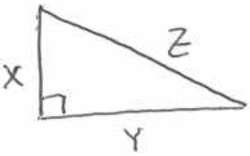
UN PROBLEMA DIOFANTEO :

Trovare un triangolo rettangolo con lati <u>interi</u>, la cui area sia un quadrato, <u>intero</u>.



$$\begin{cases} X^2+Y^2=Z^2 \\ \frac{1}{2}XY=W^2 \end{cases} \quad \text{o} \quad \begin{cases} X^2+Y^2-Z^2=0 \\ XY-2W^2=0 \end{cases} \qquad (1)$$

Questo è un sistema di equazioni <u>diofantee</u>, cioè polinomiali ed a coefficienti in $\mathbb{Z}$.

Ne cerchiamo le soluzioni <u>in $\mathbb{Z}^4$</u>, con la restrizione

$0 < X \le Y$.

Osserviamo che entrambe le equazioni in (1) sono <u>omogenee</u>. Quindi <u>l'ambiente naturale</u> in cui cercare di risolverle è <u>$\mathbb{P}^3$</u>.

Penseremo $\mathbb{P}^3$ sul campo dei numeri complessi $\mathbb{C}$.

$(X:Y:Z:W)$ sono coordinate omogenee.

$\boxed{\text{PAG. 7}}$

Risolvere un problema diofanteo significa <u>SPIEGARE</u>!

1. Vedere se esistono soluzioni (sol. <u>non banali</u>).
2. In caso affermativo, vedere se l'insieme di tali soluzioni ha una qualche "struttura".

Un passo preliminare è capire la "geometria" del problema, cioè studiare l'insieme di <u>tutte</u> le soluzioni di (1) in $\mathbb{P}^3_{\mathbb{C}}$. Lo indicheremo con $\underline{S}$.

Le due equazioni in (1) definiscono ciascuna

una superficie quadrica di $\mathbb{P}^3$

$Q_1 \quad X^2+Y^2-Z^2=0 \qquad\qquad Q_2 \quad XY-2W^2=0$

Quindi $S = Q_1 \cap Q_2$.

Analogamente a quanto si fa per le coniche, possiamo associare a Q_1 ed a Q_2 una matrice 4×4 simmetrica:

$$Q_1 \rightsquigarrow A = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & 0 \end{bmatrix} \underset{\text{SPIEG.}}{\hookleftarrow} \qquad Q_2 \rightsquigarrow B = \begin{bmatrix} 0 & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \end{bmatrix}$$

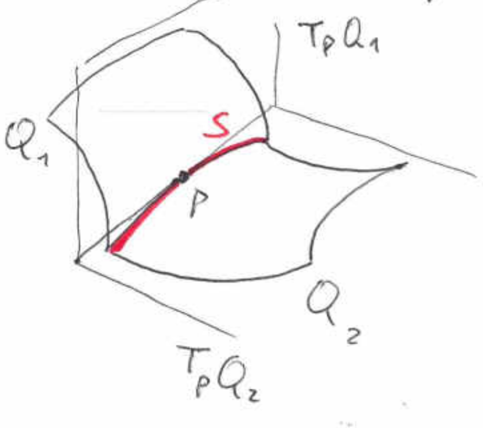
$\underline{rg(A) = rg(B) = 3}$

Da queste segue subito che sia Q_1 che Q_2 sono dei <u>coni</u>, cioè quadriche irriducibili, con un unico punto singolare: rispettivamente $E_3=(0:0:0:1)$ per Q_1 e $E_2=(0:0:1:0)$ per Q_2. Si verifica subito che

$\underline{E_3 \notin S}$ e $\underline{E_2 \notin S}$.

Quindi, sia Q_1 che Q_2 sono superfici lisce in ciascun punto di S. Cioè per ogni $P \in S$ esistono i piani tangenti T_PQ_1 e T_PQ_2.

<u>Se</u> per un dato $P \in S$ si ha che $T_PQ_1 \neq T_PQ_2$, allora le superfici Q_1 e Q_2 si intersecano



<u>TRASVERSALMENTE</u> in un intorno di P.

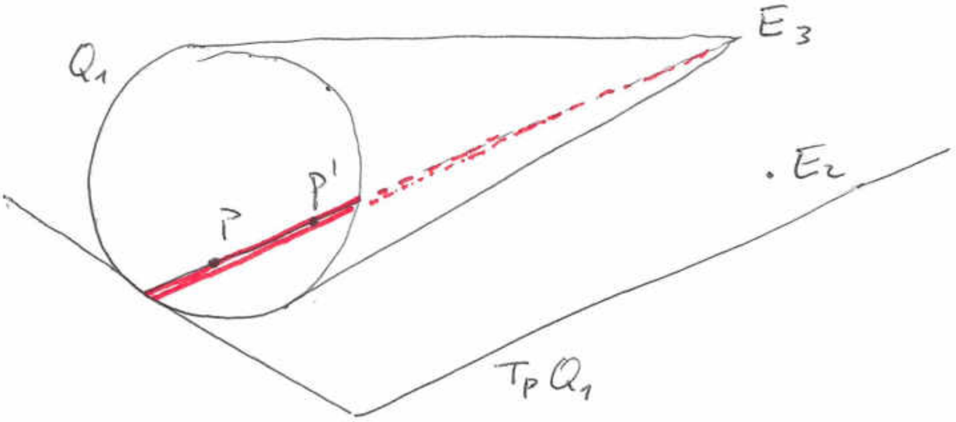
Quindi S è una <u>curva</u> non singolare in un intorno di P.

<u>Vediamo</u> se può accadere che $T_PQ_1 = T_PQ_2$.

$E_3 \notin S$

$E_3 \notin S \quad P \in S \implies P \neq E_3$

Q_1 è un cono di vertice $E_3 \Rightarrow$ la retta PE_3 è tutta contenuta in Q_1.



