

Dimostrazione dell'Ultimo Teorema di Fermat

(M. BONO - 22/04/00 – rev. 05/01/04)

Pierre de Fermat, nel 1637, partendo dalla seguente equazione:

$$x^n + y^n = z^n \quad (1)$$

dove x , y , z ed n devono appartenere tutti all'insieme dei numeri interi, enunciò quello che sarebbe stato conosciuto come il suo ultimo teorema.

Fermat affermò che l'equazione (1) ammette soluzioni, nell'ambito dei numeri interi, soltanto per n uguale a 2. Quindi per un qualsiasi n maggiore di 2 la (1) non è soddisfatta.

Tuttavia Fermat non diede nessuna dimostrazione dell'enunciato in quanto scrisse di non avere sufficiente spazio ai margini del libro su cui scrisse la (1).

Negli anni e quindi nei secoli successivi parecchi matematici tentarono di dimostrare la (1) con parziali risultati finché nel 1994 A. Wiles riuscì nell'impresa ricorrendo a sofisticati concetti matematici che sicuramente Fermat non disponeva.

Ritengo pertanto che possa esistere un'altra dimostrazione del teorema di Fermat costruita con matematica più elementare e nel seguito tenterò di fornirla.

La seguente dimostrazione del teorema di Fermat procede logicamente per tre fasi secondo i valori che l'esponente n dell'equazione di Fermat può assumere.

Considero infatti tre casi possibili:

1. n dispari,
2. n pari e potenza del 2,
3. n pari ma prodotto di un numero dispari per un numero pari.

Qualsiasi n appartiene ad una delle tre categorie individuate e per ognuna di queste categorie è possibile dimostrare il teorema di Fermat.

In realtà il teorema di Fermat è stato dimostrato "classicamente" per diversi valori di n e mi pare che rimanga da dimostrare il teorema soltanto nel caso in cui n è un numero primo. Comunque la mia dimostrazione tenta di essere così generale da comprendere tutti i casi possibili.

Prima di procedere alla dimostrazione dei tre casi è necessario introdurre alcuni concetti generali e dimostrare il caso $n = 2$, ossia che esistono triplette di numeri interi che soddisfano la (1). La dimostrazione del caso $n = 2$ fornirà anche delle formule per generare tutte le triplette di numeri soddisfacenti la relazione pitagorica (1).

Poiché il caso 1 è la parte essenziale della mia dimostrazione, ritengo utile spiegare brevemente la logica su cui si basa:

1) la (1) si può scrivere anche come: $z^n - x^n - y^n = 0$, ma

2) $z^n - x^n - y^n = (z - x - y)^n + P(x, y, z)$ (P è un polinomio omogeneo di grado n).

Se $z^n - x^n - y^n = 0$, la relazione precedente diventa:

3) $(x + y - z)^n = P(x, y, z)$;

a questo punto, mediante un opportuno cambiamento di variabili (chiameremo le nuove variabili a , b , c), si può dimostrare che il polinomio P è sempre esprimibile come prodotto di due fattori, uno dei quali è, a sua volta, il prodotto dei termini costituenti il trinomio mentre l'altro è un polinomio omogeneo di grado $n - 3$; quindi la 3) diventa:

$$4) P(a,b,c) = abc \cdot P^{n-3} = (a-b-c)^n.$$

Quindi si dimostra che la 4) è impossibile e di conseguenza la 3) non è mai soddisfatta, ossia $z^n - x^n - y^n$ deve essere sempre diverso da 0.

1. GENERALITA'

1.1 Molteplicità delle soluzioni

Se la tripletta x_1, y_1, z_1 è una soluzione di (1) allora anche la tripletta mx_1, my_1, mz_1 (m numero intero positivo) è una soluzione di (1).

Infatti la (1) diventa:

$$m^n x_1^n + m^n y_1^n = m^n z_1^n, \quad (1.1)$$

raccogliendo il fattore m^n , diventa:

$$m^n (x_1^n + y_1^n) = m^n z_1^n \quad (1.2)$$

e, dividendo entrambi i membri per m^n si ottiene

$$x_1^n + y_1^n = z_1^n \quad (1.3)$$

che, per definizione, è una soluzione di (1).

