L'ultimo teorema di Fermat per $n = 4k$ $(k \in \mathbb{N}^+)$

Domenico Annunziata, Marco Damele, Daniele Bjørn Malesani

29 gennaio 2023

Capitolo 1

L'ultimo teorema di Fermat per $n = 4k$.

L'obiettivo di queste note è dimostrare l'ultimo teorema di Fermat nel caso $n = 4k$, con $k \in \mathbb{N}^+$, ovvero dimostrare che non possono esistere X, Y e Z interi (con $XYZ \neq 0$) tali che

$$X^{4k} + Y^{4k} = Z^{4k}. \tag{1}$$

Partiamo con il seguente:

Lemma 1. *Siano $a, b \in \mathbb{N}^+$ coprimi. Se esiste $x \in \mathbb{N}^+$ tale che $ab = x^2$, allora esistono $A, B \in \mathbb{N}^+$ tali che $a = A^2$ e $b = B^2$. Inoltre, $(A, B) = 1$.*

Dimostrazione. Se $a = 1$ oppure $b = 1$, la tesi è banale. Supponiamo d'ora in poi $ab \neq 1$. Per il teorema fondamentale dell'aritmetica, a e b si possono scomporre come:

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}, \; b = q_1^{\beta_1} \cdots q_m^{\beta_m},$$

dove $p_1, \dots, p_n$ e $q_1, \dots, q_m$ sono primi distinti, mentre $\alpha_1, \dots, \alpha_n$ e $\beta_1, \dots, \beta_m$ sono opportuni interi positivi. Ora, siccome $x^2 = ab$, x avrà la forma:

$$x = p_1^{\alpha'_1} \cdots p_n^{\alpha'_n} \cdot q_1^{\beta'_1} \cdots q_m^{\beta' m} \cdot s_1^{\gamma_1} \cdots s_k^{\gamma_k},$$

dove $s_1, \dots, s_k$ sono numeri primi, mentre $\alpha'_1, \dots, \alpha'_n$, $\beta'_1, \dots, \beta'_m$, $\gamma'_1, \dots, \gamma'_k$ sono interi positivi. Quindi, dato che $x^2 = ab$, per l'unicità della scomposizione in fattori primi otteniamo che $\alpha_i = 2\alpha'_i$ $(i = 1, \dots, n)$, $\beta_i = 2\beta'_i$ $(i = 1, \dots, m)$ e $\gamma_i = 0$ $(i = 1, \dots, k)$. La tesi segue notando che:

$$a = p_1^{2\alpha'_1} \cdots p_n^{2\alpha'_n} = \left(p_1^{\alpha'_1} \cdots p_n^{\alpha'_n}\right)^2 = A^2,$$

$$b = q_1^{2\alpha'_1} \cdots q_n^{2\beta'_n} = \left(q_1^{\beta'_1} \cdots q_m^{\beta'_m}\right)^2 = B^2.$$

Dato che i fattori primi di $A = p_1^{\alpha'_1} \cdots p_n^{\alpha'_n}$ e $B = q_1^{\beta'_1} \cdots q_m^{\beta'_m}$ sono distinti, chiaramente $(A, B) = 1$. $\square$

Nota 1. *Non è difficile notare che il lemma anteriore continua a valere nel caso in cui si abbia un prodotto di più interi coprimi a due a due. Se* $x \in \mathbb{N}^+$ *e* $a_1, \ldots, a_n$ *sono tali che* $a_1 \cdots a_n = x^2$ *con* $(a_i, a_j) = 1$ *per ogni* $i \neq j$*, allora esistono* $A_1, \ldots, A_n \in \mathbb{N}^+$ *tali che* $a_i = A_i^2$ *per ogni* $i = 1, \ldots, n$.

