Ultimo Teorema di Fermat: il mio centesimino *

Guido Antonelli

4 novembre 2016

1 Introduzione

Come tutti gli appassionati di matematica che si rispettino, anch'io ho provato a cimentarmi nella risoluzione della famosa congettura di Pierre de Fermat (1601-1665), impropriamente conosciuta nei secoli passati come Ultimo Teorema di Fermat o UTF, approfittando del fatto che, anche se non sono riuscito nell'intento, mi può consolare il fatto di essere in compagnia di molti grandissimi matematici del passato e del presente, che da 300 anni hanno vanamente tentato di trovarne una dimostrazione.
Spero comunque che queste mie note possano servire a tutti coloro che accostandosi per la prima volta a questo argomento, vogliono farsi una semplice idea dell'UTF, ed anche di aver apportato qualche piccolo contributo originale all'enorme mole di letteratura esistente sull'argomento.
Nel 1637 Fermat enunciò la sua famosa congettura affermando di possederne una dimostrazione generale, che solo la ristrettezza dei margini del libro del matematico greco Diofanto, sui quali scriveva i propri commenti, non gli aveva permesso di riportare per esteso.
Tale congettura afferma che l'equazione diofantea[1] di grado n:

$$x^n + y^n = z^n \tag{1}$$

non ammette per x, y e z soluzioni intere non nulle, o più in generale soluzioni razionali non nulle, se l'esponente n è un intero maggiore di 2.
In altre parole si può affermare che la (1) per $n > 2$ ammette nel campo dei numeri interi unicamente soluzioni banali, cioè contenenti uno o più termini nulli.
Di questa congettura, ma solamente per il caso più semplice di $n = 4$, Fermat fornì una elegante dimostrazione provando che in un triangolo rettangolo a lati interi i due cateti non potevano essere quadrati perfetti e che di conseguenza la somma di due quarte potenze, in base al teorema di Pitagora, non avrebbe potuto essere un quadrato, né quindi a maggior ragione una quarta potenza.
In seguito Eulero risolse, sia pure in modo non del tutto corretto, il caso $n = 3$, che fu emendato e completato da Sophie Germain, e successivamente altri matematici fino ai giorni nostri dimostrarono la congettura per moltisimi esponenti primi maggiori di 3, senza però arrivare alla dimostrazione generale di cui parlava Fermat.
Benché il problema sia stato recentemente risolto (1995) dal matematico A.Wiles con una dimostrazione che riempie centinaia di pagine di astrusa (almeno per me) algebra moderna, e che quindi l'UTF meriti da tale momento a buon diritto la dignità di teorema e non più di semplice congettura, tuttavia resta ancora aperta la questione dell'esistenza o meno di una dimostrazione classica, che avrebbe potuto essere stata alla portata del grande Fermat.
Tra i matematici attualmente sembra tuttavia prevalere la convinzione che una tale dimostrazione non esista perché altrimenti ... sarebbe stata certamente trovata!

*Questo articolo è stato scritto con LaTeX [1].

[1] Si dice diofantea una equazione indeterminata in più incognite, in generale di tipo algebrico, per la quale si ricercano soluzioni unicamente nel campo dei numeri interi.

Le note che seguono riportano un mio personale approccio al problema, approccio che mi ha permesso di trovare con un procedimento originale tre relazioni a cui qualsiasi eventuale soluzione avrebbe dovuto in ogni caso soddisfare.
Questo risultato mi aveva fatto sperare di poter trovare una dimostrazione dell'UTF, ma ben presto mi sono accorto che ciò non era vero e che avevo anch'io riscoperto le cosiddette formule di Barlow[2], dal nome del matematico[2] che per primo le trovò intorno al 1810. La stesse formule furono poi ottenute indipendentemente da Abel nel 1823 ed in seguito da molti altri matematici del secolo scorso.
A queste formule ho aggiunto altre relazioni e considerazioni varie di divisibilità allo scopo di dare all'argomento una inquadratura il più possibile organica e soddisfacente.
Ho anche trovato e dimostrato un teorema che con poca modestia ho definito *mirabile* per il fatto che interviene in moltissimi punti dei miei ragionamenti anche se qualcuno l'ha certamente scoperto prima di me.
Ho quindi sviluppato un'analisi dell'UTF dal punto di vista dell'aritmetica modulare pervenendo alla dimostrazione di una parte del medesimo, indicata più avanti come I caso dell'UTF, *per qualsiasi esponente primo di ragionevole grandezza*, anche se non mi è stato possibile trovare una dimostrazione matematica rigorosa valida in generale.
Vorrei a questo punto aggiungere che nel 1997 avevo scoperto anch'io la seguente congettura[3], che rappresenta una generalizzazione dell'UTF; essa afferma che l'equazione diofantea:

$$x^p + y^q = z^r$$

non ammette soluzioni se x, y e z sono interi non nulli coprimi tra loro, e gli esponenti p, q e r sono interi maggiori di 2. La coprimalità è in questo caso una condizione necessaria altrimenti si avrebbe un immediato controesempio in $2^n + 2^n = 2^{n+1}$ con $n > 2$.
Con un programma elettronico questa congettura è stata da me verificata per tutti i valori dei termini inferiori a 10^{15}, osservando inoltre che se ad uno solo dei termini si permettesse di essere un quadrato perfetto, gli altri due termini della terna, con esclusione del solo caso $1^n + 2^3 = 3^2$ con $n > 3$, sarebbero sempre e solo potenze cubiche[4].
Lascio a qualche lettore interessato il compito di trovare eventuali controesempi a quest'ultima mia congettura!

Come diceva Dante *poca favilla gran fiamma seconda*. Mi auguro quindi che qualcuno leggendo questo articolo trovi uno stimolo a proseguire dove io almeno per ora mi sono fermato, ottenendo risultati assai più significativi dei miei.

Infine invito il paziente lettore a segnalarmi eventuali incongruenze od errori da me commessi, cosa peraltro facilissima quando ci si avventura da soli in argomenti di questo tipo.

Prima di procedere riportiamo alcuni simboli che useremo in seguito con il loro significato matematico:

$\mid$ = divide	Es.: $a \mid b$ indica che a divide b ovvero che b è divisibile per a.
$\nmid$ = non divide	Es.: $a \nmid b$ indica che a non divide b ovvero che b non è divisibile per a.
$(a,b) = MCD(a,b)$	Es.: $(a,b) = c$ indica che c è il massimo comun divisore tra a e b. Se $(a,b) = 1$ i due numeri a e b sono coprimi. Se $(a,p) = 1$ e p è un numero primo allora $(a,p) = 1$ equivale a $p \nmid a$.
$\parallel$ = divide esattamente	Es.: $a \parallel b$ equivale ad $a \mid b$ e $(a, b/a) = 1$.

[2]Personaggio in auge presso il popolo degli astrofili per la famosa lente, di Barlow appunto, da lui inventata.
[3]Purtroppo questa congettura era già stata scoperta da Andrew Beal nel 1993 che da buon miliardario texano offrì e, credo, offre ancora un milione di dollari a chi fosse in grado di dimostrerla.
[4]Le terne da me trovate oltre a quella citata sono le seguenti:
$13^2 + 7^3 = 8^3$ $\quad 11^3 + 37^3 = 228^2$ $\quad 23^3 + 588^2 = 71^3$ $\quad 47^3 + 549^2 = 74^3$
$56^3 + 65^3 = 671^2$ $\quad 181^2 + 104^3 = 105^3$ $\quad 57^3 + 112^3 = 1261^2$

2 Considerazioni preliminari

Non è necessario dimostrare l'UTF per tutti i valori interi dell'esponente n maggiori di 2, ma solamente per $n = 4$ e per quei valori dispari di n che sono anche numeri primi come 3, 5, 7, 11, ecc., numeri cioè che ammettono come divisori esatti solo sé stessi o l'unità.
La dimostrazione è molto semplice e segue dal fatto che ogni numero composto maggiore di 2 o è una potenza esatta di 2, e quindi necessariamente un multiplo di 4, oppure contiene tra i suoi fattori almeno un numero primo dispari:

1. Caso $n = 4\,k$: possiamo riscrivere la (1) nel modo seguente:

$$(x^k)^4 + (y^k)^4 = (z^k)^4 \qquad (k \in \mathcal{N},\ \ k > 0)$$

   Se quindi l'UTF è vero per $n = 4$ esso risulterà vero anche per $n = 4\,k$.

2. Caso $n = k\,p$ (p = numero primo dispari): possiamo riscrivere la (1) nel modo seguente:

$$(x^k)^p + (y^k)^p = (z^k)^p \qquad (k \in \mathcal{N},\ \ k > 0)$$

   Come nel caso precedente, se l'UTF è vero per il numero primo p esso risulta vero anche per $n = k\,p$.

I due casi riportati non si escludono mutuamente nel senso che esistono esponenti come 12, 20, 24, ecc. che sono multipli sia di 4 che di uno o più primi dispari, pur non essendo potenze esatte di 2; per tali valori l'UTF è certamente vero, essendo sufficiente il fatto che sia vero per $n = 4$.
Il procedimento che in genere si segue per la dimostrazione dell'UTF è quello classico per assurdo: si suppone cioè che esista almeno una terna[5] che soddisfa alla (1) e si cerca di mostrare che tale ipotesi porta ad una conclusione contraddittoria.
Senza perdere di generalità possiamo inoltre imporre le seguenti limitazioni ai valori delle variabili per il caso che a noi interessa di esponente p dispari:

1. I valori x, y e z sono tutti positivi. Infatti, se uno o più valori fossero negativi, potremmo considerarne i relativi opposti positivi eliminando i segni negativi così introdotti mediante spostamento di tali termini da un membro all'altro della formula.

2. I valori x e y sono minori di z. Questo deriva dal fatto che i tre valori, in base al punto precedente, sono supposti positivi e non nulli; possiamo inoltre assumere $x < y$ (se ciò non fosse vero, basta scambiare formalmente tra loro le variabili), escludendo unicamente il caso $x = y$, per il quale si avrebbe $x^p + y^p = 2y^p = z^p$, che non ammette soluzioni intere per y e z in quanto $2^{1/p}$ è irrazionale[6].

3. I valori x, y e z sono coprimi, vale cioè $(x, y, z) = 1$. Infatti se x, y e z non fossero coprimi, essi ammetterebbero un massimo comun divisore k, e quindi la (1) sarebbe soddisfatta anche dai valori x/k, y/k e z/k, coprimi tra loro. Una TdF coprima è detta fondamentale o primitiva.

[5] Le terne in questione sono dette *terne di Fermat* (TdF), anche se di fatto non esistono!

[6] Un'altra semplice dimostrazione è la seguente: se $2y^p = z^p$ è verificata da due valori interi y e z coprimi tra loro (se non lo fossero, basterà prima dividerli per il loro massimo comun divisore), allora z sarà necessariamente pari e di conseguenza z^p conterrà un fattore del tipo 2^{mp} con $m \geq 1$, $p \geq 3$ e quindi $mp \geq 3$. Ma il primo membro contiene solo il fattore 2^1 in quanto y è coprimo con z e quindi dispari. Di conseguenza l'uguaglianza è impossibile c.v.d.

4. Se la terna è coprima i valori x, y e z sono coprimi anche a coppie. Infatti se per assurdo x ed y ammettessero un divisore comune k, ponendo $x = k\,u$ e $y = k\,v$ con u e v interi positivi, si potrebbe scrivere:

$$k^p\,(u^p + v^p) \;=\; z^p$$

e quindi:

$$(u^p + v^p) \;=\; \frac{z^p}{k^p} \;=\; \left(\frac{z}{k}\right)^p$$

Ora perché l'ultima espressione sia soddisfatta è necessario che sia anche $z = k\,w$, con w intero, in contrasto con l'ipotesi iniziale che la terna sia primitiva, che cioè non ammetta un divisore comune diverso da 1. In modo simile si dimostra facilmente che la stessa conclusione vale anche per le coppie (x, z) e (y, z) per cui l'asserto risulta così dimostrato.

Per questa ragione in quanto segue quando parleremo di terna strettamente coprima si intenderà che la coprimalità vale anche per tutte e tre le possibili coppie.

Con ovvie considerazioni vale anche la proprietà inversa: se una qualsiasi coppia di variabili di una TdF è coprima, allora anche la terna è (strettamente) coprima e di conseguenza sono coprime anche le altre possibili coppie.