1.2 Le soluzioni devono essere tra loro prime

I tre numeri x_1, y_1 e z_1 soluzioni di (1) devono essere tra loro primi. Infatti supponendo che y_1 sia multiplo di x_1 , ossia $y_1 = mx_1$ (m numero intero), la (1) diventa:

$$x_1^n + m^n x_1^n = z_1^n \quad (1.4)$$

e quindi

$$(m^n + 1)x_1^n = z_1^n. \quad (1.5)$$

Ossia anche z_1 deve essere un multiplo di x_1 ; posto $z_1 = kx_1$ (k numero intero) la (1.5) diventa:

$$(m^n + 1)x_1^n = k^n x_1^n \quad (1.6)$$

e pertanto deve essere

$$m^n + 1 = k^n \quad (1.7)$$

che è impossibile; quindi le eventuali soluzioni dell'equazione di Fermat devono essere formate da numeri tra loro primi.

1.3 z deve essere minore di $x + y$

Infatti se Z fosse uguale a $x + y$ l' n -esima potenza di Z diventerebbe:

$$z^n = x^n + y^n + \dots > x^n + y^n. \quad (1.8)$$

2. IL CASO $n = 2$

In questo caso si vuole dimostrare che esistono delle triplette di numeri x_1 , y_1 e z_1 che soddisfano la (1) e si vogliono fornire le formule con cui ottenere queste triplette.

La (1) nel caso di $n = 2$ diventa:

$$x^2 + y^2 = z^2 \quad (2.1)$$

che si può anche scrivere:

$$z^2 - y^2 = x^2 \quad (2.2)$$

ma $z^2 - y^2 = (z + y)(z - y)$ ossia è il prodotto di due fattori che devono essere dei quadrati per soddisfare il secondo membro della (2.2) (è possibile che il secondo fattore, $z - y$, sia uguale a 1).

Poniamo allora

$$z + y = a^2 \text{ e} \quad (2.3 \text{ a})$$

$$z - y = b^2. \quad (2.3 \text{ b})$$

Dalla (2.2) si ha $x^2 = a^2 b^2$, ossia $x = a \cdot b$. (2.4)

Risolvendo le (2.3) si ottiene:

$$z_1 = \frac{a^2 + b^2}{2}, \quad y_1 = \frac{a^2 - b^2}{2} \text{ e, dalla (2.4), } x_1 = a \cdot b. \quad (2.5)$$

Le (2.5) permettono di ottenere, al variare di a e di b , tutte le terne di numeri interi che soddisfano la (2.1).

Affinché le equazioni (2.5) forniscano dei numeri interi è necessario che a e b siano entrambi numeri pari o entrambi numeri dispari (con a maggiore di b per la seconda delle 2.5). Inoltre, volendo considerare solamente soluzioni non multiple (punto 1.1 delle generalità), è necessario che a e b siano tra loro primi.

Infatti se poniamo $a = kb$, e calcoliamo x , y e z dalle (2.5), si nota che sia x che y che z hanno in comune il fattore b^2 .

Quindi occorre non considerare il caso in cui a e b sono entrambi numeri pari in quanto avrebbero in comune il fattore 2.

Vediamo ora la dimostrazione formale delle (2.5); calcoliamo pertanto i quadrati di x_1 , y_1 e z_1 :

$$x_1^2 = a^2 \cdot b^2, \quad y_1^2 = \frac{a^4 - 2a^2b^2 + b^4}{4}, \quad z_1^2 = \frac{a^4 + 2a^2b^2 + b^4}{4} \quad (2.6)$$

e sommiamo quindi x_1^2 e y_1^2 : si osserva facilmente che il risultato è z_1^2 .

Sempre dalle definizioni (2.5) si ricava inoltre che:

$$z_1 + x_1 = \frac{(a+b)^2}{2}, \quad z_1 - x_1 = \frac{(a-b)^2}{2} \text{ e} \quad (2.7 \text{ a})$$

$$z_1 + y_1 = a^2, \quad z_1 - y_1 = b^2. \quad (2.7 \text{ b}) \equiv (2.3)$$

Inoltre si dimostra in appendice che, sempre ipotizzando a e b numeri dispari, x_1 e z_1 devono essere numeri dispari mentre y_1 deve essere un numero pari.