Esempio 1. *Utilizziamo il lemma anteriore per risolvere l'equazione diofantea*

$$4X^2 + 28X - 15 = Y^2$$

Dobbiamo determinare tutti gli interi X *e* Y *tali che* $4X^2 + 28X - 15 = Y^2$. *Se* X *e* Y *sono soluzioni dell'equazione, allora* $(2X - 1)(2X + 15) = Y^2$. *Osserviamo che* $2X - 1$ *e* $2X + 15$ *sono coprimi per ogni valore di* X. *Infatti se* p *è un eventuale divisore primo comune, esso dovrebbe essere dispari, tuttavia si avrebbe* $2X + 15 \equiv 0 \pmod{p}$ *e* $2X - 1 \equiv 0 \pmod{p}$. *Sottraendo membro a membro, si avrebbe* $16 \equiv 0 \pmod{p}$*, da cui* $p = 2$*, che è assurdo. Per il lemma precedente, consegue che esistono due interi* a *e* b *tali che* $2X + 15 = a^2$ *e* $2X - 1 = b^2$. *Sottraendo membro a membro, si trova* $a^2 - b^2 = 16$*, da cui* $a = 5$ *e* $b = 3$ *oppure* $a = 4$ *e* $b = 0$. *Segue che* $X = 5$ *e* $Y = 15$ *oppure* $Y = -15$ *(mentre non ci sono soluzioni intere corrispondenti ad* $a = 4$*,* $b = 0$*). Sostituendo tali valori nell'equazione iniziale si ottengono delle identità, quindi le uniche soluzioni sono* $(5, 15)$ *e* $(5, -15)$.

Esempio 2. *Trovare le soluzioni intere positive dell'equazione:*

$$X^3 - Y^2 Z^2 - 7X = 0.$$

Sia (x, y, z) *una soluzione con* x*,* y *e* z *interi positivi. Allora* $x(x^2 - 7) = (yz)^2$. *Sia* $d = (x, x^2 - 7)$. *Allora* $d \mid x$ *e* $d \mid x^2 - 7$*, quindi* $d \mid 7$ *e necessariamente* $d = 1$ *oppure* $d = 7$.

Se $d = 1$*, allora esistono, per il lemma 1,* a *e* b *interi positivi tali che* $x = a^2$ *e* $x^2 - 7 = b^2$. *Quindi* $a^4 - 7 = b^2$ *da cui* $(a^2 - b)(a^2 + b) = 7$. *Dato che* $a^2 - b < a^2 + b$ *e* 7 *è primo, deve essere* $a^2 - b = 1$ *e* $a^2 + b = 7$*, quindi* $a = 2$*,* $b = 3$ *e* $x = 4$*,* $yz = 6$. *Le possibili coppie di soluzioni sono* $(y, z) = (2, 3)$ *e* $(y, z) = (1, 6)$ *(oltre a quelle con* z *e* y *scambiati).*

Se invece $d = 7$ *allora* $x = 7v$ *e* $x^2 - 7 = 7u$ *con* u *e* v *interi coprimi. Segue che* $uv = (yz/7)^2$ *quindi, sempre per il lemma 1,* $u = a^2$ *e* $v = b^2$*, con* a *e* b *interi positivi. Allora* $x^2 - 7 = 7a^2$*, ed, essendo* $x = 7v$*, si ha* $7v^2 = a^2 + 1$ *e cioè* $a^2 \equiv -1 \pmod{7}$*, che è assurdo perché* -1 *non è un residuo quadratico mod 7.*

Esercizio 1. *Si dimostri che l'equazione diofantea*

$$4X^4 - 16X^3 + 20X^2 - 8X - 3 = Y^2$$

non ha soluzioni.

Iniziamo ora lo studio delle terne pitagoriche.

Definizione 1. *Una terna pitagorica è una terna di numeri interi positivi* (X, Y, Z) *tali che* $X^2 + Y^2 = Z^2$.

L'esempio più famoso è la terna $(3, 4, 5)$, ma ci sono in realtà infinite possibilità. Per esempio, per ogni intero positivo k, la terna $(3k, 4k, 5k)$ è pitagorica. Per il teorema di Pitagora, i triangoli le cui lunghezze dei lati formano una terna pitagorica sono rettangoli. Non è difficile osservare che, se (X, Y, Z) è una terna pitagorica tale che due suoi qualsiasi elementi hanno un fattore comune, allora anche il terzo lo ha. Quindi i fattori di una terna o sono tutti mutualmente coprimi oppure hanno tutti un fattore comune. Queste osservazioni portano alla definizione di terna pitagorica primitiva.

