LICEO *B. RUSSELL* – A.S. 2011/2012 –
TERNE PITAGORICHE

Definizione. Chiamiamo *terna pitagorica* una terna di numeri naturali a, b, c che possono essere i lati di un triangolo rettangolo. Poiché un tale triangolo soddisfa il teorema di Pitagora, dal punto di vista algebrico una terna pitagorica è una terna (a, b, c) di numeri naturali non nulli che soddisfa la relazione

$$\boxed{a^2 + b^2 = c^2 \qquad\qquad a, b, c \in \mathbb{N}^\star}$$

Notiamo che se (a, b, c) è una terna pitagorica, anche la terna $a' = ka,\ b' = kb,\ c' = kc$ con $k \in \mathbb{N}$ è una terna pitagorica. Infatti:

$$(a')^2 + (b')^2 = (ka)^2 + (kb)^2 = k^2a^2 + k^2b^2 = k^2\left(a^2 + b^2\right) = k^2c^2 = (kc)^2 = (c')^2$$

Parliamo di *terne pitagoriche primitive* riferendoci a terne (a, b, c) in cui $\mathrm{MCD}(a, b, c) = 1$.

Il più piccolo e quindi più famoso esempio di terna pitagorica primitiva è $3, 4, 5$. Infatti:

$$3^2 + 4^2 = 5^2$$

Tutti i numeri qui considerati sono Naturali non nulli, senza ulteriormente specificarlo. Vogliamo cercare le terne pitagoriche primitive. In realtà se una terna pitagorica è primitiva, vale anche la condizione, più forte, che tutte le tre coppie di numeri (a, b), (b, c) e (a, c) sono coprime. Vale infatti la seguente proprietà.

Proprietà 1. Se $\mathrm{MCD}(a, b, c) = 1$ allora $\mathrm{MCD}(a, b) = \mathrm{MCD}(a, c) = \mathrm{MCD}(b, c) = 1$.

Dimostrazione. Supponiamo per assurdo che $\mathrm{MCD}(a, b) \neq 1$. Di conseguenza a e b sono divisibili per uno stesso numero maggiore di 1; sia quindi p un numero primo che divide a e b. Allora $a = pk$ e $b = ph$, quindi

$$c^2 = (pk)^2 + (ph)^2 = p^2\left(k^2 + h^2\right)$$

Quindi p^2 divide c^2 e p divide anche c. Avendo supposto $\mathrm{MCD}(a, b, c) = 1$ otteniamo un asurdo, quindi deve essere $\mathrm{MCD}(a, b) = 1$.

In maniera del tutto anolaga si dimostra che anche $\mathrm{MCD}(b, c)$ e $\mathrm{MCD}(a, c)$ devono essere 1.

□

Cercando terne pitagoriche primitive possiamo quindi supporre a, b, c a due a due *coprimi*.

Analizziamo i possibili quadrati di numeri naturali. Distinguiamo il caso pari e dispari.

- Se n è un numero pari, allora $n = 2k$ e $n^2 = 4k^2$, cioè il resto della divisione di n^2 per 4 è 0.
- Viceversa se n è dispari, allora $n = 2k + 1$ e $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, cioè il resto della divisione di n^2 per 4 è 1.

Abbiamo quindi dimostrato la seguente proprietà.

Proprietà 2. Tutti i quadrati divisi per 4 danno resto 0 o 1 (cioè sono della forma $4m$ o $4m+1$ con $m \in \mathbb{N}$).

Supponiamo che (a, b, c) sia una terna pitagorica primitiva. Abbiamo osservato con la Proprietà 1 che a e b non possono essere entrambi pari (altrimenti sono entrambi divisibili per 2). Supponiamo ora che a e b siano entrambi dispari, cioè $a = 2k + 1$ e $b = 2h + 1$. Allora

$$a^2 + b^2 = (2k + 1)^2 + (2h + 1)^2 = 4k^2 + 4k + 1 + 4h^2 + 4h + 1 = 4\left(k^2 + k + h^2 + h\right) + 2.$$

Abbiamo però osservato con la Proprietà 2 che un numero del tipo $4t + 2$ non può essere un quadrato, quindi $a^2 + b^2 \neq c^2$. Di conseguenza a e b devono essere uno pari e l'altro dispari (notiamo quindi che c è dispari).

In conclusione:

Se (a, b, c) è una terna pitagorica primitiva allora

- $\mathrm{MCD}(a, b) = \mathrm{MCD}(a, c) = \mathrm{MCD}(b, c) = 1$.
- a e b sono di diversa parità (cioè uno pari e l'altro dispari); c è dispari.

Possiamo supporre a dispari e b pari; ricordiamo che c è dispari. Dalla relazione $a^2 + b^2 = c^2$, otteniamo

$$a^2 = c^2 - b^2 = (c - b)(c + b)$$

Date: January 9, 2012.