Vediamo ora un esempio: poniamo $a = 7$, $b = 3$, dalle (2.5) si ha allora $x = 21$, $y = 20$ e $z = 29$.

$$\text{Quindi } x^2 = 441, \quad y^2 = 400 \quad \text{e} \quad z^2 = 841, \quad \text{inoltre } z + x = 50 = \frac{(7+3)^2}{2}, \quad z - x = 8 = \frac{(7-3)^2}{2}, \\ z + y = 49 = 7^2 \quad \text{e} \quad z - y = 9 = 3^2.$$

Utilizzando lo stesso metodo di risoluzione si può dimostrare che anche l'equazione $x^n + y^n = z^n$ è risolubile analiticamente e che valgono formule simili alle (2.5). In questo caso le formule risolutive diventano:

$$x_1 = a \cdot b, \quad y_1 = \frac{a^n - b^n}{2} \quad \text{e} \quad z_1 = \frac{a^n + b^n}{2}.$$

Anche in questo caso si può procedere ad una dimostrazione formale ed ottenere delle equazioni analoghe alle (2.6).

3. IL CASO n DISPARI

Consideriamo ora il caso in cui n è un numero intero dispari.

La (1), ossia $x^n + y^n = z^n$, si può anche scrivere:

$$z^n - x^n - y^n = 0 \tag{3.1}$$

ma,

$$z^n - x^n - y^n = (z - x - y)^n + P^n(x, y, z) \tag{3.2}$$

dove con $P^n(x, y, z)$ si intende un polinomio omogeneo di grado n in x , y e z mentre il termine $z - x - y$ è negativo per la (1.8).

Introducendo le variabili ausiliarie a , b , c definite come:

$$a = x + y, \quad b = z - y \quad \text{e} \quad c = z - x \tag{3.3}$$

(a , b , c sono quindi tutti numeri interi e positivi), con le quali x, y, z vengono scritti come:

$$z = \frac{a + b + c}{2}, \quad x = \frac{a + b - c}{2}, \quad y = \frac{a - b + c}{2} \quad (\text{e } z - x - y = \frac{-a + b + c}{2}) \tag{3.4}$$

e riscrivendo la (3.2) con le nuove variabili si ottiene:

$$P^n(a, b, c) = \left(\frac{a + b + c}{2}\right)^n - \left(\frac{a + b - c}{2}\right)^n - \left(\frac{a - b + c}{2}\right)^n - \left(\frac{-a + b + c}{2}\right)^n \tag{3.5}$$

A questo punto, sviluppando le potenze mediante la formula dell' n -esima potenza di un trinomio:

$$(a \pm b \pm c)^n = n! \cdot \sum_{p, q, r=0}^n \frac{a^p \cdot (\pm 1)^q b^q \cdot (\pm 1)^r c^r}{p! q! r!} \tag{3.6}$$

con p, q, r numeri interi tali che $p + q + r = n$ (nell'appendice si fornirà la formula generale dell' n -esima potenza di un polinomio), si osserva che il secondo membro della (3.5) si semplifica e si riduce a:

$$\frac{4n!}{2^n} \cdot \sum_{p,q,r=1}^n \frac{a^p b^q c^r}{p! q! r!}.$$

Infatti, sviluppando le potenze a secondo membro della (3.5) utilizzando la (3.6), si nota che si possono ottenere soltanto 4 tipi di termini:

1. monomi di grado n ,
2. binomi con un termine con esponente pari ed uno con esponente dispari la cui somma è pari a n ,
3. trinomi con due termini con esponente pari ed uno con esponente dispari (la cui somma è pari a n) e
4. trinomi con tutti i termini con esponente dispari (la cui somma è pari a n).

Ora, i coefficienti dei termini con gli stessi esponenti sono uguali (vedi 3.6) e, a causa dei segni dei termini a secondo membro, i termini dei primi tre tipi si elidono a 2 a 2, mentre i termini dell'ultimo tipo risultano tutti con lo stesso segno, dando origine al fattore 4:

$$(a + b + c)^n - (a + b - c)^n - (a - b + c)^n - (-a + b + c)^n = 4n! \cdot \sum_{p,q,r=1}^n \frac{a^p b^q c^r}{p! q! r!} \quad (3.7)$$

Quindi il polinomio $P^n(a, b, c)$ della (3.5) diventa:

$$P^n(a, b, c) = \frac{4n!}{2^n} \cdot \sum_{p,q,r=1}^n \frac{a^p b^q c^r}{p! q! r!} \quad (3.8)$$

con p, q, r numeri interi **dispari** tali che $p + q + r = n$.