Inoltre, ~~[illegible]~~ il piano tangente a Q_1 è lo stesso per tutti i punti $P' \in Q_1$, con P' sulla retta PE_3, $P' \neq E_3$.

$Q_1 \cap T_P Q_1$ è la retta PE_3 CONTATA 2 VOLTE.

~~Lo stesso~~ vale per il cono Q_2, col suo vertice E_2.

Fatti analoghi valgono

Quindi, supponiamo che per un certo $P \in S$ si abbia $T_P Q_1 = T_P Q_2$.

Allora tale piano contiene sia E_2 che E_3, cioè è un piano del fascio di sostegno la retta $E_2 E_3$.

$$\begin{cases} X = 0 \\ Y = 0 \end{cases} \text{ equazioni cart. di } E_2E_3 \implies \lambda X + \mu Y = 0$$

è l'equazione per il generico piano di tale fascio. $(\lambda, \mu) \neq (0,0)$.

Le indeterminate X, Y giocano un ruolo simmetrico nelle (1). Quindi, supponiamo $\lambda \neq 0$ e poniamo $t = \mu/\lambda$

$$\begin{cases} X + tY = 0 \\ X^2 + Y^2 - Z^2 = 0 \end{cases} \Rightarrow \begin{cases} X = -tY \\ X^2 + Y^2 - Z^2 = 0 \end{cases} \quad (1+t^2)Y^2 - Z^2 = 0$$

rappresenta una retta contata 2 volte

$\iff 1 + t^2 = 0 \iff \underline{t = \pm i}$

Ma un'analoga situazione si dovrebbe avere per Q_2:

$$\begin{cases} X = -tY \\ XY - 2W^2 = 0 \end{cases} \quad -tY^2 - 2W^2 = 0$$

rappresenta una retta contata 2 volte $\iff \underline{t = 0}$

Riassumendo:

- i piani del fascio di sostegno la retta E_2E_3 che intersecano Q_1 in una retta contata due volte sono

$$X + iY = 0 \qquad e \qquad X - iY = 0 \qquad (i \in \mathbb{C} \quad i^2 = -1)$$

- i piani dello stesso fascio, che intersecano Q_2 in una retta contata due volte sono

$$X = 0 \qquad e \qquad Y = 0$$

Pertanto possiamo concludere che per ogni $P \in S$ si ha $\underline{T_P Q_1 \neq T_P Q_2}$. Quindi, per quanto osservato sopra

<u>S è una curva priva di punti singolari</u>.

Per proseguire abbiamo bisogno di richiamare il

<u>TEOREMA DI BEZOUT</u>

$\mathbb{P}$ piano <u>proiettivo</u>, sul campo $\mathbb{C}$ dei numeri complessi

$C, D \subset \mathbb{P}$ due curve definite risp. dalle equazioni

$F = 0 \qquad G = 0 \qquad F, G \in \mathbb{C}[X_0, X_1, X_2]$ pol. <u>omogenei</u>

$\deg(F) = m \quad \deg(G) = n$.

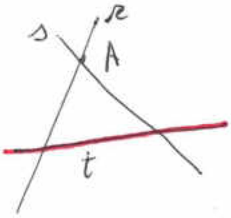
Supponiamo che C, D non abbiano componenti irriducibili in comune. Allora si può provare che $C \cap D$ è un insieme <u>finito</u>.

Se $P \in C \cap D$ è possibile associare a P un numero intero ≥ 1 chiamato la molteplicità di intersezione di C e D in P. Questa è ben definita ed <u>unica</u>, nel senso che i vari modi possibili per definirla danno lo stesso risultato. Tutti questi modi sono faccende delicate.... $i(P, C \cap D; \mathbb{P})$

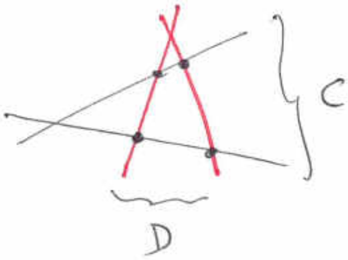
Allora, se C, D sono come sopra, il teorema di Bezout afferma che

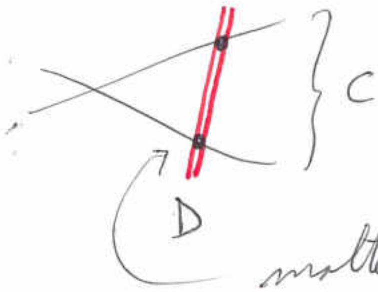
$$\sum_{P\in C\cap D} i(P, C\cap D) = m\cdot n$$

Per esempio, se $m=n=2$ allora ci dice che due coniche prive di componenti irriducibili comuni si intersecano in 4 punti purché questi vengano contati con molteplicità. Vediamo qualche caso concreto:

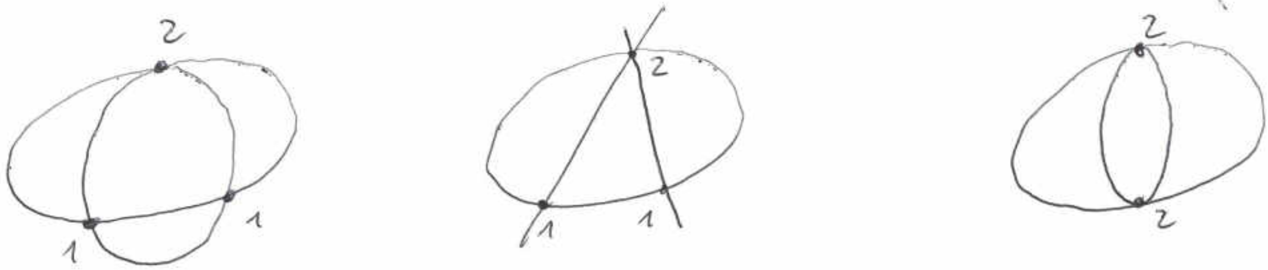
- 

  $C = r\cup t$ $\quad D = s\cup t$ sono due coniche con una componente irriducibile comune $C\cap D = t\cup\{A\}$, che possiede infiniti punti.

