

Block Notes Matematico

Sulle soluzioni intere delle equazioni di grado n a più variabili

La congettura EUTF e la congettura $n=k$

ing. Rosario Turco

Abstract

In questo articolo l'autore esamina il problema della ricerca di soluzioni intere per equazioni a più variabili di grado n ; inoltre introduce la teoria delle congruenze, una tecnica più semplice che permette di stabilire l'esistenza di soluzioni primitive. L'articolo è, quindi, anche un attraversamento storico di tecniche disponibili su tale argomento.

Introduzione

Il problema della ricerca delle soluzioni intere di una equazione a più variabili, tutte dello stesso grado n , è un problema classico, che coinvolge le equazioni diofantee, l'ultimo Teorema di Fermat etc.

L'Ultimo Teorema di Fermat (UTF) afferma che "l'equazione $x^n + y^n = c^n$, con $n > 2$, non ammette soluzioni intere".

Una possibile estensione dell'UTF potrebbe essere la **Congettura EUTF**, proposta dall'autore e da dimostrare:

"L'equazione

$$x_1^n + x_2^n + x_3^n + \dots + x_k^n = c^n \quad (1)$$

ammette sempre soluzioni intere se e solo se $n = k$ "

La congettura ipotizza che si otterrebbero sempre soluzioni intere se il numero di variabili (o dimensioni) è uguale al grado n dell'equazione. Il nome EUTF deriva dal fatto che la congettura rappresenta una estensione dell'UTF; in particolare se è vera la congettura EUTF, di conseguenza, è vero anche l'UTF, già dimostrato da Andrew Wiles; l'EUTF sarebbe in altri termini un ulteriore percorso dimostrativo dell'UTF.

Nel seguito sono mostrate le evidenze ed eventuali percorsi di dimostrazione dell'EUTF.

Definizioni

Alcune definizioni di partenza. *Una soluzione si dice banale* se è rappresentata da un insieme di numeri tutti uguali. Ad esempio l'equazione dell'UTF ha come soluzione banale $(0,0)$. *Una soluzione non banale primitiva* è una qualsiasi soluzione o insieme di valori che non hanno multipli in comune.

Le evidenze di una congettura EUTF

I casi da considerare sono tre:

- $n < k$
- $n = k$
- $n > k$.

Iniziamo a vedere le evidenze o tracce che suggeriscono la congettura.

Caso $n < k$

Se $n < k$ abbiamo situazioni che non sempre hanno soluzioni intere. Un primo esempio è costituito dalle equazioni diofantee di primo grado del tipo:

$$ax + by = c$$

In esse è evidente che $k=2$ e $n=1$. È noto che essa ammette soluzioni se il termine c è un multiplo del MCD(a,b). In altri termini non ammette sempre soluzioni.

Sempre con $n < k$ possiamo fare un altro esempio, di grado maggiore all'esempio precedente, come l'equazione

$$x^2 + y^2 - 3z^2 = 0 \quad (1)$$

Questa equazione ha $k=3$ e $n=2$, la definiremo nel seguito come *equazione trinomia di secondo grado*. La (1) non ha soluzioni intere primitive ma ha sicuramente soluzioni reali non banali. Difatti poniamo $x = 2X+Y-Z$, $y = X + 2Y - Z$ e $z = -X - Y + Z$ da qui l'equazione di partenza (1) diventa:

$$2X^2 + 2XY + 2Y^2 - Z^2 = 0 \quad (2)$$

Dalla (2) si passa alla (1) se si pone che $X = x + z$, $Y = y + z$, $Z = -x + y - 3z$. Lo studio della (2) fu uno dei primi lavori di Fermat. Possiamo osservare che se (km, kn, kp) fosse una soluzione non banale della (2) allora una soluzione primitiva si ottiene dividendola per il MCD k , ottenendo cioè (m,n,p) ; per cui sarebbe vera l'identità:

$$2m^2 + 2mn + 2n^2 = p^2 \quad (3)$$

Dalla (3) poichè a destra dell'uguaglianza abbiamo termini tipici di forma $2k$, quindi pari, allora p^2 e p sono pari. Inoltre per il concetto di soluzione primitiva, almeno uno tra m ed n è dispari; ma se è vero questo arriviamo ad una contraddizione, perché $2m^2 + 2mn + 2n^2$ non può essere divisibile per 4 mentre p è pari e p^2 , quindi, è divisibile per 4; per cui la (3) è in contraddizione. Ovviamente abbiamo anche tenuto conto che il prodotto di due pari è pari, il prodotto di due dispari è dispari, il prodotto di un pari e un dispari è pari.

Il caso $n < k$, quindi, in alcuni casi può avere soluzioni ed in altri no.