Definizione 2. *Sia* (X, Y, Z) *una terna pitagorica. Essa è detta primitiva se* $(X, Y, Z) = 1$.

Consideriamo una terna pitagorica primitiva (a, b, c). Per quanto appena detto, $(a, c) = (a, b) = (b, c) = 1$. Inoltre a e b hanno parità opposta. Infatti, essendo coprimi non possono essere entrambi pari, ma non possono nemmeno essere entrambi dispari, altrimenti c sarebbe pari (cioè $c = 2j$ per un opportuno intero j) e quindi, se $a = 2h + 1$, $b = 2k + 1$ (per opportuni h e k interi), si avrebbe $a^2 + b^2 = 4(k^2 + h^2 + k + h) + 2 \equiv 2 \pmod 4$, mentre $c^2 \equiv 0 \pmod 4$. Nel seguito, assumeremo che a sia pari e b dispari, ma ovviamente il loro ruolo è del tutto simmetrico.

Teorema 1. *Esistono infinite terne pitagoriche primitive.*

Dimostrazione. Siano m ed n interi positivi con $m > n$, $(m, n) = 1$ e parità opposta. Come vedremo nel teorema seguente, le soluzioni dell'equazione di Pitagora sono date dalle seguenti formule (formule di Euclide):

$$\begin{aligned} a &= 2mn; \\ b &= m^2 - n^2; \\ c &= m^2 + n^2. \end{aligned} \tag{2}$$

Dato che

$$a^2 + b^2 = 4m^2n^2 + m^4 - 2m^2n^2 + n^4 = (m^2 + n^2)^2 = c^2,$$

la terna (a, b, c) è pitagorica. Dimostriamo ora che è primitiva, cioè che $(a, b, c) = 1$. Supponiamo che p sia un numero primo che divide a, b e c. Siccome m ed n hanno parità opposta, b è dispari, quindi $p \neq 2$. Se $p > 2$, p divide a e quindi uno tra m ed n, ad esempio n. Ma p divide anche b e quindi, dato che $n^2 = m^2 - b$, divide anche n, che è assurdo essendo m ed n coprimi per costruzione. Segue che (a, b, c) è primitiva. □

Nasce allora la seguente domanda: tutte le terne pitagoriche primitive hanno la forma (2)? La risposta è positiva, come afferma il seguente:

Teorema 2. *Sia (a, b, c) una terna pitagorica primitiva (con a pari). Allora esistono $m, n \in \mathbb{N}^+$, con $m > n$, $(m, n) = 1$ e parità opposta, tali che:*

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2. \tag{3}$$

Dimostrazione. Abbiamo $a^2 = c^2 - b^2 = (c - b)(c + b)$. Siccome a, $c - b$ e $c + b$ sono tutti pari, esistono tre interi r, s e t tali che $a = 2r$, $c - b = 2s$ e $c + b = 2t$, da cui, sommando e sottraendo:

$$r^2 = st, \quad b = t - s, \quad c = t + s.$$

I numeri s e t sono primi tra loro. Infatti, se per assurdo p è un primo che divide sia s che t, allora divide anche $t + s = c$ e $t - s = b$, che è un assurdo. Dato che $st = r^2$, per il lemma anteriore esistono m ed n interi positivi tali che $s = n^2$ e $t = m^2$ (si noti che $t > s$ e quindi $m > n$). Sostituendo, si ottengono le formule (3).