- 

- 

  molteplicità = 2



ecc.

Un altro caso importante del teorema di Bezout, che ci sarà utilissimo tra un momento, è quello in cui D è una retta, cioè $n=1$:

nel piano proiettivo complesso, ogni curva di grado m, che non contenga una retta tra le sue componenti, è intersecata da una qualsiasi retta in m punti, purché questi vengano contati con molteplicità. <u>INTERPRETAZIONE GEOMETRICA DEL GRADO</u>

COMMENTARE!

PROPOSIZIONE

Un qualsiasi piano H di $\mathbb{P}^3$ interseca S in 4 punti.

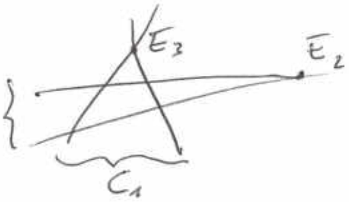
TEATRO

Dim.

$H \cap Q_1 = C_1$ è una conica. C_1, C_2 sono coniche

$H \cap Q_2 = C_2$ —— " —— nel piano proiettivo su $\mathbb{C}$ H.

Se C_1, C_2 sono entrambe spezzate in due rette, allora non hanno nessuna componente in comune per ovvi motivi ed il risultato segue da Bezout.



La stessa conclusione si ha se una tra C_1 e C_2 è irriducibile e l'altra si spezza in due rette.

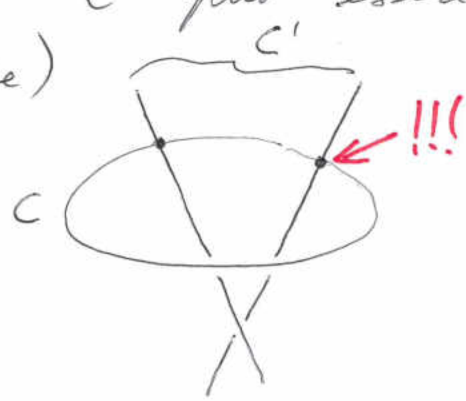
Infine, siano C_1, C_2 entrambe irriducibili.

Se $C_1 \neq C_2$ concludiamo come sopra.

Può essere $C_1 = C_2$? Poniamo $C_1 = C_2 = C$

Ma allora $C \subset Q_1 \cap Q_2 = S \Rightarrow S = C \cup C'$

Chi è C' ? C' può essere formato o da due rette (sghembe)



Si può dimostrare che ~~[illegible]~~ $C \cup C'$ è connesso

Ma nei punti di $C \cap C'$ la curva S non sarebbe liscia. Assurdo SPIEGARE

oppure C' è una conica.

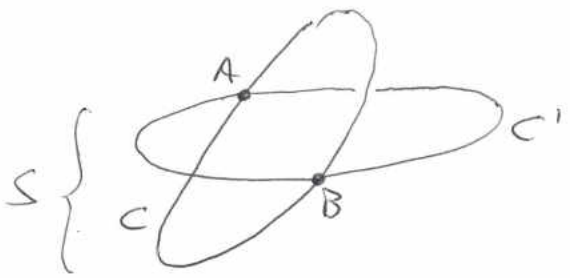
In tal caso $C' \subset H'$ H' piano di $\mathbb{P}^3$.

$H \neq H'$ (si esclude che $H = H'$ basandosi sempre sul fatto che S è privo di punti singolari)

$H \cap H' = R$ è una retta. Infine

$C = H \cap Q_1 \qquad C' = H' \cap Q_1$ da cui

$$R \cap Q_1 = \{A, B\} = H \cap H' \cap Q_1 = (H \cap Q_1) \cap (H' \cap Q_1) = C \cap C'$$



e di nuovo questo contrasta col fatto che S sia una curva liscia. ∎

Ritorniamo al sistema di equazioni diofantee (1).

L'omogeneità delle equazioni in (1) ci permette di dire che possiamo cercare le sue soluzioni in $\mathbb{Q}^4$: se ne troviamo una $(x_0 : y_0 : z_0 : w_0)$, moltiplicandola per il m.c.m dei denominatori di x_0, y_0, z_0, w_0 troviamo una soluzione in $\mathbb{Z}^4$. SPIEGARE!

Quel che abbiamo guadagnato rispetto a lavorare su $\mathbb{Z}$ è che $\mathbb{Q}$ è un campo!

Quindi, fino a che ci farà comodo, penseremo i coeff. delle equaz. in (1) presi in $\mathbb{Q}$ e cercheremo le soluz. di (1) in $\mathbb{Q}^4$.

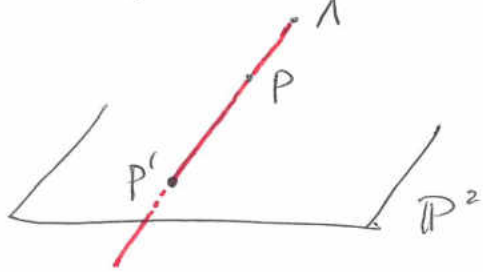
Un'altra osservazione da fare è che lavorando in $\mathbb{P}^3$ si usano "troppe" indeterminate.

Illustreremo adesso un procedimento che permette di risparmiare sul numero di indeterminate, passeremo da 4 a 3, e permette anche di calare il grado da 4 a 3. SPIEGARE

una coincidenza ...