Caso $n = k$

Col caso $n = k$ esistono molte evidenze dell'esistenza di identità che rivelano la presenza di soluzioni intere (anche negative se n è dispari):

$$3^2 + 4^2 = 5^2 \quad \text{terna pitagorica}$$

$$1^3 + 12^3 + (-9)^3 = 10^3 \quad \text{quaterna di Ramanujan}$$

È facile implementare un algoritmo per tentativi, in PARI/GP, per trovare soluzioni intere per n qualsiasi. Maggiore è l'intervallo di interi esaminato, maggiore è il numero di soluzioni che si possono trovare, proprio perché potenzialmente sono infinite.

Caso $n > k$

È il caso dell'UTF. Se $n = 3$ e $k=2$ non ha nessuna soluzione intera non banale. L'UTF ha una dimensione in meno rispetto a n . Se fosse vera la congettura EUTF, l'UTF ne sarebbe un corollario.

Teoria delle congruenze

Occorre fare poi altre considerazioni. Sia, ad esempio, $a x^2 + b y^2 + c z^2 = 0$ l'equazione trinomia di secondo grado con $abc \neq 0$ e senza fattori in comune, sia (m, n, p) una soluzione primitiva dell'equazione.

Ora un approccio d'analisi prevede in generale due possibilità:

- Per ogni intero h potremmo trovare degli interi (X, Y, Z) , senza fattori in comune, tali che $aX^2 + bY^2 + cZ^2 = 0$ è divisibile per h . Basta, difatti, scegliere $X = m$, $Y = n$, $Z = p$. Qui stiamo ipotizzando il caso in cui esista la soluzione primitiva.
- Al contrario, non sapendo se l'equazione $a x^2 + b y^2 + c z^2 = 0$ abbia effettivamente soluzioni primitive, ammettendo di aver trovato un intero h per cui non riusciamo a trovare degli interi (X, Y, Z) , senza fattori in comune, tali che $aX^2 + bY^2 + cZ^2 = 0$ è divisibile per h , allora h è un *contro-esempio* che ci fa concludere che la nostra equazione non ammette soluzioni primitive.

L'approccio di analisi di cui sopra è abbastanza efficace perché è più facile andare alla ricerca di un intero h per cui l'equazione è divisibile, anziché cercare le soluzioni primitive. Non dimentichiamo che equazioni di questo tipo hanno potenzialmente infinite soluzioni.

Per sfruttare l'approccio di sopra dobbiamo introdurre le congruenze (vedi [1]). Tali tecniche erano note a *Fermat* e *Legendre* e furono perfezionate da *Gauss*.

Siano r, s, t tre interi. Il simbolismo $r \equiv s \pmod{t}$ si legge dicendo: " r congruo s modulo t ", se $r-s$ è multiplo di t .

Ora sia data una equazione del tipo $a x^2 + b y^2 + c z^2 = 0$ con a, b, c coefficienti non nulli e sia data una terna di interi (m, n, p) tali che:

$$a m^2 + b n^2 + c p^2 \equiv 0 \pmod{h} \quad (4)$$

Cioè tale che la parte sinistra della congruenza sia divisibile per h . Allora la (4) è la soluzione della congruenza associata alla equazione. Queste tecniche sono state usate anche nella congettura di Birch e Swinnerton-Dyer (vedi [4]).

Occorre tener presente che ogni soluzione di una equazione è sicuramente anche soluzione della congruenza associata all'equazione, il contrario non è sempre vero. Ad esempio la terna $(0,1,1)$ è soluzione della congruenza $2x^2 + y^2 + z^2 \equiv 0 \pmod{2}$ ma non è soluzione dell'equazione $2x^2 + y^2 + z^2 = 0$.

Le congruenze sono comunque oggetti più semplici da trattare rispetto alle equazioni. Difatti se esiste una soluzione (m,n,p) di una congruenza modulo h , allora esiste anche una soluzione (m',n',p') tale che m',n',p' sono interi compresi tra 0 e $h-1$. Se (m,n,p) sono tre interi soluzioni della congruenza $ax^2 + by^2 + cz^2 \equiv 0 \pmod{h}$; se chiamiamo r_m, r_n, r_p i resti di m,n,p nelle divisioni con h , ovviamente r_m, r_n, r_p sono interi compresi tra 0 e $h-1$. Inoltre è dimostrabile che la terna (r_m, r_n, r_p) è anch'essa soluzione della congruenza dell'equazione, ovvero divisibile per h .

