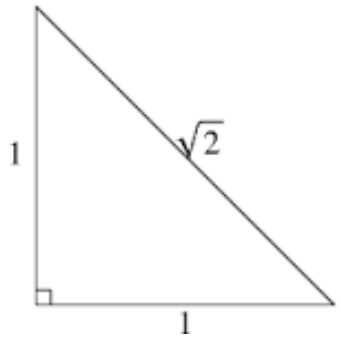
Dal problema di Waring per numeri naturali a quello per polinomi omogenei in più variabili: una passeggiata tra Algebra, Geometria (Algebrica) e Teoria dei Numeri

Francesco Russo

DMI–UNICT

22 marzo 2017

Numeri irrazionali e geometria elementare

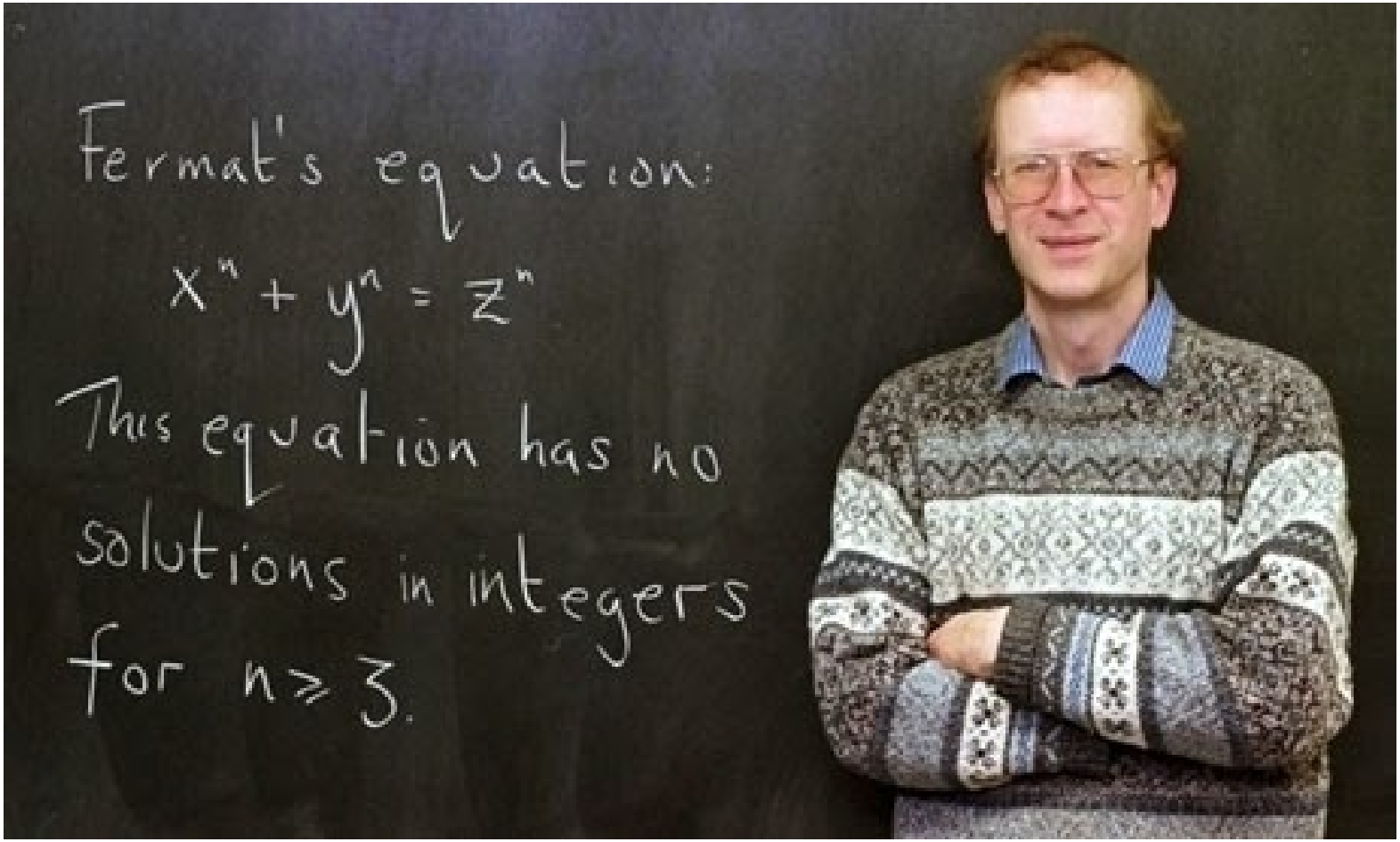


$$\mathbb{N} = \{1, 2, \ldots\};$$

$\mathbb{R} \setminus \mathbb{Q} = \{\alpha \in \mathbb{R},\ \alpha \notin \mathbb{Q}\}$ numeri irrazionali

