

2 Le equazioni diofantee $X^4+Y^4 = Z^2$, $X^4+Y^4 = Z^4$

Innanzitutto, cominciamo con il ricordare l'enunciato del celeberrimo: **“Ultimo” Teorema di Fermat.**

L'equazione

$$X^n + Y^n = Z^n, \text{ con } n \geq 3,$$

non ammette soluzioni intere (x, y, z) con $xyz \neq 0$.

Ci limitiamo qui a dare qualche informazione essenziale su tale enunciato, rinviando per annotazioni storiche ad una vasta ed eccellente bibliografia disponibile sull'argomento (cfr. E.T. Bell [2], H.M. Edwards [5], P. Ribenboim [11], S. Singh [14], A. van der Porten [15], A. Weil [16]).

Fermat ha scritto tale enunciato in una nota a margine della sua copia dell'*Arithmetica* di Diofanto attorno al 1635. Molto probabilmente il nome di Ultimo Teorema di Fermat (in breve, UTF) deriva dal fatto che dei numerosi teoremi enunciati da Fermat questo è l'ultimo del quale, fino al 1995, non si conosceva ancora una risposta definitiva sulla sua validità. Negli oltre tre secoli dalla morte di Fermat, molti illustri matematici hanno lavorato su tale problema.

Finalmente nel 1995, A. Wiles utilizzando una varietà di risultati profondi, sviluppati in molteplici settori della matematica ed, in particolare, ponendosi nell'ambito della teoria delle curve ellittiche ha dimostrato la celebre Congettura di Taniyama-Shimura, la quale era già noto implicare l'UTF (risultati di G. Frey, J.-P. Serre, K. Ribet).

Non è dato di sapere con certezza se Fermat avesse veramente trovato una dimostrazione per l'UTF, ma ciò sembra improbabile. Opinione diffusa è che egli abbia avuto l'idea, estremamente geniale, di operare in quello che oggi si chiama anello degli interi del campo delle radici n -esime dell'unità, idea perseguita successivamente da E. Kummer attorno al 1850, e di aver “ingenuamente” creduto che tale anello, come l'anello \mathbb{Z} degli interi, fosse sempre un dominio a fattorizzazione unica (in breve, UFD); ma ciò in generale non è vero. Anzi, nel 1964, C.L. Siegel ha dimostrato, dopo un lungo percorso al quale hanno contribuito numerosi matematici, che tale anello è un UFD solamente per un numero finito di valori di n .

In ogni caso, Fermat stesso dimostrò completamente la validità dell'UTF nel caso $n = 4$ (e questa è una delle poche dimostrazioni complete di tutta la sua opera in Teoria dei Numeri). Per far ciò, egli applicò il suo metodo della “*discesa infinita*” di cui era, a ragione, particolarmente orgoglioso.

Il caso $n = 4$ ha un rilievo particolare perché permette di ricondurre

l'enunciato dell'UTF ad uno analogo, relativo "solamente" ad esponenti primi dispari. Infatti, è evidente che se l'UTF è dimostrato per un esponente m , esso è pure dimostrato per ogni multiplo di m . Infatti, per ogni $k \geq 1$, si ha che:

$$X^{km} + Y^{km} = Z^{km} \quad \text{se e soltanto se} \quad U^m + V^m = W^m$$

dove $U = X^k$, $V = Y^k$, $W = Z^k$. Poiché ogni intero $n \geq 3$ è divisibile per 4 oppure per un primo dispari p , è evidente che basta dimostrare l'UTF nel caso in cui $n = 4$ e in quello in cui $n = p$ è un primo dispari.

In questo paragrafo ci proponiamo di dare una dimostrazione completa dell'UTF nel caso $n = 4$.

Osserviamo, innanzitutto, che:

Proposizione 2.1. *Se l'equazione diofantea:*

$$X^4 + Y^4 = Z^2 \tag{2.1.1}$$

non ha soluzioni (x, y, z) non banali (cioè con $xyz \neq 0$), allora l'equazione diofantea:

$$X^4 + Y^4 = Z^4 \tag{2.1.2}$$

non ha soluzioni (x, y, z) non banali.