5. Tra i valori x, y e z uno solo può essere pari, mentre i due rimanenti sono necessariamente dispari. Questo fatto si dimostra facilmente con semplici considerazioni sulla parità dei due membri della (1), tenuto conto della coprimalità della terna, oppure più semplicemente dalla precedente osservazione riguardante la coprimalità a coppie.

Non vi sono tuttavia elementi per ritenere che solo x od y possano essere pari, come avviene, e facilmente si dimostra, per le terne pitagoriche (TdP) primitive. Pertanto in una eventuale TdF anche z potrebbe essere pari.

In conclusione, poiché l'UTF è stato già dimostrato da Fermat per $n = 4$ (vedi Appendice A), resta unicamente da dimostrare che:

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

non ammette soluzioni se x, y e z sono interi positivi coprimi con $0 < x < y < z$, e p è un numero primo dispari.

Seguendo la letteratura sull'argomento distingueremo inoltre per l'UTF due possibili casi a seconda che xyz sia o meno divisibile per l'esponente p. Per uniformità con la scelta di altri autori assumeremo:

1. Caso I: p non divide xyz, cioè nessuna variabile di una TdF è divisibile per p.
2. Caso II: p divide xyz, cioè una (ed una sola) variabile di una TdF è divisibile per p.

3 Teoremi di Fermat ed Eulero

Pierre de Fermat enunciò anche il seguente (non ultimo) teorema che porta il suo nome: un numero primo p divide esattamente $a^{p-1}-1$ se a e p sono coprimi. Con formalismo matematico possiamo scrivere:

$$a^{p-1} \equiv 1 \pmod{p} \qquad \text{se} \quad (a,p)=1$$

che sta ad indicare che la divisione di a^{p-1} per p dà resto 1 se il massimo comun divisore di a e p vale 1, o anche che a^{p-1} è congruo ad 1 modulo p se a e p sono coprimi.
Nel seguito utilizzeremo indifferentemente anche la seguente forma che risulta talvolta più comoda:

$$a^{p-1} \pmod{p} = 1 \qquad \text{se} \quad (a,p)=1$$

Moltiplicando ambo i membri per $a \pmod{p}$ si ottiene l'interessante relazione:

$$a^{p} \equiv a \pmod{p} \tag{3}$$

Si può notare che questa uguaglianza non richiede più la condizione $(a,p)=1$. Infatti essendo p un numero primo o tale condizione è verificata oppure a è divisibile per p, nel qual caso i termini a primo e a secondo membro sono entrambi nulli e quindi uguali. Un risultato analogo ed ancor più generale si dimostrerà in seguito per $p=3$.
Inoltre dal teorema di Fermat segue immediatamente che per un qualsiasi intero $k>1$:

$$a^{k(p-1)} \equiv 1^{k} = 1 \pmod{p} \qquad \text{se} \quad (a,p)=1$$

Ora sostituendo in modo puramente formale p con q_k e ponendo $n-1 = k(q_k-1)$ con n intero dispari non necessariamente primo, per ogni primo q_k associabile ad n possiamo scrivere la seguente relazione:

$$a^{n-1} \equiv 1 \pmod{q_k} \qquad \text{se} \quad (a,q_k)=1 \quad \text{e} \quad n-1=k(q_k-1)$$

Ad esempio per $n=25$ i q_k primi associabili ad n sono: 2, 3, 5, 7, 13 e quindi per $a=11$, coprimo con questa lista di primi, si avrà:

$$11^{24} \pmod{2} = 11^{24} \pmod{3} = 11^{24} \pmod{5} = 11^{24} \pmod{7} = 11^{24} \pmod{13} = 1$$

Successivamente Eulero estese il teorema di Fermat anche ai numeri non primi introducendo la funzione toziente $\phi(n)$ di un numero intero n. Tale funzione, intera a sua volta, rappresenta il numero di interi compresi tra 1 e $n-1$, estremi inclusi, che non hanno alcun divisore[7] in comune con n.
Il teorema di Eulero rappresenta quindi una generalizzazione di quello di Fermat e viene espresso della seguente relazione:

$$a^{\phi(n)} \equiv 1 \pmod{n} \qquad \text{se} \quad (a,n)=1$$

Nel caso particolare che il numero n sia primo risulta ovviamente $\phi(n)=n-1$, in quanto un numero primo, non ha fattori comuni con nessuno degli interi compresi tra 1 e $n-1$, e si ricade così nel teorema di Fermat.

[7] In questo caso l'unità non viene considerata tra i possibili divisori di un numero, e viene quindi computata nel calcolo del toziente.

4 Alcune osservazioni su coprimalità e divisibilità

1. Definizione di coprimalità

   Due numeri interi x e y si dicono coprimi se nella loro scomposizione non sono presenti fattori primi comuni, ovvero se $(x, y) = 1$. Per convenzione il numero 1 si considera sempre coprimo con tutti gli altri numeri.

   Questa definizione è resa possibile dal fatto che ogni numero intero è scomponibile in uno ed un solo modo come prodotto di potenze intere di numeri primi[8] con esponente ≥ 1.

   La coprimalità non gode della proprietà riflessiva (un numero non è mai coprimo con sé stesso), né della proprietà transitiva (se x è coprimo con y ed y è coprimo con z, x non è necessariamente coprimo con z), mentre gode della proprietà simmetrica (se x è coprimo con y, y è coprimo con x).

   Come immediata conseguenza della definizione di coprimalità segue il fatto che se due numeri composti sono coprimi, qualsiasi sottomultiplo del primo è coprimo con qualsiasi sottomultiplo del secondo.

   Da queste affermazioni derivano le seguenti proprietà:

2. Proprietà I: Coprimalità del prodotto

   Se un numero x è coprimo con y e z allora esso è coprimo anche con il prodotto yz.

3. Proprietà II: Moltiplicazione per costante

   Se due numeri x ed y sono coprimi, allora sono ugualmente coprime anche le espressioni hx e ky se $(h, ky) = (k, hx) = 1$.

4. Proprietà III: Variazione di esponenti

   Se x ed y sono coprimi, risultano coprime tra loro tutte le coppie di numeri nelle quali il primo ed il secondo numero contengono rispettivamente gli stessi fattori primi di x e di y, anche se con differenti esponenti purché interi positivi o eventualmente nulli.

   In particolare, se due numeri x e y sono coprimi, allora sono ugualmente coprimi tutti i numeri interi del tipo x^h e y^k ottenuti elevando x e y a potenza intera o razionale (se il numero così ottenuto è intero).

5. Proprietà IV: Combinazioni lineari

   Se due numeri x ed y sono coprimi, allora sono coprime con x ed y, oltre alla somma $x+y$ ed alla differenza $x-y$, anche le espressioni:

   - $hx + ky$, se $(h, ky) = (k, hx) = 1$
   - $hx + y$, se $(h, y) = 1$
   - $x + ky$, se $(k, x) = 1$.

[8] Per garantire l'unicità della scomposizione è necessario che l'unità non venga considerata tra i numeri primi, e si trascuri l'ordine con cui vengono scritti i fattori primi presenti. Con queste precisazioni due numeri interi sono quindi uguali se e solo se si scompongono nello stesso modo.

6. Proprietà V: Coprimalità lineare

Un numero x è sempre coprimo con $y = ax + b$ indipendentemente dal valore di a alla sola condizione che sia $(x, b) = 1$ con $b \neq 0$. Per dimostrare questa proprietà è sufficiente considerare un qualsiasi primo q presente nella scomposizione di x. Dividendo y per q si ottiene:

$$\frac{y}{q} = \frac{ax + b}{q} = \frac{ax}{q} + \frac{b}{q}$$

dove il primo termine ax/q è certamente intero perché q divide x, mentre il secondo b/q è una frazione propria od impropria non riducibile in quanto q, essendo un fattore di x è certamente coprimo con b, e di conseguenza y/q non sarà intero. Ripetendo lo stesso ragionamento per tutti i fattori primi di x, la proprietà risulta dimostrata.

Viceversa se x e b non sono coprimi ma vale la relazione $(x, b) = c$ con $c > 1$ allora sarà anche di conseguenza $(x, y) = c$. Infatti dividendo y per ciascuno dei fattori primi q di x il rapporto y/q sarà intero ogni qual volta q divida c e frazionario non riducibile negli altri casi.

7. Proprietà VI: Coprimalità di una terna e coprimalità a coppie

Per tre numeri qualsiasi x, y, e z legati dalla relazione $x + y = z$ si hanno le seguenti proprietà di coprimalità:

- Se la terna non è coprima, allora esiste un fattore comune $k = (x, y, z)$ tale che x/k, y/k e z/k rappresentano numeri interi coprimi che soddisfano alla medesima relazione iniziale.
- Se la terna è coprima, allora sono coprime contemporaneamente tutte le coppie ottenibili dalla terna, cioè:
$$(x, y) = (x, z) = (y, z) = 1$$
- Se una qualsiasi coppia di variabili è coprima, allora la terna è coprima e di conseguenza sono coprime per quanto detto al punto precedente anche le altre coppie restanti.

E' interessante osservare che, indipendentemente dalla coprimalità o meno della terna, vale sempre e comunque la relazione:

$$(x, y, z) = (x, y) = (x, z) = (y, z)$$

8. Proprietà VII: Somma/differenza di coprimi di parità diversa

Se due numeri interi x e y sono coprimi e di parità diversa, allora sono coprime tra loro e con x e y anche la loro somma e la loro differenza.

Infatti ponendo:

$$\gamma = y - x \qquad\qquad \delta = y + x$$

dalla coprimalità di x ed y in base al punto precedente si deduce che:

$$(\gamma, x) = (\gamma, y) = (\delta, x) = (\delta, y) = 1$$

oltre al fatto che γ e δ sono interi dispari.

Resta ancora da dimostrare che $(\gamma, \delta) = 1$ e per fare questo basta sommare e sottrarre le formule precedenti ottenendo:

$$\delta - \gamma = 2x \qquad\qquad \delta + \gamma = 2y$$

Da una qualsiasi di queste relazioni, ad esempio la prima, per la proprietà II si trova che:

$$(\gamma, 2x) = (\gamma, x) = 1$$

poiché $(2, \gamma) = 1$ e di conseguenza la terna è coprima e quindi $(\gamma, \delta) = 1$.

9. Proprietà VIII: Semisomma/semidifferenza di coprimi dispari

Se due numeri interi dispari x e y sono coprimi, allora sono coprime tra loro e con x e y anche la loro semisomma e la loro semidifferenza.

Infatti ponendo:

$$\gamma = \frac{y-x}{2} \qquad\qquad \delta = \frac{y+x}{2}$$

si ottengono le relazioni:

$$\delta - \gamma = x \qquad\qquad \delta + \gamma = y$$

Per dimostrare il teorema è sufficiente dimostrare che $(x, \delta, \gamma) = (y, \delta, \gamma) = 1$ e per fare questo utilizzeremo la proprietà VI sulla coprimalità a coppie.

Ad esempio consideriamo γ ed x e dimostriamo che deve essere $(x, \gamma) = 1$.

Supponiamo per assurdo che la tesi sia falsa e che sia $d_x = (x, \gamma) > 1$. Possiamo pertanto scrivere:

$$\frac{\gamma}{d_x} = \frac{y/d_x - x/d_x}{2} = \text{ intero}$$

Ora poiché x/d_x è un intero dispari anche y/d_x dovrà essere un intero (dispari), ma questo è assurdo perché y è per ipotesi coprimo con x e quindi non contiene nessuno dei suoi fattori.

In modo analogo possiamo dimostrare che $(y, \gamma) = 1$, e di conseguenza la proprietà in oggetto è dimostrata.

Come casi particolari delle due precedenti proprietà osserviamo che se y è un numero pari, anche $y+1$ e $y-1$ sono coprimi tra loro e con y, mentre se y è un numero dispari, anche $(y+1)/2$ e $(y-1)/2$ sono coprimi tra loro e con y.

Questi risultati, che si ottengono facilmente con ragionamenti analoghi a quelli sopra riportati, confermano la correttezza di considerare il numero 1 coprimo con tutti gli altri numeri, come già si è fatto per il calcolo del toziente di un numero. Se si accetta questa convenzione, gli stessi risultati derivano immediatamente dai precedenti teoremi ponendo $x = 1$.

10. Proprietà IX: Divisibilità per 2 e 2^m di somma e differenza di numeri dispari

Dati due numeri dispari qualsiasi x e y, diversi tra loro, la loro somma e differenza sono sempre rappresentate da due numeri pari, di cui uno è divisibile *esattamente* per 2 mentre l'altro è divisibile per 2^m con $m \geq 2$.