- $p \in \mathbb{N}$ numero primo $\Rightarrow \sqrt{p} \in \mathbb{R}$ **irrazionale**;
- π è un numero **trascendente**, i.e. non è radice di nessun polinomio $p(t)$ con coefficienti in $\mathbb{Z}$ ($=$ *numeri algebrici*);
- $\sqrt{p}$ è radice del polinomio $t^2 - p$ con coefficienti in $\mathbb{Z}$;
- trascendente $\Rightarrow$ irrazionale.

Ultimo Teorema di Fermat, Andrew Wiles 1993/1994



Passaggio ai numeri razionali

$$\textit{se esistessero } a, b, c \in \mathbb{N} : a^n + b^n = c^n \iff$$

$$\left(\frac{a}{c}\right)^n + \left(\frac{b}{c}\right)^n = 1 \iff$$

$P = (\frac{a}{c}, \frac{b}{c})$ con entrambe le coordinate razionali non nulle *apparterrebbe* alla curva di Fermat di equazione $x^n + y^n = 1$.

Pertanto l' Ultimo Teorema di Fermat è conseguenza di:

Teorema (Ultimo *Teorema* di Fermat 1630, Wiles 1993/94)

Per ogni $n \geq 3$ la curva di equazione $x^n + y^n = 1$ non ha punti con entrambe le coordinate razionali non nulle.

Intuizione e punti con entrambe le coordinate razionali

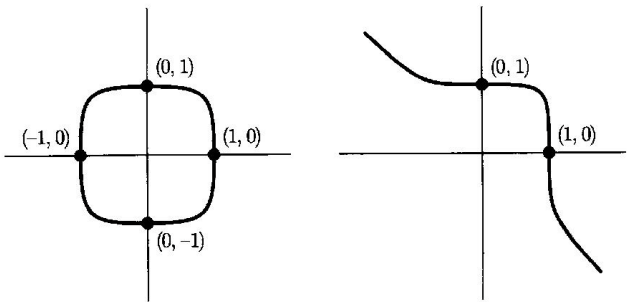


Figure: 1

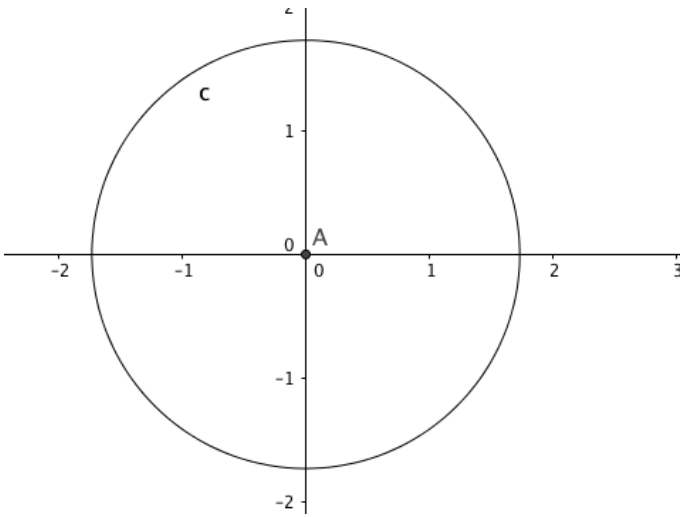


Figure: 2

1. $x^4 + y^4 = 1$ e $x^5 + y^5 = 1$ (nessun tale punto con $x \cdot y \neq 0$, FERMAT)
2. $x^2 + y^2 = 3$ (NESSUN PUNTO CON ENTRAMBE LE COORDINATE IN $\mathbb{Q}$!)
3. $x^2 + y^2 = 5$ (∞ PUNTI CON ENTRAMBE LE COORDINATE IN $\mathbb{Q}$!)

