1 Terne pitagoriche

Uno dei più antichi "problemi diofantei" è quello di determinare tutti i triangoli rettangoli che hanno i lati di lunghezza intera.

Sebbene, in generale, si attribuisce alla Scuola di Pitagora (VI sec., a.C.) lo studio dell'equazione $X^2 + Y^2 = Z^2$, sicuramente già i Babilonesi, mille anni prima, avevano una conoscenza molto approfondita di tale equazione e di molte sue soluzioni (incluse alcune non ovvie come ad esempio (6480, 4961, 8161)).

Nel libro X degli *Elementi* di Euclide (III sec. a.C.) e nel libro II dell'*Arithmetica* di Diofanto (III sec. d.C) sono elencate più o meno esplicitamente le soluzioni della equazione in oggetto e, sicuramente, esse appaiono nell'*Algebra* di Brahmegupta (VII sec. d.C). Segnaliamo, infine, che un intero volume dal titolo *Pythagorean Triangles* (New York, 1962) è stato dedicato da W. Sierpiński alla tematica di questo paragrafo.

Definizione 1.1. Una *terna pitagorica* (in breve, *tp*) è una terna di numeri interi non nulli (x, y, z) tale che $x^2 + y^2 = z^2$. Una *terna pitagorica* è detta *primitiva* (in breve, *tpp*) se, inoltre, $\text{MCD}(x, y, z) = 1$.

Osservazione 1.2. Si noti che (cfr. il successivo Lemma 1.6 (b)), se (x, y, z) è una tp, allora le seguenti affermazioni sono equivalenti.

(i) (x, y, z) è tpp;

(ii) $\text{MCD}(x, y) = 1$;

(iii) $\text{MCD}(x, z) = 1$;

(iv) $\text{MCD}(y, z) = 1$.

Lemma 1.3. *Ogni tp può essere ottenuta da una tpp moltiplicando gli elementi della terna per un intero opportuno.*

Dimostrazione. Sia (x, y, z) una tp. Supponiamo che $\text{MCD}(x, y, z) = d \neq 1$. Allora $x = dx_1$, $y = dy_1$, $z = dz_1$ con $x_1, y_1, z_1 \in \mathbb{Z}$ e $\text{MCD}(x_1, y_1, z_1) = 1$. È immediato che (x_1, y_1, z_1) è una tp (primitiva). Infatti:

$$x_1^2 + y_1^2 = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = z_1^2 \ .$$

□

Osservazione 1.4. È immediato che, se (x, y, z) è una tp, allora $(\pm x, \pm y, \pm z)$ è ancora una tp per ogni possibile scelta dei segni. Pertanto, nel seguito, ci limiteremo a considerare tpp nelle quali $x > 0$, $y > 0$, $z > 0$, cioè *tpp positive.*

Lemma 1.5. *Sia (x, y, z) una tpp positiva. Allora*

$$x \not\equiv y \pmod 2$$

(cioè x è pari (rispettivamente, dispari) se, e soltanto se, y è dispari (rispettivamente, pari)).

Dimostrazione. Se, per assurdo, x e y sono entrambi pari, allora $2 \mid (x^2 + y^2)$, cioè $2 \mid z^2$, quindi $2 \mid z$ e pertanto $2 \mid \mathrm{MCD}(x, y, z)$.

Se, per assurdo, x ed y sono entrambi dispari, allora $x^2 \equiv 1 \equiv y^2 \pmod 4$, dunque $2 \equiv z^2 \pmod 4$ e ciò è assurdo, perché il quadrato di ogni intero è congruo a $0, 1 \pmod 4$.

$\square$

Lemma 1.6. *Sia (x, y, z) una tpp positiva. Allora:*

(a) *a meno di uno scambio tra x e y, si ha che x è pari, y è dispari, z è dispari;*

(b) $\mathrm{MCD}(x, y) = \mathrm{MCD}(y, z) = \mathrm{MCD}(x, z) = 1$.

Dimostrazione. (a) Se x è pari allora, per il lemma precedente, y è dispari. Se, per assurdo, z è pari, allora risulta $y^2 = x^2 - z^2 \equiv 0 - 0 = 0 \pmod 4$, mentre $y^2 \equiv 1 \pmod 4$.

