Problemi di Aritmetica e di determinazione di radici di equazioni algebriche mediante risultati elementari di Teoria degli Insiemi e di Algebra Lineare

Francesco Russo

DMI–Unict, Catania
20 maggio 2021

Numeri primi somma di due quadrati

Teorema (Fermat 1630, Gauss 1798; Corso di Algebra, primo anno)

Sia $p \geq 2$ un numero primo. Sono condizioni equivalenti:

(I) $p = 2$ *oppure* $p = 4r + 1$ *per qualche* $r \in \mathbb{N}$;

(II) $p = a^2 + b^2$ *con* $a, b \in \mathbb{N}$;

(III) $p = a^2 + b^2$ *con* $a, b \in \mathbb{Q}$.

Godfrey Hardy nel suo libro *Apologia di un matematico* annovera questo risultato tra i più interessanti fino ad allora ottenuti in Matematica. Aggiunge anche che una sua dimostrazione non sia di facile comprensione per un principiante.
La dimostrazione che vedremo, come altre più recenti, non erano note a Hardy. Queste dimostrazioni sembrano essere alla portata anche di chi si stia avvicinando agli studi matematici e mostrano come l' approccio non costruttivo (*mostrare l' esistenza di una soluzione senza determinarla*) possa rivelarsi particolarmente interessante.

Numeri primi somma di due quadrati

Se $p = 2$, allora $2 = 1^2 + 1^2$ è somma di due quadrati. D'ora in poi supporremo che il numero primo p sia > 2.

$$a = 4r + s \Rightarrow a^2 = 4r' + s^2 = 4r'' + s', \quad s' \in \{0, 1\}.$$

$$b = 4t + u \Rightarrow b^2 = 4t' + u^2 = 4t'' + u', \quad u' \in \{0, 1\}.$$

$$\Rightarrow a^2 + b^2 = 4c + d, \quad d \in \{0, 1, 2\}.$$

In conclusione se p è un numero primo e se:

$$p = a^2 + b^2 > 2, \quad a, b \in \mathbb{N} \Rightarrow p = 4r + 1$$

Quindi l'implicazione rilevante è assumere $p = 4r + 1$ e provare che $p = a^2 + b^2$.

Una dimostrazione NON *costruttiva*

Sia S un insieme finito e sia $F : S \to S$ una involuzione, i.e. una funzione tale che

$$F(F(s)) = s \text{ per ogni } s \in S.$$

L'insieme S si divide in due sottoinsiemi disgiunti

$$Fix(F) = \{s \in S \text{ tali che } s = F(s)\} \text{ detti } \textit{elementi fissi di } F$$

e

$$S \setminus Fix(F) = \{s \in S \text{ tali che } s \neq F(s)\}.$$

F involuzione $\Rightarrow S$ **e** $Fix(F)$ **hanno la stessa parità perche'**
$\#(S \setminus Fix(F)) = 2r$.
In particolare,

$$\#(S) \textbf{ DISPARI implica } Fix(F) \neq \emptyset.$$

Involuzioni su $S = \{(x, y, z) \in \mathbb{N}^3$ tali che $x^2 + 4yz = p\}$ con $p = 4r + 1$

Sia $p = 4r + 1$ e sia

$$(1, 1, r) \in S = \{(x, y, z) \in \mathbb{N}^3 \text{ tali che } x^2 + 4yz = p = 4r + 1\}.$$

$F : S \to S$ definita da $F(x, y, z) = (x, z, y)$ è una involuzione :

$$F(F(x, y, z)) = F(x, z, y) = (x, y, z).$$

Se mostriamo che $Fix(F) \neq \emptyset$, avremo che esiste

$$(x, y, y) \in Fix(F) \subseteq S$$

$$\Rightarrow p = x^2 + 4y^2 = x^2 + (2y)^2.$$

É quindi sufficiente dimostrare $\#(S)$ dispari

Involuzione di Zagier su S

$S = \{(x,y,z) \in \mathbb{N}^3 \text{ tali che } x^2 + 4yz = p = 4r+1\} = S_1 \cup S_2 \cup S_3$
$S_1 = \{(x,y,z) \in \mathbb{N}^3 \text{ tali che } x < y - z\}$;
$S_2 = \{(x,y,z) \in \mathbb{N}^3 \text{ tali che } y - z < x < 2y\}$;
$S_3 = \{(x,y,z) \in \mathbb{N}^3 \text{ tali che } x > 2y\}$.