La sommatoria deve essere estesa a tutte le possibili triplette dei numeri p, q ed r **dispari** tali che la loro somma sia uguale ad n , facendo variare i 3 indici da 1 a n .

Dal momento che, a seguito delle semplificazioni, in tutti i termini della sommatoria sono sempre presenti le variabili a, b, c (p, q ed r sono sempre tutti diversi da zero) è possibile raccoglierle a fattor comune e portarle fuori dalla sommatoria:

$$P^n(a, b, c) = \frac{4n!}{2^n} \cdot abc \cdot \sum_{p,q,r=0}^{n-3} \frac{a^p b^q c^r}{p! q! r!} = abc \cdot P^{n-3}(a, b, c) \quad (3.9)$$

Questa volta la sommatoria è estesa a tutte le possibili triplette dei numeri p, q ed r **pari** tali che la loro somma sia uguale ad $n - 3$. Questo fatto comporta che nel caso $n = 3$ il polinomio si riduce al prodotto delle tre variabili ausiliarie per una costante che, in questo caso, è uguale a 3.

Se $z^n - x^n - y^n = 0$, la (3.2) si riduce a:

$$(x + y - z)^n = P(x, y, z) \quad (3.10)$$

Trasformando la (3.10) in termini di a, b, c , si ottiene:

$$\left(\frac{a - b - c}{2}\right)^n = \frac{4n!}{2^n} \cdot \sum_{p,q,r=1}^n \frac{a^p b^q c^r}{p! q! r!} \quad (3.11)$$

moltiplicando i due membri per 2^n e raccogliendo a fattor comune il termine abc del secondo membro, la (3.11) diventa:

$$(a-b-c)^n = 4n! \cdot abc \cdot \sum_{p,q,r=0}^{n-3} \frac{a^p b^q c^r}{p! q! r!} = abc \cdot P^{n-3}(a,b,c) \quad (3.12)$$

Avendo fattorizzato il secondo membro è possibile scrivere la seguente uguaglianza:

$$(a-b-c)^j \cdot (a-b-c)^k = abc \cdot P^{n-3}(a,b,c) \quad (3.13)$$

dove $j+k=n$.

La (3.13) implica che:

$$(a-b-c)^j = abc \quad (3.14)$$

che, a sua volta, si può fattorizzare come segue:

$$(a-b-c)^{j_1} \cdot (a-b-c)^{j_2} \cdot (a-b-c)^{j_3} = abc \quad (3.15)$$

$$(j_1 + j_2 + j_3 = j)$$

Di conseguenza le tre variabili ausiliarie non sono tra loro prime ma si possono esprimere come multipli di una di esse; ad esempio, se $b = \min\{a, b, c\}$ sarà:

$$a = \alpha b; c = \beta b \quad (3.16)$$

Consideriamo ora le variabili principali x, y, z e ipotizziamo che sia:

$$y = x + i \text{ e } z = x + j \quad (3.17)$$

Esprimendo ora le variabili ausiliarie nei termini di x, y, z mediante le (3.3) si ha:

$$\begin{cases} a = x + x + i = 2x + i \\ b = x + j - x - i = j - i \\ c = x + j - x = j \end{cases} \quad (3.18)$$

e riscrivendo le (3.16) con le (3.18) otteniamo:

$$\begin{cases} a = \alpha b \\ c = \beta b \end{cases} \rightarrow \begin{cases} 2x + i = \alpha \cdot (j - i) \\ j = \beta \cdot (j - i) \end{cases} \quad (3.19)$$

La seconda delle (3.19) dà:

$$j = \frac{\beta}{\beta - 1} \cdot i \quad (3.20)$$

che ha soluzioni nei numeri interi soltanto per $\beta = 2$, e determina:

$$j = 2i \quad (3.21)$$

Sostituendo ora la (3.21) nella prima delle (3.19) si ottiene:

$$2x + i = ai \rightarrow x = \frac{\alpha - 1}{2} \cdot i \quad (3.22)$$

La (3.22), sostituita nella prima delle (3.17), determina:

$$y = \frac{\alpha + 1}{2} \cdot i \quad (3.23)$$

mentre, sostituita nella seconda delle (3.17), ricordando la (3.21) determina:

$$z = \frac{\alpha + 3}{2} \cdot i \quad (3.24)$$

Ossia, il fatto di esprimere a e c come multipli di b determina che x, y, z risultano con il fattore comune i contrariamente alla loro definizione (capitolo 1.2).

