Università degli Studi di Cagliari
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Matematica

L'Ultimo Teorema di Fermat per $n = 3$ e $n = 4$

Relatore
Prof. Andrea Loi

Tesi di Laurea di
Sara Manca

Anno Accademico 2008/2009

Introduzione

Sia n un numero intero positivo. Il ben noto *Ultimo Teorema di Fermat* afferma che l'equazione $x^n+y^n = z^n$ non ammette soluzioni intere positive se $n \geq 3$. Questo teorema è stato dimostrato da Andrew John Wiles [2] nel 1994 (si veda anche [3]).

In questa tesi descriviamo le dimostrazione di questo teorema nel caso $n = 3$ (Capitolo 2) e $n = 4$ (Capitolo 1). Le dimostrazioni presentate sono dovute a Eulero quella nel caso in cui $n = 3$, e a Fermat quella per $n = 4$. Il materiale di questa tesi si basa sul Capitolo 1 e 2 di [1].

Indice

Capitolo 1

L'Ultimo Teorema di Fermat per $n = 4$

1.1 Terne pitagoriche e il teorema della discesa infinita

Teorema 1.1.1. *Siano x, y, z tre numeri interi positivi tali che*

$$x^2 + y^2 = z^2 \tag{1.1}$$

allora esistono p e q coprimi, di opposta parità e $p > q$ tali che:

$$\begin{cases} x = 2pq \\ y = p^2 - q^2 \\ z = p^2 + q^2 \end{cases} \tag{1.2}$$

Dimostrazione. Consideriamo x, y, z tali che $x^2 + y^2 = z^2$, supponiamo che x, y, z siano primi fra di loro. Se due di essi avrebbero un fattore comune, allora per la (1.1) sarà comune anche al terzo, inoltre, se tutti e tre avessero un fattore comune d tale per cui:

$$\begin{cases} x = x^{'}d \\ y = y^{'}d \\ z = z^{'}d \end{cases}$$

sostituendo $d^2(x'^2 + y'^2) = d^2 z'^2$e semplificando d^2 otterremo che gli interi $x' = \frac{x}{d}, y' = \frac{y}{d}, z' = \frac{z}{d}$ formerebbero una nuova terna pitagorica detta primitiva. Ogni terna può essere quindi ridotta ad una primitiva semplicemente dividendo per il massimo comun divisore.

Possiamo aggiungere che x, y, z non possono essere dispari (ma nemmeno tutti e tre pari, poichè abbiamo supposto essere coprimi), in quanto, se lo fossero dall'equazione (1.1) avremo al primo membro la somma di due numeri dispari, che chiaramente, non darà un numero dispari ma pari. Al tempo stesso z non potrà essere pari, in quanto, se lo fosse risulterebbe $z = 2n$ che al quadrato è un multiplo di 4, tale multiplo dovrebbe essere uguale alla somma di due numeri dispari anch'essi al quadrato, che come si vede in seguito è impossibile:

$$(2n)^2 = (2m + 1)^2 + (2k + 1)^2$$

Quindi z deve essere dispari e x e y avranno parità opposta (uno pari e uno dispari). Poniamo x pari e y dispari. Dall'equazione (1.1):

$$x^2 = z^2 - y^2 = (z - y)(z + y)$$

otteniamo che $x, z + y, z - y$ sono pari, in quanto somma di due numeri dispari, di conseguenza esisteranno u, v, w tali che

$$x = 2u$$

$$z + y = 2v$$

$$z - y = 2w$$

quindi dalla (1.1)

$$(2u)^2 = (2v)(2w)$$

$$u^2 = vw \tag{1.3}$$

Naturalmente v e w devono essere coprimi, in quanto qualsiasi loro fattore comune dividerebbe anche z e y per via delle seguenti uguaglianze

$$v + w = z$$

$$v - w = y$$

ma, come detto precedentemente, z e y sono primi fra di loro.

