrati, 63 numeri esprimibili come somma di due quadrati, 92 numeri per i quali è necessario far ricorso a tre quadrati, infine 31 numeri per i quali di quadrati ne sono necessari quattro. l'istogramma della fig. 5 illustra la situazione: la maggior parte dei numeri è scomponibile nella somma di tre quadrati; quelli che ne richiedono quattro sono meno numerosi di quelli che ne richiedono due; la schiera meno numerosa è quella dei quadrati perfetti.

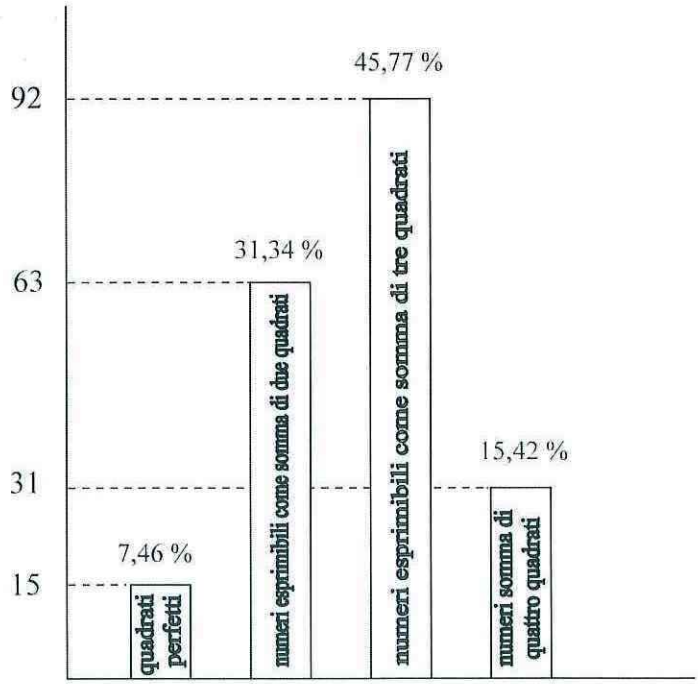


Fig. 5

Naturalmente, il fatto che nel campione esaminato non esistono numeri che richiedano più di quattro quadrati, non dimostra che ciò sia

vero in generale: potrebbe non essere così per numeri maggiori di 200. L'esame condotto permette solo di fare una congettura di un certo grado di plausibilità. Plausibilità che s'accrescerebbe se ottenessimo risultati analoghi su un campione più esteso. E tuttavia, per questa strada non raggiungeremmo mai la certezza matematica. Nella teoria dei numeri, più che in altre branche, l'esame di molti casi particolari è stato assai spesso il mezzo per arrivare ad ipotizzare conclusioni di carattere generale, ma solo la dimostrazione ha, successivamente, dato la certezza. Tra l'altro, in questa disciplina molte sono state le congetture formulate sulla base dì un tal metodo di ricerca, mai smentite dall'osservazione e che, tuttavia non sono state ancora dimostrate. Né, d'altra parte, mancano esempi di congetture a cui investigazioni condotte su casi particolari assegnavano un alto grado di plausibilità e che, invece, si sono rivelate fallaci.

Della proprietà di cui ci stiamo occupando esistono, però, numerose dimostrazioni. Noi cercheremo di esporre, nel §3, quella di Lagrange che ci sembra assai bella e la cui comprensione, pur nelle ineliminabili difficoltà, non richiede conoscenze matematiche di alto livello.

§ 2. Un'equazione indeterminata di Diofanto.

Uno dei problemi trattati da Diofanto nella sua *Aritmetica* , il IV, 29, chiede di risolvere in numeri razionali l'equazione

$$x^2 + y^2 + z^2 + t^2 + x + y + z + t = a \tag{1}$$

Vediamo come risolve Diofanto la sua equazione, traducendo, ovviamente, il suo procedimento nei simboli della matematica moderna. Aggiungiamo quattro volte 1/4 (cioè 1) al primo membro della (1). Per mantenere l'uguaglianza dovremo aggiungere 1 anche al secondo membro, sicché, variando l'ordine degli addendi e associando opportunamente, la nostra equazione diventa:

$$(x^2 + x + \frac{1}{4}) + (y^2 + y + \frac{1}{4}) + (z^2 + z + \frac{1}{4}) + (t^2 + t + \frac{1}{4}) = a + 1$$

Osserviamo, ora, che le espressioni entro parentesi sono quadrati di binomi:

$$x^2 + x + \frac{1}{4} = (x + \frac{1}{2})^2$$

e così per le altre. Possiamo allora scrivere:

$$(x+\frac{1}{2})^2+(y+\frac{1}{2})^2+(z+\frac{1}{2})^2=a+1$$

A questo punto Diofanto dice l'equazione risolta, poiché può scomporre il numero $a+1$ in somma di quattro quadrati. In effetti, se questa scomposizione è

$$a+1=X^2+Y^2+Z^2+T^2$$

basta porre :

$$x+\frac{1}{2}=X \qquad y+\frac{1}{2}=Y \qquad z+\frac{1}{2}=Z \qquad t+\frac{1}{2}=T$$

per ottenere la soluzione richiesta.

Diofanto opera su numeri particolari e, per tentativi, ottiene facilmente la scomposizione dei numeri che gli interessano in somme di quattro quadrati. Ma intende indicare metodi generali, quindi mostra implicitamente di ritenere *sempre possibile* questa scomposizione. Per la prima volta nella storia della matematica si presenta la necessità di rappresentare un numero come somma di, al massimo, quattro quadrati. La congettura che ciò sia sempre possibile è esatta, come abbiamo già accennato nel precedente paragrafo e come dimostreremo nel prossimo. La chiameremo, perciò, congettura di Diofanto. Enunciamola con precisione:

Ogni numero naturale può essere espresso sotto forma di somma di non più di quattro quadrati.