Per finire osserviamo che, essendo s e t coprimi, lo sono anche m ed n, e, dato che $n^2 + m^2 = c$ con c dispari, m ed n hanno parità opposta. □

Nota 2. *Si può aggiungere che, se m ed n non sono coprimi oppure non sono entrambi dispari, allora la terna (a, b, c) definita dalla (2) è pitagorica ma non primitiva. Le formule di Euclide possono quindi generare terne sia primitive che derivate. Esistono però terne derivate non esprimibili tramite le formule di Euclide, per esempio $(9, 12, 15)$. Per esprimere tutte le terne pitagoriche, sia primitive che derivate, si può usare la seguente formula generatrice, in funzione dei tre interi positivi k, m ed n:*

$$\begin{aligned} a &= k \cdot (2mn); \\ b &= k \cdot (m^2 - n^2); \\ c &= k \cdot (m^2 + n^2). \end{aligned}$$

Al variare di m ed n (coprimi e di parità opposta), le formule di Euclide (2) restituiscono tutte le terne primitive una ed una sola volta. Infatti, *assumendo che esistano due coppie di interi positivi* (m, n) *ed* (h, k) *tali che*

$$\begin{aligned} a &= m^2 - n^2 = k^2 - h^2, \\ b &= 2mn = 2kh, \\ c &= m^2 + n^2 = k^2 + h^2, \end{aligned}$$

allora sommando e sottraendo la prima e la terza equazione, si trova $m = k$ *ed* $n = h$.

Esercizio 2. *Dimostrare che, se* (a, b, c) *è una terna pitagorica, allora il prodotto* abc *è multiplo di* 60.

Esercizio 3. *Dimostrare che, se* (a, b, c) *è una terna pitagorica primitiva,* c *non è multiplo di* 3.

Esercizio 4.

Esistono terne pitagoriche (a, b, c) *in cui* $c = b + 1$*? Sono primitive?*

Esercizio 5.

I numeri triangolari T_k *sono numeri della forma* $T_k = k(k+1)/2$ *per qualche* $k \in \mathbb{N}$*, e corrispondono alla somma dei primi* k *numeri interi positivi. Verificare che, per ogni* $k \in \mathbb{N}^+$*, esiste una terna primitiva* (a, b, c) *tale che* $b = 4T_k$.

Teorema 3 (ultimo teorema di Fermat per $n = 4k$)**.** *Sia* $k \in \mathbb{N}^+$*. Allora non esiste* $(X, Y, Z) \in \mathbb{Z}^3$*, con* $XYZ \neq 0$*, tale che* $X^{4k} + Y^{4k} = Z^{4k}$.

Dimostrazione. Supponiamo che per assurdo esista $(x, y, z) \in \mathbb{Z}^3$, con $xyz \neq 0$, tale che $x^{4k} + y^{4k} = z^{4k}$. Allora $X = x^k$, $Y = y^k$ e $Z = z^k$ sono tre interi tali che $X^4 + Y^4 = Z^4$ e $XYZ \neq 0$. Ora, detto $d = (X, Y, Z)$, definiamo $X' = X/d$, $Y' = Y/d$ e $Z' = (Z/d)^2$. X', Y' e Z' sono coprimi, perché $d = (X, Y, Z)$. Inoltre $X'Y'Z' \neq 0$, e vale:

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

Quindi anche X', Y' e Z' sono tre interi coprimi il cui prodotto è non nullo e $X'^4 + Y'^4 = Z'^2$. Quindi l'insieme

$$K = \left\{ z \in \mathbb{N}^+ : \exists (x, y) \in \mathbb{Z}^2 : x^4 + y^4 = z^2,\ xyz \neq 0,\ (x, y, z) = 1 \right\} \subset \mathbb{N}$$

è non vuoto. Essendo K un sottoinsieme non vuoto di $\mathbb{N}$, ammette minimo, diciamolo w. Quindi, essendo $w \in K$, esistono due interi u e v tali che $u^4 + v^4 = w^2$, $uvw \neq 0$ e $(u, v, w) = 1$. Siccome (u^2, v^2, w) è una terna pitagorica primitiva, devono esistere due interi coprimi p e q, di parità opposta e tali che $p > q > 0$ per cui (assumendo senza perdita di generalità che u sia pari):

$$u^2 = 2pq, \quad v^2 = p^2 - q^2, \quad w = p^2 + q^2.$$

Dalla seconda equazione deduciamo che $p^2 = q^2 + v^2$ e pertanto anche (q, v, p) è una terna pitagorica primitiva e quindi esistono due interi a e b coprimi, di parità opposta, con $a > b > 0$, tali che:

$$q = 2ab, \quad v = a^2 - b^2, \quad p = a^2 + b^2.$$

Ora, a, b e p sono interi a due a due coprimi tali che $u^2 = 4abp$ e quindi, per il lemma 1, esistono U, V e W interi positivi coprimi tali che:

$$a = U^2, \quad b = V^2, \quad p = W^2.$$

Tuttavia dal fatto che $p = a^2 + b^2$ si deduce:

$$W^2 = U^4 + V^4.$$

Ma allora $W \in K$ e $W < W^2 = p < p^2 + q^2 = w$, da cui $W < w$, che è un assurdo essendo $w = \min(K)$.