(b) Supponiamo, ad esempio, che $\mathrm{MCD}(y, z) = d \neq 1$ e sia p un primo tale che $p \mid d$. Allora si ha che $p \mid y^2$, $p \mid z^2$ dunque $p \mid z^2 - y^2 = x^2$ da cui $p \mid x$. Quindi $p \mid \mathrm{MCD}(x, y, z) = 1$, donde un assurdo.

$\square$

Lemma 1.7. *Siano $a, b, c, n \in \mathbb{N}^+$. Se $ab = c^n$ e $\mathrm{MCD}(a, b) = 1$, allora esistono due interi positivi a_1, b_1 tali che*

$$a = a_1^n\,, \quad b = b_1^n\ .$$

Dimostrazione. Supponiamo, per evitare casi banali, che siano $a > 1$ e $b > 1$. Sia, inoltre,

$$a = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r} \quad \text{con } p_i \text{ primo, } e_i > 0, p_i \neq p_j, 1 \leq i \neq j \leq r \ ;$$

$$b = q_1^{f_1} q_2^{f_2} \cdot \ldots \cdot q_s^{f_s} \quad \text{con } q_j \text{ primo, } f_j > 0, q_i \neq q_j, 1 \leq i \neq j \leq s \ .$$

Poiché $\mathrm{MCD}(a, b) = 1$, la fattorizzazione in primi distinti di ab risulta:

$$ab = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r} q_1^{f1} q_2^{f_2} \cdot \ldots \cdot q_s^{f_s} \ .$$

Se, dunque, la fattorizzazione in primi di c è

$$c = z_1^{g_1} z_2^{g_2} \cdot \ldots \cdot z_t^{g_t} \quad \text{con } z_i \text{ primo, } g_i > 0, \ z_i \neq z_j, \ 1 \leq i \neq j \leq t \ ,$$

allora, risulta:

$$p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r} q_1^{f_1} q_2^{f_2} \cdot \ldots \cdot q_s^{f_s} = z_1^{ng_1} z_2^{ng_2} \cdot \ldots \cdot z_t^{ng_t} \ .$$

Quindi, per il Teorema Fondamentale dell'Aritmetica, $\{p_1, p_2, \ldots, p_r, q_1, q_2,$ ..., $q_s\} = \{z_1, z_2, \ldots, z_t\}$ ed inoltre ciascuno degli interi $e_i, f_j,$ per $1 \leq \mathrm{i} \leq \mathrm{r}, 1 \leq \mathrm{j} \leq \mathrm{s}$, deve essere divisibile per n. Ponendo

$$a_1 := p_1^{e_1/n} p_2^{e_2/n} \cdot \ldots \cdot p_r^{e_r/n} \ , \quad b_1 := q_1^{f_1/n} q_2^{f_2/n} \cdot \ldots \cdot q_s^{f_s/n} \ ,$$

si perviene alla conclusione.

□

Teorema 1.8. *Tutte le tpp positive (x, y, z) con x pari sono date dalle formule*

$$x = 2st, \quad y = s^2 - t^2, \quad z = s^2 + t^2$$

al variare di s e t tra gli interi tali che:

$$s > t > 0 \, , \quad \mathrm{MCD}(s, t) = 1 \quad e \quad s \not\equiv t \pmod 2.$$

Dimostrazione. Sia (x, y, z) una tpp positiva con $2 \mid x$. Si noti, che $z > y$, allora, $z - y$ e $z + y$ sono entrambi pari e positivi, dunque

$$z - y = 2u \, , \quad z + y = 2v \, , \quad \text{con } u, v > 0 \ .$$

Quindi:

$$x^2 = z^2 - y^2 = (z + y)(z - y) = 4uv \ ,$$

cioè $(x/2)^2 = uv$. Si ha inoltre che $\mathrm{MCD}(u, v) = 1$. Se infatti, per assurdo, $\mathrm{MCD}(u, v) = d \neq 1$, allora $d \mid (v - u) = y$ e $d \mid (v + u) = z$, mentre $\mathrm{MCD}(y, z) = 1$ per il Lemma 1.6 (b). Applicando, ora, il Lemma 1.7 nel caso in cui $a = u$, $b = v$, $c = x/2$, $n = 2$, otteniamo che $u = t^2$, $v = s^2$ per due opportuni interi positivi s e t. È facile assicurarsi che si ha $s > t > 0$, essendo $v > u$, perché $y = v - u > 0$. Dunque, abbiamo:

$$\begin{cases} x^2 = 4s^2t^2 \\ y = v - u = s^2 - t^2 \\ z = v + u = s^2 + t^2 \end{cases} \quad \text{cioè} \quad \begin{cases} x = 2st \\ y = s^2 - t^2 \\ z = s^2 + t^2 \,. \end{cases}$$

Inoltre, $\mathrm{MCD}(s, t) = 1$, in quanto $\mathrm{MCD}(u, v) = 1$. Se, infine, $s \equiv t \pmod 2$ allora s e t sono entrambi pari o entrambi dispari; in ambedue i casi y e z risultano entrambi pari, contro l'asserto del Lemma 1.6 (a).