§ 3. La dimostrazione di Lagrange della congettura di Diofanto

Per facilitare la comprensione di questa dimostrazione, procederemo per tappe successive. Ogni tappa costituisce un teorema che ci avvicina progressivamente alla conclusione.

Teorema 1. *Se m e n sono due numeri naturali ciascuno dei quali può essere considerato somma di quattro quadrati, anche il loro prodotto mn può esserlo.*

E' facile verificare la seguente identità:

$$(2)\qquad \begin{aligned}&(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2)=(-ae+bf+cg+dh)^2+\\&(af+be+ch-dg)^2+(ag-bh+ce+df)^2+(ah+bg-cf+de)^2\end{aligned}$$

La verifica richiede solo che si sviluppi il primo membro eseguendo il prodotto dei due polinomi ed il secondo membro mediante la regola che dà al quadrato di un polinomio qualsiasi. L'effettiva esecuzione dei calcoli è abbastanza lunga e laboriosa, ma non difficile.

Se in (2) poniamo:

$$m=a^2+b^2+c^2+d^2$$

$$n=e^2+f^2+g^2+h^2$$

$$A=-ae+bf+cg+dh$$

$$B=af+eb+ch-gd$$

$$C=ag-bh+ce+df$$

$$D=ah+bg-cf+de$$

otteniamo: $mn=A^2+B^2+C^2+D^2$. Che è quanto volevasi dimostrare.

L'utilità del teorema 1 consiste in questo: se riusciremo a dimostrare che ogni numero *primo* è esprimibile come somma di non più di quattro quadrati, potremo concludere che anche ogni numero naturale lo è, dal momento che questo può sempre essere pensato come prodotto di fattori primi.

Teorema 2. *Dato un numero primo p maggiore di 2 è possibile trovare un numero m tale che il prodotto mp possa essere considerato somma di quattro quadrati e tale, altresì, che* $1 \leq m \leq p$.

Osserviamo, preliminarmente, che p è un numero dispari, perché primo e maggiore di 2. Pertanto, $p-1$ e $p+1$ sono pari e $\frac{p-1}{2}$, $\frac{p+1}{2}$ sono interi.

Compiliamo la lista dei numeri

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

e, dopo aver diviso ciascuno di essi per p, formiamo l'insieme R dei resti ottenuti: esso conterrà $\frac{p+1}{2}$ numeri, compresi fra 0 e $p-1$ (il resto è sempre minore del divisore), tutti diversi tra loro. Infatti, se due di essi fossero uguali, dovrebbero esistere due numeri naturali x_1 e x_2 compresi fra 0 e $\frac{p-1}{2}$ i cui quadrati darebbero lo stesso resto r dividendoli per p. In altri termini, dovremmo avere:

$$x_1^2 = q_1 p + r$$
$$x_2^2 = q_2 p + r$$

dove q_1 e q_2 indicano i due quozienti. Supponendo che sia x_2 il maggiore dei due numeri x_1, x_2, sottraendo membro a membro otteniamo:

$$(x_2^2 - x_1^2) = p(q_2 - q_1)$$

ossia

$$(x_2 - x_1)(x_2 + x_1) = p(q_2 - q_1)$$

Se quest'ultima uguaglianza fosse vera, p, essendo primo, dovrebbe essere divisore di $(x_2 - x_1)$ oppure di $(x_2 + x_1)$, ma ciò è impossibile

perché entrambi questi numeri sono minori di p. Dunque è assurda l'ipotesi che esistano due resti uguali: essi sono tutti differenti.

Torniamo ora al nostro insieme R dei resti e formiamone un secondo nel seguente modo: a ciascun $r \in R$ aggiungiamo 1 e sottraiamo la somma da p. Otteniamo $\frac{p+1}{2}$ numeri, compresi tra 0 e $p-1$ e, anch'essi, tutti differenti. Indichiamone con S l'insieme. Almeno uno dei numeri $s \in S$ deve appartenere anche ad R. Infatti, R conta $\frac{p+1}{2}$ dei p numeri $0,1,2,\ldots,p-1$; di questi ne restano fuori di R soltanto $\frac{p-1}{2}$. Ma anche in S ci sono $\frac{p+1}{2}$ dei p numeri precedenti, dunque R ed S devono avere in comune almeno un numero.

Consideriamo uno di questi numeri di cui l'osservazione precedente ci assicura l'esistenza. Lo indichiamo con r per ricordarci che appartiene ad R e con s per ricordarci che appartiene ad S. Naturalmente è $r = s$. Teniamo presente che r è il resto ottenuto dividendo per p un numero x^2 tale che $0 \le x \le \frac{p-1}{2}$. Quindi:

(3) $$x^2 = pq + r \qquad (q = \text{quoziente})$$

Inoltre, s è ottenuto dividendo per p un numero y^2 tale che $0 \le y \le \frac{p-1}{2}$, aggiungendo 1 al resto e sottraendo da p la somma. Cioè

(4) $$y^2 = q'p + r'$$

(5) $$s = p - (r' + 1)$$

Tenendo conto della condizione (5) e di $r = s$, la (3) e la (4) si possono scrivere:

$$x^2 = pq + r$$
$$y^2 = pq' + p - r - 1$$

da cui, per addizione, otteniamo:

$$x^2 + y^2 = p(q + q' + 1) - 1$$

posto $m = q + q' + 1$ l'ultima eguaglianza può scriversi:

$$mp = x^2 + y^2 + 1$$

Ricordando, infine, che $x \leq \frac{p-1}{2}$ e $y \leq \frac{p-1}{2}$ abbiamo anche

$$mp \leq (\frac{p-1}{2})^2 + (\frac{p-1}{2})^2 + 1 = \frac{p^2 - 2p + 3}{2} < \frac{p^2}{2} < p^2$$

e,conseguentemente, $m < p$.