La (1.3) ha senso solo se v e w sono dei quadrati, quindi esistono p e q tali che

$$v = p^2$$

$$w = q^2$$

Naturalmente $(p, q) = (v, w) = 1$, sostituendo avremo:

$$z = v + w = p^2 + q^2$$

$$y = v - w = p^2 - q^2$$

dove $p > q$ (poichè y è un intero positivo), inoltre hanno opposta parità poichè z e y sono dispari. Se esprimiamo x in funzione di p e q otteniamo:

$$x^2 = z^2 - y^2 = (z - y)(z + y) = 2w2v = 4p^2q^2$$

da questa ricaviamo che

$$x = 2pq$$

Di conseguenza, qualunque sia p e q tali che $p > q$, siano coprimi e abbiano opposta parità, otteniamo delle terne pitagoriche date da:

$$\begin{cases} x = 2pq \\ y = p^2 - q^2 \\ z = p^2 + q^2 \end{cases}$$

□

Lemma 1.1.2 (La discesa infinita)**.** *Non esiste una proprietà che, se soddisfatta da un intero positivo, possa essere soddisfatta da un intero positivo più piccolo.*

Il metodo della discesa infinita dimostra che alcune proprietà o relazioni sono impossibili, se applicate a numeri interi positivi, infatti, se si prova che queste valgono per qualsiasi numero, queste devono valere anche se si considerano numeri più piccoli; ma questi ultimi, a loro volta, per le stesse motivazioni precedenti, devo valere per alcuni numeri ancora più piccoli, così fino all'infinito. Questo processo è impossibile, in quanto una sequenza di numeri interi non può decrescere all'infinito.

1.2 Dimostrazione dell'Ultimo Teorema di Fermat per $n = 4$

Teorema 1.2.1. *L'equazione*

$$x^4 + y^4 = z^4 \tag{1.4}$$

non ammette soluzioni intere positive quando $xyz \neq 0$.

Dimostrazione. Per dimostrare questo teorema consideriamo il caso in cui $x^4 + y^4 = z^2$ poiche la (1.4) posso scriverla come $x^4 + y^4 = (z^2)^2$.

Per le stesse ragioni viste nel Teorema 1.1.1 avremo che x, y, z sono coprimi, quindi lo saranno anche x^2, y^2, z^2, inoltre, esendo terne pitagoriche, dalla (1.2) possiamo scrivere:

$$\begin{cases} x^2 = 2pq \\ y^2 = p^2 - q^2 \\ z^2 = p^2 + q^2 \end{cases}$$

dove p e q sono coprimi, di parità opposta e $p > q > 0$ (vedi la dimostrazione del Teorema 1.1.1).

Dalla seconda delle precedenti equazioni possiamo scrivere

$$y^2 + q^2 = p^2$$

nuovamente avremo che y, p, q sono delle terne pitagoriche, dove p è dispari (vedi Teorema 1.1.1), quindi q sarà pari poichè hanno opposta parità, potremmo scrivere:

$$\begin{cases} q = 2ab \\ y = a^2 - b^2 \\ p = a^2 + b^2 \end{cases}$$

dove a e b sono coprimi, di parità opposta e $a > b > 0$.

Scriviamo x in funzione di a e b:

$$x^2 = 2pq = 2(a^2 + b^2)(2ab) = 4ab(a^2 + b^2)$$

dove $ab(a^2 + b^2)$ è un quadrato. Inoltre, ab e $(a^2 + b^2)$ sono coprimi, infatti, se $P|ab$, allora dovrebbe dividere a oppure b, ma non entrambi in quanto sono coprimi,

quindi non può dividere (a^2+b^2). Poiché ab e (a^2+b^2) sono quadrati, allora, essendo ab un quadrato e a e b coprimi, anche a e b sono dei quadrati, poniamo che $a = X^2$ e $b = Y^2$, così:

$$X^4 + Y^4 = a^2 + b^2 = p < p^2 + q^2 = z^2 < z^4 = x^4 + y^4$$

Iterando il procedimento si troveranno delle nuove soluzioni $X' < X$ e $Y' < Y$ tali che

$$(X')^4 + (Y')^4 < z^4$$

procedendo così all'infinito.
Si è così arrivati ad una discesa infinita di interi positivi, che come abbiamo visto nel Lemma 1.1.2 della discesa infinita è impossibile. Questo dimostra il teorema, poichè se la somma di due quarte potenze non può essere un quadrato, non potrà neppure essere una quarta potenza.

□

Da questo teorema, segue che, l'equazione $x^{4m} + y^{4m} = z^{4m}$ non ammette soluzioni quando m è un intero positivo, infatti, posto $X = x^m$, $Y = y^m$ e $Z = z^m$ otterrei l'equazione $X^4 + Y^4 = Z^4$ che come visto nel Teorema 1.2.1 non ammette soluzioni intere positive; quindi quando n divide 4 l'equazione $x^n + y^n = z^n$ non ammette soluzioni. Un esponente $n > 2$, che non è divisibile per 4 e non è potenza di 2, deve essere diviso da qualche primo $p \neq 2$, poniamo $n = pm$; per provare che $x^n + y^n = z^n$ è impossibile, è sufficiente provare che $x^p + y^p = z^p$ è impossibile. La dimostrazione del Teorema di Fermat per $n = 4$ ci consente di ricondurre il caso genarale al caso in cui $n > 2$ e che sia un numero primo.