Quindi non è possibile esprimere a e c come multipli di b e di conseguenza non è possibile risolvere la (3.14) né la (3.12).

In altri termini il secondo membro della (3.2)

$$z^n - x^n - y^n = (z - x - y)^n + P^n(x, y, z) \quad (3.2)$$

non si annulla mai nell'ambito dei numeri interi e la (3.1) non è soddisfatta come la (1).

4. IL CASO n PARI E POTENZA DEL 2

In questo caso n deve essere della forma: $n = 2^p$ ($p > 1$) e quindi l'equazione (1) diventa:

$$x^{2^p} + y^{2^p} = z^{2^p}, \quad (4.1)$$

che può anche essere scritta come:

$$z^{2^p} - y^{2^p} = x^{2^p}. \quad (4.2)$$

Il primo membro dell'equazione (4.2) può essere scomposto in fattori:

$$z^{2^p} - y^{2^p} = (z^{2^{p-1}} + y^{2^{p-1}}) \cdot \dots \cdot (z^2 + y^2)(z^2 - y^2). \quad (4.3)$$

Analogamente agli altri casi precedenti, questa scomposizione in fattori implica che:

$$\left\{ \begin{array}{l} z^{2^{p-1}} + y^{2^{p-1}} = a^{2^p}, \\ z^{2^{p-2}} + y^{2^{p-2}} = b^{2^p}, \\ \dots \\ z^2 + y^2 = i^{2^p}, \\ z^2 - y^2 = j^{2^p}. \end{array} \right. \quad (4.4)$$

Tutte queste equazioni devono essere contemporaneamente soddisfatte.

Sulle prime equazioni non si può dire nulla, tuttavia le ultime due mediante le sostituzioni $i^{2^{p-1}} = I$ e $j^{2^{p-1}} = J$ diventano:

$$\begin{cases} z^2 + y^2 = I^2 & (4.5 \text{ a}) \\ z^2 - y^2 = J^2 & (4.5 \text{ b}) \end{cases}$$

che sono della forma (2.1) e pertanto risolvibili.

Applicando le (2.5) si ottiene:

$$\begin{cases} z_a = ab, & y_a = \frac{a^2 - b^2}{2} & (4.6 \text{ a}) \\ z_b = \frac{s^2 + t^2}{2}, & y_b = \frac{s^2 - t^2}{2} & (4.6 \text{ b}) \end{cases}$$

ovviamente, i due valori di z e di y devono essere uguali, quindi:

$$\begin{cases} y: & \frac{a^2 - b^2}{2} = \frac{s^2 - t^2}{2} & (4.7 \text{ a}) \\ z: & ab = \frac{s^2 + t^2}{2}. & (4.7 \text{ b}) \end{cases}$$

Dalla (4.7 a), risolvendola per s^2 si ottiene:

$$s^2 = a^2 - b^2 + t^2 \quad (4.8)$$

che, sostituita nella (4.7 b) permette di ottenere t^2 :

$$t^2 = \frac{a^2 - b^2 - 2ab}{2}, \quad (4.9)$$

ricordando le (4.6 a) la (4.9) è equivalente a

$$t^2 = y - z. \quad (4.10)$$

Ma l'eguaglianza (4.10) impone che y sia maggiore di z poiché t^2 è un numero positivo, condizione che è in contrasto con quella espressa nell'equazione (4.5 b) che per gli stessi motivi impone che z sia maggiore di y . Pertanto l'unico valore possibile per y e z è lo 0 che è una soluzione banale della (1) se lo si assegna anche a x .

Quindi poiché non sono soddisfatte le ultime due equazioni delle (4.4), non è soddisfatta neppure la (4.1).