Il teorema 2 è ora dimostrato, giacché abbiamo ottenuto

(7) $$mp = x^2 + y^2 + 1^2 + 0^2 \quad \text{con} \quad 1 \leq m < p$$

Osservazione. Il teorema 2 è, per noi, una tappa di avvicinamento al teorema dì Lagrange e a questi fini interessa solo che il prodotto *mp* sia somma di quattro quadrati. Perciò lo abbiamo scritto nella forma (7). Esso, però, dice qualche cosa di più. Dei quattro quadrati in cui *mp* viene scomposto, solo due (x^2 e y^2) variano al variare di p ; gli altri due sono 0^2 e 1^2 per ogni *p*. La relazione (7) può scriversi: $mp - 1 = x^2 + y^2$ e ciò significa *che per ogni numero primo p esiste almeno un numero naturale m minore di p tale che* $mp - 1$ *può scriversi sotto forma di somma di due quadrati.*

Teorema 3. *Se p è un numero primo maggiore di 2 ed m il più piccolo numero naturale per il quale mp possa esprimersi come somma di quattro quadrati, allora deve essere* $m = 1$.

Possiamo scrivere l'ipotesi di questo teorema nella forma

(8) $$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

essendo m il più piccolo dei numeri che verificano l'uguaglianza e x_1, x_2, x_3, x_4 quattro numeri naturali.

Sappiamo già che $m<p$. Facciamo ora vedere che m non può essere pari; se fosse così, anche il prodotto mp sarebbe pari e allora i quattro numeri x_1, x_2, x_3, x_4 dovrebbero essere:

a) o tutti e quattro pari,
b) o tutti e quattro dispari,
c) o due pari e due dispari (in questa eventualità x_1, x_2 indichino quelli dispari, x_3, x_4 quelli pari).

In tutti e tre i casi i numeri

$$(x_1 + x_2),\ (x_1 - x_2),\ (x_3 + x_4),\ (x_3 - x_4)$$

sono pari ed i numeri

$$\frac{x_1 + x_2}{2},\ \frac{x_1 - x_2}{2},\ \frac{x_3 + x_4}{2},\ \frac{x_3 - x_4}{2}$$

sono interi. Eseguendo i calcoli è facile verificare che:

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = \frac{1}{2}\left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)$$

quindi, tenendo conto dell'ipotesi (8):

$$\text{(9)} \qquad \frac{mp}{2} = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

Quest'ultima uguaglianza ci dice che si ottiene una scomposizione in quattro quadrati anche applicando a p il coefficiente $m/2$, che è minore di m. Ma ciò contrasta con l'ipotesi che m sia il fattore minimale.

A questo punto sappiamo che m è dispari, ma non ci basta: vogliamo concludere che è $m = 1$. Possiamo raggiungere lo scopo ragionando ancora per assurdo, cioè facciamo vedere che se m è maggiore di 1 non può essere il coefficiente minimale supposto. L'ipotesi assurda a cui abbiamo accennato può essere espressa da $m \geq 3$.

Dividiamo ciascuno degli x che compaiono nella (8) per m, assumendo però come quoziente quello approssimato per difetto o per eccesso che meglio approssima il quoziente esatto .

Ciò implica che qualche resto potrà risultare negativo, ma in valore assoluto sarà minore o uguale a $\frac{m-1}{2}$. Pertanto, indicando con q_1, q_2, q_3, q_4 quozienti così ottenuti e con y_1, y_2, y_3, y_4 i corrispondenti resti, avremo:

$$x_1 = q_1 m + y_1 \text{ con } -\frac{m-1}{2} \le y_1 \le \frac{m-1}{2} \quad \Rightarrow \quad y_1 = x_1 - q_1 m$$

$$x_2 = q_2 m + y_2 \text{ con identica limitazione per } y_2 \quad \Rightarrow y_2 = x_2 - q_2 m$$

$$x_3 = q_3 m + y_3 \text{ con identica limitazione per } y_3 \quad \Rightarrow \quad y_3 = x_3 - q_3 m$$

$$x_4 = q_4 m + y_4 \text{ con identica limitazione per } y_4 \quad \Rightarrow y_4 = x_4 - q_4 m$$

Calcoliamo ora la somma dei quadrati dei resti; in virtù delle ultime uguaglianze scritte avremo:

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = (x_1 - q_1 m)^2 + (x_2 - q_2 m)^2 + (x_3 - q_3 m)^2 + (x_4 - q_4 m)^2 =$$
$$= x_1^2 + x_2^2 + x_3^2 + x_4^2 - 2m(x_1 q_1 + x_2 q_2 + x_3 q_3 + x_4 q_4) + m^2(q_1^2 + q_2^2 + q_3^2 + q_4^2)$$

e, tenendo conto della (8):

$$\begin{aligned} & y_1^2 + y_2^2 + y_3^2 + y_4^2 = \\ (10) \quad & = mp - 2m(x_1 q_1 + x_2 q_1 + x_3 q_3 + x_4 q_4) + m^2(q_1^2 + q_2^2 + q_3^2 + q_4^2) = \\ & = m[p - 2(x_1 q_1 + x_2 q_2 + x_3 q_3 + x_4 q_4) + m(q_1^2 + q_2^2 + q_3^2 + q_4^2)] = mn \end{aligned}$$

avendo indicato con n il numero naturale dato dall'espressione entro parentesi quadra. n non può essere nullo; se così fosse risulterebbe $y_1^2 + y_2^2 + y_3^2 + y_4^2 = 0$ e la somma di numeri non negativi (le y compaiono al quadrato) è nulla solo se sono nulli tutti gli addendi. Cioè l'uguaglianza scritta implicherebbe $y_1 = y_2 = y_3 = y_4 = 0$ e quindi

$$x_1 = mq_1, x_2 = mq_2, x_3 = mq_3, x_4 = mq_4$$

e, ancora per la (8),

$$mp = m^2(q_1^2 + q_2^2 + q_3^2 + q_4^2) \quad \Rightarrow \quad p = m(q_1^2 + q_2^2 + q_3^2 + q_4^2)$$

conclusione assurda perché p è numero primo.