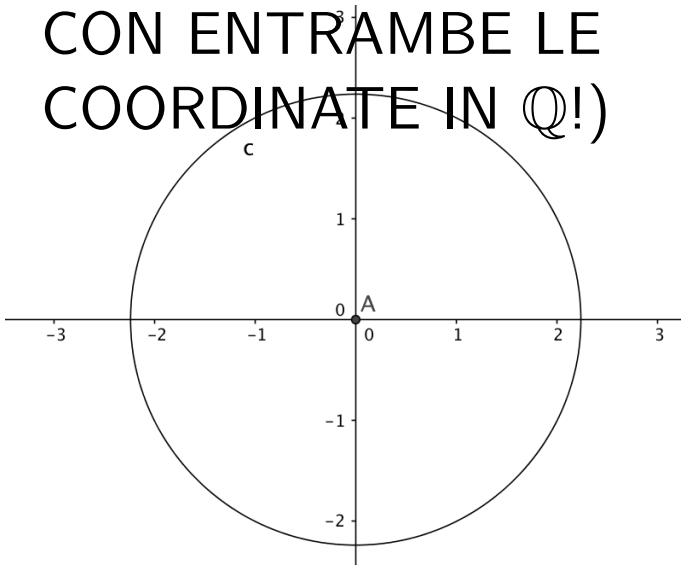


Figure: 3

Esercizio Corso di Geometria 2

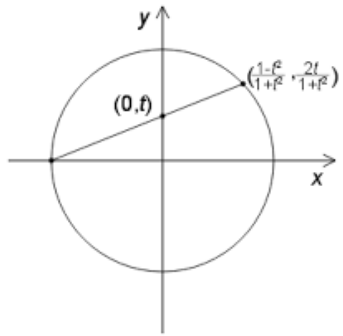
Esercizio (Corso di Geometria 2, ultimo esercizio, ultima lista)

Per ogni $n \geq 3$ **NON** *esistono* $p(t)$, $q(t)$, $r(t)$ *polinomi non nulli con coefficienti in* $\mathbb{Q}$ *(e nemmeno in* $\mathbb{R}$ *e nemmeno in* $\mathbb{C}$*!) tali che*

$$\left(\frac{p(t)}{r(t)}\right)^n + \left(\frac{q(t)}{r(t)}\right)^n = 1.$$

Se esistessero tali polinomi, allora sostituendo $t = \frac{\alpha}{\beta}$ con $\alpha, \beta \in \mathbb{Z}$ e razionalizzando l' espressione avremmo (infinite) soluzioni razionali (e quindi anche intere) non nulle dell' equazione di Fermat.

Soluzioni con coordinate razionali non nulle di $x^2 + y^2 = 1$



$$\begin{cases} x^2 + y^2 = 1 \\ y = t(x+1) \quad \text{[rette per il punto } (-1,0)\text{]} \end{cases}$$

$$x^2 + \frac{2t^2}{t^2+1}x + \frac{t^2-1}{t^2+1} = 0$$

$$\Rightarrow (x = -1 \text{ e}) x = \frac{1-t^2}{t^2+1} \Rightarrow (y = 0 \text{ e}) y = t(x+1) = \frac{2t}{t^2+1}.$$

Siano $p(t) = 1 - t^2$, $q(t) = 2t$, $r(t) = t^2 + 1$ polinomi in t con coefficienti in $\mathbb{Z}$.

