

Somma di quattro quadrati

Stefano Maragnoli e Ilaria Dorigatti

Seminario di Algebra

Il problema di Waring

Waring si domandò se

Il problema di Waring

Waring si domandò se

dato un numero k naturale
esiste un numero s dipendente da k ,

Il problema di Waring

Waring si domandò se

dato un numero k naturale
esiste un numero s dipendente da k ,

tale che *tutti* i numeri naturali n si possano
scrivere come somma di s potenze k -esime.

Ovvero:

Il problema di Waring

Waring si domandò se

dato un numero k naturale
esiste un numero s dipendente da k ,

tale che *tutti* i numeri naturali n si possano
scrivere come

$$n = x_1^k + x_2^k + \cdots + x_s^k$$

I numeri $G(k)$ e $g(k)$

Definiamo

I numeri $G(k)$ e $g(k)$

Definiamo

$$g(k)$$

I numeri $G(k)$ e $g(k)$

Definiamo

$g(k)$ come il valore minimo di s per il quale *tutti* i numeri sono rappresentabili con s potenze k -esime

I numeri $G(k)$ e $g(k)$

Definiamo

$g(k)$ come il valore minimo di s per il quale *tutti* i numeri sono rappresentabili con s potenze k -esime

... e $G(k)$

I numeri $G(k)$ e $g(k)$

Definiamo

$g(k)$ come il valore minimo di s per il quale *tutti* i numeri sono rappresentabili con s potenze k -esime

... e $G(k)$ come il valore minimo di s per il quale *quasi tutti i numeri* (cioè tutti tranne un numero finito) sono rappresentabili con s potenze k -esime

I numeri $G(k)$ e $g(k)$

Definiamo

$g(k)$ come il valore minimo di s per il quale *tutti* i numeri sono rappresentabili con s potenze k -esime

... e $G(k)$ come il valore minimo di s per il quale *quasi tutti* i numeri sono rappresentabili con s potenze k -esime

I numeri $G(k)$ e $g(k)$

Definiamo

$g(k)$ come il valore minimo di s per il quale *tutti* i numeri sono rappresentabili con s potenze k -esime

... e $G(k)$ come il valore minimo di s per il quale *quasi tutti* i numeri sono rappresentabili con s potenze k -esime

$$G(k) \leq g(k)$$

Il *nostro* problema

Vogliamo dimostrare che

Il *nostro* problema

Vogliamo dimostrare che

ogni intero positivo è somma di 4 quadrati.

Il *nostro* problema

Vogliamo dimostrare che

ogni intero positivo è somma di 4 quadrati.

Ovvero:

Il *nostro* problema

Vogliamo dimostrare che

ogni intero positivo è somma di 4 quadrati.

Ovvero:

$$g(2) = 4$$

OSSERVAZIONE:

OSSERVAZIONE:

$$(a^2 + b^2 + c^2 + d^2) \cdot (\alpha^2 + \beta^2 + \gamma^2 + \delta^2) =$$

OSSERVAZIONE:

$$(a^2 + b^2 + c^2 + d^2) \cdot (\alpha^2 + \beta^2 + \gamma^2 + \delta^2) =$$

= semplici calcoli algebrici =

OSSERVAZIONE:

$$\begin{aligned} & (a^2 + b^2 + c^2 + d^2) \cdot (\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = \\ & \quad = \text{semplici calcoli algebrici} = \\ & = (a\alpha + b\beta + c\gamma + d\delta)^2 + (a\beta - b\alpha + c\delta - d\gamma)^2 + \\ & \quad + (a\gamma - c\alpha + b\delta - d\beta)^2 + (a\delta - d\alpha + b\gamma - c\beta)^2 \end{aligned}$$