Sia $G : S \to S$ l'involuzione definita da

$$(x,y,z) \mapsto \begin{cases} (x+2z, z, y-x-z) & \text{if } x < y-z \\ (2y-x, y, x-y+z) & \text{if } y-z < x < 2y \\ (x-2y, x-y+z, y) & \text{if } x > 2y \end{cases}$$

Si verifica che $G(S_1) = S_3$, $G(S_2) = S_2$ (e quindi $G(S_3) = S_1$)

$\Rightarrow Fix(G) = \{(x,y,z) \in S_2 \ : \ (x,y,z) = (2y-x, y, x-y+z)\} \Rightarrow x = y.$

$x(x+4z) = p \Rightarrow 1 = x = y \Rightarrow Fix(G) = (1,1,r) \Rightarrow \#(S)$ **DISPARI**.

Radici reali di un polinomio (monico) $f(x) \in \mathbb{R}[x]$

Sia $f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ e sia $\sigma \in S_n$ una permutazione.

$$(\sigma \cdot f)(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Definizione polinomio simmetrico

$f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ *si dice* **simmetrico** *se*

$$\sigma \cdot f = f \quad \forall \sigma \in S_n.$$

Esempi (polinomi simmetrici elementari):

$$s_1(x_1, \ldots, x_n) = x_1 + \ldots + x_n, \; s_2(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n} x_i x_j,$$

$$s_3(x_1, \ldots, x_n) = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k, \ldots, s_n(x_1, \ldots, x_n) = x_1 \ldots x_n$$

Caratterizzazione polinomi simmetrici

Teorema

Sia $f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\underline{x}]$.

$f(\underline{x})$ *e' simmetrico* $\iff \exists\, g(\underline{x}) \in \mathbb{K}[\underline{x}] : f(\underline{x}) = g(s_1(\underline{x}), \ldots, s_n(\underline{x}))$.

k–esima funzione di Newton

$$S_k(x_1, \ldots, x_n) = x_1^k + \ldots + x_n^k.$$

$S_0(\underline{x}) = x_1^0 + \ldots + x_n^0 = n, S_1(\underline{x}) = x_1 + \ldots + x_n = s_1(\underline{x})$,
$S_2(\underline{x}) = x_1^2 + \ldots + x_n^2 = s_1(\underline{x})^2 - 2s_2(\underline{x})$, $S_3(\underline{x})$=Esercizio!

Formula radici/coefficienti $f(x) \in \mathbb{R}[x]$ monico

$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots a_{n-1} x + a_n = \prod_{i=1}^{n}(x - \alpha_i)$,
$\alpha_i \in \mathbb{C}$ *non necessariamente distinti. Allora, uguagliando, abbiamo:*
$a_1 = -s_1(\alpha_1, \ldots, \alpha_n) \in \mathbb{R}$, $a_2 = s_2(\alpha_1, \ldots, \alpha_n) \in \mathbb{R}$,
$\ldots$, $a_n = (-1)^n s_n(\alpha_1, \ldots, \alpha_n) \in \mathbb{R}$.

Funzioni elementari di Newton delle radici di $f(x) \in \mathbb{R}[x]$

$$\mathbb{R}[x] \ni f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots a_{n-1} x + a_n = \prod_{i=1}^{n} (x - \alpha_i).$$

$$S_1(\alpha_1, \ldots, \alpha_n) = \alpha_1 + \ldots + \alpha_n = s_1(\alpha_1, \ldots, \alpha_n) = -a_1;$$

$$S_2(\alpha_1, \ldots, \alpha_n) = \alpha_1^2 + \ldots + \alpha_n^2 = s_1(\alpha_1, \ldots, \alpha_n)^2 - 2s_2(\alpha_1, \ldots, \alpha_n)$$

$$= (-a_1)^2 - 2a_2 = a_1^2 - 2a_2;$$

$$V = \frac{\mathbb{R}[x]}{\langle f(x) \rangle} = \mathcal{L}(1, \overline{x}, \ldots, \overline{x}^{n-1}),$$

spazio vettoriale reale di dimensione $n \geq 1$, che e' anche un anello.