Allora

$$\left(\frac{p(t)}{r(t)}\right)^2 + \left(\frac{q(t)}{r(t)}\right)^2 = 1.$$

Sostituendo

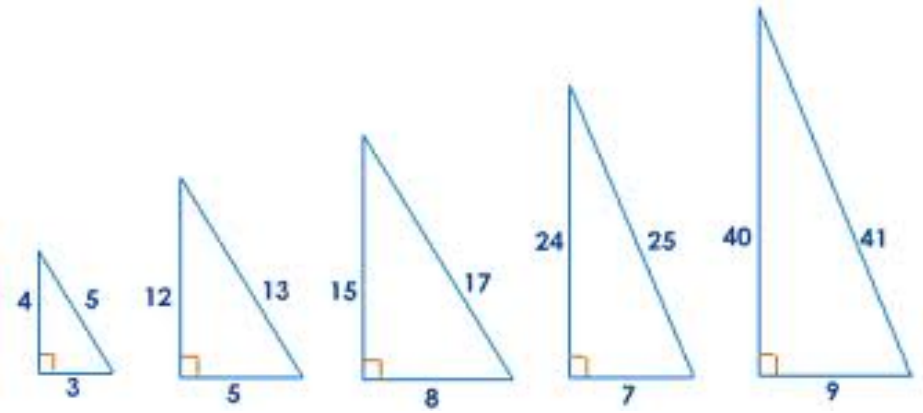
$$t = \frac{\beta}{\alpha} \in \mathbb{Q},\ \alpha, \beta \in \mathbb{Z}$$

e razionalizzando otteniamo le coordinate di **TUTTI** i punti sul cerchio unitario con entrambe le coordinate razionali

$$P = (\frac{\alpha^2 - \beta^2}{\alpha^2 + \beta^2}, \frac{2\alpha\beta}{\alpha^2 + \beta^2}).$$

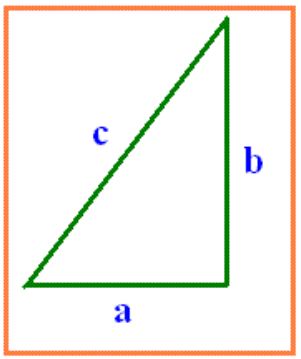
($P = (a, b)$ con $a, b \in \mathbb{Q}$ e $a \neq -1 \Rightarrow t = \frac{y}{x+1} = \frac{b}{a+1} \in \mathbb{Q}$)

Terne pitagoriche



(a, b, c) con $a, b, c \in \mathbb{N}$ si dice **terna pitagorica** se

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



Formula per le terne pitagoriche

Siano $\alpha, \beta \in \mathbb{N}$ con $\alpha > \beta$, allora **ABBIAMO APPENA DIMOSTRATO** che

$$(\alpha^2 - \beta^2, 2\alpha\beta, \alpha^2 + \beta^2)$$

sono **TUTTE** le terne pitagoriche.

Infatti, se $a, b, c \in \mathbb{N}$, $c \neq 0$ sono tali che

$$a^2 + b^2 = c^2 \iff \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1 \iff$$

$P = (\frac{a}{c}, \frac{b}{c})$ appartiene al cerchio unitario $x^2 + y^2 = 1$.