Dunque

$$(a^2 + b^2 + c^2 + d^2) \cdot (\alpha^2 + \beta^2 + \gamma^2 + \delta^2) =$$

Dunque

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2) \cdot (\alpha^2 + \beta^2 + \gamma^2 + \delta^2) &= \\ &= A^2 + B^2 + C^2 + D^2\end{aligned}$$

con $A, B, C, D \in \mathbf{Z}$

Nel corso di Algebra abbiamo dimostrato che

Nel corso di Algebra abbiamo dimostrato che
il prodotto di due numeri esprimibili come
somma di due quadrati è anch'esso
somma di due quadrati

Nel corso di Algebra abbiamo dimostrato che

il prodotto di due numeri esprimibili come
somma di due quadrati è anch'esso
somma di due quadrati

sfruttando il fatto che la norma di un intero di
Gauss è somma di due quadrati:

$$\|a + ib\| = a^2 + b^2 \quad \text{in } \mathbf{Z}[i]$$

Analogamente potevamo sfruttare il fatto che nel corpo degli *ipercomplessi*

Analogamente potevamo sfruttare il fatto che nel corpo degli *ipercomplessi*

la norma di un *quaternione* è
somma di quattro quadrati:

Analogamente potevamo sfruttare il fatto che nel corpo degli *ipercomplessi*

la norma di un *quaternione* è
somma di quattro quadrati:

$$\|q\| = \|a + ib + jc + kd\| = a^2 + b^2 + c^2 + d^2$$

OSSERVAZIONE

OSSERVAZIONE

+



OSSERVAZIONE
+
TEOREMA FONDAMENTALE
DELL' ARITMETICA

OSSERVAZIONE
+
TEOREMA FONDAMENTALE
DELL' ARITMETICA



OSSERVAZIONE
+
TEOREMA FONDAMENTALE
DELL' ARITMETICA



Ci basta dimostrare che

OSSERVAZIONE
+
TEOREMA FONDAMENTALE
DELL' ARITMETICA



Ci basta dimostrare che
*Ogni numero **primo** è somma di 4 quadrati.*

Le dimostrazioni

La dimostrazione che daremo si basa sul seguente

Le dimostrazioni

La dimostrazione che daremo si basa sul seguente

Lemma: Sia p un numero primo.
Allora esistono interi x, y che soddisfano la seguente relazione:

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

Le dimostrazioni

La dimostrazione che daremo si basa sul seguente

Lemma: Sia p un numero primo.
Allora esistono interi x, y che soddisfano la seguente relazione:

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

Notare che il caso $p = 2$ è banale: $2 = 1^2 + 1^2 + 0^2 + 0^2$

Dunque, poiché p è primo, è dispari.

Le dimostrazioni

Dimostrazione:

Poiché gli elementi non nulli in $\mathbf{Z}/p\mathbf{Z}$, con p primo, sono $p - 1$ e

Le dimostrazioni

Dimostrazione:

Poiché gli elementi non nulli in $\mathbf{Z}/p\mathbf{Z}$, con p primo, sono $p - 1$ e

$$a^2 = (-a)^2,$$

Le dimostrazioni

Dimostrazione:

Poiché gli elementi non nulli in $\mathbf{Z}/p\mathbf{Z}$, con p primo, sono $p - 1$ e

$$a^2 = (-a)^2,$$

i quadrati non nulli sono

$$\frac{p - 1}{2}$$

Le dimostrazioni

Ma $0^2 = 0 \Rightarrow$ anche 0 è un quadrato.

Le dimostrazioni

Ma $0^2 = 0 \Rightarrow$ anche 0 è un quadrato.
I quadrati in $\mathbf{Z}/p\mathbf{Z}$ sono dunque

$$\frac{p-1}{2} + 1 = \frac{p+1}{2}$$

Le dimostrazioni

Ma $0^2 = 0 \Rightarrow$ anche 0 è un quadrato.
I quadrati in $\mathbf{Z}/p\mathbf{Z}$ sono dunque

$$\frac{p-1}{2} + 1 = \frac{p+1}{2}$$

Considero ora i seguenti insiemi:

Le dimostrazioni

Ma $0^2 = 0 \Rightarrow$ anche 0 è un quadrato.
I quadrati in $\mathbf{Z}/p\mathbf{Z}$ sono dunque

$$\frac{p-1}{2} + 1 = \frac{p+1}{2}$$

Considero ora i seguenti insiemi:

$$S = \{\text{quadrati modulo } p\} = \{y^2 : y \in \mathbf{Z}/p\mathbf{Z}\}$$

Le dimostrazioni

Ma $0^2 = 0 \Rightarrow$ anche 0 è un quadrato.
I quadrati in $\mathbf{Z}/p\mathbf{Z}$ sono dunque

$$\frac{p-1}{2} + 1 = \frac{p+1}{2}$$

Considero ora i seguenti insiemi:

$$S = \{\text{quadrati modulo } p\} = \{y^2 : y \in \mathbf{Z}/p\mathbf{Z}\}$$

$$S' = \{-1 - x^2 : x^2 \in S\}$$

Le dimostrazioni

Poiché

$$S = \{ y^2 : y \in \mathbf{Z}/p\mathbf{Z} \}$$
$$S' = \{ -1 - x^2 : x^2 \in S \}$$

hanno lo stesso numero di elementi,

Le dimostrazioni

Poiché

$$S = \{ y^2 : y \in \mathbf{Z}/p\mathbf{Z} \}$$
$$S' = \{ -1 - x^2 : x^2 \in S \}$$

hanno lo stesso numero di elementi, che è *maggiore* della metà del numero di elementi di $\mathbf{Z}/p\mathbf{Z}$,

Le dimostrazioni

Poiché

$$S = \{ y^2 : y \in \mathbf{Z}/p\mathbf{Z} \}$$
$$S' = \{ -1 - x^2 : x^2 \in S \}$$

hanno lo stesso numero di elementi, che è *maggiore* della metà del numero di elementi di $\mathbf{Z}/p\mathbf{Z}$, allora esistono interi x ed y per i quali sussiste la congruenza:

Le dimostrazioni

Poiché

$$S = \{ y^2 : y \in \mathbf{Z}/p\mathbf{Z} \}$$
$$S' = \{ -1 - x^2 : x^2 \in S \}$$

hanno lo stesso numero di elementi, che è *maggiore* della metà del numero di elementi di $\mathbf{Z}/p\mathbf{Z}$, allora esistono interi x ed y per i quali sussiste la congruenza:

$$y^2 = -1 - x^2 \pmod{p} \Leftrightarrow x^2 + y^2 + 1 \equiv 0 \pmod{p}.$$

Le dimostrazioni

Poiché

$$S = \{ y^2 : y \in \mathbf{Z}/p\mathbf{Z} \}$$
$$S' = \{ -1 - x^2 : x^2 \in S \}$$

hanno lo stesso numero di elementi, che è *maggiore* della metà del numero di elementi di $\mathbf{Z}/p\mathbf{Z}$, allora esistono interi x ed y per i quali sussiste la congruenza:

$$y^2 = -1 - x^2 \pmod{p} \Leftrightarrow x^2 + y^2 + 1 \equiv 0 \pmod{p}.$$

□

Le dimostrazioni

Noi dimostreremo il teorema utilizzando il

Le dimostrazioni

Noi dimostreremo il teorema utilizzando il
metodo della discesa infinita

Le dimostrazioni

Noi dimostreremo il teorema utilizzando il

metodo della discesa infinita

dovuto a Fermat.

Le dimostrazioni

Noi dimostreremo il teorema utilizzando il

metodo della discesa infinita

dovuto a Fermat.

Esistono tuttavia altre dimostrazioni...

Le dimostrazioni

Noi dimostreremo il teorema utilizzando il

metodo della discesa infinita

dovuto a Fermat.

Esistono tuttavia altre dimostrazioni...

- una è basata sull'algebra dei quaternioni

Le dimostrazioni

Noi dimostreremo il teorema utilizzando il

metodo della discesa infinita

dovuto a Fermat.

Esistono tuttavia altre dimostrazioni...

- una è basata sull'algebra dei quaternioni
- una è basata sulla dimostrazione data da Eulero.