Capitolo 2

L'Ultimo Teorema di Fermat per $n = 3$

2.1 Strumenti necessari per la dimostrazione

Lemma 2.1.1. *Siano p e q interi positivi, coprimi e di opposta parità. Se $2p$ e $p^2 + 3q^2$ hanno un fattore comune $k \neq 1$ allora $k = 3$.*

Dimostrazione. Per ipotesi p e q hanno opposta parità, di conseguenza $p^2 + 3q^2$ sarà dispari, quindi ogni fattore comune a $2p$ e $p^2 + 3q^2$ deve essere comune a p e $p^2 + 3q^2$, infatti, se supponiamo che k sia un loro fattore comune, non potrà sicuramente essere 2 poichè $p^2 + 3q^2$ è dispari. Inoltre questo fattore, sarà a sua volta comune a p e $3q^2$, infatti potremmo scrivere:

$$p = Pk$$

$$p^2 + 3q^2 = Qk$$

quindi

$$3q^2 = k(Q - P^2)$$

ma poichè p e q sono primi fra loro, può essere solo 3.

□

Lemma 2.1.2. *Siano a e b due interi con opposta parità e coprimi. Se $2a$, $a + 3b$ e $a - 3b$ hanno un fattore comune $k \neq 1$ allora $k = 3$.*

Dimostrazione. Per ipotesi a e b hanno opposta parità quindi $a-3b$ e $a+3b$ sono dispari, di conseguenza ogni fattore comune a $2a$, $a+3b$ e $a-3b$ deve essere comune sia ad a che a $a \pm 3b$, infatti, se supponiamo che k sia un loro fattore comune non potrà sicuramente essere 2 poichè $a+3b$ e $a-3b$ sono dispari. Inoltre questo fattore sarà a sua volta comune ad a e $3b$, infatti

$$a = Ak$$

$$a + 3b = Bk$$

avremo

$$3b = k(B - A)$$

Però a e b sono coprimi, quindi questo fattore può essere solo 3. □

Lemma 2.1.3. *Siano a e b interi coprimi e di opposta parità, allora $2b$, $a+b$ e $a-b$ sono coprimi.*

Dimostrazione. Sappiamo che a e b hanno opposta parità, di conseguenza $a+b$ e $a-b$ sono dispari. Se $2b$ e $a \pm b$ avessero un fattore in comune non potrà sicuramente essere 2, quindi ogni fattore comune a $2b$ e $a \pm b$ sarà comune a b e $a \pm b$, ma a e b per ipotesi sono primi fra di loro, questo implica che non esiste un fattore che sia comune ad $2b$ e $a \pm b$. □

Lemma 2.1.4. *Se $A = BC$ è il prodotto di due interi B, C, e se questi possono essere scritti nella forma $B = x^2 + cy^2$, $C = u^2 + cv^2$, con x, y, u, v, c interi positivi, allora esisteranno a, b interi positivi tali che*

$$A = a^2 + cb^2$$

Dimostrazione. Posto $a = xu - cyv$ e $b = xv + yu$ avremo

$$A = a^2 + cb^2 = (xu - cyv)^2 + c(xv + yu)^2$$

ma da quanto supposto precedentemente, A è il prodotto BC, quindi

$$(x^2 + cy^2)(u^2 + cv^2) = (xu - cyv)^2 + c(xv + yu)^2 \tag{2.1}$$

questo implica che posso scrivere A usando la seguente formula

$$a + ib\sqrt{c} = (x + iy\sqrt{c})(u + iv\sqrt{c}) \tag{2.2}$$

infatti, quest'equazione è equivalente alla (2.1) se consideriamo i moduli. □

Nel Lemma 2.1.4 abbiamo considerato un generico intero c, successivamente considereremo il caso particolare in cui $c = 3$.