Intuizione e punti con entrambe le coordinate razionali

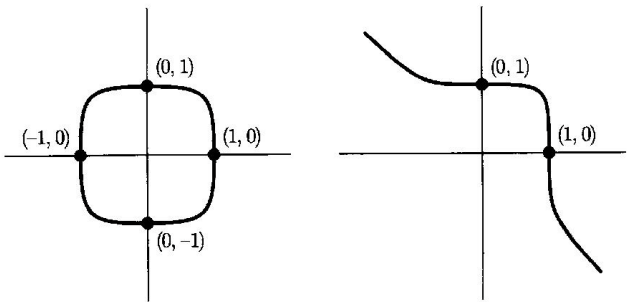


Figure: 1

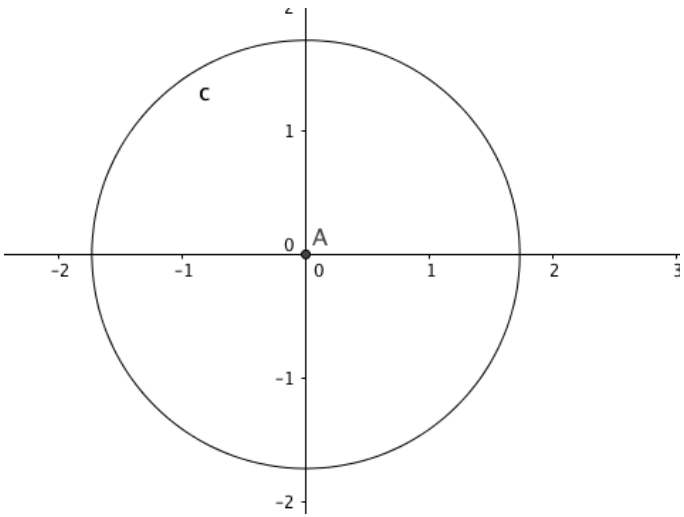


Figure: 2

1. $x^4 + y^4 = 1$ e $x^5 + y^5 = 1$ (nessun tale punto con $x \cdot y \neq 0$, FERMAT)
2. $x^2 + y^2 = 3$ (NESSUN PUNTO CON ENTRAMBE LE COORDINATE IN $\mathbb{Q}$!)
3. $x^2 + y^2 = 5$ (∞ PUNTI CON ENTRAMBE LE COORDINATE IN $\mathbb{Q}$!)

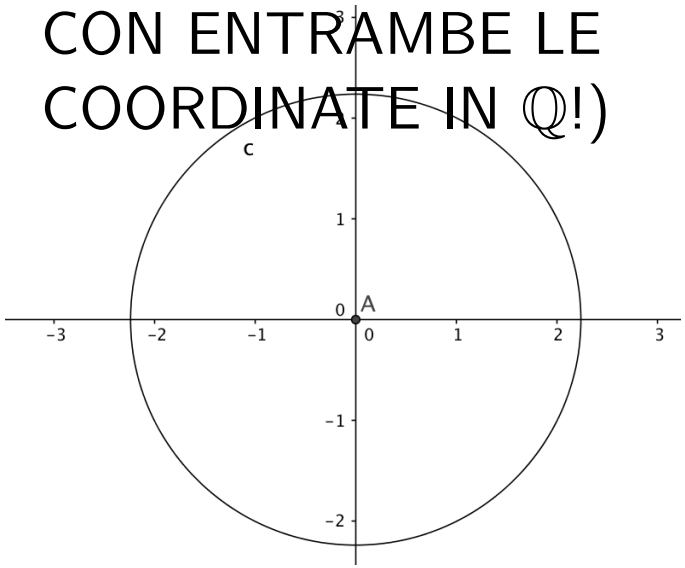


Figure: 3

Numeri primi e fattorizzazione in $\mathbb{Z}[i]$

Se $a+ib \in \mathbb{Z}[i]$, sia $N(a+ib) = a^2+b^2$ la *norma di* $a+ib$.

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) $[-1] = [p-1]$ *è un quadrato in* $\mathbb{Z}_p$, *i.e.* $[-1] = [x]^2$ *ha almeno una soluzione.*

(III) p *non è un elemento primo in* $\mathbb{Z}[i]$;

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

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

Circonferenze $x^2 + y^2 = p$, $p \geq 2$ numero primo

Corollario

Sono condizioni equivalenti:

(I) $p = 2$ *oppure* $p = 4r + 1$ *per qualche* $r \in \mathbb{N}$ *(e.g.* $p = 5, 13, 17, \ldots$*);*

(II) *Su* $x^2 + y^2 = p$ *esiste un punto con entrambe le coordinate razionali;*

(III) *Su* $x^2 + y^2 = p$ *esistono infiniti punti con entrambe le coordinate razionali.*

Somma di 2 quadrati

Teorema dei due quadrati, Fermat 1640

Sia

$$2 \leq n = p_1^{m_1} \cdots p_r^{m_r}$$

fattorizzazione di $n \in \mathbb{N}$ *in primi distinti* $p_1, \ldots, p_r$, $r \geq 1$. *Sono condizioni equivalenti:*

(I) $n = a^2 + b^2$ *con* $a, b \in \mathbb{N} \cup 0$;

(II) *Se* $p_i = 4r_i + 3$ *per qualche* $r_i \in \mathbb{N}$, *allora* $m_i = 2s_i$ *è pari.*

Mostriamo che $(II) \Rightarrow (I)$: A meno di riordinare i primi

$$n = m^2 \cdot p_1 \cdots p_s \text{ con } p_i \equiv 1 \text{ (mod. 4)}.$$

Allora $p_i = a_i^2 + b_i^2 = N(a_i + ib_i)$ e se $a + ib = \prod_{i=1}^{s}(a_i + ib_i)$

$$n = m^2 N(a_1 + ib_1) \cdots N(a_s + ib_s) = m^2 N(a + ib) =$$

$$= m^2(a^2 + b^2) = (ma)^2 + (mb)^2.$$

Somma di 2 quadrati

Teorema dei due quadrati, Fermat 1640

Sia

$$2 \leq n = p_1^{m_1} \cdots p_r^{m_r}$$

fattorizzazione di $n \in \mathbb{N}$ *in primi distinti* $p_1, \ldots, p_r$, $r \geq 1$. *Sono condizioni equivalenti:*