Dimostrazione. Se (x_0, y_0, z_0) fosse una soluzione non banale (cioè $x_0 y_0 z_0 \neq 0$) di (2.1.2), allora (x_0, y_0, z_0^2) sarebbe una soluzione non banale di (2.1.1). \square

Vogliamo ora dimostrare che l'equazione diofantea (2.1.1) non ha soluzioni non banali, utilizzando il *metodo della discesa infinita* di Fermat. A tal scopo supporremo che esista una soluzione (x, y, z) di (2.1.1) con $x \neq 0$, $y \neq 0$, e $z \geq 0$; ne sceglieremo una del tipo suddetto con z minimo positivo ed applicando, essenzialmente due volte, il teorema fondamentale sulle terne pitagoriche, mostreremo che è possibile trovare un'altra soluzione (x_1, y_1, z_1) di (2.1.1) con $x_1 \neq 0$, $y_1 \neq 0$ e $z \geq z_1 \geq 0$, pervenendo così ad un assurdo.

Teorema 2.2. *L'equazione diofantea:*

$$(2.1.1) \quad X^4 + Y^4 = Z^2$$

non ammette soluzioni intere (x, y, z) con $xyz \neq 0$.

Dimostrazione. Supponiamo che esistano soluzioni non banali di (2.1.1). Consideriamo allora una soluzione (x, y, z) di (2.1.1) con $x \neq 0, y \neq 0, z > 0$ e z il minimo intero positivo per il quale (x, y, z) sia una soluzione non banale di (2.1.1). Possiamo, ovviamente, supporre che anche x ed y siano positivi.

I Passo: $\text{MCD}(x, y) = d = 1$.

Se, per assurdo, $d \neq 1$, poiché $d^4 \mid (x^4 + y^4)$ e quindi $d^2 \mid z$ (basta ragionare sui fattori primi di d), allora $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2})$ sarebbe ancora una soluzione (intera) di (2.1.1) con $z \geq \frac{z}{d^2} \geq 0$.

II Passo: $x^2 = 2ab, y^2 = a^2 - b^2, z = a^2 + b^2$ con $a, b \in \mathbb{Z}, 0 \leq b \leq a, a$ dispari e b pari e $\text{MCD}(a, b) = 1$.

Essendo $\text{MCD}(x, y) = 1, (x^2, y^2, z)$ è una terna pitagorica primitiva. Quindi, a meno di un eventuale (ma inessenziale) scambio tra x e y , esistono $a, b \in \mathbb{Z}, a \geq b \geq 0$, tali che $x^2 = 2ab, y^2 = a^2 - b^2, z = a^2 + b^2, \text{MCD}(a, b) = 1$ e $a \not\equiv b \pmod{2}$ (cfr. Teorema 1.8). Se, per assurdo, a fosse pari, allora b sarebbe dispari e, quindi, $y^2 \equiv -b^2 \equiv -1 \equiv 3 \pmod{4}$, donde una contraddizione, perché un quadrato di un intero è congruo a 0 oppure 1 (mod 4).

III Passo: $b = 2uv, y = u^2 - v^2, a = u^2 + v^2$ con $u, v \in \mathbb{Z}, 0 \leq v \leq u, \text{MCD}(u, v) = 1$ e $u \not\equiv v \pmod{2}$.

Infatti, $b^2 + y^2 = a^2$ con b pari e $\text{MCD}(a, b, c) = 1$, essendo $\text{MCD}(a, b) = 1$; cioè (b, y, a) è una terna pitagorica primitiva.

IV Passo: Conclusione.