Notiamo, ancora, che, per le limitazioni a cui obbediscono le y,

$$mn = y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq 4\left(\frac{m-1}{2}\right)^2 = (m-1)^2 < m^2$$

e da $mn < m^2$ consegue $m < n$.

Per l'ultimo passo della nostra laboriosa dimostrazione dobbiamo riprendere l'identità (2), utilizzata per la dimostrazione del teorema 1, e porre in essa

$$a = x_1,\ b = x_2,\ c = x_3,\ d = x_3,\ e = -y_1,\ f = y_2,\ g = y_3,\ h = y_4$$

Otteniamo:

$$\begin{aligned} &(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\ (11) \quad &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ &+ (x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2 \end{aligned}$$

Le relazioni (8) e (10) ci dicono che il primo membro della (11) è uguale a m^2np. Il primo numero il cui quadrato compare al secondo membro della (11) è

$$\begin{aligned} &(x_1y_1 + x_2y_2 + x_3y_3 +_4 y_4) = \\ &= x_1(x_1 - mq_1) + x_2(x_2 - mq_2) + x_3(x_3 - mq_3) + x_4(x_4 - mq_4) = \\ &= x_1^2 + x_2^2 + x_3^2 + x_4^2 - m(q_1x_1 + q_2x_2 + q_3x_3 + q_4x_4) = \\ &= m[p - (q_1x_1 + q_2x_2 + q_3x_3 + q_4x_4)] = mz_1 \end{aligned}$$

avendo indicato con z_1 il numero intero che si ottiene calcolando l'espressione entro parentesi quadra.

In modo del tutto analogo si può vedere che anche il secondo, il terzo e il quarto numero i cui quadrati compaiono al secondo membro della

(11) possono scriversi in maniera simile: mz_2, mz_3, mz_4 dove z_2, z_3, z_4 sono numeri interi. In definitiva, la (11) diventa:

$$m^2np = m^2(z_1^2 + z_2^2 + z_3^2 + z_4^2) \quad \Leftrightarrow \quad np = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

Ed eccoci in porto: abbiamo dimostrato che $n<m$, sicché anche l'ipotesi che $m \geq 3$ sia il coefficiente minimale conduce ad una contraddizione. In conclusione, se m è minimale non può essere pari e non può essere maggiore o uguale a 3. Perciò deve essere uguale ad 1.

Teorema 4. *Ogni numero naturale n può essere considerato somma di quattro quadrati.*

Che il teorema sia vero per $n = 0$, $n = 1$, $n = 2$ si constata direttamente; che sia vero per n primo dispari è immediata conseguenza del teorema 3. Rimane solo il caso di n composto.

Scomponiamo n in prodotto di fattori primi: $n = p_1p_2p_3 \ldots p_r$ ($p_1, p_2, p_3 \ldots$ indicano numeri primi non necessariamente distinti). p_1 e p_2 si possono scrivere come somme di quattro quadrati e, per il teorema 1, lo stesso accade per il loro prodotto (p_1p_2). Ma allora, sempre per il teorema 1, anche $(p_1p_2)p_3$ si può scrivere allo stesso modo. Così continuando fino ad esaurire tutti i fattori del prodotto si arriva alla conclusione desiderata.

§ 4. Qualche osservazione sulla dimostrazione di Lagrange

Ripercorriamo per grandi linee la dimostrazione di Lagrange: una sintesi ci aiuterà a meglio penetrarne la logica interna e, nello stesso tempo, ci offrirà l'occasione per soffermare l'attenzione su alcuni dettagli che debbono essere meglio chiariti.

La nostra dimostrazione parte con la constatazione che, se due numeri sono scomponibili in somme di quattro quadrati, anche il loro prodotto lo è. Questo consente di restringere il campo di indagine: basterà provare l'assunto per i numeri primi (sarà, poi, semplice passare al caso generale).

Il secondo passo consiste nel far vedere che per ogni numero primo p esiste un coefficiente m (minore di p) che consente di scrivere il prodotto mp nella forma $x^2 + y^2 + 1$. A questa conclusione si giunge attraverso la considerazione di un insieme R di resti ottenuti dividendo per p i quadrati dei numeri naturali compresi tra 0 e $\frac{p-1}{2}$. Ad R è stato associato un secondo insieme S i cui elementi sono stati ottenuti da quelli di R seguendo una regola ben precisa (da ogni $r \in R$ è stato ottenuto un $s \in S$ tale che $s = p - r - 1$). Osservato che R ed S debbono avere almeno un elemento in comune, si sono potute scrivere le equazioni

$$x^2 = qp + r$$
$$y^2 = q'p + p - r - 1$$

(con x e y numeri compresi tra 0 e $\frac{p-1}{2}$) da cui per addizione si è dedotto $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ con $m = q + q' + 1$.

Il terzo passo consiste nel far vedere che, se m è il più piccolo dei coefficienti da applicare a p perché mp sia scomponibile in somma di quattro quadrati, allora deve essere $m = 1$. Qui è forse necessaria un po' di attenzione in più: non si afferma che l'equazione $mp = x^2 + y^2 + 1$ si può sempre soddisfare con $m = 1$, perché ciò non è vero. L'equazione per la quale il coefficiente minimale vale 1 è:

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

E ciò è ben diverso. Chiariamo con un esempio. Applichiamo il procedimento descritto nella dimostrazione del teorema 2 al caso $p = 13$. Cerchiamo, cioè, i fattori m tali che $1 \le m < 13$ per i quali risulti

$$m \cdot 13 = x^2 + y^2 + 1$$

Abbiamo $\frac{p-1}{2} = 6$, $\frac{p+1}{2} = 7$. I sette quadrati $0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ divisi per 13, danno i resti che compongono l'insieme R:

$$R = \{0, 1, 4, 9, 3, 12, 10\}$$

Conseguentemente l'insieme S è:

$$S = \{12, 11, 8, 3, 9, 0, 2\}$$

e l'insieme degli elementi comuni è:

$$R \cap S = \{0, 9, 3, 12\}$$

Calcoliamo m, x e y per ciascuno degli elementi di $R \cap S$.