(I) $n = a^2 + b^2$ *con* $a, b \in \mathbb{N} \cup 0$;

(II) *Se* $p_i = 4r_i + 3$ *per qualche* $r_i \in \mathbb{N}$, *allora* $m_i = 2s_i$ *è pari.*

Mostriamo che $(I) \Rightarrow (II)$ per induzione su n. Se $n = 2$, e' vero.

$$a^2 + b^2 = n \text{ e sia } p \equiv 3 \text{ (mod. 4) con } p/n.$$

Allora p è primo in $\mathbb{Z}[i]$ e

$$p/a^2 + b^2 = (a + ib)(a - ib) \Rightarrow \ p/a \text{ e } p/b$$

$$n = p^2(c^2 + d^2) \text{ con } c^2 + d^2 = m < n.$$

Somma di tre quadrati

Teorema dei tre quadrati, Legendre 1797

Dato $n \in \mathbb{N}$ *esistono* $a, b, c \in \mathbb{N} \cup 0$ *tali che*

$$n = a^2 + b^2 + c^2$$

se e solamente se

$$n \neq 4^m(8r + 7),\ m, r \in \mathbb{N} \cup 0.$$

Osserviamo che 7 è il minor intero per cui occorrono effettivamente 4 quadrati.

Somma di 4 quadrati

Precedentemente Lagrange ha dimostrato il seguente risultato:

Teorema dei 4 quadrati, Lagrange 1770

Dato $n \in \mathbb{N}$ *esistono* $a, b, c, d \in \mathbb{N} \cup 0$ *tali che*

$$n = a^2 + b^2 + c^2 + d^2.$$

È sufficiente provarlo per n che non possiedano quadrati nella loro fattorizzazione, i.e.

$$n = p_1 \cdots p_r \text{ con } p_i \text{ primi distinti.}$$

Infatti se

$$n' = m^2 \cdot n = m^2 \cdot (p_1 \cdots p_r) =$$

$$= m^2(a^2 + b^2 + c^2 + d^2) = (ma)^2 + (mb)^2 + (mc)^2 + (md)^2.$$

Lemma, Somma di due quadrati modulo p

Sia $p \geq 2$ un primo. Allora ogni $[r] \in \mathbb{Z}_p$ è somma di due quadrati in $\mathbb{Z}_p$, i.e. esistono $[a], [b] \in \mathbb{Z}_p$ tali che $[r] = [a]^2 + [b]^2$. In particolare $[x]^2 + [y]^2 = [-1]$ ha soluzioni.

Sia $p \geq 3$. Sia $S_1 = \{[x]^2,\ [x] \in \mathbb{Z}_p\}$ e $S_2 = \{[r] - [y]^2,\ [y] \in \mathbb{Z}_p\}$.

$$[x]^2 = [z]^2 \Rightarrow [x] = \pm[z] \Rightarrow \#(S_1) = 1 + \frac{p-1}{2} = \frac{p+1}{2}.$$

$$\text{Analogamente } \#(S_2) = \frac{p+1}{2} \Rightarrow S_1 \cap S_2 \neq \emptyset$$

$$\Rightarrow \exists\ [x], [y] \in \mathbb{Z}_p\ :\ [x]^2 = [r] - [y]^2 \Rightarrow [r] = [x]^2 + [y]^2.$$

Corollario, Somma di due quadrati modulo n

Sia $n = p_1 \cdots p_r$ con p_i primi distinti. Allora ogni $[s] \in \mathbb{Z}_n$ é somma di due quadrati in $\mathbb{Z}_n$, i.e. esistono $[a], [b] \in \mathbb{Z}_n$ tali che $[s] = [a]^2 + [b]^2$.