Indichiamo i due numeri come $x = 2h+1$ e $y = 2k+1$ con $h > k$ e la loro somma e differenza con $s = 2(h+k+1)$ e $d = 2(h-k)$.

A seconda della parità di h e k si avranno i seguenti casi:

(a) h e k hanno uguale parità.
Poiché $(h+k)$ e $(h-k)$ sono entrambi pari risulta di conseguenza che $(h+k+1)$ è dispari e quindi $2 \parallel s$ mentre $4 \mid d$.

(b) h e k hanno diversa parità.
Poiché $(h+k)$ e $(h-k)$ sono entrambi dispari risulta di conseguenza che $(h+k+1)$ è pari e quindi $4 \mid s$ mentre $2 \parallel d$.

11. Proprietà X: Divisibilità per 3

La somma o la differenza di due numeri qualsiasi x e y non divisibili per 3 è sempre divisibile per 3. Infatti ciascuno dei due numeri sarà del tipo $3m+1$ o $3m+2$ e di conseguenza in tutti i casi possibili o la loro somma o la loro differenza sarà del tipo $3m$.

5 Questioni di divisibilità collegate all'UTF

All'equazione (2) possiamo aggiungere la seguente equazione:

$$x + y = z + \alpha \qquad\qquad (0 < \alpha < x\,, \quad \alpha \in \mathcal{N}) \tag{4}$$

E' ovvio che questa nuova equazione sembrerebbe a prima vista non portare alcun progresso nel compito che ci siamo proposti in quanto introduce una nuova variabile intera α; tuttavia nel prosieguo si vedrà che da questa equazione è possibile derivare un certo numero di proprietà a cui le TdF devono soddisfare. L'intervallo di variazione di α è così giustificato:

1. $\alpha > 0$ - Tenendo conto della (2), si può scrivere:

$$(x+y)^p = x^p + p\,x^{p-1}\,y + \binom{p}{2} x^{p-2}\,y^2 + \ldots + p\,x\,y^{p-1} + y^p > x^p + y^p = z^p$$

   Estraendo la radice p-esima, segue $x + y > z$ e quindi:

$$\alpha = x + y - z > 0$$

2. $\alpha < x$ - Dalla (4) tenendo presente che $y < z$, si ottiene facilmente:

$$\alpha = x + y - z < x + z - z = x$$

1. Fattori del parametro α

   Se applichiamo l'operatore $(\text{mod } p)$ alla (2) tenendo conto della (3) otteniamo immediatamente:

$$x + y \equiv z \ (\text{mod } p) \tag{5}$$

   Applicando anche alla (4) lo stesso operatore $(\text{mod } p)$ otteniamo invece:

$$x + y \equiv z + \alpha \ (\text{mod } p)$$

   Dal confronto è immediato desumere che $\alpha \equiv 0 \ (\text{mod } p)$ cioè che p divide sempre α.

   Avendo utilizzato la (3), la conclusione resta ugualmente valida anche se una qualsiasi delle variabili fosse divisibile per p.

   Veniamo ora a considerare tutti i numeri primi q_k che insieme a p soddisfanno alla seguente relazione:

$$p - 1 = k\,(q_k - 1) \qquad\qquad (k \in \mathcal{N}, \quad k > 0\,) \tag{6}$$

   Applicando l'operatore $(\text{mod } q_k)$ al termine x^p per il teorema di Fermat si avrebbe:

$$x^p = (x^{q_k - 1})^k \ x \equiv x \ (\text{mod } q_k)$$

   e analogamente per le variabili y^p e z^p.

   Possiamo quindi ripetere per q_k la stesso ragionamento fatto in precedenza per p, concludendo che α è divisibile anche per q_k. Come prima questa conclusione resta valida anche nel caso che una delle variabili x, y o z sia divisibile per q_k.

E' immediato concludere che per $p > 3$ i valori $q_1 = 2,\ q_2 = 3$ e $q_{max} = p$ saranno sempre presenti nella scomposizione di α in quanto soddisfanno la (6) indipendentemente dal valore di p, mentre altri eventuali primi q_k sono al contrario dipendenti da tale valore.

Per $p = 2$ si ha solamente $q_1 = 2 \equiv p$; per $p = 3$ si hanno i valori $q_1 = 2$ e $q_2 = 3 \equiv p$.

In linea generale il numero di questi valori tenderà a crescere con p, ma ad alcuni valori di p della forma $2^m 3^n + 1$ corrisponde una lista particolarmente lunga di divisori q_k di α come nei seguenti esempi dove sulla destra è riportato anche il loro prodotto:

$$p = 37 \qquad q_k = 2, 3, 5, 7, 13, 19, 37 \qquad \prod_{i=1}^{n} q_k = 1.919.190$$

$$p = 73 \qquad q_k = 2, 3, 5, 7, 13, 19, 37, 73 \qquad \prod_{i=1}^{n} q_k = 140.100.870$$

$$p = 433 \qquad q_k = 2, 3, 5, 7, 13, 17, 19, 37, 73, 109, 433 \qquad \prod_{i=1}^{n} q_k = 112.409.792.943.630$$

Ora poiché si ha sempre $\alpha < x < y < z$ si può enunciare un interessante risultato: *per ogni primo p non possono esistere TdF i cui termini siano minori del valore del prodotto dei divisori q_k di α aumentato di una unità.*

Così ad esempio se volessimo cercare una controprova dell'UTF per $p = 37$ sarebbe del tutto inutile cercarla tra i numeri minori di 1.919.191, e nel caso di $p = 73$ tra i minori di 140.100.871, e infine per $p = 433$ tra i minori di 112.409.792.943.631!

Vedremo tuttavia più avanti che per ciascun esponente p possono essere stabiliti limiti inferiori per le variabili di una TdF assai superiori a quelli qui sopra indicati.

La presenza del primo $q_1 = 2$ dimostra banalmente il fatto che la parità di un numero o di una espressione non viene modificata se si aggiunge una quantità pari. Infatti la somma $x+y$ uguaglierà il valore di z sommato ad una costante certamente pari.

Più interessante è il fatto che da $q_2 = 3$ si deduce che la costante α, per qualsiasi valore di $p > 2$ risulta sempre divisibile anche per 3.

L'algoritmo usato per conseguire questo risultato ci porta anche alla conclusione del tutto generale che, se n è un numero dispari non necessariamente primo, per un qualsiasi numero a non divisibile per 3, vale la relazione:

$$a^{n-1} \equiv 1 \pmod 3 \qquad \text{se} \quad (a, 3) = 1$$

ed anche:

$$a^n \equiv a \pmod 3$$

senza più la condizione che 3 non divida a, analogamente a quanto visto in precedenza al Capitolo 3 applicando l'operatore (mod p).

Ed infine α risulta sempre divisibile per p, mentre questo non si verifica necessariamente per almeno una delle variabili della TdF.

2. Divisibilità del prodotto xyz per particolari valori dipendenti da p

Se le variabili x, y e z verificano la (2) e se $q = 2p + 1$ è primo, allora $q \mid xyz$ [9].

Infatti per il teorema di Fermat per ciascun termine della (2), ad esempio per la x, possiamo scrivere:

$$x^{2p} \pmod q = \begin{cases} 1 & \text{se } q \nmid x \\ \\ 0 & \text{se } q \mid x \end{cases}$$

[9] Dire che $q \mid xyz$ equivale a dire che una delle variabili della TdF è divisibile per q.

ed estraendo la radice quadrata di entrambi i membri abbiamo di conseguenza:

$$x^p \pmod q = \begin{cases} \sqrt{1} = \pm 1 & \text{se } q \nmid x \\ \\ \sqrt{0} = 0 & \text{se } q \mid x \end{cases}$$

Se ora supponiamo per assurdo che nessuna delle variabili sia divisibile per q, i valori possibili saranno solamente $+1$ e $-1 \equiv q - 1$. Di conseguenza applicando l'operatore (mod q) alla (2) otteniamo:

$$(\pm 1) + (\pm 1) = \pm 1$$

Ma l'uguaglianza è impossibile e quindi resta dimostrato che almeno una delle variabili deve essere divisibile per q.

Come casi particolari possiamo citare:

$p = 3 \;\;,\;\; q = 2 \cdot 3 + 1 = 7$ (primo) $\quad ==> \quad 7 \mid xyz.$

$p = 5 \;\;,\;\; q = 2 \cdot 5 + 1 = 11$ (primo) $\quad ==> \quad 11 \mid xyz.$

$p = 7 \;\;,\;\; q = 2 \cdot 7 + 1 = 15$ (composto) $\quad ==> \quad 15$ può dividere o non dividere $xyz.$

$p = 11 \;\;,\;\; q = 2 \cdot 11 + 1 = 23$ (primo) $\quad ==> \quad 23 \mid xyz.$

Dimostriamo ora che il ragionamento può estendersi anche al caso che sia $q = 4p + 1$, esaminando in dettaglio il caso $p = 3$ per il quale $q = 4 \cdot 3 + 1 = 13$ è anch'esso primo.

Per fare questo prendiamo le terze potenze dei numeri compresi tra 1 e 12 estremi inclusi, che sono quindi rappresentativi di tutti gli interi coprimi con 13, ed applichiamo loro l'operatore (mod 13) riducendo i resti a valori compresi tra -6 e $+6$.

$$1^3 \equiv 1 \pmod{13} \qquad 2^3 = 8 \equiv -5 \pmod{13} \qquad 3^3 = 27 \equiv 1 \pmod{13}$$

$$4^3 = 64 \equiv -1 \pmod{13} \qquad 5^3 = 125 \equiv -5 \pmod{13} \qquad 6^3 = 216 \equiv -5 \pmod{13}$$

$$7^3 = 343 \equiv 5 \pmod{13} \qquad 8^3 = 512 \equiv 5 \pmod{13} \qquad 9^3 = 729 \equiv 1 \pmod{13}$$

$$10^3 = 1000 \equiv -1 \pmod{13} \quad 11^3 = 1331 \equiv 5 \pmod{13} \quad 12^3 = 1728 \equiv -1 \pmod{13}$$

Risulta immediato constatare che i soli valori possibili per le terze potenze dei numeri non divisibili per 13 sono ± 1 e ± 5, dove i valori ± 5 rappresentano le due radici quadrate di -1. Infatti il loro quadrato è pari a $+25 \pmod{13} = -1$.

Di conseguenza applicando l'operatore (mod 13) alla (2) per $p = 3$ le possibili combinazioni sarebbero:

$$\binom{\pm 1}{\pm 5} + \binom{\pm 1}{\pm 5} = \binom{\pm 1}{\pm 5}$$

Come si può facilmente verificare nessuna scelta tra i possibili valori può soddisfare l'uguaglianza e quindi per $p = 3$ resta dimostrato che $13 \mid xyz$.

Il ragionamento non vale solo nel caso $p = 3$ ma si estende anche a qualsiasi altro valore di p a condizione che $q = 4p + 1$ sia primo, come ad esempio succede per $p = 7$ per il quale risulta $q = 4 \cdot 7 + 1 = 29$.

Per dimostrare questo in modo generale per tutti i $p \geq 5$ osserviamo che i possibili valori sono sempre in numero di 4 e che essendo sempre necessariamente presenti i valori ± 1, l'unica seconda coppia di numeri che potrebbe smentire l'asserto sarebbe ± 2. Ma questo non può succedere perché il quadrato di ± 2 è sempre $+4$ e non può mai valere -1.

Riprenderemo più avanti questo argomento che ha avuto una grande importanza tra i matematici che hanno studiato l'UTF in quanto attraverso ragionamenti e considerazioni di questo tipo si perviene a dimostrare il I caso ($p \nmid xyz$) dell'UTF per una grande quantità di esponenti.

Aggiungiamo che se invece si fosse scelto $k = 6$ (e lo stesso avverrebbe in generale se $6 \mid k$), non si potrebbe dimostrare che un primo del tipo $q = 6p+1$ sia un divisore di xyz; avremmo infatti un immediato controesempio per $p = 3$ e $q = 6 \cdot 3 + 1 = 19$:

$$1^3 \equiv 1 \pmod{19} \qquad 2^3 = 8 \equiv 8 \pmod{19} \qquad 3^3 = 27 \equiv 8 \pmod{19}$$

$$4^3 = 64 \equiv 7 \pmod{19} \quad 5^3 = 125 \equiv -8 \pmod{19} \quad 6^3 = 216 \equiv 7 \pmod{19}$$

Senza proseguire oltre si può concludere che ad esempio una combinazione $1 + 7 = 8$ sarebbe possibile, inficiando in tal modo la dimostrazione che $q \mid xyz$.