Lemma 2.1.5. *Se p e q sono coprimi allora ogni fattore dispari di $p^2 + 3q^2$ sarà a sua volta della forma $c^2 + 3d^2$.*

Dimostrazione. Sia x un fattore dispari di $p^2 + 3q^2$. Dividendo sia p che q per x avremo $p = mx \pm c$ e $q = nx \pm d$, dove $|c| < \frac{1}{2}x$ e $|d| < \frac{1}{2}x$. Poichè

$$p^2 + 3q^2 = (mx \pm c)^2 + 3(nx \pm d) = c^2 + 3d^2 + Ax$$

è divisibile per x, lo sarà anche $c^2 + 3d^2$, quindi scriviamo $c^2 + 3d^2 = xy$, dove $y < x$.
Naturalmente c e d non potranno avere un fattore comune maggiore di 1, in quanto, questo fattore dovrebbe dividere x, di conseguenza sia p che q e questo va in contraddizione con l'ipotesi che p e q sono coprimi. Quindi, iterando il procedimento, l'equazione $c^2 + 3d^2 = xy$ potrà essere divisa dal più grande fattore comune di c e d, dando un'equazione della forma $e^2 + 3f^2 = zx$, dove $z < x$ in quanto

$$zx = e^2 + 3f^2 < c^2 + 3d^2 < (\frac{1}{2}x)^2 + 3(\frac{1}{2}x)^2 = x^2.$$

Se x non fosse della forma $p^2 + 3q^2$, z avrebbe un fattore dispari che non potrà essere scritto nella stessa forma. Quindi, l'esistenza di un numero dispari x, fattore di un numero della forma $p^2 + 3q^2$, il quale non sia esso stesso della forma $c^2 + 3d^2$ implica l'esistenza di un numero dello stesso tipo che però sarà più piccolo, ma questo porterebbe ad una discesa infinita (vedi Lemma 1.1.2 della discesa infinita) che è impossibile, quindi x deve essere della forma $c^2 + 3d^2$. □

Lemma 2.1.6. *Siano a, b, p, q interi positivi tali che $P = a^2 + 3b^2$ sia primo. Se $P|p^2 + 3q^2$ allora $P|aq - pb$ oppure $P|aq + pb$.*

Dimostrazione. Osserviamo che

$$3(aq + pb)(aq - pb) = a^2(p^2 + 3q^2) - p^2(a^2 + 3b^2)$$

L'ipotesi che $P|p^2 + 3q^2$ implica che $P = a^2 + 3b^2$ deve dividere uno dei tre interi $3, (aq + pb), (aq - pb)$, non potendo dividere 3 (in quanto $P = a^2 + 3b^2 > 3$) deve dividere $aq - pb$ oppure $aq + pb$. □

Lemma 2.1.7. *Siano p e q interi positivi, coprimi e di opposta parità tali per cui p^2+3q^2 sia un cubo, allora devono esistere degli interi a e b (non necessariamente positivi) primi fra loro e di opposta parità tali per cui*

$$p = a^3 - 9ab^2$$

$$q = 3a^2b - 3b^3$$

Dimostrazione. Per dimostrare che $p^2 + 3q^2$ sia un cubo effettuiamo la seguente fattorizzazione:

$$p^2 + 3q^2 = (p + iq\sqrt{3})(p - iq\sqrt{3})$$

Se dimostriamo che

$$p + iq\sqrt{3} = (a + ib\sqrt{3})^3$$

allora con semplici passaggi otteniamo

$$(p + iq\sqrt{3})(p - iq\sqrt{3}) = [(a + ib\sqrt{3})(a - ib\sqrt{3})]^3$$

che è equivalente a $p^2 + 3q^2 = (a^2 + 3b^2)^3$. Inoltre, risolvendo il cubo otteniamo

$$p + iq\sqrt{3} = (a + ib\sqrt{3})^3 = a^3 + 3a^2ib\sqrt{3} - 9ab^2 - 3b^3i\sqrt{3}$$

con $p = a^3 - 9ab^2$ e $q = 3a^2b - 3b^3$, e dove a e b sono coprimi, in quanto ogni loro fattore comune dovrebbe dividere sia p che q ed è impossibile poichè questi sono primi fra loro, saranno inoltre di opposta parità poichè se fossero entrambi pari o entrambi dispari dalle suddette uguaglianze anche p e q dovrebbero essere pari, ma non è possibile poichè abbiamo supposto che avessero opposta parità.

A questo punto ci resta da dimostrare che $p+iq\sqrt{3} = (a+ib\sqrt{3})^3$, consideriamo i seguenti passi:

Passo 1 *Se p e q sono coprimi e $p^2 + 3q^2$ è pari, allora*

$$p + iq\sqrt{3} = (1 \pm i\sqrt{3})(u + iv\sqrt{3})$$

dove u e v sono degli interi relativamente primi e il segno viene scelto appropiatamente.