Quando $f(x) \in \mathbb{R}[x]$ ha radici distinte?

Risposta abituale: sia $f'(x) \in \mathbb{R}[x]$ la derivata prima, allora

$f(x)$ ha n radici (complesse) distinte $\iff$ m.c.d.$(f(x), f'(x)) = 1$.

Dato $[g(x)] \in V$, dove $[g(x)]$ denota la classe di equivalenza di $g(x) \in \mathbb{R}[x]$,definiamo l' applicazione lineare:

$$L_{[g(x)]} : V \to V$$

$$L_{[g(x)]}([h(x)]) = [g(x)] \cdot [h(x)] = [g(x) \cdot h(x)].$$

Sia

$$\mathrm{tr}([g(x)]) = \mathrm{tr}(L_{[g(x)]} : V \to V) \in \mathbb{R}$$

la *traccia di* $[g(x)]$ e sia

$$\phi_{f(x)} : V \times V \to \mathbb{R}$$

la forma bilineare simmetrica definita da

$$\phi_{f(x)}([g(x)], [m(x)]) = \mathrm{tr}(L_{[g(x)\cdot m(x)]} : V \to V).$$

Esempio: $f(x) = x^2 - s_1 x + s_2 \in \mathbb{R}[x]$

$$V = \frac{\mathbb{R}[x]}{\langle x^2 - s_1 x + s_2 \rangle} = \mathcal{L}(1, \overline{x}), \quad \mathcal{B} = \{1, \overline{x}\}$$

$$\left[\phi_{f(x)}\right]_{\mathcal{B}} = \begin{bmatrix} \mathrm{tr}(L_{1\cdot 1}) & \mathrm{tr}(L_{1\cdot \overline{x}}) \\ \mathrm{tr}(L_{\overline{x}\cdot 1}) & \mathrm{tr}(L_{\overline{x}^2}) \end{bmatrix}$$

$$L_1 = i_V \Rightarrow tr(L_1) = 2$$

$$L_{\overline{x}}(1) = \overline{x}, \; L_{\overline{x}}(\overline{x}) = \overline{x}^2 = -s_2 + s_1 \overline{x}$$

$$[L_{\overline{x}}]^{\mathcal{B}}_{\mathcal{B}} = \begin{bmatrix} 0 & -s_2 \\ 1 & s_1 \end{bmatrix} \quad [L_{\overline{x}^2}]^{\mathcal{B}}_{\mathcal{B}} = \begin{bmatrix} -s_2 & -s_2 \\ s_1 & s_1^2 - s_2 \end{bmatrix}$$

$$\left[\phi_{f(x)}\right]_{\mathcal{B}} = \begin{bmatrix} 2 & s_1 \\ s_1 & s_1^2 - 2s_2 \end{bmatrix} = \begin{bmatrix} 2 & S_1 \\ S_1 & S_2 \end{bmatrix}$$

$$\det(\left[\phi_{f(x)}\right]) = 2S_2 - S_1^2 = 2(s_1^2 - 2s_2) - s_1^2 = (-s_1)^2 - 4s_2 = \Delta(f).$$

Matrice di $\phi_{f(x)}$ rispetto alla base $\mathcal{B} = \{1, \overline{x}, \ldots, \overline{x}^{n-1}\}$

Se $\mathcal{B} = \{1, \overline{x}, \ldots, \overline{x}^{n-1}\}$ e se $\phi_{f(x)} : V \times V \to \mathbb{R}$, allora:

$$B = B(f) := \left[\phi_{f(x)}\right]_{\mathcal{B}} = \begin{bmatrix} S_0 & S_1 & S_2 & \ldots & S_{n-1} \\ S_1 & S_2 & S_3 & \ldots & S_n \\ S_2 & S_3 & S_4 & \ldots & S_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_{n-1} & S_n & S_{n+1} & \ldots & S_{2n-2} \end{bmatrix}$$

si dice **matrice Bezoutiana di** $f(x)$. Siano

$$A(x) = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ x_1 & x_2 & x_3 & \ldots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \ldots & x_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \ldots & x_n^{n-1} \end{bmatrix}, \quad \det(A) = \prod_{i<j}(x_i - x_j),$$

la matrice e il determinante di **Van der Monde**.