1) Per $r = 0$ le equazioni (6) diventano:

$$x^2 = 13q$$
$$y^2 = 13q' + 12$$

dalle quali otteniamo $q = 0$, $x = 0$, $q' = 1$, $y = 5$ e quindi

$$m = 0 + 1 + 1 = 2 \qquad \text{e} \qquad 2 \cdot 13 = 0^2 + 5^2 + 1^2 .$$

2) per $r = 9$, operando analogamente, abbiamo:

$$x^2 = 13q + 9$$
$$y^2 = 13q' + 3$$

che implicano $q = 0$, $x = 3$, $q' = 1$, $y = 4$ e quindi

$$m = 0 + 1 + 1 = 2 \qquad \text{e} \qquad 2 \cdot 13 = 3^2 + 4^2 + 1^2 .$$

3) per $r = 3$ ed $r = 12$, si ottengono gli stessi valori ottenuti per $r = 9$ ed $r = 0$, rispettivamente (a parte lo scambio tra x e y).

Come si vede, il valore $m = 1$ non è stato trovato, ossia non abbiamo scomposto in somma di quattro quadrati il numero primo 13. Ciò è in accordo col fatto, facilmente verificabile, che 13 non si può scrivere nella forma $x^2 + y^2 + 1$ (anche se in tal forma si può scrivere un suo multiplo). In altri termini, l'equazione $13 = x^2 + y^2 + 1$ non ha soluzioni intere. Ma alla scomposizione di 13 possiamo giungere mediante la (9), la quale ci assicura che quando m è pari, come per noi si è verificato, $m/2$ è un coefficiente, minore di m, che, applicato a p, fa sì che il prodotto $(m/2)p$ sia scomponibile in somma di quattro quadrati. Per x_1, x_2, x_3 ed x_4 possiamo prendere i valori ottenuti con i calcoli precedenti, ossia

$x_1 = 5, x_2 = 1, x_3 = 0, x_4 = 0$ (ricavati da $r = 0$), oppure $x_1 = 3, x_2 = 1, x_3 = 4$ $x_4 = 0$ (ricavati da $r = 9$). Nel primo caso otteniamo:

$$\frac{2}{2} \cdot 13 = \left(\frac{5+1}{2}\right)^2 + \left(\frac{5-1}{2}\right)^2 + \left(\frac{0+0}{2}\right)^2 + \left(\frac{0+0}{2}\right)^2$$

ossia

$$13 = 3^2 + 2^2 + 0^2 + 0^2$$

nel secondo:

$$\frac{2}{2} \cdot 13 = \left(\frac{3+1}{2}\right)^2 + \left(\frac{3-1}{2}\right)^2 + \left(\frac{4+0}{2}\right)^2 + \left(\frac{4-0}{2}\right)^2$$

ossia

$$13 = 2^2 + 1^2 + 2^2 + 2^2$$

Riprendiamo il filo della dimostrazione di Lagrange: stavamo dicendo che il coefficiente *minimale m* che rende *mp* scomponibile in somma di quattro quadrati vale 1.

A ciò si giunge facendo vedere che l'ipotesi *m = numero pari* conduce ad un assurdo ed altrettanto accade con l'ipotesi *m = numero dispari maggiore o uguale a tre*. Dunque, non rimane che *m* = 1. E ciò equivale ad affermare che ogni numero primo è scomponibile nel modo che ci interessa.

L'ultimo passo è semplice: ogni numero naturale è scomponibile, ed in unico modo, in prodotto di fattori primi e l'applicazione del teorema 1 porta rapidamente alla conclusione.

CINEMATICA E SEZIONE AUREA

Una "storia semplice", sorprendentemente complessa

La sezione aurea è uno degli argomenti di matematica che da sempre ha affascinato gli studiosi, matematici e non, per la bellezza degli oggetti in cui è riscontrabile e per gli stupefacenti aspetti numerici legati ad essa.

Si ricorda la definizione riportata dai manuali di geometria:

"***La sezione, o parte aurea, di un segmento è il segmento medio proporzionale tra tutto il segmento e la parte rimanente***".

Detta L la lunghezza di un segmento e x la lunghezza della sua parte aurea si imposta la proporzione:

$$L : x = x : (L - x)$$

da cui si ottiene l'equazione $x^2 = L\,(L - x)$,

la cui soluzione positiva $$x = \frac{\sqrt{5} - 1}{2} L$$

individua il numero (irrazionale algebrico) legato alla sezione aurea.

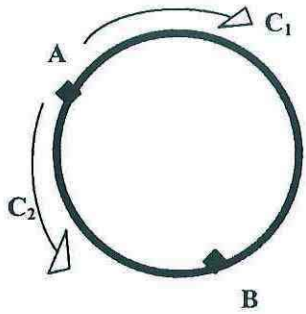
Tale particolare numero ricorre con frequenza incredibile in natura e in numerosi manufatti umani, ovunque si riconosca la bellezza che deriva dall'armonia delle proporzioni ed è una dimostrazione meravigliosa che l'uomo creatore e la natura si servono degli stessi strumenti, nel creare le forme, per arrivare alla bellezza.
La sezione aurea si ritrova nell'architettura, nella scultura, nella pittura, nella musica, ma prima nei fiori, nei rami degli alberi, nei crostacei, nelle conchiglie.
Dalla "De divina proportione" di Luca Pacioli in poi, vastissima è la letteratura sulla sezione aurea, svariati gli ambiti in cui essa è coinvolta, ...perfino nel gioco delle carte, vedi "***I numeri d'oro dal Partenone al bridge***", (articolo di Gaetano Corleo, pubblicato su Lettera Pristem).

Anche la fisica non sfugge a tale coinvolgimento, si pensi alla scienza delle vibrazioni e allo studio dei suoni.

Scopo del presente lavoro è quello di evidenziare che anche in cinematica la sezione aurea si intreccia sorprendentemente con i moti più semplici: il moto uniforme e il moto uniformemente accelerato.