Se $p^2 + 3q^2$ è pari, allora p e q avranno la stessa parità, cioè sono entrambi dispari, in quanto essendo coprimi non possono essere entrambi pari. Di

conseguenza p, q sono della forma $4n \pm 1$ e quindi $p+q$ oppure $p-q$ deve essere divisibile per 4. Supponiamo che lo sia $p+q$ (poichè nel caso in cui lo sia $p-q$ si procede allo stesso modo). Osserviamo che (vedi (2.1))

$$4(p^2+3q^2) = (1^2+3\cdot 1^2)(p^2+3q^2) = (p-3q)^2+3(p+q)^2.$$

Dividiamo per 4^2 il primo e secondo membro dell'uguaglianza precedente avremo $\frac{p^2+3q^2}{4}$ che può essere scritto nella forma u^2+3v^2 dove $u = \frac{p-3q}{4}$ e $v = \frac{p+q}{4}$ (osservando che u e v sono interi in quanto $p+q$ è divisibile per 4). Quest'equazione posso risolverla per p e q in termini di u e v, infatti posso scrivere:

$$u + iv\sqrt{3} = \frac{(p+iq\sqrt{3})(1+i\sqrt{3})}{4}$$

da questa moltiplicando entrambi i membri per $1-i\sqrt{3}$ otteniamo

$$(1-i\sqrt{3})(u+iv\sqrt{3}) = p+iq\sqrt{3}$$

dove u e v sono relativamente primi e ciò conclude la dimostrazione del primo passo.

Passo 2 *Se p e q sono coprimi e p^2+3q^2 è divisibile per un numero primo dispari P, allora, $P = a^2+3b^2$, con a e b interi, e*

$$p+iq\sqrt{3} = (a \pm ib\sqrt{3})(u+iv\sqrt{3})$$

dove u e v sono degli interi relativamente primi e il segno viene scelto appropiatamente.

Dal Lemma 2.1.5 sappiamo che se p e q sono coprimi allora qualsiasi fattore dispari divida p^2+3q^2 sarà anch'esso della stessa forma, quindi, poichè P è un primo dispari che divide p^2+3q^2, lo potremmo scrivere come $P = a^2+3b^2$. In questo caso, per il Lemma 2.1.6, avremo che $aq-pb$ oppure $aq+pb$ deve essere divisibile per P. Supponiamo che lo sia $aq+pb$ (poichè nel caso in cui lo sia $aq-pb$ si procede allo stesso modo). Scriviamo:

$$P(p^2+3q^2) = (a^2+3b^2)(p^2+3q^2)$$

per la (2.1) avremo

$$P(p^2+3q^2) = (a^2+3b^2)(p^2+3q^2) = (ap-3bq)^2+3(aq+pb)^2.$$

Dividiamo per P^2 il primo e secondo membro dell'uguaglianza precedente avremo $\frac{p^2+3q^2}{P}$ che può essere scritto nella forma u^2+3v^2 dove $u=\frac{ap-3bq}{P}$ e $v=\frac{aq+pb}{P}$ (osservando che u e v sono interi in quanto $aq+pb$ è divisibile per $P=a^2+3b^2$). Quest'equazione posso scriverla come

$$u+iv\sqrt{3}=\frac{(a+ib\sqrt{3})(p+iq\sqrt{3})}{P}$$

moltiplicando entrambi i membri per $a-ib\sqrt{3}$ otteniamo:

$$(u+iv\sqrt{3})(a-ib\sqrt{3})=p+iq\sqrt{3}$$

Concludendo così la dimostrazione del secondo passo.

Passo 3 *Siano p e q coprimi, allora*

$$p+iq\sqrt{3}=\pm(a_1\pm ib_1\sqrt{3})(a_2\pm ib_2\sqrt{3})\cdots(a_n\pm ib_n\sqrt{3}) \tag{2.3}$$

dove a_i e b_i sono interi e $a_i^2+3b_i^2$ può essere 4 oppure un numero primo dispari.