3. Scomposizione di somma e differenza di potenze dispari

Riportiamo qui brevemente le note formule di scomposizione che interessano le TdF:

$$\begin{aligned} z^p - y^p &= (z-y)\,(z^{p-1} + z^{p-2}y + z^{p-3}y^2 - \cdots + zy^{p-2} + y^{p-1}) \\ z^p - x^p &= (z-x)\,(z^{p-1} + z^{p-2}x + z^{p-3}x^2 - \cdots + zx^{p-2} + x^{p-1}) \\ x^p + y^p &= (x+y)\,(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1}) \end{aligned} \tag{7}$$

E' interessante osservare che poiché x, y e z sono coprimi tra loro, solo una delle tre variabili sarà pari e quindi in tutte le formule la seconda espressione tra parentesi a secondo membro è sempre e comunque dispari, in quanto formata da p termini dispari, se entrambe le variabili che vi compaiono sono dispari, oppure da $p-1$ termini pari ed un termine dispari nel caso che le due variabili abbiano differente parità.

Una seconda osservazione del tutto generale riguarda il fatto che, se entrambe le variabili a primo membro sono dispari, allora la somma o la differenza delle loro potenze è necessariamente pari e conterrà quindi un fattore del tipo 2^m. Il medesimo fattore 2^m dovrà di conseguenza ritrovarsi nella prima espressione tra parentesi a secondo membro, in quanto l'altra quantità tra parentesi, essendo dispari come detto in precedenza, non potrebbe contenere 2 tra i suoi fattori.

Riferendoci poi a variabili che fanno parte di una TdF si ottiene un risultato ancora più sorprendente. Senza perdere di generalità supponiamo ad esempio che la variabile pari sia la x e che essa quindi contenga nella sua scomposizione un fattore del tipo 2^m con $m \geq 1$. In questo caso possiamo scrivere:

$$x^p = z^p - y^p = 2^{mp}\,Q_x^p$$

dove $Q_x = x/2^m$ è un intero dispari.

Tenendo presente la prima delle (7) il termine $(z-y)$ non conterrà più semplicemente 2^m, bensì 2^{mp}, cioè la potenza p-esima di 2^m. Possiamo così riscrivere la (4) nel modo seguente:

$$z - y = x - \alpha = 2^{mp}\,Q_{zy}$$

L'ultima uguaglianza può essere così riscritta:

$$2^m\,Q_x - 2^w\,Q_\alpha = 2^{mp}\,Q_{zy}$$

con l'introduzione di altre costanti intere dispari, designate mediante la lettera Q ed un indice di riferimento, e dell'esponente w incognito.

E' facile dimostrare che deve sempre essere $w = m$.

Supponiamo infatti per assurdo che sia $m \neq w$ e mettiamo in evidenza nel primo membro un fattore 2^m:

$$2^m \, (Q_x - Q_\alpha \, 2^{w-m}) \; = \; 2^{mp} \, Q_{zy}$$

e quindi dividendo per tale fattore:

$$Q_x - Q_\alpha \, 2^{w-m} \; = \; 2^{m(p-1)} \, Q_{zy}$$

Ora se fosse $w > m$ i due membri avrebbero parità differente e quindi non potrebbero essere uguali, mentre se fosse $w < m$ si avrebbe l'assurdo che il secondo membro intero dovrebbe uguagliare un primo membro contenente il termine frazionario $Q_\alpha / 2^{m-w}$.

In conclusione resta provato che dovrà essere $m = w$ e quindi si avrà:

$$Q_x - Q_\alpha \; = \; 2^{m(p-1)} \, Q_{zy}$$

concludendo di conseguenza che $Q_x - Q_\alpha$ è un numero pari contenente il fattore $2^{m(p-1)}$.

Ad analoga conclusione si perviene se la variabile pari è y o z; si è quindi dimostrato che la costante α non solo è pari ma contiene il fattore 2 con lo stesso esponente m presente nell'unica variabile pari della TdF.

Questo risultato non è valido per le TdP, come si può facilmente verificare, e neppure per le TdF con esponente pari.

Con passaggi relativamente semplici è possibile trasformare le (7) nelle seguenti forme che saranno utilizzate più avanti:

$$\begin{aligned}
z^p - y^p \; &= \; (z-y)\left((z-y)(z^{p-2} + 2z^{p-3}y + 3z^{p-4}y^2 - \cdots + (p-1)y^{p-2}) + py^{p-1}\right) \\
z^p - x^p \; &= \; (z-x)\left((z-x)(z^{p-2} + 2z^{p-3}x + 3z^{p-4}x^2 - \cdots + (p-1)x^{p-2}) + px^{p-1}\right) \qquad (8) \\
x^p + y^p \; &= \; (x+y)\left((x+y)(x^{p-2} - 2x^{p-3}y + 3x^{p-4}y^2 - \cdots - (p-1)y^{p-2}) + py^{p-1}\right)
\end{aligned}$$

Un'ulteriore forma delle stesse identità può essere ottenuta ponendo:

$$x = a - y \qquad\qquad z = b + y \qquad\qquad z = c + x$$

Con queste posizioni si ottengono le seguenti formule:

$$\begin{aligned}
(b+y)^p - y^p \; &= \; b^p + p\,b^{p-1}y + p\,\frac{p-1}{2}\,b^{p-2}\,y^2 + \cdots + p\,\frac{p-1}{2}\,b^2\,y^{p-2} + p\,b\,y^{p-1} \\
(c+x)^p - x^p \; &= \; c^p + p\,c^{p-1}x + p\,\frac{p-1}{2}\,c^{p-2}\,x^2 + \cdots + p\,\frac{p-1}{2}\,c^2\,x^{p-2} + p\,c\,x^{p-1} \qquad (9) \\
(a-y)^p + y^p \; &= \; a^p - p\,a^{p-1}y + p\,\frac{p-1}{2}\,a^{p-2}\,y^2 - \cdots - p\,\frac{p-1}{2}\,a^2\,y^{p-2} + p\,a\,y^{p-1}
\end{aligned}$$

4. Un teorema mirabile (TM)

La generalizzazione del ragionamento seguito nel paragrafo precedente per dimostrare che α contiene lo stesso fattore 2^m della variabile pari presente in una TdF, ci porta ad enunciare il seguente mirabile teorema:

In ogni relazione del tipo $x + y = z$ tra numeri interi relativi non nulli, per ciascun fattore primo q, presente con esponente > 0 in almeno uno dei tre termini, esiste sempre almeno un termine che contiene il fattore q^m con il valore massimo m dell'esponente, mentre i restanti due termini contengono un identico fattore q^i con $0 \leq i \leq m$.

In altre parole in una siffatta terna non possono coesistere termini che contengano uno stesso fattore primo con tre diversi esponenti o un solo termine che contenga il fattore primo con il minimo esponente. Nel caso particolare che sia $i = m$ i tre termini conterrebbero tutti lo stesso fattore q^m.

Per la dimostrazione facciamo l'ipotesi che sia z la variabile che contiene il fattore q^m, mentre per assurdo le variabili x ed y contengono rispettivamente due diversi fattori q^a e q^b con $a < b \leq m$; possiamo allora scrivere:

$$q^a\, Q_x + q^b\, Q_y \;=\; q^m\, Q_z$$

e quindi dividendo ambo i membri per q^b:

$$\frac{Q_x}{q^{b-a}} + Q_y \;=\; q^{m-b}\, Q_z$$

dove con Q_x, Q_y ed Q_z si sono indicati i residui della fattorizzazione di x, y e z che non contengono più il fattore primo q.

Ma l'ultima uguaglianza è assurda perché il primo membro, a differenza del secondo, non può essere intero per la presenza di Q_x/q^{b-a} a meno che non sia $a = b$ c.v.d.

Naturalmente se la generica terna, inizialmente non coprima con riguardo a q, venisse resa tale dividendo per q^a, si hanno due alternative: o il fattore q scompare da tutte le variabili, essendo presente in esse con il medesimo esponente q^a, oppure il fattore q resta presente in una sola variabile, mentre nelle altre esso scompare dalla fattorizzazione in quanto avrebbe a questo punto esponente nullo.

Come applicazione del TM prendiamo in considerazione una relazione del tipo:

$$q^a\, Q_x + q^b\, Q_y \;=\; z$$

dove al primo membro sono evidenziati i fattori q^a e q^b mentre nulla sappiamo del secondo membro z. Ebbene il TM ci permette di stabilire che:

- Se $a \neq b$ allora z conterrà esattamente il fattore q^m (cioè $q^m \parallel z$) con $m = min(a, b)$.
- Se $a = b$ allora z conterrà un fattore q^m (cioè $q^m \mid z$) con $m \geq a$.

5. Il teorema mirabile generalizzato (TMG)

Il teorema in oggetto può essere generalizzato sotto due diversi aspetti:

(a) Generalizzazione rispetto a q

Il fattore q non deve necessariamente essere un numero primo, ma può essere un qualsiasi numero composto c, o al limite un'espressione complessa, alla sola condizione che tutti i fattori primi, presenti nella scomposizione di tale numero od espressione, siano presenti nella relazione solamente in c e nelle sue potenze. Per la dimostrazione basta considerare il fatto che il teorema mirabile è valido separatamente per ciascuno dei singoli numeri primi q_i in cui può essere fattorizzato c ed è quindi valido anche per il loro prodotto.

Come applicazione del TMG prendiamo in considerazione una relazione del tipo:

$$c^a\, Q_x + c^b\, Q_y \;=\; z$$

dove al primo membro sono evidenziati i fattori c^a e c^b mentre nulla sappiamo del secondo membro z. Ebbene il TMG ci permette di stabilire che:

- Se $a \neq b$ allora z conterrà esattamente il fattore c^m (cioè $c^m \parallel z$) con $m = min(a, b)$.
- Se $a = b$ allora z conterrà un fattore c^m (cioè $c^m \mid z$) con $m \geq a$.

In questo secondo caso si osserva che i fattori primi di c potranno comparire in z anche con potenze differenti tra loro purché tutte maggiori od uguali ad a.

(b) Generalizzazione a una relazione del tipo $\displaystyle\sum_{i=1}^{N} a_i = 0$

Per un qualsiasi primo q presente in uno o più termini a_i della relazione $\displaystyle\sum_{i=1}^{N} a_i = 0$ tra numeri interi relativi non nulli, risultano vere le seguenti affermazioni:

i. Il termine contenente q^m $(m \geq 0)$ con il minimo esponente non può mai essere unico.

ii. In caso diverso si potranno sostituire i 2 o più termini contenenti q^m con il minimo esponente mediante la loro somma; quest'ultima, se non nulla, conterrà nella sua scomposizione un fattore q^n con $n > m$.

iii. Alla nuova relazione così ottenuta potrà applicarsi nuovamente quanto detto ai punti precedenti in modo ricorsivo.

Se inizialmente o nel corso del processo sopra descritto si verificasse che il termine contenente q con il minimo esponente risultasse unico, si deve concludere che la relazione iniziale non può essere mai soddisfatta nel campo degli interi relativi ed è quindi falsa.

6. Alcuni rapporti necessariamente interi

Dividendo membro a membro le equazioni (2) e (4) possiamo scrivere:

$$\frac{x^p + y^p}{x + y} \;=\; \frac{z^p}{z + \alpha} \;=\; \frac{z^p + \alpha^p}{z + \alpha} - \frac{\alpha^p}{z + \alpha}$$

Poiché la prima frazione è intera, anche le successive frazioni dovranno esserlo, e così le seguenti analoghe frazioni:

$$\frac{z^p - y^p}{z - y} \;=\; \frac{x^p}{x - \alpha} \;=\; \frac{x^p - \alpha^p}{x - \alpha} + \frac{\alpha^p}{x - \alpha} \qquad \frac{z^p - x^p}{z - x} \;=\; \frac{y^p}{y - \alpha} \;=\; \frac{y^p - \alpha^p}{y - \alpha} + \frac{\alpha^p}{y - \alpha}$$

Inoltre saranno interi anche i seguenti rapporti ottenuti moltiplicando tra loro i precedenti e semplificando mediante la (4):

$$\frac{(xz)^p}{xz - \alpha y} \quad , \quad \frac{(yz)^p}{yz - \alpha x} \quad , \quad \frac{(xy)^p}{xy - \alpha z} \qquad \text{e} \qquad \frac{(xyz)^p}{xyz - \alpha(xz + yz - xy)}$$

Dal rapporto $\alpha^p/(z + \alpha)$ necessariamente intero e non nullo e quindi maggiore od uguale ad 1, si può ricavare un limite inferiore per α:

$$\alpha^p \;\geq\; z + \alpha \;>\; z$$

da cui segue $\alpha > \sqrt[p]{z}$.