PROIEZIONE DI S IN UN $\mathbb{P}^2$

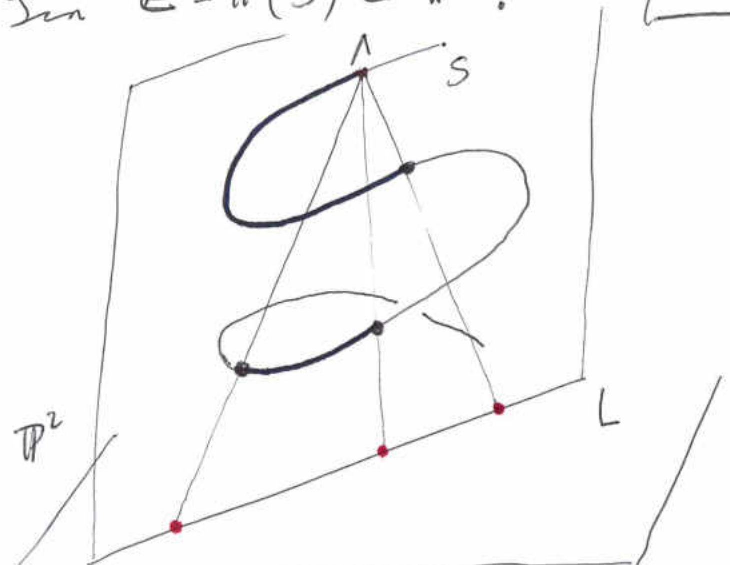
Preso un punto $\Lambda \in \mathbb{P}^3$ ed un piano $\mathbb{P}^2 \subset \mathbb{P}^3$ tale che $\Lambda \notin \mathbb{P}^2$, possiamo associare ad ogni punto P di $\mathbb{P}^3$, con $P \neq \Lambda$ il punto P' di $\mathbb{P}^2$ dato dall'intersezione $P\Lambda \cap \mathbb{P}^2$



Otteniamo così un'applicazione
$\pi : \mathbb{P}^3 - \{\Lambda\} \longrightarrow \mathbb{P}^2$.
Vedremo che l'immagine di S in π è una curva <u>algebrica</u> in $\mathbb{P}^2$, detta proiezione di S sul piano $\mathbb{P}^2$.

Che cosa succede se <u>$\Lambda \in S$</u> ? Cioè: chi è $\pi(\Lambda)$?
Possiamo prendere come retta da intersecare con $\mathbb{P}^2$ la <u>retta tangente</u> ad S in Λ. TEATRO

Sia $E = \pi(S) \subset \mathbb{P}^2$. <u>Qual'è il grado di E?</u>



Sia $L \subset \mathbb{P}^2$ una qualsiasi retta.
Poiché $\Lambda \notin \mathbb{P}^2$, esiste un unico piano $H \subset \mathbb{P}^3$ che contiene sia L che Λ.
$H \cap S$ è formato da 4 punti se questi vengono contati con molteplicità.

Uno di questi quattro punti è Λ. Quindi fuori da Λ vi sono 3 punti di $H \cap S$. Le loro immagini in π sono tre punti di L. Dunque
$E \cap L$ consta di 3 punti (contati con molteplicità)

ovvero <u>E ha grado 3</u>.

Scegliamo come Λ il punto $\underline{(0:1:1:0)}$ di S (9
e come $\mathbb{P}^2$ il piano di equazione $z=0$. COMMENTARE

$A=(x:y:z:w)$ $A\neq\Lambda$. La retta $A\Lambda$ ha equaz. parametriche

$$\begin{cases} \rho X = \lambda x \\ \rho Y = \lambda y + \mu \\ \rho Z = \lambda z + \mu \\ \rho W = \lambda w \end{cases}$$

$\rho \in \mathbb{C}^*$

Intersechiamo tale retta col piano $Z=0$:

$\lambda z+\mu=0$ $\lambda=1$ $\mu=-z$ quindi

$\boxed{A'=\pi(A)=(x:y-z:w)}$ (2)

Calcoliamo $\pi(S)$ (è un calcolo "brutale" ...)

$\forall (x:y:z:w)\in S$ $A\neq\Lambda$

è soddisfatta: $x^2+y^2-z^2=0$, da cui $(y-z)(y+z)=-x^2$ $\overset{\text{allegramente}}{\Longrightarrow}$

$$y+z=\frac{-x^2}{y-z} \Rightarrow 2y = y-z+y+z = y-z-\frac{x^2}{y-z} \Rightarrow y=\frac{(y-z)^2-x^2}{2(y-z)}$$

Sostituisco quest'espressione di y nella seconda delle (1):

$xy-2w^2=0$ è soddisfatta $\Rightarrow$ $x\,\dfrac{(y-z)^2-x^2}{2(y-z)}-2w^2=0$ $\Rightarrow$

$$x(y-z)^2-x^3-4(y-z)w^2=0$$

Quindi $\pi(S)$ è la curva ottenuta intersecando la superficie di equazione:

(3) $X(Y-Z)^2-X^3-4(Y-Z)W^2=0$ $\Leftarrow$ È L'EQ DI...

con il piano $Z=0$.