Dal II e III Passo si ricava che

$$x^2 = 2ab = 4(u^2 + v^2)uv .$$

Poiché $\text{MCD}(u, v) = 1$, anche $\text{MCD}(u, u^2 + v^2) = \text{MCD}(v, u^2 + v^2) = 1$, quindi $u, v, u^2 + v^2$ sono quadrati di interi (Lemma 1.7), dunque:

$$u = x_1^2, \quad v = y_1^2, \quad u^2 + v^2 = z_1^2 \quad \text{con} \quad x_1, y_1, z_1 \in \mathbb{N}^+ .$$

Quindi $x_1^4 + y_1^4 = z_1^2$, con $x_1 \neq 0$ e $y_1 \neq 0$ (ad esempio, se fosse $x_1 = 0$, allora $u = 0, b = 0, x = 0$). Inoltre,

$$z_1 \leq z_1^2 = u^2 + v^2 = a \leq a^2 \leq a^2 + b^2 = z ,$$

donde la conclusione. □

2 Esercizi e complementi

2.1. Mostrare che l'equazione $1/X^4 + 1/Y^4 = 1/Z^4$ non ammette soluzioni intere. [*Suggerimento.* Se (a, b, c) è una soluzione intera dell'equazione data, allora moltiplicando ambo i membri per $(abc)^4$, si ricava che $(bc)^4 + (ac)^4 - (ab)^4 = 0$.]

2.2. (P. Fermat) Mostrare che l'equazione diofantea

$$X^4 - Y^4 = Z^2$$

non ha soluzioni (x, y, z) con $x, y, z > 0$.

[*Suggerimento.* Supponiamo che l'equazione diofantea data abbia soluzioni (x, y, z) "positive" e sia (x_0, y_0, z_0) una soluzione con il valore minimo positivo per la x . È subito visto che $\text{MCD}(x_0, y_0) = d = 1$, altrimenti $(x_0/d, y_0/d, z_0/d)$ sarebbe un'altra soluzione con $x_0/d < x_0$.

Caso 1. y_0 dispari. Notiamo che (z_0, y_0^2, x_0^2) è una tppp (= terna pitagorica primitiva positiva). Quindi $z_0 = 2st$, $y_0^2 = s^2 - t^2$, $x_0^2 = s^2 + t^2$ con $\text{MCD}(s, t) = 1$, $s > t > 0$ ed $s \not\equiv t \pmod{2}$. D'altra parte

$$s^4 - t^4 = (s^2 + t^2)(s^2 - t^2) = x_0^2 y_0^2,$$

dunque $(s, t, x_0 y_0)$ è un'altra soluzione dell'equazione data con $s^2 < s^2 + t^2 = x_0^2$ e, quindi, $s < x_0$.

Caso 2. y_0 pari. Notiamo che (y_0^2, z_0, x_0^2) è una tppp. Quindi

$$y_0^2 = 2st, \quad z_0 = s^2 - t^2, \quad x_0^2 = s^2 + t^2, \quad \text{con } \text{MCD}(s, t) = 1, \quad s > t > 0 \text{ ed } s \not\equiv t \pmod{2}.$$

Si supponga, per fissare le idee, che s sia pari e t dispari. Essendo $\text{MCD}(2s, t) = 1$, da $y_0^2 = 2st$, ricaviamo che esistono $a, b > 0$ tali che $2s = a^2$, $t = b^2$. È subito visto che a deve essere pari, quindi $a = 2c$ e, dunque, $s = 2c^2$. Da ciò segue che:

$$x_0^2 = s^2 + t^2 = 4c^4 + b^4.$$

Quindi $(2c^2, b^2, x_0)$ è una tppp. Pertanto:

$$2c^2 = 2uv, \quad b^2 = u^2 - v^2, \quad x_0 = u^2 + v^2 \quad \text{con } \text{MCD}(u, v) = 1, \quad u > v > 0, \quad u \not\equiv v \pmod{2}.$$

Dunque da $c^2 = uv$, si ricava che $u = z^2$ e $v = w^2$. Sostituendo, abbiamo:

$$b^2 = u^2 - v^2 = z^4 - w^4$$

quindi (z, w, b) è un'altra soluzione dell'equazione diofantea data con $z = \sqrt{u} < u^2 + v^2 = x_0$.]