6 Lemmi notevoli

1. Lemma I: In una TdF z non può essere né primo né potenza di un primo

   Supponiamo per assurdo che sia $z = q^m$ dove q è un numero primo ed m un intero ≥ 1. In questo caso dovrà essere intero il seguente rapporto:

   $$\frac{z^p}{z+\alpha} = \frac{q^{mp}}{q^m+\alpha}$$

   La condizione richiesta implica che sia:

   $$q^m + \alpha = q^i$$

   con $i > m$ in quanto $\alpha > 0$. Si ha quindi per α:

   $$\alpha = q^i - q^m = q^m\,(q^{i-m} - 1) > q^m = z$$

   Ma questa conclusione è assurda in quanto $\alpha < x < z$, e pertanto l'ipotesi iniziale è falsa, e il lemma è dimostrato.

2. Lemma II: In una TdF se x è primo o potenza di un primo allora $\alpha = x - 1$ e $z = y + 1$

   Poniamo $x = q^m$ dove q è un numero primo ed m un intero ≥ 1. In questo caso dovrà essere intero il seguente rapporto:

   $$\frac{x^p}{x-\alpha} = \frac{q^{mp}}{q^m-\alpha}$$

   La condizione richiesta implica che sia:

   $$q^m - \alpha = q^i$$

   con $i < m$ in quanto $\alpha > 0$ ed il numeratore è divisibile solo per potenze intere di q. Utilizzando la (4) si ha anche:

   $$z - y = q^m - \alpha = q^i$$

   Sostituendo ora q^i nella prima delle (9) al posto della variabile b e ricordando la (2) possiamo riscrivere la relazione $x^p = z^p - y^p$, evidenziando un fattore q^i, nella forma seguente:

   $$\begin{aligned} q^{mp} &= q^i\left((q^i)^{p-1} + p\,(q^i)^{p-2}\,y + p\,\frac{p-1}{2}\,(q^i)^{p-3}y^2 + \ldots + p\,\frac{p-1}{2}\,q^i\,y^{p-2} + p\,y^{p-1}\right) = \\ &= q^i\left(q^i\left((q^i)^{p-2} + p\,(q^i)^{p-3}\,y + p\,\frac{p-1}{2}\,(q^i)^{p-4}y^2 + \ldots + p\,\frac{p-1}{2}\,y^{p-2}\right) + p\,y^{p-1}\right) \end{aligned}$$

   In base al TM, perché l'uguaglianza sia possibile con riferimento al fattore primo q (q^{mp} è certamente il termine con l'esponente più grande poiché $m > i$), è necessario che i due termini entro le parentesi più esterne contengano la stessa potenza di q e di conseguenza il termine $p\,y^{p-1}$ dovrebbe contenere anch'esso il fattore q^i.

   Ma escludendo che y^{p-1} possa contenere il fattore q^i in quanto y è coprimo con x e quindi anche con q, perché q^i divida esattamente p si distinguono i due casi seguenti:

- $i \geq 1$ - Se fosse $i > 1$ allora p dovrebbe essere multiplo di q, ma ciò è impossibile poiché p è primo, e quindi resta la possibilità che sia $i = 1$ e quindi $p = q$ e $x = p^m$. Ma questa conclusione è impossibile in quanto riprendendo lo sviluppo precedente dopo la sostituzione di q^i con p possiamo mettere in evidenza un termine p^2 ottenendo così:

$$q^{mp} = p^{mp} = p^2 \left(p \left(p^{p-3} + p^{p-3}\, y + \frac{p-1}{2}\, p^{p-4} y^2 + \ \ldots \ + \frac{p-1}{2}\, y^{p-2} \right) + y^{p-1} \right)$$

  Applicando ora nuovamente il TM rispetto al fattore primo p si può solamente concludere che la relazione scritta non può essere mai soddisfatta nel campo dei numeri interi e quindi l'ipotesi $i = 1$ è assurda.
- $i = 0$ - Questa è l'unica possibilità valida restante e corrisponde all'enunciazione del lemma in oggetto, per cui si ha di conseguenza $\alpha = q^m - 1 = x - 1$ e $z = y + 1$ c.v.d.

Il precedente ragionamento, oltre a dimostrare il lemma in oggetto, porta ad escludere che sia $x = p^m$ in quanto la relazione $\alpha = p^m - 1$ risulterebbe in contraddizione con il TM rispetto a p in quanto $p \mid \alpha$.

E' interessante confrontare i risultati precedenti con il caso delle TdP $(p = 2)$, per le quali si possiedono le formule risolutive distinguendo due diversi casi:

- $x = 2^m$ - L'espressione di x^2 è in questo caso la seguente:

$$2^{2m} = 2^i \, (2^i + 2y) = 2^{2i} + 2^{i+1} y$$

  Poiché $(2, y) = 1$ e $m \geq i$, l'unico valore ammissibile sulla base del TM è $i = 1$; con semplici passaggi, si ottengono le seguenti soluzioni:

$$x = 2^m \qquad\qquad y = 2^{2\,(m-1)} - 1 \qquad\qquad z = 2^{2\,(m-1)} + 1$$

  che definiscono TdP primitive per ogni valore intero di m maggiore dell'unità.
  Si osservi che tali espressioni verificano *identicamente* l'equazione pitagorica che risulta quindi soddisfatta per qualsiasi valore reale o complesso di m. Restando al caso di valori di m interi positivi o nulli si osserva che per $m = 0$ si avrebbe una soluzione con termini frazionari $\{1, -3/4, 5/4\}$, mentre per $m = 1$ si ha la soluzione banale $\{2, 0, 2\}$.
  Le TdP valide si ottengono quindi solo per $m \geq 2$: per $m = 2$ si ottiene la terna $\{4, 3, 5\}$, per $m = 3$ la terna $\{8, 15, 17\}$, per $m = 4$ la terna $\{16, 63, 65\}$, e così via.
- $x = q^m$ con q primo dispari - L'espressione di x^2 è in questo caso la seguente:

$$q^{2m} = q^i \, (q^i + 2y) = q^{2i} + 2q^i y$$

  Poiché $(q, y) = 1$ l'unico valore ammissibile sulla base del TM è $i = 0$ che dà origine alle seguenti soluzioni:

$$x = q^m \qquad\qquad y = \frac{1}{2}\,(q^{2m} - 1) \qquad\qquad z = \frac{1}{2}\,(q^{2m} + 1)$$

  che definiscono TdP primitive per ogni primo dispari q ed ogni valore intero di m maggiore di 0. Il caso $m = 0$ darebbe origine alla terna banale $\{1, 0, 1\}$ indipendentemente dal valore di q. Prendendo ad esempio $q = 5$ si avrebbero per $m = 1, 2, 3$ le terne primitive $\{5, 12, 13\}$, $\{25, 312, 313\}$ e $\{125, 7812, 7813\}$ rispettivamente.

3. Lemma III: In una TdF y non può essere né primo né potenza di un primo

   Supponiamo per assurdo che sia $y = q^m$ dove q è un numero primo. In questo caso dovrà essere intero il seguente rapporto:

$$\frac{y^p}{y-\alpha} = \frac{q^{mp}}{q^m-\alpha}$$

La condizione richiesta implica che sia:

$$q^m - \alpha = q^i$$

con $i < m$ in quanto $\alpha > 0$.

Ripetendo anche in questo caso lo stesso ragionamento fatto per x possiamo affermare che i può unicamente assumere il valore 0 e di conseguenza $\alpha = y - 1$ e $z = x + 1$. Ma queste relazioni sono manifestamente assurde perché in contraddizione con l'ipotesi che sia $x < y < z$ e con la relazione $\alpha < x$ precedentemente dimostrata.

In conclusione l'ipotesi iniziale è falsa ed il lemma è così dimostrato.

7 Scomposizione delle potenze p-esime di x, y e z

Vogliamo a questo punto dimostrare che è sempre possibile esprimere ciascuna potenza x^p, y^p e z^p in forma simbolica nel prodotto di due termini tra loro coprimi. Questo implica che ogni termine dovrà necessariamente essere una potenza p-esima in quanto i diversi fattori primi in gioco risulteranno presenti in uno solo dei due termini una volta dimostrata la coprimalità di questi ultimi.
La dimostrazione porterà anche nel modo più naturale a distinguere il caso in cui nessuna variabile sia divisibile per l'esponente p dal caso in cui vi sia invece una variabile contenente tra i suoi fattori p^m con $m \geq 1$, mostrando che in entrambi i casi tale scomposizione risulta sempre possibile.
Consideriamo ad esempio la variabile x e la prima delle (9), che qui riscriviamo, utilizzando per maggior chiarezza al posto di b il simbolo h con il valore $(z-y)$, nell'ipotesi che la relazione di Fermat sia vera:

$$\begin{aligned} x^p &= h^p + p\,h^{p-1}y + p\,\frac{p-1}{2}\,h^{p-2}\,y^2 + \cdots + p\,\frac{p-1}{2}\,h^2\,y^{p-2} + p\,h\,y^{p-1} = \\ &= h\left(h\left(h^{p-2} + p\,h^{p-3}y + p\,\frac{p-1}{2}\,h^{p-4}\,y^2 + \cdots + p\,\frac{p-1}{2}\,y^{p-2}\right) + p\,y^{p-1}\right) \end{aligned}$$

Assegniamo ora a k l'espressione a secondo membro compresa tra le parentesi più esterne:

$$k = h\left(h^{p-2} + p\,h^{p-3}y + p\,\frac{p-1}{2}\,h^{p-4}\,y^2 + \cdots + p\,\frac{p-1}{2}\,y^{p-2}\right) + p\,y^{p-1} \tag{10}$$

Con questa posizione la relazione precedente diventa:

$$x^p = h\,k \tag{11}$$

e domandiamoci ora se h e k, siano o meno coprimi.
Se la risposta fosse positiva avremmo dimostrato l'assunto e h e k dovranno essere di conseguenza due potenze p-esime.
Diversamente facciamo l'ipotesi che h e k non siano coprimi: esisterà allora certamente un fattore comune $d_{hk} = (h,k) > 1$ per il quale dividere ambo i membri della (10):

$$\frac{k}{d_{hk}} = \frac{h}{d_{hk}}\left(h^{p-2} + p\,h^{p-3}y + p\,\frac{p-1}{2}\,h^{p-4}\,y^2 + \cdots + p\,\frac{p-1}{2}\,y^{p-2}\right) + \frac{p\,y^{p-1}}{d_{hk}}$$

Poiché il primo membro ed il primo termine del secondo membro sono entrambi interi, dovrà essere intero anche $p\,y^{p-1}/d_{hk}$.
Ma y^{p-1} non può essere divisibile per d_{hk} in quanto d_{hk} è un fattore di h e $(h,y) = (z-y,y) = 1$ per la proprietà IV del Cap. 4, mentre p, essendo primo, è divisibile solo per se stesso o per l'unità, per cui si deve concludere che h e k o sono coprimi, oppure hanno p come massimo comun divisore, cioè dovrà essere $(h,k) = p$.
In quest'ultimo caso in base alla (11) possiamo facilmente concludere che x deve contenere necessariamente un fattore di tipo p^m con $m \geq 1$, e quindi x^p un fattore p^{mp}; a loro volta, per la stessa (11), h e k dovranno contenere i fattori p^{mp-1} e p.
Indicando con H e K due quantità tra loro coprime non divisibili per p, potremo distinguere le seguenti due alternative:

$$1)\quad \begin{cases} h = H\,p^{mp-1} \\ k = K\,p \end{cases} \qquad\qquad 2)\quad \begin{cases} h = H\,p \\ k = K\,p^{mp-1} \end{cases}$$

E' facile mostrare che solamente la prima delle due alternative è possibile, in quanto la seconda porterebbe ad un risultato assurdo. Infatti sostituendo quest'ultima nella (10) si avrebbe:

$$\begin{aligned} K\,p^{mp-1} &= H\,p\left((H\,p)^{p-2} + H^{p-3}\,p^{p-2}\,y + \ldots + p\,\frac{p-1}{2}\,y^{p-2}\right) + p\,y^{p-1} = \\ &= H\,p^2\left(H^{p-2}\,p^{p-3} + (H\,p)^{p-3}\,y + \ldots + \frac{p-1}{2}\,y^{p-2}\right) + p\,y^{p-1} \end{aligned}$$