Viceversa, se s e t sono due interi positivi verificanti le condizioni enunciate nel Teorema, è immediato vedere che (x, y, z) è una tp positiva. Resta da verificare che (x, y, z) è primitiva. Supponiamo, per assurdo, che $p \mid x, y, z$, essendo p un primo diverso da 2 (perché x è pari mentre y è dispari, dal momento che s e t non hanno la stessa parità). Ora $p \mid (z + y) = 2s^2$ e $p \mid (z - y) = 2t^2$, dunque $p \mid s$ e $p \mid t$, quindi $p \mid \mathrm{MCD}(s, t)$ donde un assurdo. $\square$

Nella seguente tavola sono descritte tutte le terne pitagoriche primitive positive, in funzione di s e t quando $s \leq 5$:

s	t	$x = 2st$	$y = s^2 - t^2$	$z = s^2 + t^2$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41

Corollario 1.9. *Tutte e sole le soluzioni (x, y, z), con x pari, dell'equazione diofantea $X^2 + Y^2 = Z^2$ sono date da*

$$x = \pm 2std\,, \quad y = \pm(s^2 - t^2)d\,, \quad z = \pm(s^2 + t^2)d$$

dove s, t, d sono interi, inoltre s e t verificano le condizioni enunciate nel Teorema 1.8, ed una qualunque scelta dei segni è possibile. $\square$

Corollario 1.10. *Sia* (x, y, z) *una tpp. Allora,* $3 \mid x$ *oppure* $3 \mid y$.

Dimostrazione. Non è restrittivo supporre che (x, y, z) sia una tpp positiva, con x pari. Per il Teorema 1.8 esistono quindi due interi positivi opportuni s, t tali che:

$$x = 2st\,, \quad y = s^2 - t^2\,, \quad z = s^2 + t^2\ .$$

Possiamo supporre che $3 \nmid s$, $3 \nmid t$, perché se $3 \mid s$ oppure se $3 \mid t$, allora $3 \mid x$. Quindi, per il Piccolo Teorema di Fermat, si ha

$$s^2 \equiv 1 \pmod 3 \quad t^2 \equiv 1 \pmod 3$$

da cui $y = s^2 - t^2 \equiv 0 \pmod 3$. $\square$

1 Esercizi e Complementi

1.1. Sia (x, y, z) una tp. Allora almeno uno tra gli interi x, y, z, è divisibile per 5.
[*Suggerimento.* Se $5 \nmid a$ allora è facile vedere che $a^2 \equiv 1, 4 \pmod 5$. Quindi, se $5 \nmid x$ e $5 \nmid y$ allora $x^2 + y^2 \equiv 0, 2, 3 \pmod 5$. Poiché $z^2 \equiv 1, 4 \pmod 5$ oppure $5 \mid z$, dal fatto che $z^2 = x^2 + y^2$ concludiamo facilmente che $5 \mid z$.]

1.2. Mostrare che l'unica tp positiva del tipo $(n-1, n, n+1)$, con $n \in \mathbb{N}$, $n \geq 2$, si ottiene per $n = 4$.
[*Suggerimento.* Basta esplicitare i calcoli.]

1.3. (**P. Fermat**) Chiamiamo *triangolo pitagorico* un triangolo rettangolo avente lati di lunghezza intera. Mostrare che:

(a) esistono triangoli pitagorici differenti aventi la stessa area;

(b) due triangoli pitagorici con la stessa area e stessa ipotenusa sono uguali, cioè hanno tutti i lati della stessa lunghezza;

(c) per ogni intero positivo Δ, esistono al più un numero finito di triangoli pitagorici aventi area uguale a Δ;

(d) per ogni intero positivo n, esistono un numero $N \geq n$ di triangoli pitagorici aventi la stessa area e ipotenusa differenti.

[*Suggerimento.* (a) Considerare ad esempio $(21, 20, 29)$ e $(35, 12, 37)$.