Per il *Teorema Cinese del Resto*:

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}.$$

Allora il Corollario segue dal Lemma: se $[s]_{p_i} = [a_i]_{p_i}^2 + [b_i]_{p_i}^2$, siano

$$[a] = ([a_1]_{p_1}, \ldots, [a_r]_{p_r}) \text{ e } [b] = ([b_1]_{p_1}, \ldots, [b_r]_{p_r})$$

$$[a]^2 + [b]^2 = ([a_1]_{p_1}^2 + [b_1]_{p_1}^2, \ldots, [a_r]_{p_r}^2 + [b_r]_{p_r}^2) =$$

$$= ([s]_{p_1}, \ldots, [s]_{p_r}) = [s].$$

Matrici quadrate complesse e matrici hermitiane

Data $A = [a_{i,j}] \in \mathbb{C}^{n,n}$, definiamo $A^* = [\overline{a_{j,i}}] = \overline{(A^t)} = (\overline{A})^t \in \mathbb{C}^{n,n}$.

$$\text{Se } A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathbb{C}^{2,2}, \text{ allora } A^* = \begin{pmatrix} \overline{\alpha} & \overline{\gamma} \\ \overline{\beta} & \overline{\delta} \end{pmatrix}$$

Alcune proprietà immediate analoghe a quelle della trasposizione di matrici reali:

$$(A^*)^* = A,\ (A \cdot B)^* = B^* \cdot A^*,\ (A^{-1})^* = (A^*)^{-1}.$$

$A \in \mathbb{C}^{n,n}$ si dice *hermitiana* se $A = A^*$; $\quad A = A^* \Rightarrow a_{i,i} \in \mathbb{R}$

$$A = A^*,\ C \in \mathbb{C}^{n,n} \Rightarrow C \cdot A \cdot C^* \text{ hermitiana.}$$

$n = p_1 \cdots p_r$ con p_i primi distinti

Dato $n = p_1 \cdots p_r > 0$ con p_i primi distinti, per il Corollario precedente esistono $a, b, m \in \mathbb{N} \cup 0$ tali che:

$$-1 + n \cdot m = a^2 + b^2 \Rightarrow n \cdot m - (a + ib)(a - ib) = 1.$$

Possiamo costruire la matrice

$$A = \begin{pmatrix} n & a + ib \\ a - ib & m \end{pmatrix} = A^* \in \mathbb{Z}[i]^{2,2} \subset \mathbb{C}^{2,2} \text{ con } \det(A) = 1.$$

$$D = \begin{pmatrix} d_{1,1} & d_{1,2} \\ d_{2,1} & d_{2,2} \end{pmatrix} \in \mathbb{Z}[i]^{2,2}, \quad D = D^* \Rightarrow d_{1,1},\ d_{2,2} \in \mathbb{Z}.$$

Identità 4 quadrati per $n = p_1 \cdots p_r$, p_i primi distinti

Teorema, Newman 1972

Sia $n = p_1 \cdots p_r > 0$ con p_i primi distinti e sia

$$A = \begin{pmatrix} n & a+ib \\ a-ib & m \end{pmatrix} = A^* \in \mathbb{Z}[i]^{2,2} \text{ con } \det(A) = 1.$$

Allora esiste $B \in \mathbb{Z}[i]^{2,2}$ con $\det(B) = 1$ tale che $A = B \cdot B^*$.

Corollario, Somma 4 quadrati, Lagrange 1770

Ogni intero $n > 0$ è somma di 4 quadrati.

Possiamo supporre $n = p_1 \cdots p_r$ con p_i primi distinti;

$$A = \begin{pmatrix} n & a+ib \\ a-ib & m \end{pmatrix} = \begin{pmatrix} x+iy & w+iz \\ \spadesuit & \clubsuit \end{pmatrix} \cdot \begin{pmatrix} x-iy & \overline{\spadesuit} \\ w-iz & \overline{\clubsuit} \end{pmatrix}$$

$\Rightarrow n = x^2 + y^2 + w^2 + z^2$ con $x, y, w, z \in \mathbb{Z}$.

Teorema di Newman versus Teorema di Sylvester

$$A = \begin{pmatrix} n & a+ib \\ a-ib & m \end{pmatrix} = A^*,$$

$n > 0$ e $\det(A) = 1 \Rightarrow A$ matrice hermitiana definita positiva.

per il Criterio dei Minori Principali.
Quindi esiste $B \in \mathbb{C}^{n,n}$ tale che

$$A = B \cdot B^*.$$

Il punto cruciale nel Teorema di Newman è di poter prendere $B \in \mathbb{Z}[i]^{2,2}$.....