Analizziamo ora i due numeri $c-b$ e $c+b$. Vogliamo dimostrare la seguente proprietà:

Proprietà 3. $c+b$ e $c-b$ sono coprimi.

Dimostrazione. Dal momento che c e b sono uno dispari e l'altro pari, $c-b$ e $c+b$ sono dispari. Vogliamo dimostrare che $c+b$ e $c-b$ sono coprimi. Infatti supponiamo che p sia un divisore di entrambi. Notiamo che p è dispari perché lo sono $c \pm b$. Per ovvie ragioni se p divide due numeri, allora divide anche la loro somma e la loro differenza. Quindi

- p divide $(c+b)+(c-b)=2c$;
- p divide $(c+b)-(c-b)=2b$;

Poiché p è dispari ne segue che p divide b e c. Quindi ogni divisore p di $c+b$ e $c-b$ deve anche essere un divisore di b e c, e, dal momento che b e c sono coprimi, deve essere $p=1$. Di conseguenza $c+b$ e $c-b$ sono comprimi.

□

Torniamo ora all'equazione

$$a^2=(c-b)(c+b)$$

e prestiamo attenzione a questo passaggio delicato. Dal momento che $c \pm b$ sono coprimi segue che devono essere entrambi un quadrato. Cerchiamo di dare un'idea della dimostrazione di questo fatto. Sia p un divisore di a, allora come osservato all'inizio p^2 divide a^2 cioè p^2 divide $(c-b)(c+b)$. Questi due fattori p non possono dividere l'uno $c-b$ e l'altro $c+b$ perché $c \pm b$ non hanno divisori in comune. Quindi p^2 divide $c-b$ oppure p^2 divide $c+b$. In sostanza tutti i fattori p^2 di a^2 dividono o $c+b$ o $c-b$ che di conseguenza sono a loro volta dei quadrati. Vediamo un esempio. Proviamo a scrivere $a^2=15^2=125$ come prodotto di due numeri coprimi. Scomponiamo 125 in fattori primi: $125=15^2=(3\cdot 5)^2=3^2\cdot 5^2$. Di conseguenza abbiamo due sole fattorizzazioni con numeri coprimi

$$125=1\cdot 125=1^2\cdot 15^2$$
$$125=9\cdot 25=3^2\cdot 5^2$$

In entrambi i casi i due fattori sono quadrati.

Un altro esempio. Consideriamo $a^2=63^2=3969$. Di conseguenza $3969=3^4\cdot 7^2$ e le sole possibili fattorizzazioni con numeri coprimi sono

$$3969=1\cdot 63^2=1\cdot 3969$$
$$3969=3^4\cdot 7^2=9^2\cdot 7^2=81\cdot 49$$

Anche in questo caso i due fattori sono quadrati.

Essendo quindi $c \pm b$ due quadrati, esistono $h,k\in\mathbb{N}$ tali che

$$c+b=h^2 \qquad \text{e} \qquad c-b=k^2$$

ovvero

$$(c+b)+(c-b)=h^2+k^2 \qquad \Rightarrow \qquad c=\frac{h^2+k^2}{2}$$
$$(c+b)-(c-b)=h^2-k^2 \qquad \Rightarrow \qquad b=\frac{h^2-k^2}{2}$$

Inoltre

$$a^2=(c+b)(c-b)=h^2k^2 \qquad \Rightarrow \qquad a=hk$$

Notiamo che $c \pm b$ sono dispari, quindi h e k sono dispari (e coprimi, affinchè lo siano $c \pm b$) e $h^2 \pm k^2$ sono pari, quindi divisibili per 2. Inoltre presi a, b, c in questo modo:

$$a^2+b^2=(hk)^2+\left(\frac{h^2-k^2}{2}\right)^2=h^2k^2+\frac{h^4-2h^2k^2+k^4}{4}=\frac{4h^2k^2+h^4-2h^2k^2+k^4}{4}=\frac{h^4+2h^2k^2+k^4}{4}$$
$$=\left(\frac{h^2+k^2}{2}\right)^2=c^2$$

e otteniamo in effetti una terna pitagorica.

Infine:

Possiamo costruire **ogni** terna pitagorica primitiva prendendo due numeri naturali h e k, con $h > k$, dispari e coprimi e ponendo

$$\begin{cases} a = hk \\ b = \dfrac{h^2 - k^2}{2} \\ c = \dfrac{h^2 + k^2}{2} \end{cases}$$

Proviamo con qualche esempio

h	k	$a = hk$	$b = \dfrac{h^2 - k^2}{2}$	$c = \dfrac{h^2 + k^2}{2}$	$a^2 + b^2 = c^2$
3	1	3	4	5	9+16=25
5	1	5	12	13	25+144=169
5	3	15	8	17	225+64=289