Sappiamo che se p^2+3q^2 è pari, allora è divisibile per 4, inoltre, se non fosse uguale a 1, avrà un fattore P che può essere 4 oppure un numero primo dispari. Quindi possiamo ricondurre tutto al primo o al secondo passo, cioè

$$p+iq\sqrt{3}=(a_1\pm ib_1\sqrt{3})(p_1+iq_1\sqrt{3})$$

dove p_1 e q_1 sono coprimi. A questo punto, posso fare lo stesso ragionamento fatto precedentemente, cioè scrivendo

$$p_1+iq_1\sqrt{3}=(a_2+ib_2\sqrt{3})(p_2+iq_2\sqrt{3})$$

con l'unica eccezione che $p_1^2+3q_1^2=\frac{p^2+3q^2}{P}$, dove $P=a^2+3b^2$, è più piccolo di p^2+3q^2. Iterando questo procedimento si arriverà ad una fase in cui

$$p+iq\sqrt{3}=(a_1\pm ib_1\sqrt{3})\cdots(a_n\pm ib_n\sqrt{3})(u+iv\sqrt{3}).$$

Ma questo procedimento non potrà continuare all'infinito, infatti si arriverà ad un punto in cui $u^2+3v^2=1$, cioè $u=\pm1$ e $v=0$ quindi $u+iv\sqrt{3}=\pm1$, e questo completa la fattorizzazione.

Passo 4 *Siano p e q coprimi, allora i termini della fattorizzazione (2.3) sono completamente determinati a meno della scelta dei segni, dalla seguente fattorizzazione di p^2+3q^2, cioè*

$$p^2+3q^2=(a_1^2+3b_1^2)(a_2^2+3b_2^2)\cdots(a_n^2+3b_n^2)$$

fatta di numeri primi dispari oppure divisibili per 4. Inoltre, se nella (2.3) appare il fattore $a+ib\sqrt{3}$, non ci sarà $a-ib\sqrt{3}$ e viceversa.

La prima cosa da dimostrare è che $P=a^2+3b^2$ determina a e b, a meno del segno, nel caso in cui P sia un primo dispari oppure 4. Vediamo cosa succede quando P è un numero primo dispari, in quanto quello in cui $P=4$ è chiaro (infatti $a=b=\pm 1$). Supponiamo che P sia un primo dispari e che esista $j=1,2,\ldots,n$ tale che $\widetilde{a}_j+i\widetilde{b}_j\sqrt{3}$ soddisfi l'uguaglianza

$$\widetilde{a}_j^2+3\widetilde{b}_j^2=a_j^2+3b_j^2$$

allora, per il Passo 2 $(\widetilde{a}_j^2+3\widetilde{b}_j^2|a_j^2+3b_j^2)$ si ottiene

$$a_j+ib_j\sqrt{3}=(\widetilde{a}_j+i\widetilde{b}_j\sqrt{3})(u+iv\sqrt{3})$$

considerando i moduli $u^2+3v^2=1$, dove $u=1$ e $v=0$. Quindi, come volevamo dimostrare esiste un'unica rappresentazione.

Per quando riguarda la seconda affermazione, basta notare che $a+ib\sqrt{3}$ e $a-ib\sqrt{3}$ combinati danno il fattore a^2+3b^2, ma questo è impossibile se p e q sono coprimi.

Passo 5 Consideriamo $p^2+3q^2=P_1P_2\ldots P_n$ una fattorizzazione composta esclusivamente da fattori che siano numeri primi dispari e 4, come visto nel Passo 4; se questa fattorizzazione contiene esattamente k fattori di 4, allora, 2^{2k} è la più grande potenza di 2 che divide p^2+3q^2, ma, dalle ipotesi sapiamo che p^2+3q^2 è un cubo, segue che $2k$, e conseguentemente k sarà multiplo di 3. Inoltre ogni numero dispari primo P della fattorizzazione deve avere molteplicità che sia multiplo di 3. In questo modo, n sarà multiplo di 3, e i fattori $P_1P_2\ldots P_n$ possono essere ordinati in modo tale che $P_{3k+1}=P_{3k+2}=P_{3k+3}$. Da questo segue che, nella fattorizzazione di $p+iq\sqrt{3}$ data nel Passo 3, i fattori corrispondenti ad ogni gruppo di tre P_i sono identici poichè l'unica

scelta possibile è quella del segno di $a \pm ib\sqrt{3}$, in quanto non possono esserci entrambi. Inoltre, se prendiamo un fattore da ogni gruppo di tre e li moltiplichiamo fra di loro, allora, dato un numero $c + id\sqrt{3}$ tale che

$$p + iq\sqrt{3} = \pm(c + id\sqrt{3})^3$$

infatti

$$-(c + id\sqrt{3})^3 = (-c - id\sqrt{3})^3$$

ottenendo così proprio quanto volevamo dimostrare.

□

Osservazione 2.1.8. *Si può notare che gli interi a e b menzionati nel Lemma precedente non necessariamente devono essere positivi, come si può vedere dai seguenti esempi.*

Esempio 2.1.9. *Consideriamo $a = -2$ e $b = 1$, se sostituiti nelle*

$$p = a^3 - 9ab^2$$

$$q = 3a^2b - 3b^3$$

avremo che $p, q > 0$, $(p, q) = 1$ e $p + q \equiv 1 \mod 2$.