Dimostrazione Teorema di Newman

Procederemo per induzione su $N(a+ib) = a^2 + b^2 \in \mathbb{N} \cup 0$, dove $n > 0$ e

$$A = \begin{pmatrix} n & a+ib \\ a-ib & m \end{pmatrix} = A^*.$$

Se $N(a+ib) = 0$, essendo $n > 0$ e $\det(A) = 1$ abbiamo $A = I_{2\times 2}$ e possiamo prendere $B = I_{2\times 2}$. Sia allora $N(a+ib) = a^2 + b^2 > 0$.

Scelta di $C \in \mathbb{Z}[i]^{2,2}$

Possiamo quindi supporre $N(a+ib) = a^2 + b^2 > 0$, $m > 0$ e anche $0 < n \leq m$, il rimanente caso $0 < m \leq n$ essendo analogo.

Se $C = \begin{pmatrix} 1 & 0 \\ x - iy & 1 \end{pmatrix} \in \mathbb{Z}[i]^{2,2} \Rightarrow C \cdot A \cdot C^* = A' = \begin{pmatrix} n & a' + ib' \\ a' - ib' & m' \end{pmatrix}$

con $a' = nx + a$, $b' = ny + b$, $A' = (A')^*$ e $\det(A') = 1$.

È ora facile scegliere $x, y \in \mathbb{Z}$ tali che $(a')^2 + (b')^2 < a^2 + b^2$.
Vediamo come:

Scelta di $C \in \mathbb{Z}[i]^{2,2}$

Sia $a' = nx + a$, $b' = ny + b$ con $o < n \leq m$ e $n \cdot m = a^2 + b^2 + 1$.

1. Se $a > \frac{n}{2}$, prendiamo $x = -1$ e $y = 0$, Allora $(a')^2 = (a - n)^2 < a^2$ e $b' = b$ e $(a')^2 + (b')^2 < a^+ b^2$.
2. Se $a < -\frac{n}{2}$, prendiamo $x = 1$ e $y = 0$;
3. Se $b > \frac{n}{2}$, prendiamo $x = 0$ e $y = -1$;
4. Se $b < -\frac{n}{2}$, prendiamo $x = 0$ e $y = 1$.
5. $|a| \leq \frac{n}{2}$ e $|b| \leq \frac{n}{2}$ è impossibile: se $n = 1$, è ovvio. Se $n > 1$, avremmo

$$n^2 \leq n \cdot m = a^2 + b^2 + 1 \leq (\frac{n}{2})^2 + (\frac{n}{2})^2 + 1 = \frac{n^2}{2} + 1 < n^2.$$

Questa contraddizione mostra che esiste A' con $(a')^2 + (b')^2 < a^2 + b^2$.

Scelta di $C \in \mathbb{Z}[i]^{2,2}$

Ipotesi di induzione:

$$\Rightarrow A' = B' \cdot (B')^* \Rightarrow B' \cdot (B')^* = C \cdot A \cdot C^*$$

$$\Rightarrow A = (C^{-1} \cdot B') \cdot (C^{-1} \cdot B')^*.$$

Se

$$B = (C^{-1} \cdot B') \in \mathbb{Z}[i]^{2,2} \Rightarrow \det(B) = (\det(C))^{-1} \cdot \det(B') = 1 \cdot 1 = 1.$$

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 $n \equiv 7 \pmod 8$ 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

Sia $\mathbb{C}[x_0, \ldots, x_n]$ l' anello dei polinomi con coefficienti complessi nelle variabili $x_0, \ldots, x_n$, $n \geq 1$.

$$\mathbb{C}[x_0, \ldots, x_n]_d = \{f \in \mathbb{C}[x_0, \ldots, x_n] \text{ omegeneo di grado } d \geq 1\}.$$

$f \in \mathbb{C}[x_0, \ldots, x_n]_d$ si dice *forma omogenea di grado d*.

Se $d = 1$, diremo forma lineare; se $d = 2$, forma quadratica, etc, etc.

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 Sylvester 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

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

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

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

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*).