□

Nota 3. *Si noti che, nel corso della dimostrazione del teorema precedente, abbiamo verificato che neppure l'equazione* (4) *ammette soluzioni (questo procedimento è dovuto allo stesso Fermat). La condizione* $(X', Y', Z') = 1$ *è in realtà ininfluente. Se infatti esistesse un fattore comunue* $a \in \mathbb{N}^+$ *tale che per esempio* $X' = a\xi$ *e* $Y' = av$*, allora:*

$$(a\xi)^4 + (av)^4 = (Z')^2,$$

e quindi esiste $\zeta \in \mathbb{N}^+$ *tale che* $Z' = a^2\zeta$ *e quindi* $\xi^4 + v^4 = \zeta^2$*. Essendo* $\zeta < Z'$*, applicando ancora il principio del buon ordinamento si conclude che non può esistere una soluzione neppure se* $(X', Y') \neq 1$*. Si raggiunge la medesima conclusione se* $(X', Z') \neq 1$ *oppure* $(Y', Z') \neq 1$*.*

Esempio 3. *Dimostriamo che per ogni* $k \in \mathbb{N}^+$ *il numero* $2^{1/(4k)}$ *non è razionale. Sia* $k \in \mathbb{N}^+$ *e supponiamo per assurdo che* $2^{1/(4k)}$ *sia razionale. Allora* $2^{1/(4k)} = a/b$ *per opportuni interi* a *e* b *non nulli. Quindi:*

$$2 = \left(2^{1/(4k)}\right)^{4k} = \left(\frac{a}{b}\right)^{4k} = \frac{a^{4k}}{b^{4k}} \implies 2b^{4k} = b^{4k} + b^{4k} = a^{4k},$$

che è assurdo per l'ultimo teorema di Fermat appena dimostrato.

Esempio 4. *Risolviamo l'equazione diofantea*

$$X(X^2+1) = Y^4. \tag{5}$$

Ovviamente $(X,Y) = (0,0)$ *è una soluzione (banale). Supponiamo ora che* $(X,Y) \neq (0,0)$*. Se per assurdo* X *fosse pari, esisterebbe un intero* K *tale che* $X = 2K$ *e quindi* $2K(4K^2+1) = Y^4$*. Ora, siccome* $2K$ *e* $4K^2+1$ *sono coprimi (se per assurdo* p *dividesse* $2K$*, allora dividerebbe* $(2K)^2 = 4K^2$ *e quindi non potrebbe dividere* $4K^2+1$*), si avrebbe che* $2K = a^2$ *e* $4K^2+1 = b^2$ *per opportuni interi coprimi* a *e* b*, e quindi* $a^4+1^4 = b^2$*. Ma nella dimostrazione del teorema 3, abbiamo mostrato che l'equazione* (4) *non ammette soluzioni non banali.*

Supponiamo quindi che X *sia dispari, ovvero* $X = 2Q+1$ *per un qualche intero* Q*. Sostituendo nella* (5)*, si ottiene* $2(2Q+1)(2Q^2+2Q+1) = Y^4$*. Questo vuol dire che* Y *è pari, diciamo* $Y = 2P$*, da cui* $(2Q+1)(2Q^2+2Q+1) = 8P^4$*, che è un assurdo perché i due membri hanno parità opposta.*

In conclusione, l'equazione (5) *non ha soluzioni non banali.*

Esercizio 6. *Determinare le soluzioni dell'equazione diofantea:*

$$X^6 - 4X^3Y^2 - 4Z^4 = 0.$$