$$A \cdot A^t = \begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ 1 & x_2 & \dots & x_2^{n-1} \\ 1 & x_3 & \dots & x_3^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \dots & x_n^{n-1} \end{bmatrix} =$$

$$= \begin{bmatrix} S_0 & S_1 & S_2 & \dots & S_{n-1} \\ S_1 & S_2 & S_3 & \dots & S_n \\ S_2 & S_3 & S_4 & \dots & S_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_{n-1} & S_n & S_{n+1} & \dots & S_{2n-2} \end{bmatrix} = B$$

$$\det(B) = \det(A) \cdot \det(A^t) = \prod_{i<j} (x_i - x_j)^2 = \Delta(f).$$

Numero radici distinte

Teorema (Bézout, Cayley, Sylvester)

$\mathbb{R}[x] \ni f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots a_{n-1}x + a_n = \prod_{i=1}^{n}(x - \alpha_i)$. *Allora il numero di radici complesse distinte di* $f(x)$ *é uguale al rango di* $B(f)$. *In particolare,* $f(x)$ *ha* n *radici distinte se e solamente se* $\det(B) = \Delta(f) \neq 0$.

Supponiamo d'ora in poi:

$$f(x) = \prod_{i=1}^{r}(x - \alpha_i) \cdot \prod_{j=1}^{s}(x - \alpha_j)(x - \overline{\alpha_j}),$$

con $n = r + 2s$, con $\alpha_i \in \mathbb{R}$, con $\alpha_j \in \mathbb{C} \setminus \mathbb{R}$ e con tutti gli α_k distinti. Sia $(x - \alpha_j)(x - \overline{\alpha_j}) = x^2 + b_j x + c_j$.

$$V \simeq \frac{\mathbb{R}[x]}{\langle x - \alpha_1 \rangle} \times \dots \times \frac{\mathbb{R}[x]}{\langle x - \alpha_r \rangle} \times \frac{\mathbb{R}[x]}{\langle x^2 + b_1 x + c_1 \rangle} \times \dots \times \frac{\mathbb{R}[x]}{\langle x^2 + b_s x + c_s \rangle}$$

Isomorfismo di anelli

$$V \simeq \frac{\mathbb{R}[x]}{\langle x-\alpha_1\rangle}\times\ldots\times\frac{\mathbb{R}[x]}{\langle x-\alpha_r\rangle}\times\frac{\mathbb{R}[x]}{\langle x^2+b_1x+c_1\rangle}\times\ldots\times\frac{\mathbb{R}[x]}{\langle x^2+b_sx+c_s\rangle}$$

$$V \ni \mathrm{v} = (a_1,\ldots,a_r,\beta_1+\gamma_1\overline{x},\ldots,\beta_s+\gamma_s\overline{x}) =$$

$$= \sum_{i=1}^{r} a_i\mathrm{v}_i + \sum_{j=1}^{s}\beta_j\mathrm{w}_{2j-1} + \sum_{j=1}^{s}\gamma_j\mathrm{w}_{2j}$$

$\mathcal{B}' = \{\mathrm{v}_1,\ldots,\mathrm{v}_r,\mathrm{w}_1,\mathrm{w}_2,\ldots,\mathrm{w}_{2s-1},\mathrm{w}_{2s}\}$ base corrispondente

Siano $i\neq j$ e $(m,t)\neq(2j-1,2j)$, allora

$$\mathrm{v}_i\cdot\mathrm{v}_j = 0_V = \mathrm{v}_p\cdot\mathrm{w}_q,\quad \mathrm{w}_m\cdot\mathrm{w}_t = 0_V$$

$$\mathrm{v}_i\cdot\mathrm{v}_j = (0,\ldots,0,1,0\ldots,0)\cdot(0,\ldots,0,0,1,\ldots,0) = (0,\ldots,0) = 0_V.$$

$$\text{se } i\neq j \Rightarrow \phi_{f(x)}(\mathrm{v}_i,\mathrm{v}_j) = \mathrm{tr}(L_{0_V}) = 0.$$