Poiché per $p \geq 3$ solamente il termine $p\,y^{p-1}$ contiene il fattore primo p con il minimo esponente, la relazione precedente è certamente errata in quanto in contraddizione con il TM[10].
Al contrario la prima alternativa rispetta i vincoli imposti da tale teorema, come si vede effettuando la sostituzione nella (10):

$$K\,p \;=\; H\,p^{mp-1}\left((H\,p^{mp-1})^{p-2} + p\,(H\,p^{mp-1})^{p-3}\,y + \;\ldots\; + p\,\frac{p-1}{2}\,y^{p-2}\right) + p\,y^{p-1}$$

In conclusione se h e k sono coprimi allora la (11) rappresenta la scomposizione cercata, mentre se h e k ammettono il fattore comune p, allora potremo sempre scrivere:

$$x^p \;=\; (p\,h)\left(\frac{k}{p}\right) \tag{12}$$

evidenziando così con le parentesi i due termini coprimi.
Abbiamo quindi dimostrato che indipendentemente dal fatto che p divida o meno x è sempre possibile scomporre la potenza x^p nel prodotto di due termini tra loro coprimi e questa coprimalità ha come immediata conseguenza il fatto che tali termini devono a loro volta essere potenze p-esime come si era detto all'inizio del paragrafo[11].
La stessa procedura può essere seguita per trattare in modo analogo le variabili y e z raggiungendo le medesime conclusioni.
Possiamo quindi esprimere le potenze p-esime delle variabili di Fermat nel modo seguente:

$$x^p \;=\; r^p\,R^p \qquad\qquad y^p \;=\; s^p\,S^p \qquad\qquad z^p \;=\; t^p\,T^p \tag{13}$$

Di conseguenza tali variabili saranno così esprimibili:

$$x \;=\; r\,R \qquad\qquad y \;=\; s\,S \qquad\qquad z \;=\; t\,T \tag{14}$$

In queste relazioni sono state introdotte 6 nuove grandezze r, R, s, S, t e T tutte tra loro coprime, per le quali nel seguito saranno fornite le espressioni analitiche in funzione di x, y e z.

Prima di procedere oltre è necessario riportare qui di seguito un'importante identità algebrica scoperta da Lamé nel 1840, riscritta nella forma datagli successivamente da Werebrusow[2] e da me modificata secondo i simboli e le convenzioni di segno adottate:

$$(x+y-z)^p - (x^p+y^p-z^p) \;=\; \left[\frac{p!}{2^{p-2}}\;\sum\frac{(z-y)^{2i}\,(z-x)^{2j}\,(x+y)^{2k}}{(2i+1)!\;(2j+1)!\;(2k+1)!}\right](z-y)\,(z-x)\,(x+y)$$

dove la sommatoria va estesa a tutti i valori interi $i,j,k \;\geq\; 0$ che soddisfanno alla condizione $i+j+k=(p-3)/2$ (questa estensione della sommatoria si intende sottintesa nel seguito).

Ora si può osservare che nella formula è presente a primo membro il termine $(x^p+y^p-z^p)$ che si dovrà annullare nell'ipotesi fatta inizialmente che le variabili appartengano ad una TdF, trasformando quindi l'identità di Lamé in una equazione perfettamente equivalente alla forma classica dell'UTF:

$$(x+y-z)^p \;=\; \alpha^p \;=\; \left[\frac{p!}{2^{p-2}}\;\sum\frac{(z-y)^{2i}\,(z-x)^{2j}\,(x+y)^{2k}}{(2i+1)!\;(2j+1)!\;(2k+1)!}\right](z-y)\,(z-x)\,(x+y) \tag{15}$$

[10] E' interessante osservare che per $p=2$ non si raggiungerebbe la stessa conclusione, perché in tal caso si avrebbe:

$$K\,2^{2m-1} \;=\; 2\,H + 2\,y$$

che è una relazione perfettamente in linea con il TM.

[11] Abbiamo visto precedentemente che x, (a differenza di y e z) può essere primo o potenza di un primo. In tal caso, in base al Lemma II del capitolo 6, si avrebbe $h = z-y = 1^p = 1$ e le due potenze p-esime, rappresentate da h e h, sarebbero sempre coprime e di conseguenza x non potrebbe essere divisibile per p escludendo quindi la possibilità che sia $x=p^m$ $(m \geq 1)$. La stessa conclusione si ottiene ponendo $b=1$ nella prima delle (9):

$$p^{mp} \;=\; 1 + p\,y + p\,\frac{p-1}{2}\,y^2 + \;\ldots\; + p\,\frac{p-1}{2}\,y^{p-2} + p\,y^{p-1}$$

Si vede infatti che questa relazione è assurda perché il secondo membro, a differenza del primo, non è divisibile per p in quanto la divisione darebbe resto 1.

In altre parole se si potesse dimostrare che la (15) è falsa o contraddittoria, l'UTF risulterebbe dimostrato.
Introducendo a questo punto un'ulteriore grandezza u e ricordando le formule viste in precedenza, si potrà scrivere α^p nella forma seguente:

$$\alpha^p \;=\; u^p\, r^p\, s^p\, t^p \tag{16}$$

Di conseguenza α sarà esprimibile come:

$$\alpha \;=\; u\, r\, s\, t \tag{17}$$

Anche per la nuova grandezza u, di cui si dimostrerà nel seguito la coprimalità con tutte le altre 6 precedentemente introdotte, se ne fornirà l'espressione analitica in funzione di x, y e z.
Nei capitoli successivi tratteremo separatamente i due casi, rappresentati rispettivamente dalle relazioni (11) e (12), in cui risulta conveniente suddividere l'UTF, come peraltro viene fatto da altri autori.

Può essere interessante confrontare i risultati precedenti con quelli che si ottengono per l'equazione pitagorica cioè nel caso $p = 2$.
Una prima osservazione consiste nel fatto che z^2, essendo somma di due quadrati, non è scomponibile come gli altri termini x^2 ed y^2. In secondo luogo si può facilmente dimostrare che in una TdP primitiva z non può mai essere pari mentre tra x ed y dovrà essere sempre presente una variabile pari divisibile per 4, valore quest'ultimo che è una potenza dell'esponente p. Prendendo per comodità a riferimento la scomposizione di x^2 (senza il vincolo che sia $x < y$) si hanno quindi due casi:

1. Le variabili x e z sono dispari, mentre y è pari.

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

   Per la proprietà VII del Cap. 4 i due termini in parentesi sono sempre coprimi e quindi possiamo scrivere:

   $$(z - y) \;=\; m^2 \qquad\qquad (z + y) \;=\; n^2$$

   da cui si deriva una prima versione delle formule risolutive con m ed n coprimi, entrambi dispari ed $n > m$:

   $$x = mn \qquad y = \frac{n^2 - m^2}{2} \qquad z = \frac{n^2 + m^2}{2}$$

2. Le variabili x è pari, mentre y e z sono dispari.

   $$\left(\frac{x}{2}\right)^2 \;=\; \left(\frac{z - y}{2}\right)\left(\frac{z + y}{2}\right)$$

   Per la proprietà VIII del Cap. 4 i due termini in parentesi sono coprimi e quindi possiamo scrivere:

   $$\left(\frac{z - y}{2}\right) \;=\; m^2 \qquad\qquad \left(\frac{z + y}{2}\right) \;=\; n^2$$

   da cui si deriva una seconda versione delle formule risolutive con m ed n coprimi, di parità diversa ed $n > m$:

   $$x = 2mn \qquad y = n^2 - m^2 \qquad z = n^2 + m^2 \tag{18}$$

   Non è invece corretto seguire in questo caso la procedura utilizzata in precedenza per le TdF in quanto tra $(z - y)$ e $(z + y)$ non risulterebbe possibile stabilire quale dei due binomi è divisibile esattamente per 2 e quale invece contiene 2 con un esponente dispari ≥ 3.

8 Caso I - L'esponente p non divide xyz

Le espressioni analitiche delle 6 quantità precedentemente introdotte si ottengono prendendo le radici p-esime delle seguenti relazioni:

$$\begin{aligned} r^p &= z - y & R^p &= (z^{p-1} + z^{p-2}\,y + \ldots + z^2\,y^{p-3} + z\,y^{p-2} + y^{p-1}) \\ s^p &= z - x & S^p &= (z^{p-1} + z^{p-2}\,x + \ldots + z^2\,x^{p-3} + z\,x^{p-2} + x^{p-1}) \\ t^p &= x + y & T^p &= (x^{p-1} - x^{p-2}\,y + \ldots + x^2\,y^{p-3} - x\,y^{p-2} + y^{p-1}) \end{aligned} \tag{19}$$

Con semplici passaggi le tre espressioni a sinistra permettono di ricavare le seguenti condizioni a cui le variabili delle TdF devono soddisfare:

$$\begin{aligned} x &= \frac{1}{2}\,(t^p - s^p + r^p) \\ y &= \frac{1}{2}\,(t^p + s^p - r^p) \\ z &= \frac{1}{2}\,(t^p + s^p + r^p) \end{aligned} \tag{20}$$

A queste possiamo aggiungere l'analoga espressione per α:

$$\alpha = x + y - z = \frac{1}{2}\,(t^p - s^p - r^p)$$

L'espressione per u^p si ottiene facilmente confrontando la (15) con la (16) e tenendo conto delle (19):

$$u^p = \frac{p!}{2^{p-2}} \sum \frac{(z-y)^{2i}\,(z-x)^{2j}\,(x+y)^{2k}}{(2i+1)!\,(2j+1)!\,(2k+1)!} \tag{21}$$

Utilizzando infine le (19), la (4) e le (14) possiamo scrivere le seguenti relazioni:

$$\begin{aligned} r^p &= z - y = x - \alpha = r\,R - \alpha \\ s^p &= z - x = y - \alpha = s\,S - \alpha \\ t^p &= x + y = z + \alpha = t\,T + \alpha \end{aligned} \tag{22}$$

Applicando il TMG alla prima relazione $r^p = r\,R - \alpha$, con riferimento alla quantità r, e tenendo presente che $(r, R) = 1$, si conclude necessariamente che il parametro α deve contenere r tra i suoi fattori, come già era evidente dalla (17), anzi più precisamente sarà $r \parallel \alpha$ (cioè r divide esattamente α).
Ripetendo lo stesso ragionamento per s e per t si conclude che $rst \parallel \alpha$ e di conseguenza il quarto fattore di α, che abbiamo indicato con la lettera u, dividerà anch'esso esattamente α e sarà quindi coprimo con tutti gli altri, ed infine, poiché 2 divide certamente rst, il fattore u sarà necessariamente sempre dispari.
Ma le stesse relazioni forniscono anche un'altra importante informazione se applichiamo il TMG con riferimento alle quantità R, S e T. Infatti poiché tali grandezze sono coprime con r, s e t, e di conseguenza anche con r^p, s^p e t^p, esse dovranno essere coprime con α e quindi anche con il fattore u. Se si potesse dimostrare il contrario l'UTF sarebbe dimostrato.

9 (Quasi) dimostrazione del I Caso dell'UTF

Sulla base del teorema di Sophie Germain (1776-1831), che d'ora innanzi indicheremo con $TdSG$, e delle considerazioni che seguono, è possibile dimostrare il I Caso dell'UTF *per qualsiasi primo di ragionevole grandezza*.
Con questa espressione si vuole significare che la dimostrazione è risultata numericamente sempre possibile, mediante l'utilizzo di un semplice programma di calcolo, per qualsiasi esponente p, senza eccezione alcuna, fino ai limiti fisici della macchina e del programma.
In termini strettamente matematici la dimostrazione non è quindi valida.
Prima di procedere ad esporre il $TdSG$ è interessante analizzare da un punto di vista generale i residui (mod q) di un numero di tipo a^p dove p e q sono entrambi primi e $(a, q) = 1$.
Attribuendo ad a tutti i valori possibili compresi tra 1 e $q-1$, si possono distinguere i seguenti casi:

1. $q > p, \quad q \neq kp + 1$

   I residui sono costituiti dagli stessi numeri compresi tra 1 e $q-1$ in sequenza non ordinata.