La discesa infinita

Si tratta di dimostrare il seguente lemma:

La discesa infinita

Si tratta di dimostrare il seguente lemma:

Supponiamo che per un primo p esista un intero m t.c.

La discesa infinita

Si tratta di dimostrare il seguente lemma:

Supponiamo che per un primo p esista un intero m t.c. $1 < m < p$ e $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

La discesa infinita

Si tratta di dimostrare il seguente lemma:

Supponiamo che per un primo p esista un intero m t.c. $1 < m < p$ e $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Allora esiste un intero n , $0 < n < m$ t.c.

La discesa infinita

Si tratta di dimostrare il seguente lemma:

Supponiamo che per un primo p esista un intero m t.c. $1 < m < p$ e $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Allora esiste un intero n , $0 < n < m$ t.c.

$$np = y_1^2 + y_2^2 + y_3^2 + y_4^2.$$

La discesa infinita

Si tratta di dimostrare il seguente lemma:

Supponiamo che per un primo p esista un intero m t.c. $1 < m < p$ e $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Allora esiste un intero n , $0 < n < m$ t.c.

$$np = y_1^2 + y_2^2 + y_3^2 + y_4^2.$$

Da ciò si deduce che p stesso è somma di quattro quadrati.

La discesa infinita

Dimostrazione:

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

La discesa infinita

Dimostrazione:

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

Pongo $y_i \equiv x_i \pmod{m}$,

La discesa infinita

Dimostrazione:

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

Pongo $y_i \equiv x_i \pmod{m}$, con $y_i \in \mathbf{Z}$ e
 $-\frac{m}{2} < y_i \leq \frac{m}{2} \quad i = 1, \dots, 4.$

La discesa infinita

Dimostrazione:

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

Pongo $y_i \equiv x_i \pmod{m}$, con $y_i \in \mathbf{Z}$ e
 $-\frac{m}{2} < y_i \leq \frac{m}{2} \quad i = 1, \dots, 4.$

Allora $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m}$

La discesa infinita

Dimostrazione:

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

Pongo $y_i \equiv x_i \pmod{m}$, con $y_i \in \mathbf{Z}$ e
 $-\frac{m}{2} < y_i \leq \frac{m}{2} \quad i = 1, \dots, 4.$

Allora $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m}$

$\Rightarrow \exists r \in \mathbf{Z}, r \geq 0$ t.c. $rm = y_1^2 + y_2^2 + y_3^2 + y_4^2.$

La discesa infinita

Affermiamo che

La discesa infinita

Affermiamo che

$$r \neq 0 \text{ e } r \neq m$$

La discesa infinita

Affermiamo che

$$r \neq 0 \text{ e } r \neq m$$

Altrimenti otteniamo la seguente contraddizione:

La discesa infinita

Affermiamo che

$$r \neq 0 \text{ e } r \neq m$$

Altrimenti otteniamo la seguente contraddizione:

$$m \mid p, \text{ ove } p \text{ è un numero primo e } 1 < m < p$$

La discesa infinita

Ricapitolando abbiamo:

La discesa infinita

Ricapitolando abbiamo:

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

$$rm = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

La discesa infinita

Ricapitolando abbiamo:

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

$$rm = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

Moltiplicando mp e rm ottengo

La discesa infinita

Ricapitolando abbiamo:

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

$$rm = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

Moltiplicando mp e rm ottengo

$$\begin{aligned} m^2rp = & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + \\ & + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ & + (x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2)^2 + \\ & + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2 \end{aligned}$$

La discesa infinita

Ogni termine alla destra dell'uguale

La discesa infinita

Ogni termine alla destra dell'uguale

$$\begin{aligned}m^2rp = & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + \\ & + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ & + (x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2)^2 + \\ & + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2\end{aligned}$$

La discesa infinita

Ogni termine alla destra dell'uguale è

divisibile per m^2

La discesa infinita

Ogni termine alla destra dell'uguale è

divisibile per m^2

poiché $y_i \equiv x_i \pmod{m}$, $i = 1, \dots, 4$.