A tal fine si propone il seguente ***problema***:

Su una pista circolare di lunghezza L due ciclisti partono in verso opposto dal medesimo punto A. Il primo ciclista procede con velocità costante in modulo, mentre il secondo viaggia di moto circolare uniformemente accelerato, partendo da fermo.



Sapendo che i due ciclisti s'incontrano la prima volta in un punto B della pista e la seconda volta nel punto A da cui sono partiti, quant'è lungo il tratto AB percorso dal primo ciclista al momento del primo incontro?

oooooooooo

Soluzione

Detti: V_1 la velocità costante (in modulo) del primo ciclista;

T il tempo costante (periodo) impiegato dal primo ciclista per percorrere ogni giro completo;

a l'accelerazione costante (in modulo) del secondo ciclista,

affinchè i due percorrano lo stesso giro nello stesso tempo, deve essere:

per il primo ciclista $L = V_1 T$

per il secondo $L = \frac{1}{2} a T^2$ da cui $a = \frac{V_1^2}{L}$ (1) .

Indicati con x_1 e x_2 gli spazi percorsi dai due al generico tempo t,

essendo $x_1 = V_1 t$,

utilizzando la (*1*) si ottiene:

$$x_2 = \frac{1}{2}at^2 = \frac{1}{2}\left(\frac{2V_1^2}{L}\right)t^2 = \frac{(V_1 t)^2}{L} = \frac{x_1^2}{L}.$$

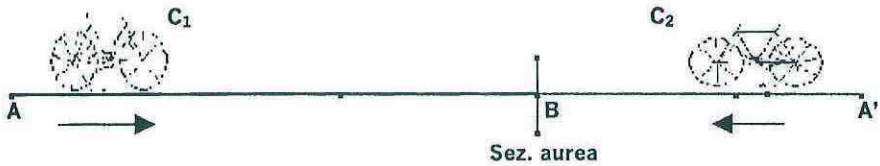
Affinché i due ciclisti si incontrino in B deve essere $x_1 + x_2 = L$

ovvero $x_1 + \frac{x_1^2}{L} = L$ pertanto $x_1^2 + Lx_1 - L^2 = 0$

da cui $x_{11} = \frac{-1-\sqrt{5}}{2}L$ e $x_{12} = \frac{-1+\sqrt{5}}{2}L$

Considerata la soluzione positiva si osserva che lo spazio percorso dal primo ciclista al momento del primo incontro in B, con il secondo ciclista, è pari alla parte aurea della lunghezza L della pista, e poiché lo spazio percorso dal primo ciclista è proporzionale al tempo (viaggia di moto uniforme), anche il tempo t necessario per il primo incontro sarà la parte aurea del periodo T per percorrere un giro completo.

Relativamente al primo giro il problema si può semplificare considerando i due ciclisti che si muovano sopra un segmento, pari alla circonferenza rettificata, in senso inverso percorrendo lo stesso spazio L nello stesso tempo T, il primo di moto uniforme e il secondo di moto naturalmente accelerato.

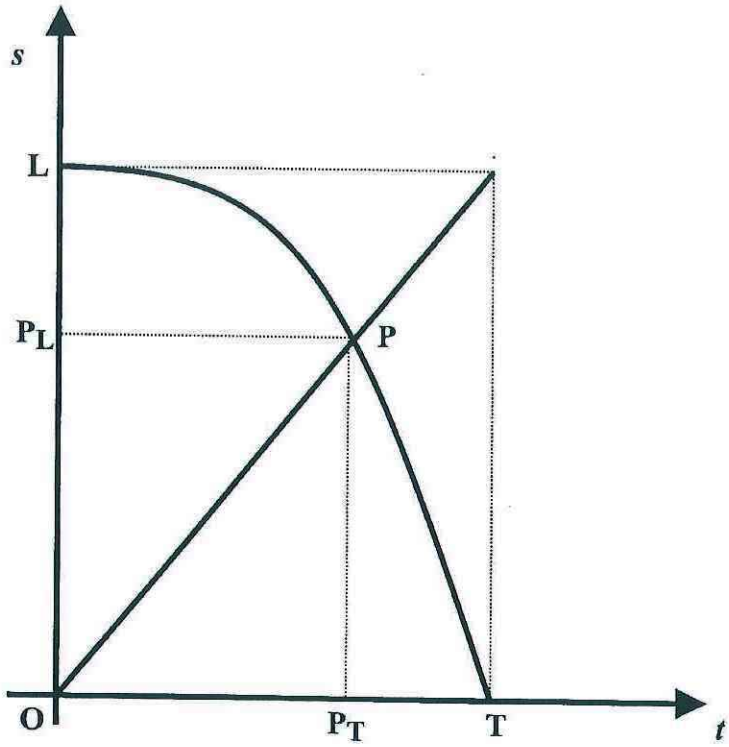


I due ciclisti si incontrano nel punto B, che a partire da A, individua la parte aurea della lunghezza L segmento.

L'INTERPRETAZIONE GRAFICA

Dal punto di vista grafico il problema presenta un'interessante particolarità, infatti, se si rappresentano nello stesso piano cartesiano **sOt** le leggi orarie dei moti descritti dai due ciclisti, assumendo A come punto di riferimento per gli spazi e positivo il verso del moto del primo ciclista, si ha:

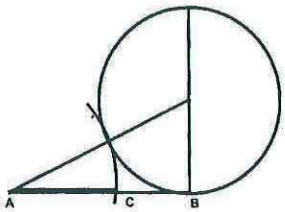
$$x_1 = V_1 t \qquad \text{e} \qquad x_2 = -\tfrac{1}{2} a t^2 + L$$



La retta, rappresentante il moto uniforme, e la parabola, rappresentante il moto uniformemente accelerato, si incontrano in un punto **P** le cui coordinate sono rispettivamente la parte aurea di ***T*** e di ***L***.