2. $q > p, \quad q = kp + 1, \quad (k \text{ pari})$

   I residui sono costituiti solamente da k valori diversi tra loro. Infatti per il teorema di Fermat possiamo scrivere:

   $$a^p = a^{\frac{q-1}{k}} = \sqrt[k]{a^{q-1}} \equiv \sqrt[k]{1} \pmod{q}$$

   da cui segue $(a^p)^k \equiv 1 \pmod{q}$ e di conseguenza a^p assumerà solo quei k valori la cui potenza k-esima vale 1.

   Inoltre se r_a è un residuo di $a^p \pmod{q}$, tra i residui sarà anche presente $-r_a \equiv q - r_a$ che è il residuo di $(q-a)^p$. Saranno infine residui anche r_a^{-1} e $-r_a^{-1}$, che corrispondono rispettivamente a $(a^{-1})^p$ e $(-a^{-1})^p \pmod{q}$.

3. $q \leq p, \quad q = (p-1)/k + 1, \quad ((p-1)/k \text{ intero pari})$

   I residui sono costituiti dagli stessi numeri compresi tra 1 e $q-1$ in sequenza ordinata; ciò corrisponde al fatto dimostrato in precedenza che in questo caso $a^p \equiv a \pmod{q}$.

   Si osserva inoltre che utilizzando al posto del primo q un numero composto n che sia un qualsiasi prodotto tra primi q_i corrispondenti a differenti valori k_i si ottiene ugualmente $a^p \equiv a \pmod{n}$.

4. $q < p, \quad q \neq (p-1)/k + 1$

   I residui sono costituiti dagli stessi numeri compresi tra 1 e $q-1$ in sequenza non ordinata.

Il $TdSG$ utilizza i valori di q di cui al precedente punto 2. e tra questi quelli in particolare per i quali k vale esattamente 2; per questa ragione i primi p per i quali $q = 2p + 1$ risulta anch'esso primo sono detti primi di Sophie Germain. Come già dimostrato in precedenza in questo caso q risulta essere un divisore di xyz $(q \mid xyz)$.

Senza perdere di generalità e supponendo che sia x la variabile di Fermat divisibile per q (cioè $q \mid x$), possiamo riscrivere la prima delle (20) nel modo seguente ed applicare ad essa l'operatore (mod q):

$$2x = t^p - s^p + r^p \equiv 0 \pmod{q}$$

Con lo stesso ragionamento con cui si è dimostrato che $q \mid xyz$ possiamo affermare che $q \mid rst$ e poiché $q \nmid st$ in quanto s e t sono fattori di y e z a loro volta coprimi con x, dovrà essere $q \mid r$.

Riprendiamo ora dalla terza delle (19) la definizione di T^p ed applichiamo a questa grandezza l'operatore (mod q) tenendo presente che $q \mid x$:

$$T^p = (x^{p-1} - x^{p-2}\,y + \ldots + x^2\,y^{p-3} - x\,y^{p-2} + y^{p-1}) \equiv y^{p-1} \pmod{q}$$

In modo analogo operando sulla prima delle (22):

$$r^p \;=\; z - y \;\equiv\; 0 \pmod{q}$$

segue che $z \equiv y \pmod{q}$.

Ritornando infine alla prima delle (19) e sostituendo z con y abbiamo per R^p:

$$R^p \;=\; (z^{p-1} + z^{p-2}\,y + \ldots + z^2\,y^{p-3} + z\,y^{p-2} + y^{p-1}) \;\equiv\; py^{p-1} \;\equiv\; pT^p \pmod{q}$$

Ora poiché l'inverso di T certamente esiste in quanto q è primo e non divide T, possiamo scrivere:

$$(RT^{-1})^p \;\equiv\; p \pmod{q} \tag{23}$$

Ma si è visto che i possibili valori di $a^p \pmod{q}$ sono solamente +1 e -1 e quindi la (23) è assurda. Siamo perciò pervenuti ad una contraddizione dalla quale si deduce che l'ipotesi che p non divida xyz è falsa e quindi le formule utilizzate all'inizio del capitolo, basate su tale ipotesi, non sono applicabili. Alle stesse conclusioni saremmo ugualmente giunti se al posto di T^p avessimo inizialmente utilizzato S^p per il quale si troverebbe:

$$S^p \equiv z^{p-1} \;\equiv y^{p-1} \equiv T^p \pmod{q}$$

Successivamente Adrien-Marie Legendre (1752-1833) dimostrò che per $p > 3$ lo stesso risultato, da cui seguiva la dimostrazione del I caso dell'UTF, valeva più in generale per un primo q della forma $q = kp + 1$ per i valori 4, 8, 10, 14, 16 di k per i quali i residui di $a^p \pmod{q}$ sono sempre diversi da p.

Si osservi che a secondo membro della (23) si potrebbe sostituire p con k (o con i loro complementi a q), in quanto dalla definizione di q risulta che tra p e k intercorre la relazione:

$$k \equiv -1/p \pmod{q} \tag{24}$$

e di conseguenza se tra i residui vi è p tra gli stessi sarà presente anche k per quanto detto in precedenza al punto 2.

Infine si nota che tra i valori di k non compaiono né 6 né 12 e più in generale si è osservato che non possono mai venire utilizzati i primi q divisibili per 6.

Un programma da me realizzato calcola per ogni esponente p i residui di a^p per i primi q della forma $q = kp + 1$ iniziando da $k = 2$ e procedendo per valori crescenti di k pari e non divisibili per 6.

Una volta trovati i residui per un dato valore di q viene eseguita la verifica che essi siano tali da non poter soddisfare l'equazione di Fermat in nessuna combinazione di valori possibili, dimostrando in tal modo che $q \mid xyz$, e verificando contemporaneamente che tra i residui non sia presente p.

Se entrambe le condizioni sono verificate, il I caso dell'UTF è certamente vero per l'esponente p; in caso contrario si riproverà con un successivo valore di k.

Dall'analisi dei risultati per un gran numero di valori dell'esponente p si possono fare le seguenti osservazioni[12]:

1. Il I caso dell'UTF è risultato vero per *tutti gli esponenti* $p < 9857053$. Questo è il primo esponente per cui la tabella dei primi non risulta sufficiente ed è l'unico nell'intervallo $0 \div 10^7$. Al crescere dell'esponente i casi irrisolti aumentano anche se molto lentamente.

2. Al crescere di p il numero dei divisori q di xyz tende ad aumentare.

3. Per ogni p vi è un limite oltre al quale non vi sono più divisori q. Ciò è dovuto al fatto che al crescere del numero k dei residui, le possibili combinazioni aumentano con il cubo di k e l'equazione di Fermat può essere soddisfatta anche da valori non divisibili per q.

[12] A questo scopo si è utilizzato un programma in linguaggio C con le librerie matematiche standard che disponeva di una tabella dei primi fino a $4,239 \cdot 10^9$.

4. I casi nei quali q divide xyz ma tra i residui è presente p, e quindi il I caso dell'UTF non è dimostrabile per tale valore di q, sono piuttosto rari.

   Per curiosità riportiamo qui di seguito una tabella su alcuni casi incontrati. Con a si è indicato un numero per il quale risulta $a^p \equiv p \pmod q$:

Esponente p	Fattore moltiplicat. k	Modulo $q = kp + 1$ q	Valore Base a	Verifica $a^p \pmod q$
13	34	443	411	13
29	68	1973	1873	29
43	136	5849	5578	43
79	250	19751	19370	79
137	1394	190979	187386	137
151	496	74897	73376	151
167	1988	331997	6915	167
191	368	70289	1026	191
3313	34	112643	37548	3313

5. I valori minimi di k, utili alla dimostrazione del I caso, coprono quasi tutti i numeri pari con eccezione dei multipli di 6 e possono anche risultare molto elevati come avviene per $p = 8669777$ per il quale il più piccolo k utile alla dimostrazione vale 458.

Il tempo di calcolo per esaminare tutti i primi compresi tra 3 e 10^7 è stato dell'ordine del minuto primo su un modesto personal computer e si mantiene dello stesso ordine per successivi intervalli della stessa ampiezza.
In alternativa al $TdSG$ ed all'utilizzo dei primi q della forma $kp + 1$ si sarebbe potuto utilizzare l'operatore $\pmod{p^2}$ in grado di dimostrare direttamente il I caso dell'UTF mediante la verifica che qualsiasi combinazione dei residui di a^p se $(a, p) = 1$ non può soddisfare l'equazione di Fermat. Questo però accade solo per alcuni valori particolari dell'esponente p mentre il metodo precedente, per quanto si è potuto verificare, è risultato valido per tutti gli esponenti senza eccezioni.
Ad esempio per $p < 100$ l'operatore $\pmod{p^2}$ è in grado di dimostrare il I caso soltanto per i seguenti primi: 3, 5, 11, 17, 23, 29, 41, 47, 53, 71, 89.
Si è trovato inoltre che la dimostrazione è possibile per $p = 3$ anche con $\pmod{p^3}$, per $p = 5$ anche con $\pmod{p^3}$, $\pmod{p^4}$, e $\pmod{p^5}$, per $p = 11$ anche con $\pmod{p^3}$, e infine per $p = 17$ anche con $\pmod{p^3}$.
A conclusione di questo paragrafo i cui risultati sono il frutto degli innumerevoli calcoli effettuati per la dimostrazione del I caso dell'UTF per moltissimi esponenti ci è sorto il dubbio che siano vere le seguenti due congetture:

1. *Dato un qualsiasi primo p il numero di primi q della forma $q = kp + 1$ è infinito.*
2. *Al tendere all'infinito dell'esponente p, il numero dei divisori q della forma $q = kp+1$ tende ad infinito.*

Restano inoltre irrisolte due domande che sorgono spontanee e che è lasciata alla riflessione dei miei pochi lettori:

1. *Perché i primi q quando $6 \mid k$ non possono essere utilizzati per dimostrare il I caso dell'UTF?*
2. *E' possibile trovare una relazione che individui i valori di p e q che danno luogo a residui uguali a p come nella tabella sopra riportata?.*

10 Caso II - L'esponente p divide xyz

Sulla base del fatto che il I caso dell'UTF risulta virtualmente dimostrato, da qui in avanti faremo l'ipotesi che l'esponente p divida sempre xyz.

Le espressioni analitiche delle 6 quantità precedentemente introdotte si ottengono anche in questo caso prendendo le radici p-esime delle seguenti relazioni dove supponiamo senza perdere di generalità che la variabile divisibile per p sia la x:

$$\begin{aligned} r^p &= p\,(z-y) & R^p &= \frac{1}{p}\,(z^{p-1} + z^{p-2}\,y + \,\ldots\, + z^2\,y^{p-3} + z\,y^{p-2} + y^{p-1}) \\ s^p &= (z-x) & S^p &= (z^{p-1} + z^{p-2}\,x + \,\ldots\, + z^2\,x^{p-3} + z\,x^{p-2} + x^{p-1}) \\ t^p &= (x+y) & T^p &= (x^{p-1} - x^{p-2}\,y + \,\ldots\, + x^2\,y^{p-3} - x\,y^{p-2} + y^{p-1}) \end{aligned} \tag{25}$$

In questo secondo caso le relazioni da soddisfare dalle variabili della TdF saranno di conseguenza:

$$\begin{aligned} x &= \frac{1}{2}\left(t^p - s^p + \frac{1}{p}\,r^p\right) \\ y &= \frac{1}{2}\left(t^p + s^p - \frac{1}{p}\,r^p\right) \\ z &= \frac{1}{2}\left(t^p + s^p + \frac{1}{p}\,r^p\right) \end{aligned} \tag{26}$$

Analogamente la quantità α viene espressa dalla relazione:

$$\alpha = \frac{1}{2}\left(t^p - s^p - \frac{1}{p}\,r^p\right)$$

L'espressione per u^p è uguale a quella del caso I divisa per p:

$$u^p = \frac{(p-1)!}{2^{p-2}} \sum \frac{(z-y)^{2i}\,(z-x)^{2j}\,(x+y)^{2k}}{(2i+1)!\;(2j+1)!\;(2k+1)!} \tag{27}$$

Le relazioni (20) e (26) riportate a cui tutte le TdF devono soddisfare, sono note in letteratura come formule di Barlow, dal nome del matematico Peter Barlow (1776-1862) che le scoprì nel 1810, e successivamente sono state dimostrate anche da altri matematici (Abel, Legendre, Germain, Lindemann, Catalan).