La discesa infinita

Ogni termine alla destra dell'uguale è

divisibile per m^2

poiché $y_i \equiv x_i \pmod{m}$, $i = 1, \dots, 4$.

Dunque ...

La discesa infinita

Ogni termine alla destra dell'uguale è

divisibile per m^2

poiché $y_i \equiv x_i \pmod{m}$, $i = 1, \dots, 4$.

Dunque ...

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

La discesa infinita

Ogni termine alla destra dell'uguale è

divisibile per m^2

poiché $y_i \equiv x_i \pmod{m}$, $i = 1, \dots, 4$.

Dunque ...

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

con $0 < r < m$ e $a, b, c, d \in \mathbf{Z}$.

La discesa infinita

Ogni termine alla destra dell'uguale è

divisibile per m^2

poiché $y_i \equiv x_i \pmod{m}$, $i = 1, \dots, 4$.

Dunque ...

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

con $0 < r < m$ e $a, b, c, d \in \mathbf{Z}$.



Un po' di storia...

Nel 1621 *Bachet* afferma senza dimostrarlo che

“ogni intero positivo è
somma di quattro quadrati”.

Bachet



Un po' di storia...

Nel 1770 *Waring* fa la stessa osservazione di Bachet in *Meditationes algebraicae*.

Waring



Un po' di storia...

Più tardi lo stesso anno *Lagrange* prova che

$$g(2) = 4.$$

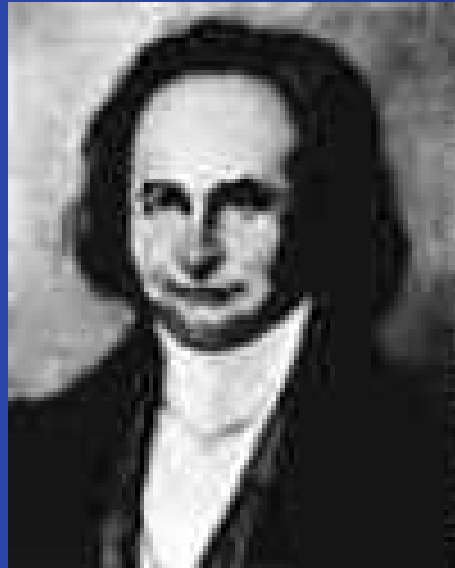
Lagrange



Un po' di storia...

Nel 1834 *Jacobi* dà una semplice formula per il numero totale di rappresentazioni di un intero come somma di quattro quadrati.

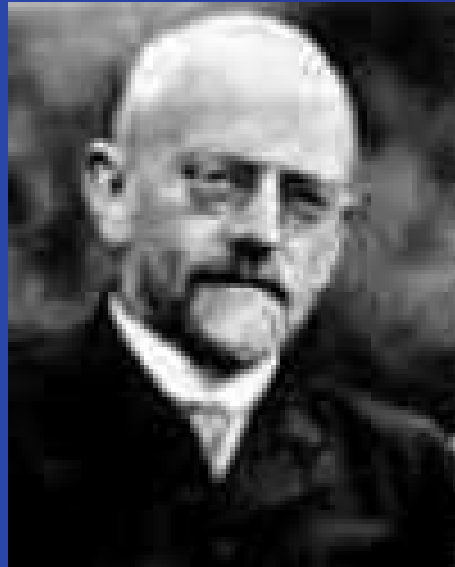
Jacobi



Un po' di storia...

Nel 1909 *Hilbert* dimostra
l'esistenza di $g(k)$ per ogni k .

Hilbert



Un po' di storia...

...e chi vuole saperne di più ...

Un po' di storia...

... e chi vuole saperne di più ...

può trovare un esaustivo resoconto della
“vicenda” dei quattro quadrati in:

Un po' di storia...

... e chi vuole saperne di più ...

può trovare un esaustivo resoconto della
“vicenda” dei quattro quadrati in:

Leonard Eugene Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966, Cap. VIII