Nelle coordinate omogenee $(X:Y:W)$ nel piano $Z=0$

dunque, l'equazione di $\pi(S)$ è

10

i) $\boxed{XY^2 - X^3 - 4YW^2 = 0}$ (4') $XY^2 - X^3 - YT^2 = 0$

Volendo, si può fare un piccolo cambiamento di coordinate $T = 2W$ e la (4) diviene

Infine, calcoliamo la retta tangente ad S in A

$F = X^2 + Y^2 - Z^2 \Rightarrow F_X = 2X \quad F_Y = 2Y \quad F_Z = -2Z \quad F_W = 0$

e $T_A Q_1$ ha equazione $Y - Z = 0$

$G = XY - 2W^2 \Rightarrow G_X = Y \quad G_Y = X \quad G_Z = 0 \quad G_W = -4W$

e $T_A Q_2$ ha equazione $X = 0$

Dunque la retta tangente ad S in A, cioè $T_A Q_1 \cap T_A Q_2$ ha equazioni

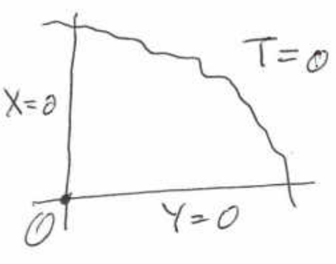
$$\begin{cases} Y - Z = 0 \\ X = 0 \end{cases}$$

e quindi interseca il piano $Z = 0$ nel punto

$(X : Y : Z : W) = (0 : 0 : 0 : 1)$ ovvero nel punto $(X : Y : T) = \underline{(0 : 0 : 1) = \pi(A)}$. D'ora in poi lo chiameremo

O.

Che tipo di punto è O per E?



Divido (4') per T^3:

$$\frac{X}{T}\left(\frac{Y}{T}\right)^2 - \left(\frac{X}{T}\right)^3 - \frac{Y}{T} = 0 \qquad u = \frac{X}{T} \quad v = \frac{Y}{T}$$

$$uv^2 - u^3 - v = 0$$

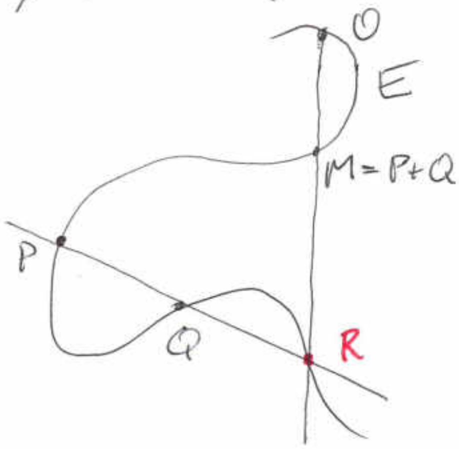
La retta tangente ad E in O ha equazione $v = 0$
Interseco tale retta tangente con E:

$$\begin{cases} u v^2 - u^3 - v = 0 \\ v = 0 \end{cases} \qquad \begin{cases} u^3 = 0 \\ v = 0 \end{cases} \Longrightarrow$$ O è punto di flesso per E

Si verifica subito a partire da (4') che la curva E è priva di punti singolari.

STRUTTURA DI GRUPPO ABELIANO DI E

Siano $P, Q \in E$ punti qualsiasi, anche uguali. Consideriamo la retta PQ. Se $P = Q$ prenderemo per tale retta la retta tangente ad E in P.



Per il Teorema di Bezout:

$PQ \cap E = \{P, Q, R\}$

Considero la retta RO

$RO \cap E = \{R, O, M\}$

$\boxed{M \overset{def}{=} P+Q} = Q+P$ chiaramente

$P + O = ?$ $\quad PO \cap E = \{P, O, R\}$ $\quad OR \cap E = \{O, R, P\}$

Dunque $P + O = P \quad \forall P \in E$

O è l'elemento neutro per tale operazione.

NB Poichè O è un flesso per E, si ha $O + O = O$.

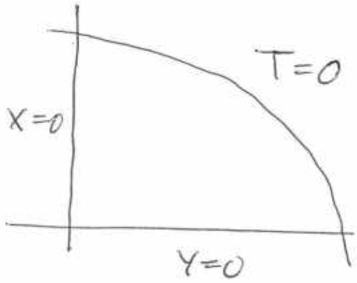
Preso comunque $P \in E$ voglio vedere se esiste "$-P$" (questo ci permetterà di usare in maniera più sostanziosa il fatto che O è punto di flesso per E)

$OP \cap E = \{O, P, Q\}$ $\quad P + Q = ?$ $\quad PQ \cap E = \{P, Q, O\}$

OO è la retta tg ad E in O. $\quad OO \cap E = \underbrace{\{O, O, O\}}_{\text{O è di flesso per E}}$

Dunque $P+Q=O$, ovvero $\underline{Q=-P}$.

È noioso verificare che <u>tale addizione è associativa</u>. Quindi <u>$(E,+)$ è un gruppo abeliano</u>.



$$XY^2-X^3-YT^2=0$$

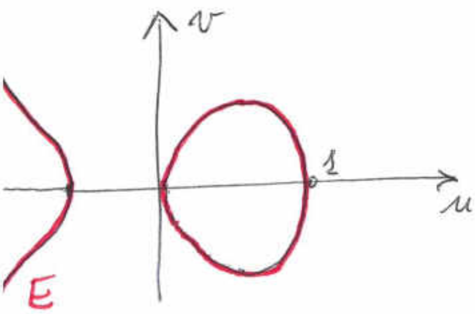
Vogliamo "spedire all'infinito" l'asse X.
Basta dividere (4') per Y^3:

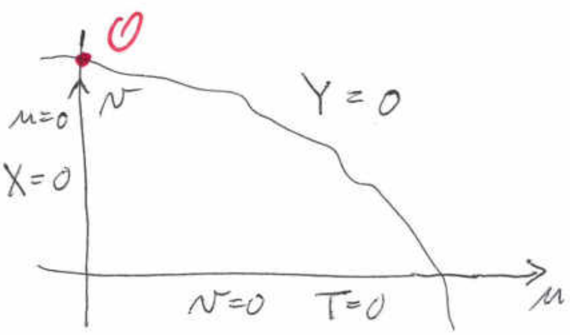
$$\frac{X}{Y}-\left(\frac{X}{Y}\right)^3-\left(\frac{T}{Y}\right)^2=0 \qquad u=\frac{X}{Y} \quad v=\frac{T}{Y} \qquad \boxed{v^2=-u^3+u}$$

Vediamo come è fatto l'insieme dei punti <u>reali</u> definiti da tale equazione:
(cioè $(u,v)\in\mathbb{R}^2$)

$$-u^3+u\geq 0 \iff u\in(-\infty,-1]\cup[0,1]$$

Fissato comunque u_0 in tale insieme, l'equazione $v^2=-u_0^3+u_0$ ha due soluzioni distinte o coincidenti. Vediamo così che <u>E è simmetrica rispetto all'asse u</u>





Quindi, se P è un qualsiasi punto del piano u,v, è facilissimo tracciare la retta PO: è la parallela all'asse v passante per P.