Esempio 2.1.10. *Consideriamo $a = -2$ e $b = 3$, se sostituiti nelle*

$$p = a^3 - 9ab^2$$

$$q = 3a^2b - 3b^3$$

avremo che $p, q > 0$, $(p, q) = 1$ e $p + q \equiv 1 \mod 2$.

Esempio 2.1.11. *Consideriamo $a = -5$ e $b = 2$, se sostituiti nelle*

$$p = a^3 - 9ab^2$$

$$q = 3a^2b - 3b^3$$

avremo che $p, q > 0$, $(p, q) = 1$ e $p + q \equiv 1 \mod 2$.

2.2 Dimostrazione dell'Ultimo Teorema di Fermat per $n = 3$

Teorema 2.2.1. *L'equazione*

$$x^3 + y^3 = z^3 \tag{2.4}$$

non ammette soluzioni intere positive quando $xyz \neq 0$.

Dimostrazione. Supponiamo che x, y, z siano coprimi, infatti, se non lo fossero, qualsiasi fattore divida due di questi, per l'equazione (2.4), dovrebbe dividere anche il terzo. Di conseguenza, uno ed uno solo tra x, y, z può essere pari, quindi possiamo distinguere i due casi:

(1) *z è pari e x, y sono dispari*

Poichè x e y sono dispari, $x - y$ e $x + y$ saranno pari, poniamo

$$x + y = 2p$$

$$x - y = 2q$$

da queste possiamo ricavare x e y in funzione di p e q

$$x = p + q$$

$$y = p - q$$

dove p e q sono coprimi, infatti, se avessero un fattore in comune, questo dovrebbe divide anche x e y, che è impossibile in quanto abbiamo detto essere primi fra loro; hanno opposta parità in quanto x è dispari. Infine possiamo assumere p e q positivi, poichè eventualmente potremmo scambiare il ruolo fra x e y, inoltre, se $x = y$ allora $z^3 = 2x^3$ ed essendo x e 2 primi fra loro, l'unico modo affinchè siano un cubo è che anche 2 sia un cubo, ma è impossibile.

Scriviamo la (2.4) in termini di p e q nel seguente modo

$$z^3 = x^3 + y^3 = (x + y)(x^2 - xy + y^2) = 2p(p^2 + 3q^2) \tag{2.5}$$

dove il prodotto $2p(p^2 + 3q^2)$ è un cubo.

(2) *x è pari e z, y sono dispari (il caso in cui y è pari si ottiene scambiando il ruolo fra x ed y)*

Per le stesse ragioni del caso precedente, poniamo

$$z - y = 2p$$

$$z + y = 2q$$

Ottenendo così

$$y = q - p$$

$$z = p + q$$

dove p e q sono positivi, infatti, $q > 0$ (in quanto $q = \frac{z+y}{2}$) e $p > q$ (poichè $z > y$), inoltre per le stesse ragioni del caso precedente, sono primi fra di loro e di opposta parità.
Sostituendo nella (2.4) con un calcolo immediato

$$x^3 = z^3 - y^3 = (z - y)(z^2 + zy + y^2) = 2p(p^2 + 3q^2) \tag{2.6}$$

dove il prodotto $2p(p^2 + 3q^2)$ è un cubo.

A questo punto ci resta da dimostrare che $2p$ e p^2+3q^2 sono coprimi e che l'unico modo affinchè il loro prodotto sia un cubo è che siano dei cubi. Per il Lemma 2.1.1 sappiamo che 3 è l'unico fattore comune a $2p$ e $p^2 + 3q^2$, quindi, possiamo dividere in due casi la dimostrazione: quello in cui 3 non divide p e conseguentemente $2p$ e $p^2 + 3q^2$ sono coprimi, e quello in cui $3|p$.

Supponiamo che 3 non divide p, e che $2p$ e $p^2 + 3q^2$ siano entrambi dei cubi. Dal Lemma 2.1.7 sappiamo che se $p^2 + 3q^2$ è un cubo allora

$$p = a^3 - 9ab^2 = a(a^2 - 9b^2) = a(a - 3b)(a + 3b)$$

$$q = 3a^2b - 3b^3 = 3b(a^2 - b^2) = 3b(a - b)(a + b)$$

così che $p^2 + 3q^2 = (a^2 + 3b^2)^3$. Se moltiplichiamo per 2 entrambi i membri, dalla prima delle suddette uguaglianze abbiamo

$$2p = 2a(a - 3b)(a + 3b)$$

che è un cubo, inoltre dal Lemma 2.1.2 sappiamo che l'unico fattore comune a $2a$ e $a \pm 3b$ può essere solo 3. Però, 3 non divide a poichè se lo facesse dovrebbe dividere anche p, contrariamente da quanto abbiamo supposto.