2.3. (Formulazione di Fermat dell'Esercizio 2.2). Non esiste una terna pitagorica (x, y, z) tale che $(1/2)xy$ sia un quadrato (cioè, l'area di un triangolo rettangolo a lati interi non può essere uguale all'area di un quadrato con lato intero).

[Suggerimento. Sia (x, y, t) una tp. Se l'area $(1/2)xy$ è uguale a u^2 con $u > 0$, allora $2xy = 4u^2$, quindi:

$$\begin{aligned}(x + y)^2 &= x^2 + y^2 + 2xy = z^2 + 4u^2 \\ (x - y)^2 &= x^2 + y^2 - 2xy = z^2 - 4u^2\end{aligned}$$

pertanto:

$$(x^2 - y^2)^2 = z^4 - (2u)^4$$

e ciò contraddice l'Esercizio 2.2.]

2.4. Provare che l'equazione $X^4 - Y^4 = 2Z^2$ non ha soluzioni negli interi positivi. [Suggerimento. Sia (x, y, z) una soluzione dell'equazione data. Poiché x e y devono essere entrambi dispari, allora si dimostra agevolmente (utilizzando il Lemma 1.7) che $x^2 + y^2 = 2a^2$, $x + y = 2b^2$, $x - y = 2c^2$ per opportuni interi (a, b, c) che possiamo prendere positivi; da qui $a^2 = b^4 + c^4$.]

2.5. L'equazione $X^4 - 4Y^4 = Z^2$ non ha soluzioni negli interi positivi. [Suggerimento. Riscrivere l'equazione nella forma seguente: $(2Y^2)^2 + Z^2 = (X^2)^2$.]

2.6. Mostrare che:

- (a) **(A.M. Legendre)** L'equazione $X^4 + Y^4 = 2Z^2$ è risolubile negli interi positivi ed ha come soluzioni intere positive soltanto le terne (k, k, k^2) , $k \geq 1$.
- (b) L'equazione $X^4 + Y^4 = kZ^2$ con $3 \leq k \leq 4$ non è risolubile negli interi positivi.

[Suggerimento. (a) È chiaro che (k, k, k^2) per $k \geq 1$ è una soluzione positiva della equazione diofantea assegnata. Viceversa se (x, y, z) è una terna di interi positivi tali che $x^4 + y^4 = 2z^2$ con $x \neq y$ allora necessariamente $x \equiv y \pmod{2}$. Supponiamo (per fissare le idee) che $x > y$ e quindi che $x^2 + y^2 = 2a$, $x^2 - y^2 = 2b$ per una opportuna scelta di $a, b > 0$. Da ciò si ricava che $x^2 = a + b$, $y^2 = a - b$ e quindi $2z^2 = x^4 + y^4 = 2(a^2 + b^2)$. Pertanto $z^2 = a^2 + b^2$ e $a^2 - b^2 = (xy)^2$ e, quindi, $a^4 - b^4 = (xyz)^2$ e ciò è assurdo per l'Esercizio 2.2.

(b) $k = 3$: basta osservare che l'equazione diofantea $U^2 + V^2 = 3Z^2$ non è risolubile (si ricordi che un quadrato di un intero è congruo a 0, 1 (mod 4)).

$k = 4$: basta osservare che $X^4 + Y^4 = (2Z)^2$ non è risolubile (Teorema 2.2).]

2.7. Verificare che la sola soluzione intera (x, y, z) , con $\text{MCD}(x, y, z) = 1$, della equazione $X^4 + Y^4 = 2Z^2$ si ha per $x = y = z = 1$.

[Suggerimento. Le soluzioni dell'equazione data soddisfano anche l'equazione $Z^4 - (XY)^4 = ((X^4 - Y^4)/2)^2$, la conclusione discende dagli Esercizi 2.2 e 2.6 (a).]