Ritorniamo al problema diofanteo originale (1).

Sia $A = (x : y : z : w) \in S$ con $\underline{x, y, z, w \in \mathbb{Q}}$

una sua soluzione. Allora, per le (2) $\pi(A) = (x : y - z : w)$

e si ha ancora $\underline{x, y - z, w \in \mathbb{Q}}$.

Infine, anche con il semplice cambiamento di coordinate:

$$\begin{cases} X = X \\ Y = \quad Y \\ T = \qquad 2W \end{cases}$$

il punto $\underbrace{\text{che}}_{(x:y:t)}$ si ottiene è ancora tale che $\underline{x, y, t \in \mathbb{Q}}$

$S(\mathbb{Q}) \overset{\text{def}}{=} \{ (x : y : z : w) \in S \mid x, y, z, w \in \mathbb{Q} \}$

$E(\mathbb{Q}) \overset{\text{def}}{=} \{ (x : y : t) \in E \mid x, y, t \in \mathbb{Q} \}$ Quindi

$$\begin{array}{ccc} S & \xrightarrow{\pi} & E \\ \cup & & \cup \\ S(\mathbb{Q}) & \xrightarrow[\pi]{} & E(\mathbb{Q}) \end{array}$$

si può provare che questa applicazione è biiettiva

Anche questa lo è.

$O \in E(\mathbb{Q})$

Siano $P, Q \in E(\mathbb{Q})$. Allora la retta PQ ha un'equazione cartesiana tutti i coeff. della quale sono in $\mathbb{Q}$.

Oppure (supponiamo per semplicità che si abbia $P \neq Q$).

sia $P = (p_1 : p_2 : p_3)$ $Q = (q_1 : q_2 : q_3)$ con $\underline{p_i, q_i \in \mathbb{Q}}$ $i = 1, 2, 3$

Allora equazioni parametriche per la retta PQ sono

$\rho x = \lambda p_1 + \mu q_1$ $(\lambda, \mu) \neq (0, 0)$ più precisamente: $(\lambda : \mu) \in \mathbb{P}^1$

$\rho y = \lambda p_2 + \mu q_2$ (5) $\rho \in \mathbb{C}^*$

$\rho t = \lambda p_3 + \mu q_3$

Anche i coefficienti dell'equazione (4') di E sono tutti razionali (sono addirittura in $\mathbb{Z}$).

Allora, per calcolare $E \cap PQ$ si fa:

$$(\lambda p_1+\mu q_1)(\lambda p_2+\mu q_2)^2-(\lambda p_1+\mu q_1)^3-(\lambda p_2+\mu q_2)(\lambda p_3+\mu q_3)^2=0$$

Mettendo a posto i calcoli si ottiene:

$\psi(\lambda,\mu)=0$ dove ψ è un polinomio (nelle indeterminate λ,μ), a coeff. in $\mathbb{Q}$, omogeneo, di grado 3.

Cioè:

(5) $\boxed{\alpha_0\lambda^3+\alpha_1\lambda^2\mu+\alpha_2\lambda\mu^2+\alpha_3\mu^3=0}$ $\quad$ $\underline{\alpha_0,\alpha_1,\alpha_2,\alpha_3\in\mathbb{Q}}$

Gli "α" sono impastati con i p_i ed i q_j.

Ma $P,Q\in E$, quindi $(\lambda:\mu)=(1:0)$ e $(\lambda:\mu)=(0:1)$ sono soluzioni di (5). Quindi necessariamente $\alpha_0=\alpha_3=0$ e la (5) diventa:

(5') $\alpha_1\lambda^2\mu+\alpha_2\lambda\mu^2=0$

Ora possiamo supporre tranquillamente $\lambda\neq 0$ e $\mu\neq 0$. Ma allora, dividendo la (5') per $\lambda\mu$ otteniamo:

$$\alpha_1\lambda+\alpha_2\mu=0$$

che ha la soluzione $(\lambda:\mu)=(\alpha_2:-\alpha_1)$ $\quad$ $\underline{\alpha_2,-\alpha_1\in\mathbb{Q}}$

Inserendo tali valori di λ,μ nella (5) si ottiene che $\underline{R\in E(\mathbb{Q})}$ dove $PQ\cap E=\{P,Q,R\}$.

Da questo e da $O\in E(\mathbb{Q})$ segue che <u>$E(\mathbb{Q})$ è un gruppo abeliano rispetto all'addizione di punti su E (è un sottogruppo di E)</u>.

<u>ESEMPIO</u> È un caso dell'Ultimo Teorema di Fermat.

$\mathbb{P}^2$ $(X:Y:Z)$ $\qquad$ E def. da $X^3+Y^3-Z^3=0$ (7)

Secondo l'UTF questa equazione <u>non ha</u> soluzioni in $\mathbb{Z}^3$ diverse da quelle "banali", in cui almeno uno tra X, Y, Z è nullo.
Il caso $n=3$ è stato <u>dimostrato</u> da Eulero.