In questo modo è dimostrato anche il caso n pari e potenza del 2.

5. IL CASO n PARI MA PRODOTTO DI UN NUMERO DISPARI

In questo caso n può essere scritto nella forma $n = (2m)(2p+1)$ e l'equazione di Fermat si può scrivere come:

$$x^{(2m)(2p+1)} + y^{(2m)(2p+1)} = z^{(2m)(2p+1)}. \quad (5.1)$$

Pertanto definendo $X = x^{(2m)}$, $Y = y^{(2m)}$ e $Z = z^{(2m)}$, la (5.1) si può riscrivere come:

$$X^{(2p+1)} + Y^{(2p+1)} = Z^{(2p+1)} \quad (5.2)$$

che è della stessa forma della (3.1) e pertanto già dimostrata.

APPENDICE

Dimostrazione che $\frac{x^2 + y^2}{2}$, con x e y dispari, è un numero dispari.

Se x ed y sono numeri dispari devono essere della forma:

$$x = (2n + 1), \quad y = (2m + 1) \tag{a.1}$$

pertanto i loro quadrati diventano:

$$x^2 = 4n^2 + 4n + 1 \quad e \quad y^2 = 4m^2 + 4m + 1 \tag{a.2}$$

e la somma dei quadrati:

$$x^2 + y^2 = 4(m^2 + n^2 + m + n) + 2. \tag{a.3}$$

Se calcoliamo ora $\frac{x^2 + y^2}{2}$ si ottiene:

$$\frac{x^2 + y^2}{2} = \frac{4(m^2 + n^2 + m + n) + 2}{2} = 2(m^2 + n^2 + m + n) + 1 \tag{a.4}$$

che è un numero dispari.

Calcoli analoghi dimostrano che la semidifferenza dei quadrati di due numeri dispari è sempre un numero pari.

Questa dimostrazione vale anche per qualsiasi altra potenza maggiore di 2.

Infine si riporta la formula per il calcolo delle potenze n-esime di polinomi:

$$(a \pm b \pm c \pm \dots \pm g)^n = n! \cdot \sum_{p,q,\dots,t=0}^n \frac{a^p \cdot (\pm 1)^q b^q \cdot (\pm 1)^r c^r \cdot \dots \cdot (\pm 1)^t g^t}{p!q! \cdot \dots \cdot t!} \tag{a.5}$$

con p, q, ..., t numeri interi tali che p + q + ... + t = n.

Ad esempio, nel caso di una quinta potenza di un polinomio di 4 termini: n = 5, gli indici p, q, r ed s ed i coefficienti dei vari termini devono assumere i seguenti valori:

p	q	r	s	n!/p!q!r!s!
5	0	0	0	1
4	1	0	0	5
4	0	1	0	5
4	0	0	1	5
3	2	0	0	10
3	1	1	0	20
3	1	0	1	20
3	0	2	0	10
3	0	1	1	20
3	0	0	2	10
2	3	0	0	10
2	2	1	0	30
2	2	0	1	30
2	1	2	0	30

p	q	r	s	n!/p!q!r!s!
2	1	1	1	60
2	1	0	2	30
2	0	3	0	10
2	0	2	1	30
2	0	1	2	30
2	0	0	3	10
1	4	0	0	5
1	3	1	0	20
1	3	0	1	20
1	2	2	0	30
1	2	1	1	60
1	2	0	2	30
1	1	3	0	20
1	1	2	1	60

p	q	r	s	n!/p!q!r!s!
1	1	1	2	60
1	1	0	3	20
1	0	4	0	5
1	0	3	1	20
1	0	2	2	30
1	0	1	3	20
1	0	0	4	5
0	5	0	0	1
0	4	1	0	5
0	4	0	1	5
0	3	2	0	10
0	3	1	1	20
0	3	0	2	10
0	2	3	0	10

p	q	r	s	n!/p!q!r!s!
0	2	2	1	30
0	2	1	2	30
0	2	0	3	10
0	1	4	0	5
0	1	3	1	20
0	1	2	2	30
0	1	1	3	20
0	1	0	4	5
0	0	5	0	1
0	0	4	1	5
0	0	3	2	10
0	0	2	3	10
0	0	1	4	5
0	0	0	5	1