Decomposizione $\phi_{f(x)}$–ortogonale di V

$$\left[\phi_{f(x)}\right]_{\mathcal{B}'}^{\mathcal{B}'} = \left[\begin{array}{c|c|c|c|cc|cc} 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \hline 0 & \ddots & 0 & \dots & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \ddots & & & & \\ \hline 0 & 0 & 0 & \dots & 2 & -b_{s-1} & 0 & 0 \\ 0 & 0 & 0 & \dots & -b_{s-1} & b_{s-1}^2 - 2c_{s-1} & 0 & 0 \\ \hline 0 & 0 & 0 & \dots & 0 & 0 & 2 & -b_s \\ 0 & 0 & 0 & \dots & 0 & 0 & -b_s & b_s^2 - 2c_s \end{array}\right]$$

su $\dfrac{\mathbb{R}[x]}{\langle x - \alpha_i \rangle}$ abbiamo segnatura $(1,0)$, $i = 1, \dots, r$;

su $\dfrac{\mathbb{R}[x]}{\langle x^2 + b_j x + c_j \rangle}$ abbiamo segnatura $(1,1)$ perché $\Delta(x^2+b_s x+c_s) < 0$.

$$\text{segnatura } \phi_{f(x)} = (r+s, s).$$

Radici reali e segnatura della matrice Bezoutiana

Teorema (Sylvester)

Sia

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots a_{n-1} x + a_n \in \mathbb{R}[x]$$

con $\mathrm{rk}(B(f)) = n$ *(*$\Leftrightarrow \Delta(f) \neq 0 \Leftrightarrow f(x)$ *ha* n *radici distinte).*

Se $B(f)$ *ha segnatura* (p, q) *con* $p + q = n$*, allora il numero di radici reali di* $f(x)$ *é uguale a* $p - q$*.*

In particolare, $f(x)$ *ha* n *radici reali distinte se e solamente se* $B(f)$ *è una forma bilineare simmetrica definita positiva.*

Problema di Waring per interi

Problema di Waring, 1770

Dato $k \in \mathbb{N}$ *esiste* $g(k) \in \mathbb{N}$ *tale che* **PER OGNI** $n \in \mathbb{N}$ *esistono* $x_1, \ldots, x_{g(k)} \in \mathbb{N} \cup 0$ *tali che*

$$n = x_1^k + \ldots + x_{g(k)}^k ?$$

Equivalentemente, **ogni intero positivo è al più somma di** $g(k)$ **potenze** k**-esime di interi positivi o nulli?**

Ovviamente $g(1) = 1$. Il Teorema dei 4 quadrati dice $g(2) = 4$.

SENZA DETERMINARE $g(k)$ Hilbert ha dimostrato:

Teorema, Hilbert 1909

Per ogni $k \in \mathbb{N}$ *ESISTE* $g(k)$.

Stima di J.A. Euler, figlio di Leonard Euler

Se $x \in \mathbb{R}$ indichiamo con $[x] \in \mathbb{Z}$ la *parte intera di* x nella sua espressione decimale, i.e. $[x] = \lfloor x \rfloor \leq x < [x] + 1 = \lceil x \rceil$.

Teorema, J. A. Euler 1770

Per ogni $k \in \mathbb{N}$

$$g(k) \geq 2^k + [(\frac{3}{2})^k] - 2.$$

Sia $q \in \mathbb{N}$ tale che

$$3^k = q \cdot 2^k + r, \;\; 0 \leq r < 2^k, \text{ i.e.}$$

$$q = [(\frac{3}{2})^k]. \text{ Sia } m = x_1^k + \ldots + x_r^k.$$

$$\text{Se } m = q \cdot 2^k - 1 < q \cdot 2^k \leq 3^k \Rightarrow x_i^k \in \{1^k, 2^k\}.$$

$$m = (q-1)\cdot 2^k + (2^k - 1)\cdot 1^k \Rightarrow g(k) \geq q - 1 + 2^k - 1 = 2^k + [(\frac{3}{2})^k] - 2.$$

alcuni valori di $g(k)$ e di m

k	$q = [(\frac{3}{2})^k]$	$m = (q-1)\cdot 2^k + (2^k - 1)\cdot 1^k$	g(k)
2	2	$7 = 2^2 + 3 \cdot 1^2$	4
3	3	$23 = 2 \cdot 2^3 + 7 \cdot 1^3$	9
4	5	$79 = 4 \cdot 2^4 + 15 \cdot 1^4$	19
5	7	$223 = 6 \cdot 2^5 + 31 \cdot 1^5$	37

Teorema, vari autori 1910–1994

Eccetto un numero FINITO di $k > 471.600.000$ *abbiamo*

$$g(k) = 2^k + [(\frac{3}{2})^k] - 2.$$

Si congettura che $g(k) = 2^k + [(\frac{3}{2})^k] - 2$ per ogni $k \geq 1$.