Vediamo le soluzioni banali in $\mathbb{R}^2$

$P(0:1:1)=(0:-1:-1)$ $\qquad$ $Q(1:0:1)=(-1:0:-1)$

$R(1:1:0)=(-1:-1:0)$

$P, Q, R \in E(\mathbb{Q})$

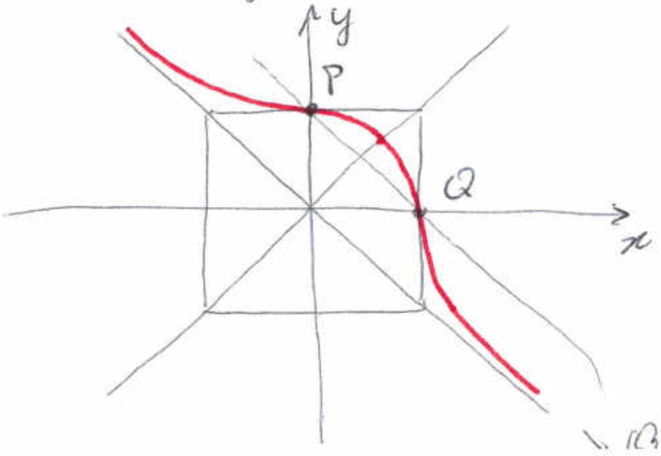
UTF, $n=3$ (Eulero) $\Rightarrow$ $E(\mathbb{Q})=\{P, Q, R\}$

Quindi $E(\mathbb{Q}),+$ è necessariamente un gruppo <u>ciclico</u> di ordine 3. Verifichiamolo un po'.

$x=\dfrac{X}{Z}$ $\quad$ $y=\dfrac{Y}{Z}$ $\qquad$ Suppongo $Z\neq 0$, divido (7) per Z^3

$x^3+y^3-1=0$

I punti in $\mathbb{R}^2$ che verificano tale relazione sono il grafico della funzione $y=\sqrt[3]{1-x^3}$.



P, Q flessi di E $\Rightarrow$
$O:=R$ è ancora flesso di E

Lo si può anche verificare direttamente.

$2P = P + P = Q \qquad 3P = Q + P = \mathcal{O}$ l'el.to neutro di $E(\mathbb{Q})$

$2Q = P$

<u>ESEMPIO</u> $E \subset \mathbb{P}^2$ sia definita da

$$(8) \qquad X^3 - 4XZ^2 - Y^2Z + 4Z^3 = 0$$

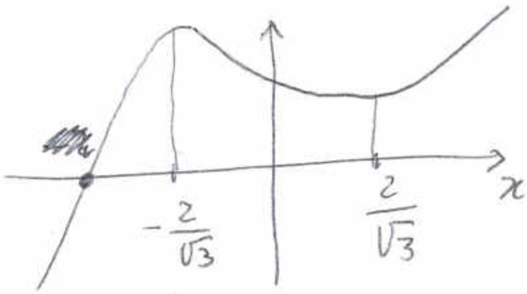
$\mathcal{O} = (0:1:0)$ è l'unico punto improprio (cioè con "Z" $= 0$) di E, ed è punto <u>di flesso</u>. <u>$\mathcal{O} \in E(\mathbb{Q})$</u>

Per studiare gli altri punti, essendo "Z" $\neq 0$ possiamo dividere (8) per Z^3

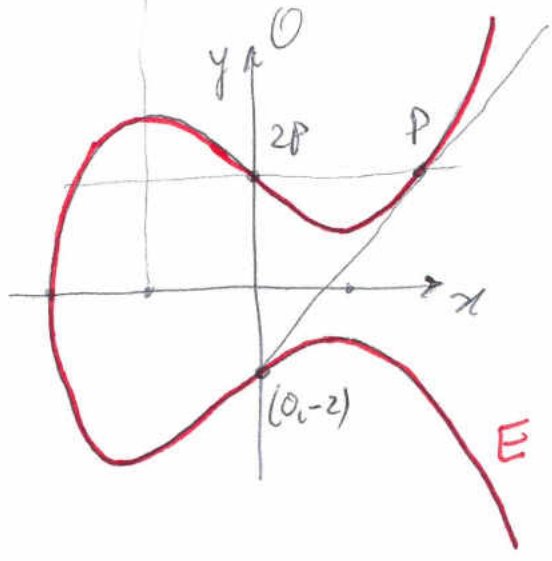
$$\left(\frac{X}{Z}\right)^3 - 4\,\frac{X}{Z} - \left(\frac{Y}{Z}\right)^2 + 4 = 0 \qquad x = \frac{X}{Z} \quad y = \frac{Y}{Z} \quad (9)\ \boxed{y^2 = X^3 - 4X + 4}$$

$$f(x) = X^3 - 4X + 4 \qquad f'(X) = 3X^2 - 4 \qquad f' = 0 \text{ per } X = \pm\frac{2}{\sqrt{3}}$$

$$f\left(\frac{2}{\sqrt{3}}\right) = \frac{-16 + 12\sqrt{3}}{3\sqrt{3}} > 0 \qquad f\left(-\frac{2}{\sqrt{3}}\right) = \frac{16 + 12\sqrt{3}}{3\sqrt{3}} > f\left(\frac{2}{\sqrt{3}}\right)$$



Quindi $X^3 - 4X + 4$ ha un'unica radice reale.