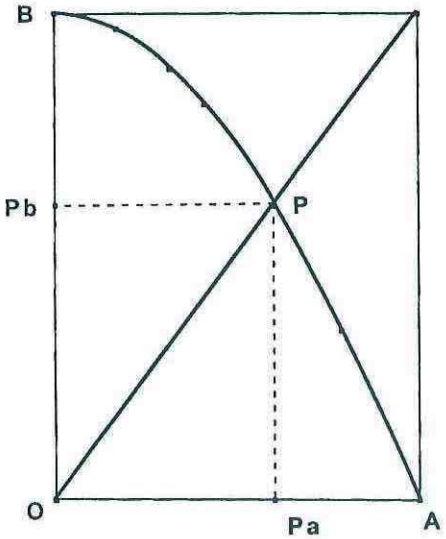
CONSEGUENZE

Sono note diverse costruzioni geometriche per la determinazione della parte aurea di un segmento, tra esse quella sotto riportata.



Ora i risultati precedentemente ottenuti consentono la risoluzione del seguente problema geometrico:

"Dati due segmenti OA e OB, di lunghezza rispettiva a e b, determinare un procedimento grafico per determinare contestualmente la parte aurea di ciascuno di essi".

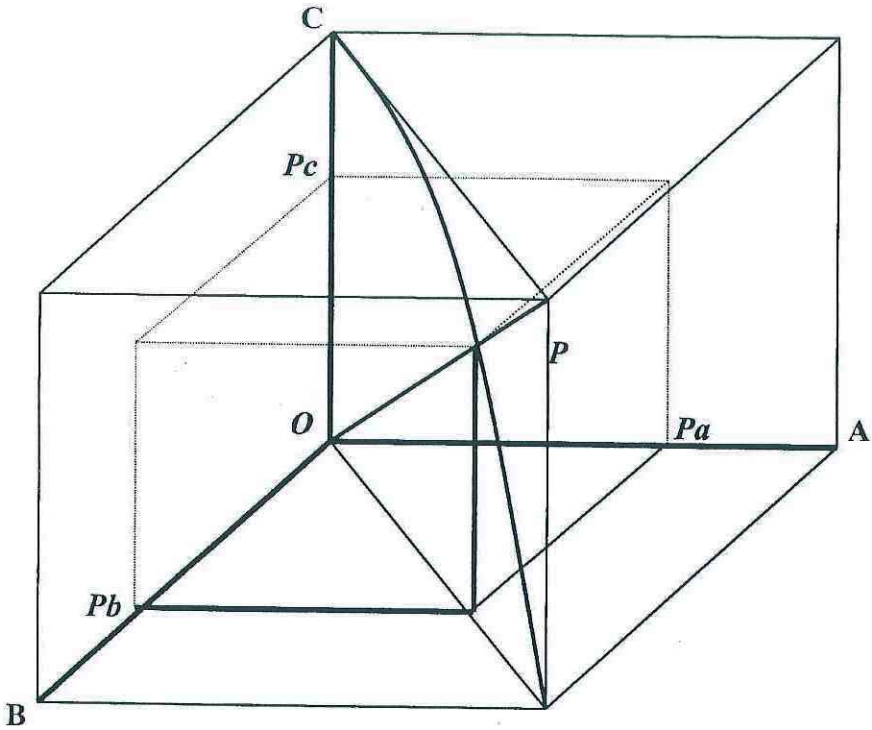


Costruzione

Nel rettangolo di lati ***a*** e ***b*** si inscriva l'arco di parabola avente il vertice coincidente con uno dei vertici del rettangolo e passante per il vertice opposto, la diagonale passante per gli altri due vertici incontrerà l'arco di parabola in un punto P.

Le proiezioni di P sui lati del rettangolo individuano su questi la parte aurea di ciascuno di essi.

La costruzione è estensibile anche a tre segmenti



$x_1 + x_2 = L,\ 2L,\ 3L\ \ldots,$ in generale $x_1 + x_2 = k\,L$ con $k \in N$.

Per le considerazioni fatte precedentemente deve verificarsi:

$$x_1 + \frac{x_1^2}{L} = kL \qquad \text{da cui} \qquad x_1^2 + Lx_1 - kL^2 = 0$$

Le soluzioni sono:

$$x_{11} = \frac{-1-\sqrt{1+4k}}{2}L \qquad \text{e} \qquad x_{12} = \frac{-1+\sqrt{1+4k}}{2}L\,.$$

Considerando la soluzione positiva x_{12}, si osserva che la quantità $1 + 4k$, al variare di $k \in N$ genera una progressione aritmetica di numeri dispari di ragione 4.
Il termine generico, $1 + 4k$, di tale progressione è un quadrato perfetto di un numero (ovviamente) dispari se è verificata la condizione:

$$1 + 4k = (2n + 1)^2 \qquad \text{con} \qquad n \in N$$

da ciò segue $k = n^2 + n$

ovvero $k = n(n+1)$ prodotto di due naturali consecutivi.

In corrispondenza di tali valori di k, la x_{12} fornisce tutti i valori interi di L e quindi i due ciclisti si incontreranno in **A.**

In particolare

posto $k_n = n(n+1)$, per ogni $n \in N$ si avrà,

$$x_{12} = \frac{-1+\sqrt{1+4k_n}}{2} L = nL \cdot$$

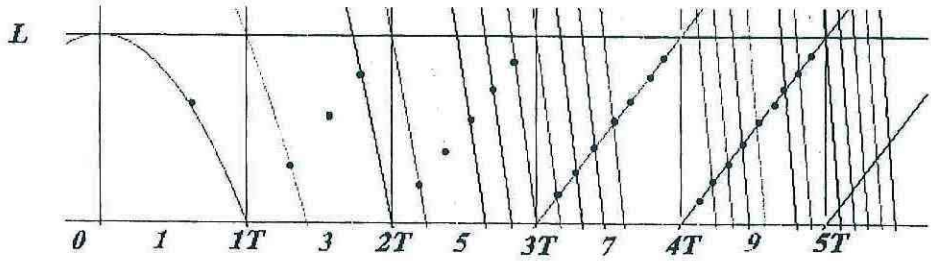
Ciò conferma che i due ciclisti si incontrano in A per ogni multiplo del periodo T

Per altri valori di $k \neq n^2 + n$ i due ciclisti si incontreranno in punti diversi da A e il numero di questi incontri è sempre più elevato visto che il secondo ciclista viaggia con velocità sempre crescente.