11 Considerazioni sui divisori q di xyz se $p \,|\, xyz$

I divisori q trovati in precedenza, che erano serviti a dimostrare il I caso del TdF, continuano a rimanere tali anche nel II caso in quanto lo studio dei residui di $a^p \pmod q$ per $q = kp + 1$ prescinde dalla divisibilità di xyz per p.
Si hanno ora due possibilità a seconda che q divida il prodotto rst oppure RST.
Benché non sia possibile risolvere sempre questo dubbio, tuttavia vi sono casi in cui non solo è possibile dimostrare che $q \,|\, rst$ ma anche che p e q devono dividere entrambe la stessa variabile di Fermat.
Senza perdere di generalità possiamo scegliere arbitrariamente la variabile divisibile per p e procedere alla seguente verifica:

1. Le variabili sono diverse: $p \,|\, x$ e $q \,|\, y$ $(q = kp + 1)$

   Dalla seconda delle (26) tenendo presente che $1/p \equiv -k \pmod q$ otteniamo:

   $$2y \,=\, t^p + s^p - \frac{1}{p}\, r^p \,\equiv\, t^p + s^p + kr^p \,\equiv\, 0 \pmod q \tag{28}$$

   Ora in maniera del tutto analoga a quanto fatto in precedenza nel caso I possiamo verificare numericamente per ciascuna coppia p e $q = kp + 1$ se tutti i possibili valori non nulli di $a^p \pmod q$ e $ka^p \pmod q$ siano o meno compatibili con l'ultima relazione di congruenza[13].

   Nel caso che tale relazione non possa essere soddisfatta da valori non nulli possiamo affermare che $q \mid rst$ e poiché q non divide rt, in quanto r e t sono fattori di x e z a loro volta coprimi con y, e certamente non divide k, dovrà essere $q \mid s$ [14].

   E' questo il caso di cui abbiamo parlato sopra per il quale si può di conseguenza affermare che $q \nmid S$, essendo quest'ultimo coprimo con s.

   Riprendiamo ora dalla terza delle (25) la definizione di T^p ed applichiamo a questa quantità l'operatore $\pmod q$ tenendo presente che $q \mid y$:

   $$T^p \,=\, (x^{p-1} - x^{p-2}\, y + \,\ldots\, + x^2\, y^{p-3} - x\, y^{p-2} + y^{p-1}) \,\equiv\, x^{p-1} \pmod q$$

   In modo analogo operiamo sulla definizione di s^p nella seconda delle (25):

   $$s^p \,=\, z - x \,\equiv\, 0 \pmod q$$

   da cui segue che $z \equiv x \pmod q$.

   Ritornando infine alla seconda delle (25) e sostituendo z con x abbiamo per S^p:

   $$S^p \,=\, (z^{p-1} + z^{p-2}\, x + \,\ldots\, + z^2\, x^{p-3} + z\, x^{p-2} + x^{p-1}) \,\equiv\, px^{p-1} \,\equiv\, pT^p \pmod q$$

   Ora poiché l'inverso di T certamente esiste in quanto q è primo e non divide T, possiamo scrivere:

   $$(S\, T^{-1})^p \,\equiv\, p \pmod q \tag{29}$$

   Siamo così pervenuti ad un risultato perfettamente analogo a quello visto nella dimostrazione del $TdSG$ per cui si può concludere che, se $a^p \pmod q$ non assume mai il valore p, allora l'ipotesi che p e q dividano variabili differenti è falsa (fatti salvi i casi poco frequenti citati nel capitolo precedente).

[13] Nella verifica si dovranno esaminare tutte le possibili combinazioni di valori con l'avvertenza tuttavia di considerare sempre due valori di a^p associati ad un solo valore di ka^p.

[14] Per i primi di Sophie Germain $(q = 2p + 1)$ questa conclusione non è mai vera perché la (28) si può annullare anche se $q \nmid rst$.

2. Le variabili sono coincidenti: $p \,|\, x$ e $q \,|\, x \quad (q = kp + 1)$

   Utilizzando la prima delle (26) possiamo scrivere:

$$2x \,=\, t^p - s^p + \frac{1}{p}\, r^p \,\equiv\, t^p - s^p - kr^p \,\equiv\, 0 \pmod{q}$$

   Verificato a questo punto che in analogia al caso precedente $q \mid r$, riprendiamo ancora dalla terza delle (25) la definizione di T^p ed applichiamo a questa quantità l'operatore (mod q) tenendo presente che $q \mid x$:

$$T^p \,=\, (x^{p-1} - x^{p-2}\, y + \,\ldots\, + x^2\, y^{p-3} - x\, y^{p-2} + y^{p-1}) \,\equiv\, y^{p-1} \pmod{q}$$

   Applichiamo a questo punto lo stesso operatore (mod q) alla prima delle (25):

$$r^p \,=\, p(z - y) \,\equiv\, 0 \pmod{q}$$

   da cui segue che $z \equiv y \pmod{q}$.

   Ritornando infine alla prima delle (25) e sostituendo z con y abbiamo per R^p:

$$R^p \,=\, \frac{1}{p}\,(z^{p-1} + z^{p-2}\, y + \,\ldots\, + z^2\, y^{p-3} + z\, y^{p-2} + y^{p-1}) \,\equiv\, y^{p-1} \,\equiv\, T^p \pmod{q}$$

   Ora poiché l'inverso di T certamente esiste in quanto q è primo e non divide T, possiamo scrivere:

$$(R\, T^{-1})^p \,\equiv\, 1 \pmod{q} \tag{30}$$

   Poiché questa relazione non è contraddittoria e può essere sempre soddisfatta qualunque sia il valore di q, si deve concludere che se q al pari di p divide rst essa dividerà la stessa quantità tra r, s o t divisa da p, salvo i casi eccezionali in cui la (29) fosse verificata..

A questo punto si possono fare le seguenti osservazioni:

1. La relazione (30) a cui si è pervenuti rende immediatamente evidente che è proprio la divisibilità di xyz per p, precedentemente "dimostrata", che fa fallire l'estensione del $TdSG$ al secondo caso a causa della differenza tra la prima delle (19) e la prima delle (25) nei 2 casi dell'UTF.

2. Nel caso $q \,|\, rst$ segue immediatamente che α è sempre divisibile per q in quanto $\alpha = urst$.

Per il momento mi fermo qui con la speranza di avere in futuro nuove idee per proseguire.

12 Conclusioni

E' indubbiamente molto difficile trarre delle conclusioni da quanto scritto.
Purtroppo l'UTF ha resistito e ancora resiste dopo trecento anni a qualsiasi tentativo di risoluzione con i metodi cosiddetti euleriani, mentre la soluzione trovata da Wiles resta con mio rammarico riservata solo a pochi iniziati.
Le note che ho scritto appariranno certamente al molto paziente lettore piuttosto disordinate, anche se ho tentato di riordinarle al meglio prima di rendere pubblico questo scritto. Ciò è dovuto al fatto che esse hanno seguito il flusso dei miei ragionamenti via via che mi si presentavano alla mente; inoltre molte altre direzioni sono state da me esplorate ma non riportate in quanto prive di un qualsiasi sbocco significativo.

Il mio centesimo l'ho messo, ora sta a voi continuare!

A Dimostrazione dell'Ultimo Teorema di Fermat per n = 4

La dimostrazione dell'UTF per $n = 4$ è stata ottenuta da Fermat dimostrando che in nessun triangolo rettangolo l'ipotenusa potrebbe assumere un valore intero se i cateti fossero quadrati perfetti. In altre parole la relazione:

$$(x^2)^2 + (y^2)^2 = z^2 \tag{31}$$

non ammette soluzioni non banali nel campo dei numeri interi.
E' infatti evidente che, se la precedente affermazione venisse dimostrata, a maggior ragione risulterebbe vero l'UTF per $n = 4$ in quanto esso può considerarsi un caso particolare della (31), quando cioè l'ipotenusa z sia anch'essa a sua volta un quadrato perfetto.

La dimostrazione che la (31) non possiede soluzioni intere non banali si basa sull'utilizzo del metodo della *discesa infinita*, metodo particolarmente ingegnoso che si fa risalire allo stesso Fermat.

L'idea di base è quella che, supposta per assurdo l'esistenza di una terna di numeri interi positivi[15] che soddisfi alla relazione (31), sia possibile dedurre da questa una seconda terna x', y' e z' con $0 < z' < z$, che soddisfi anch'essa alla stessa relazione (31).
Ripetendo indefinitamente questo procedimento si dovrebbe trovare una terna con $z' = 1$ oltre la quale non sarebbe più possibile continuare. Ma poiché una tale terna non esiste, ne consegue che l'ipotesi iniziale era falsa e di conseguenza l'UTF risulta dimostrato per $n = 4$.

La stessa conclusione si ottiene ancora più semplicemente supponendo che la terna inizialmente scelta sia già per ipotesi quella che possiede il valore minimo di z, e quindi il fatto stesso di poter trovare una seconda terna di numeri con $0 < z' < z$, dimostra che l'ipotesi di una terna minimale per z è assurda e di conseguenza cade anche l'ipotesi dell'esistenza di una qualsiasi terna.

Si può inoltre supporre senza alcuna limitazione che la terna sia strettamente coprima e che di conseguenza una sola delle tre quantità sia pari, mentre le altre due saranno dispari.

E' facile dimostrare che nel caso in esame z non può essere pari in quanto in tal caso sarebbe somma di due quadrati dispari. Ora tutti i numeri dispari sono del tipo $4k + 1$ oppure $4k + 3$, ma i loro quadrati sono solamente del tipo $4k + 1$ e quindi la somma di due quadrati dispari è sempre del tipo $4k + 2$, ma quest'ultima espressione, non essendo divisibile per 4, non può essere il quadrato di un numero pari e di conseguenza z deve essere certamente dispari.

Infine se z è dispari le altre due variabili x ed y non potranno che avere differente parità affinché la somma delle loro quarte potenze sia dispari.

Fatte queste premesse veniamo ora alla dimostrazione vera e propria.

Interpretando la (31) come un caso particolare del teorema di Pitagora ed assumendo senza perdere di generalità che x sia la variabile pari ed y quella dispari, le soluzioni se esistono saranno certamente esprimibili mediante le formule (18) che qui per chiarezza riscriviamo:

$$x = 2mn \qquad y = n^2 - m^2 \qquad z = n^2 + m^2$$

Nel caso presente, sostituendo x^2 ed y^2 a x ed y, avremo:

$$x^2 = 2mn \qquad y^2 = n^2 - m^2 \qquad z = n^2 + m^2$$

dove $n > m > 0$ e m ed n sono coprimi e di parità diversa.
Ora dalla seconda relazione riscritta come:

$$m^2 + y^2 = n^2$$

risulta che n dovrà essere dispari per le stesse ragioni addotte precedentemente per z, mentre essendo y dispari, m sarà di conseguenza necessariamente pari.

[15] Essendo l'esponente pari non si introducono limitazioni nel considerare le sole soluzioni con interi positivi.

Per quest'ultima relazione utilizziamo nuovamente le (18) introducendo due nuove quantità m' ed n' tra loro coprime con $n' > m' > 0$:

$$m = 2m'n' \qquad y = n'^2 - m'^2 \qquad n = n'^2 + m'^2$$

Sostituendo le espressioni di m ed n nella relazione $x^2 = 2mn$ si ottiene:

$$x^2 = 4m'n'(n'^2 + m'^2)$$

Ma il prodotto $m'n'(n'^2 + m'^2)$ a secondo membro è formato da tre termini tra loro coprimi e di conseguenza ciascuno di essi deve essere un quadrato perfetto di tre nuove variabili x', y' e z' certamente positive e a loro volta coprime per cui si può scrivere:

$$m' = x'^2 \qquad n' = y'^2 \qquad n'^2 + m'^2 = z'^2$$

Finalmente sostituendo le prime due espressioni nella terza otteniamo:

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

che riproduce esattamente l'equazione di partenza nelle nuove variabili x', y' e z'.
Essendo $z' > 0$ resta solo da dimostrare che è vera la relazione $z' < z$.
Sostituendo nella relazione $z = n^2 + m^2$ le variabili n ed m prima trovate si ha:

$$z = (n'^2 + m'^2)^2 + 4m'^2n'^2 > (n'^2 + m'^2)^2 = z'^4 > z'$$

essendo sicuramente $z' > 1$.

Contents

List of Tables

References

[1] Claudio Beccari, *LaTeX, Guida ad un sistema di editoria elettronica*, Editore Ulrico Hoepli, Milano, 1991

[2] Paulo Ribenboim, *Fermat's Last Theorem For Amateurs*, Springer-Verlag New York, Inc., 1999