Somma di 9 cubi

Come ultimi *misteri* di questo brevissimo viaggio tra i numeri interi enunciamo alcuni intriganti risultati e congetture per $k = 3$.

Teorema, Wieferich 1909

$$g(3) = 9, \ \textit{i. e.}$$

ogni intero è somma di al più 9 cubi.

Abbiamo visto sopra che 23 necessita proprio di 9 potenze cubiche.

Teorema, Landau (1911), Baer (1913), Dickson (1939)

Ogni intero positivo diverso da 23 e 239 è somma di al più 8 cubi

Congetture di Jacobi, 1851

Congetture, Jacobi 1851

1. *Ogni intero positivo diverso da*

$$15, 22, 23, 50, 114, 167, 175, 186, 212,$$

$$231, 238, 239, 303, 364, 420, 428, 454$$

è somma di 7 cubi.

2. *Ogni intero positivo diverso da*

$$7, 14, 15, \ldots, 5818, 8042 \ \ (138 \ \textit{eccezioni})$$

è somma di 6 cubi

3. *Ogni intero sufficientemente grande è somma di 5 cubi.*

Definizione di $G(k)$

Intero $G(k)$

Dato $k \in \mathbb{N}$ definiamo $G(k) \in \mathbb{N}$ come il minor intero tale che **PER OGNI** $n \in \mathbb{N}$ **SUFFICIENTEMENTE GRANDE** *esistono* $x_1, \ldots, x_{G(k)} \in \mathbb{N} \cup 0$ *tali che*

$$n = x_1^k + \ldots + x_{G(k)}^k$$

Equivalentemente, **ogni intero positivo SUFFICIENTEMENTE GRANDE è al più somma di $G(k)$ potenze k-esime di interi positivi o nulli**

Ovviamente $G(k) \leq g(k)$.
Gauss: ogni intero n della forma $7r + 8$, $r \in \mathbb{N}$ è somma di 4 quadrati, i.e. $G(2) = 4 = g(2)$.
Jacobi ha congetturato: $G(3) = 5$. È noto che $G(3) \leq 7 < 9 = g(3)$.

Teorema, Davenport 1939

$$G(4) = 16 < 19 = g(4).$$

La determinazione di $G(k)$ per $k > 4$ è un attivissimo filone di ricerca ma pochi risultati precisi sono noti. Negli ultimi anni l' utilizzo di moderni e potentissimi calcolatori ha permesso di ottenere notevoli progressi in questo campo.

Problema di Waring per polinomi omogenei in più variabili

Siano $n \geq 1$ e $d \geq 1$. Definiamo $W(n+1,d) \in \mathbb{N}$ come il minor intero positivo tale che per $f \in \mathbb{C}[x_0,\ldots,x_n]_d$ **GENERALE** *esistono $L_1,\ldots,L_{W(n+1,d)} \in \mathbb{C}[x_0,\ldots,x_n]_1$, $\lambda \in \mathbb{C}^* = \mathbb{C} \setminus 0$ $\lambda_1,\ldots\lambda_{W(n+1,d)} \in \mathbb{C}$ tali che*

$$\lambda \cdot f = \lambda_1 L_1^d + \ldots + \lambda_{W(n+1,d)} L_{W(n+1,d)}^d =$$

$$= (\sqrt{\lambda_1} L_1)^d + \ldots + (\sqrt{\lambda_{W(n+1,d)}} L_{W(n+1,d)})^d.$$

Equivalentemente, un polinomio omogeneo **GENERALE** *di grado d si può esprimere come somma di $W(n+1,d)$ potenze $d-$esime di forme lineari*

Dividendo per λ e prendendo la radice quadrata la condizione precedente si può scrivere come

$$f = L_1^d + \ldots + L_{W(n+1,d)}^d.$$

Teorema di Lagrange implica $W(n+1,2) = n+1$

$$\mathbb{C}[x_0,\ldots,x_n]_2 \ni f(x_0,\ldots,x_n) = \begin{pmatrix} x_0 & \cdots & x_n \end{pmatrix} \cdot A \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix}, \; A = A^t.$$