Si verifica inoltre che il numero degli incontri intermedi che avvengono in punti diversi da A segue la successione dei numeri dispari: 1, 3, 5, 7, 9,.....altra sorpresa!

Rappresentazione grafica del problema con Derive

Quanto ricavato algebricamente è possibile rappresentarlo graficamente con Derive.
Risultano evidenti gli incontri dei due ciclisti nel punto di partenza A e gli altri incontri nei punti diversi da A.

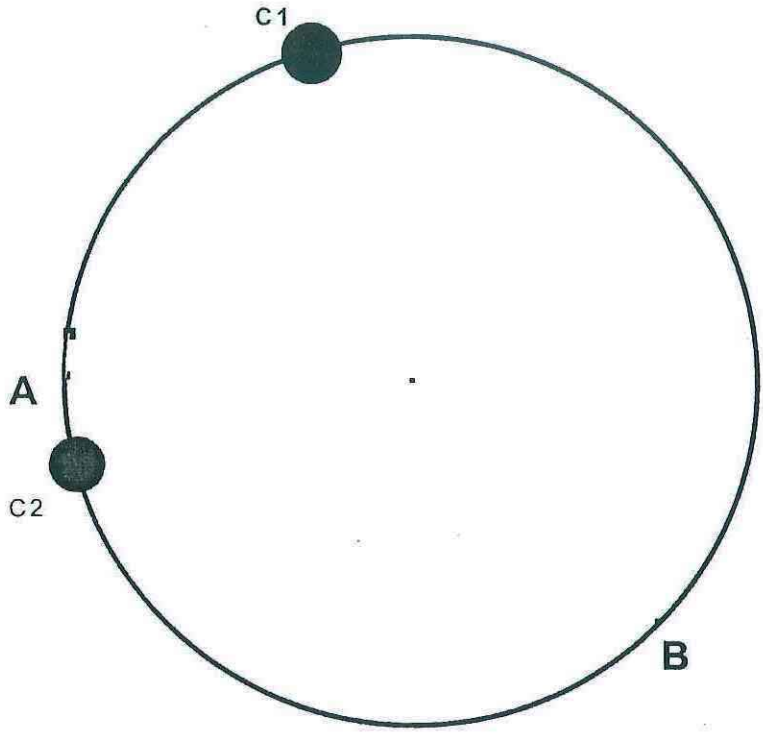


Analisi numerica con Excel

Utilizzando il foglio di calcolo, è possibile valutare numericamente le distanze dei successivi punti di incontro dal punto di partenza. I risultati sono in perfetto accordo con la rappresentazione grafica e con quanto previsto teoricamente.
Si osserva che per i valori di k =2, 6, 12, 20, ... n(n+1) i due ciclisti si incontrano in A (x_{12} = multipli interi di L).

k	$\frac{-1+\sqrt{1+4k}}{2}$	*n° giri intermedi*
1	0,618033989	1
2	1	
3	1,302775638	
4	1,561552813	3
5	1,791287847	
6	2	
7	2,192582404	
8	2,372281323	
9	2,541381265	5
10	2,701562119	
11	2,854101966	
12	3	
13	3,140054945	
14	3,274917218	
15	3,405124838	
16	3,531128874	7
17	3,653311931	
18	3,772001873	
19	3,887482194	
20	4	
21	4,109772229	

Il problema interpretato con Cabri géomètre



Il sw didattico Cabri géomètre consente la simulazione del problema con la relativa suggestiva animazione.

Interpretazione grafica delle soluzioni negative

Dell'equazione $x_1^2 + Lx_1 - kL^2 = 0$

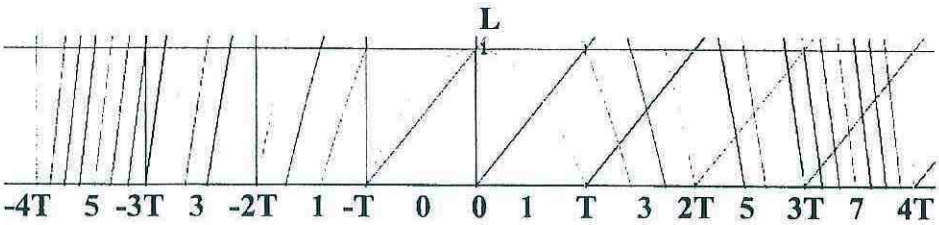
è stata considerata soltanto la soluzione positiva

$$x_{12} = \frac{-1+\sqrt{1+4k}}{2} L,$$

qual è il significato fisico e geometrico della soluzione negativa

$$x_{11} = \frac{-1-\sqrt{1+4k}}{2} L \quad ?$$

la risposta si ottiene dall'analisi del grafico precedente, per valori di t < 0



si osserva che per t < 0 i due ciclisti viaggiano nello stesso verso, per ogni periodo T si incontrano in A e gli incontri intermedi seguono la stessa legge determinata per t > 0.

Conclusioni

L'argomento, proponibile agli studenti di una terza classe secondaria superiore, offre una grande varietà di spunti didattici e in diversi ambiti, infatti al "fatto" fisico, si intrecciano, in modo coerente e convergente, cinematica, sezione aurea, geometria analitica, calcolo numerico e. . . altro, fornendo del problema una visione unitaria e armonica.
L'utilizzo dello strumento informatico arricchisce la trattazione permettendo una chiara e veloce rappresentazione degli aspetti grafici, numerici e dinamici.

CARMELO ARENA
Relazione tenuta al Convegno di Didattica della Matematica
Piazza Armerina, 2004