(b) Siano (x_1, y_1, z_1) e (x_2, y_2, z_2) le tp associate ai due triangoli. Le ipotesi si traducono nella maniera seguente: $x_1 y_1 = x_2 y_2$ e $z_1 = z_2$. Supponiamo per fissare le idee che $x_1 > y_1$ e $x_2 > y_2$ (si noti che non esistono triangoli pitagorici isosceli; cfr. Esempio 1.4). Allora essendo $z_1^2 = z_2^2$ deve essere $x_1^2 + y_1^2 = x_2^2 + y_2^2$ e quindi anche $(x_1 - y_1)^2 = (x_2 - y_2)^2$ e $(x_1 + y_1)^2 = (x_2 + y_2)^2$. Da ciò ricaviamo che $x_1 - y_1 = x_2 - y_2$ e $x_1 + y_1 = x_2 + y_2$ e quindi $x_1 = x_2$, $y_1 = y_2$.

Abbiamo già osservato in (a) che possono esistere due triangoli pitagorici distinti con la stessa area (ma, ovviamente, differenti ipotenuse).

(c) Basta osservare che i cateti di tali triangoli pitagorici devono avere lunghezze $x, y \geq 1$ con $xy = 2\Delta$.

(d) Facciamo vedere, per induzione su $n \geq 1$, che se abbiamo n triangoli pitagorici con stessa area $2\Delta_n$ e differenti ipotenuse e se almeno uno dei triangoli ha ipotenusa dispari allora possiamo costruire $n+1$ triangoli pitagorici con stessa area $2\Delta_{n+1}$ e differenti ipotenuse ed, inoltre, almeno uno di tali nuovi triangoli ha ipotenusa dispari.

Il caso $n = 1$ è ovvio (vedi (a)).

Sia $n \geq 2$ e siano (a_k, b_k, c_k) le terne pitagoriche associate agli n triangoli pitagorici assegnati, $1 \leq k \leq n$. Supponiamo che:

$$a_k b_k = 2\Delta_n \ , \quad \text{per ogni } 1 \leq k \leq n$$

$$c_h \neq c_k \ , \quad \text{se } 1 \leq h \neq k \leq n \, ,$$

e, per fissare le idee, possiamo supporre:

- c_1 dispari,
- $a_k > b_k$ per ogni k.

Poniamo, per $1 \leq k \leq n$,

$$\begin{aligned} a'_k &= 2c_1(a_1^2 - b_1^2)a_k \ , \\ b'_k &= 2c_1(a_1^2 - b_1^2)b_k \ , \\ c'_k &= 2c_1(a_1^2 - b_1^2)c_k \ , \end{aligned}$$

e, poi,

$$\begin{aligned} a'_{n+1} &= 4a_1b_1c_1^2 \ , \\ b'_{n+1} &= (a_1^2 - b_1^2)^2 \ , \\ c'_{n+1} &= 4a_1^2b_1^2 + c_1^4 \ . \end{aligned}$$

Si verifica direttamente che la terna (a'_k, b'_k, c'_k) per $1 \leq k \leq n+1$ soddisfa le condizioni enunciate.]

1.4. (a) Mostrare che non esistono triangoli pitagorici isosceli.

(b) Dedurre da (a) che $\sqrt{2} \notin \mathbb{Q}$.

[*Suggerimento.* (a) Usiamo il metodo della discesa infinita. Sia (a, a, c) un triangolo pitagorico isoscele. Dunque $c^2 = 2a^2$, da cui $2 \mid c$. Quindi $c = 2c_1$, per un qualche c_1 con $c > c_1 \geq 1$. Pertanto, $4c_1^2 = 2a^2$, cioè $2c_1^2 = a^2$, dunque $2 \mid a$, quindi $a = 2a_1$, per un qualche a_1 con $a > a_1 \geq 1$. È subito visto che (a_1, a_1, c_1) è un triangolo isoscele. La conclusione segue per assurdo, utilizzando un procedimento di "discesa infinita".

Si noti che un'altra dimostrazione di questo risultato si può ottenere osservando che non esistono triangoli pitagorici isosceli "primitivi" (cfr. Lemma 1.6 (a)).

(b) Se $\sqrt{2} = \frac{a}{b}$ con $a, b \in \mathbb{Z}$ e $b \neq 0$, allora avremmo che $2b^2 = a^2$.]