Quindi $2a$ e $a \pm 3b$ sono coprimi e devono essere tutti e tre dei cubi; posto:

$$\alpha^3 = 2a$$

$$\beta^3 = a - 3b$$

$$\gamma^3 = a + 3b$$

Avremo

$$\beta^3 + \gamma^3 = a - 3b + a + 3b = 2a = \alpha^3 \tag{2.7}$$

Questo mi da una soluzione della (2.4) con interi più piccoli rispetto alla soluzione originale. Infatti

$$\alpha^3\beta^3\gamma^3 = 2a(a + 3b)(a - 3b) = 2p$$

dalle equazioni (2.5) e (2.6) ottengo che $(\alpha\beta\gamma) < z$ (infatti se z è pari $2p|z$, mentre se x è pari $2p|x < z$), potrò quindi distinguere i tre casi:

1. $\alpha > 0, \beta > 0, \gamma > 0$
2. $\alpha < 0, \beta < 0, \gamma > 0$
3. $\alpha < 0, \beta > 0, \gamma < 0$

dal primo caso $\alpha < z$, l'equazione (2.7) è soddisfatta ed è in contrasto col Lemma della Discesa Infinita; dal secondo caso l'equazione (2.7) può essere scritta come $(-\alpha)^3 + \gamma^3 = (-\beta)^3$ con $-\beta < z$ (da $(-\alpha)(-\beta)\gamma < z$); infine anche nel terzo caso scriviamo la (2.7) come $(-\alpha)^3 + \beta^3 = (-\gamma)^3$ con $-\gamma < z$ (da $(-\alpha)\beta(-\gamma) < z$).

Consideriamo ora il caso in cui $3|p$ e non divide q, allora potremmo scrivere $p = 3s$, sostituendo

$$2p(p^2 + 3q^2) = 3^2(2s)(3s^2 + q^2)$$

dove $3^2, 2s, q^2 + 3s^2$ sono primi fra di loro, infatti 3 non può essere un loro fattore comune poichè dovrebbe dividere q, ma abbiamo supposto che 3 non divide q, inoltre non potrà essere 2 perchè se $2|q^2 + 3s^2$ allora q ed s sarebbero entrambi pari oppure dispari, che è impossibile perchè p e q sono coprimi e di opposta parità.

Essendo $3^2(2s)$ e $3s^2 + q^2$ dei cubi, per il Lemma 2.1.7 sappiamo che se $q^2 + 3s^2$ è un cubo allora

$$q = a(a - 3b)(a + 3b)$$

$$s = 3b(a + b)(a - b)$$

dove a e b sono interi coprimi di opposta parità.
Poichè $3^2(2s)$ è un cubo moltiplicando entrambi i membri della seconda delle precedenti relazioni per $3^2 2$, otterremo un cubo

$$3^2(2s) = 3^3(2b)(a + b)(a - b)$$

quindi anche $2b(a + b)(a - b)$ sarà un cubo, inoltre dal Lemma 2.1.3 abbiamo che $2b, a \pm b$ sono coprimi, allora possiamo scrivere:

$$\alpha^3 = 2b$$

$$\beta^3 = a - b$$

$$\gamma^3 = a + b$$

dove

$$\gamma^3 - \beta^3 = 2b = \alpha^3$$

Anche in questo caso abbiamo trovato una soluzione dell'equazione (2.4) con interi più piccoli, infatti

$$\alpha^3\beta^3\gamma^3 = 2b(a - b)(a + b) = \frac{2}{9}p < z^3$$

quindi $(\alpha\beta\gamma) < z$, potremo così considerare i tre casi visti precedentemente, ottenendo una discesa infinita di interi positivi.

□

Bibliografia

[1] Harold M. Edwards, *Fermat's Last Theorem*, first ediction, Springer Verlag, 1977.

[2] Wiles, Andrew, *Modular elliptic curves and Fermat's last theorem*, first print, Ann. of Math. (2) 141 (1995), no. 3, 443–551.

[3] http://en.wikipedia.org/wiki/Fermat's_Last_Theorem