Esiste $C \in \mathbb{C}^{n+1,n+1}$ invertibile tale che

$$f(C^{-1}\mathrm{x}) = \mathrm{x}^t \cdot (C^t \cdot A \cdot C)\mathrm{x} = x_0^2 + \cdots + x_r^2$$

con $r+1 = \mathrm{rk}(A)$.

$$\Rightarrow f(\mathrm{x}) = L_0^2 + \ldots + L_r^2 \text{ con } L_i \in \mathbb{C}[x_0,\ldots,x_n]_1$$

GENERALE$=\{\mathrm{rango}(A) = n+1\} \Rightarrow W(n+1,2) = n+1.$

Stima alla J.A. Euler per polinomi omogenei

Siano $\mathbb{P}^n = \mathbb{P}(\mathbb{C}[x_0, \ldots, x_n]_1)$ e $\mathbb{P}^{n(d)} = \mathbb{P}(\mathbb{C}[x_0, \ldots, x_n]_d)$.

$$n(d) = \dim_{\mathbb{C}}(\mathbb{C}[x_0, \ldots, x_n]_d) - 1 = \binom{n+d}{n} - 1.$$

$$\nu_{n,d} : \mathbb{P}^n \to \mathbb{P}^{n(d)};\ \nu_{n,d}([L]) = [L^d],$$

i.e. una forma lineare viene inviata nella sua potenza d-esima.

I punti $p = [L^d] \in \mathbb{P}^{n(d)}$ hanno dimensione $n = \dim(\mathbb{P}^n)$.

Stima alla J.A. Euler per polinomi omogenei

I punti che stanno su $\langle [L_1^d], \ldots, [L_r^d] \rangle = \mathbb{P}^{r-1}$ variando tutti gli $[L_i^d]$ possibili avranno dimensione:

$$\dim(r \text{ punti su } \nu_{n,d}(\mathbb{P}^n)) + \dim(\mathbb{P}^{r-1}) = r \cdot n + r - 1 = r \cdot (n+1) - 1.$$

Per poter riempire $\mathbb{P}^{n(d)}$ dovremo avere

$$r(n+1) - 1 \geq n(d) = \binom{n+d}{n} - 1, \text{ i.e. } r(n+1) \geq \binom{n+d}{n}$$

$$\Rightarrow r \geq \frac{\binom{n+d}{n}}{n+1} \Rightarrow r \geq \left\lceil \frac{\binom{n+d}{n}}{n+1} \right\rceil .$$

Questo suggerisce di congetturare:

$$W(n+1, d) = \left\lceil \frac{\binom{n+d}{n}}{n+1} \right\rceil .$$

Teorema di Sylvester per $n = 1$

Teorema, Sylvester 1851

Se $n = 1$, allora

$$W(n+1,d) = W(2,d) = \left\lceil \frac{\binom{1+d}{1}}{1+1} \right\rceil = \left\lceil \frac{d+1}{2} \right\rceil .$$

Per $n \geq 2$, abbiamo

$$W(n+1,2) = n+1 > \left\lceil \frac{\binom{n+2}{n}}{n+1} \right\rceil = \left\lceil \frac{n+2}{2} \right\rceil .$$

Quindi per $n \geq 2$ ci possiamo aspettare delle eccezioni al valore stimato:

$$\left\lceil \frac{\binom{n+d}{n}}{n+1} \right\rceil .$$

Teorema di Alexander-Hirschowitz

Teorema, Alexander–Hirschowitz 1995

Se $n \geq 2$, *abbiamo*

$$W(n+1,d) = \left\lceil \frac{\binom{n+d}{n}}{n+1} \right\rceil$$

eccetto per i seguenti casi:

1. $n \geq 2$, $d = 2$, $W(n+1,d) = n+1 > \lceil \frac{n+2}{2} \rceil$ (= *valore stimato*);
2. $n = 2$, $d = 4$, $W(3,4) = 6 > 5$(= *valore stimato*);
3. $n = 3$, $d = 4$, $W(4,4) = 10 > 9$(= *valore stimato*);
4. $n = 4$, $d = 3$, $W(5,3) = 8 > 7$(= *valore stimato*);
5. $n = 4$, $d = 4$, $W(5,4) = 15 > 14$(= *valore stimato*).