Elementi di $E(\mathbb{Q})$ che si vedono ad occhio dalla (9) sono

$(-2,0)$	$(0,2)$ 2P	$(0,-2)$	$(1,1)$
$(2,2)$ P	$(2,-2)$	$(-2,2)$	$(-2,-2)$ 3P

Sia $P=(2,2)$. Calcoliamo la retta tangente ad E in P

$f(x,y) = x^3 - y^2 - 4x + 4 \qquad f_x = 3x^2 - 4 \qquad f_y = -2y$

$f_x(P) = 8 \qquad f_y(P) = -4$ e la retta tangente è

$8(x-2) - 4(y-2) \iff y = 2x-2$ retta t

Interseco tale retta con E:

$$\begin{cases} x^3 - y^2 - 4x + 4 = 0 \\ y = 2x - 2 \end{cases} \qquad \begin{aligned} & x^3 - (2x-2)^2 - 4x + 4 = \\ & = x^3 - 4x^2 + 8x \cancel{-4} - 4x \cancel{+4} = \\ & = x^3 - 4x^2 + 4x = x(x-2)^2 \end{aligned}$$

Quindi, oltre a P con molteplicità 2, in tale intersezione troviamo il punto $(0,-2)$. Quindi

$\underline{2P = (0,2)} = R$

Calcoliamo $3P = 2P + P$

La retta RP è $y=2$ che, oltre che in P ed in R, interseca E anche in $(-2,2)$. Dunque

$3P = (-2,-2) = Q$

Verificare che $\quad 4P = (1,-1) \quad 5P = (6,-14) \quad 6P = (8,22)$

È possibile dimostrare che $\underline{E(\mathbb{Q}), + \simeq \mathbb{Z}, +}$

<u>TEOREMA DI MORDELL-WEIL</u> (Anni Venti del XX Secolo)

Se $E \subset \mathbb{P}^2$ è una curva definita da un'equazione del tipo $y = x^3 + ax^2 + bx + c$, con

$a, b, c \in \mathbb{Q}$ e x^3+ax^2+bx+c dotata di tre radici distinte in $\mathbb{C}$, allora $E(\mathbb{Q})$ è un gruppo abeliano finitamente generato

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T \qquad r: \text{il rango di } E$$

dove T è un gruppo finito.

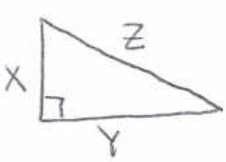
---

r è l'oggetto di una congettura. Chi la dimostrerà (o la confuterà) si prenderà 10^6 \$ .....

CONCLUSIONE

Il problema diofanteo (1) non ha soluzioni non banali. Con le parole di Fermat: "l'area di un rettangolo in numeri (interi) non può essere un quadrato (di un numero intero)".

La dimostrazione di questo è l'unica dimostrazione di Fermat che ci è rimasta. Eccola



Supponiamo che $(X, Y, Z) \in \mathbb{N}^3$ sia una terna pitagorica $X^2+Y^2=Z^2$ $(XYZ \neq 0)$

È lecito supporre che X, Y, Z siano primi tra loro.

Allora è noto che $(X, Y, Z) = (2pq, p^2-q^2, p^2+q^2)$ con p, q primi tra loro, $p>q$ e $p-q$ dispari.

L'area di tale rettangolo è

$$\frac{1}{2} XY = pq(p^2-q^2) = pq(p+q)(p-q) \qquad (9)$$

È chiaro che $p, q, p+q, p-q$ sono a due a due primi tra loro.

Quindi, se il numero in (9) è un quadrato

$\Rightarrow \quad p = x^2 \quad q = y^2 \quad p+q = u^2 \quad p-q = v^2$ dove

u, v devono essere entrambi dispari ? e primi tra loro.

Allora, posto $z = uv$, si ha:

$$x^4 - y^4 = p^2 - q^2 = (p+q)(p-q) = u^2 v^2 = z^2$$

Cioè abbiamo costruito una soluzione dell'equazione

(10) $$X^4 - Y^4 = Z^2$$

Consideriamo $v^2 \quad x^2 \quad u^2$. Si ha

$$x^2 - v^2 = p - (p-q) = q = y^2 \qquad u^2 - x^2 = p + q - p = q = y^2$$

Dunque $u^2 = v^2 + 2y^2$ da cui

$$2y^2 = (u-v)(u+v)$$

$$\mathrm{MCD}(u-v, u+v) = 2$$

Allora uno tra $u-v, u+v$ è del tipo $2r^2$ e l'altro è del tipo $4s^2$. Pertanto

$$2u = u - v + u + v = 2r^2 + 4s^2$$

analogamente

Infine

$$4y^2 = 4r^2 \cdot 4s^2 \Longrightarrow \begin{cases} u = r^2 + 2s^2 \\ \pm v = r^2 - 2s^2 \\ y = 2rs \end{cases}$$

Usando queste ultime tre relazioni otteniamo:

$x^2 - v^2 = y^2$ cioè $x^2 = v^2 + y^2 = r^4 \cancel{- 4r^2s^2} + 4s^4 \cancel{+ 4r^2s^2}$

$u^2 - x^2 = y^2$ $\qquad x^2 = u^2 - y^2 = r^4 \cancel{+ 4r^2s^2} + 4s^4 \cancel{- 4r^2s^2}$

da cui $\underline{x^2 = r^4 + 4s^2}$

Dunque $(r^2, 2s^2, x)$ è una terna pitagorica
$\qquad$ ipotenusa

Inoltre l'area di tale triangolo è $(rs)^2$, il quadrato di un numero intero.

Quindi, a partire da una (ipotetica) soluzione
$(2pq, p^2-q^2, p^2+q^2)$ del nostro problema, ne abbiamo costruita un'altra
$(r^2, 2s^2, x)$

Ora $\underline{\underline{x = \sqrt{p} < p^2+q^2}}$. Ma si ha $0 < \underset{\mathbb{N}}{x} < \underset{\mathbb{N}}{p^2+q^2}$

Se applicassimo lo stesso procedimento a partire dalla soluzione $(r^2, 2s^2, x)$ di (1), questo ci porterebbe a costruire un'altra soluzione di (1), con l'ipotenusa un numero naturale >0, e $<x$.
E questo ci dà l'assurdo. ∎

METODO DELLA DISCESA (è un'idea di Fermat)