Difatti possiamo riscrivere il tutto nel seguente modo:

$$am^2 + bn^2 + cp^2 = a[(m-r_m) + r_m]^2 + b[(n-r_n) + r_n]^2 + c[(p-r_p) + r_p]^2 =$$

$$[(m-r_m)(a(m-r_m) + 2ar_m) + (n-r_n)(a(n-r_n) + 2ar_n) + (p-r_p)(a(p-r_p) + 2ar_p) + ar_m^2 + br_n^2 + cr_p^2]$$

Il primo membro è divisibile per h per cui lo deve essere anche l'ultimo termine nella quadra ed il termine $ar_m^2 + br_n^2 + cr_p^2$. Quindi anche $ar_m^2 + br_n^2 + cr_p^2$ è soluzione della congruenza.

Il risultato che abbiamo dimostrato è che una congruenza è risolubile se e solo se esiste una soluzione costituita da numeri compresi tra 0 e $h-1$. Decidere se una congruenza ammette soluzioni è un qualcosa che si decide in pochi passi, al contrario di trovare le soluzioni intere di un'equazione.

Quindi per dimostrare che l'equazione (2), nel caso $n < k$, non ha soluzioni intere primitive, si deve cercare un intero h tale che la congruenza associata alla equazione modulo h , sia priva di soluzioni primitive. Difatti Fermat ed altri hanno così dimostrato che la (2) non soluzioni primitive.

Il **Teorema di Legendre** afferma che "per le equazioni di secondo grado (o trinomie di secondo grado), l'esistenza di soluzioni primitive di ogni congruenza associata non è solo condizione necessaria per l'esistenza di soluzioni primitive dell'equazione stessa, ma è anche condizione sufficiente".

Questo Teorema non è però vero per equazioni di grado maggiore di 2. Ad esempio ogni congruenza associata all'equazione $3x^3 + 4y^3 + 5z^3 = 0$ ammette soluzioni primitive ma l'equazione ammette solo la soluzione intera banale.

Sempre sulle equazioni di grado 2 occorre aggiungere due altri risultati del passato:

- Le equazioni trinomie del tipo $z^2 = ax^2 + by^2$ ammettono soluzioni intere non banali (ad esempio $(0,1,1)$)
- Il concetto di *residuo quadratico modulo un intero*, che spieghiamo di seguito

Metodo di Lagrange dei residui quadratici

Introduciamo il concetto di residuo quadratico modulo un intero: "Un intero a è un residuo quadratico modulo b , se esiste un intero c tale che $a \equiv c^2 \pmod{b}$ " (vedi [2]).

Il metodo che esamineremo è basato su 4 passi.

Riprendiamo l'equazione:

$$ax^2 + by^2 + cz^2 = 0$$

con $abc \neq 0$. Si suppone anche che a , b e c non abbiano lo stesso segno altrimenti sono possibili solo soluzioni banali.

Primo passo

Si trasforma l'equazione nella forma $z^2 = Ax^2 + By^2$, dove A e B non sono entrambi negativi e sono privi di quadrati. Per poterlo fare abbiamo bisogno di fare una *trasformazione lineare* cioè introducendo nuove variabili x', y', z' :

$$x = a_{11}x' + a_{12}y' + a_{13}z'$$

$$y = a_{21}x' + a_{22}y' + a_{23}z'$$

$$z = a_{31}x' + a_{32}y' + a_{33}z'$$

Da qui è evidente che abbiamo a che fare con una matrice, i cui elementi a_{ij} sono tali che la matrice è razionale con determinate non nullo e quindi invertibile. È dimostrato che se il determinante non è nullo, ogni soluzione intera della prima equazione è soluzione intera anche della seconda e viceversa.

Secondo passo

Occorre verificare se A e B sono uguali a 1, se è così l'equazione ammette soluzioni primitive e si risale alle soluzioni dell'equazione di partenza.

Terzo passo

Si controlla se l'equazione $z^2 = Ax^2 + By^2$ è priva di soluzioni primitive; cioè se $|A| \leq |B|$ e se $|A|$ non è residuo quadratico modulo $|B|$ allora l'equazione non ammette soluzioni primitive. (Vedi [2] per la dimostrazione).

Quarto passo

Se al terzo passo non si conclude che l'equazione non ammette soluzioni primitive, occorre determinarne il carattere, facendo una ulteriore trasformazione lineare che trasformi l'equazione $z^2 = Ax^2 + By^2$ dove A è residuo quadratico modulo B in una equazione $z^2 = A'x^2 + B'y^2$ dove $|B'| < |B|$ e si riprende dal passo 2, secondo questo metodo che fu battezzato da Fermat come metodo a discesa infinita.

Lagrange dimostrò che dopo un numero di passi finiti l'equazione di partenza si trasforma in una equazione $z^2 = Ax^2 + By^2$ dove $B = \pm 1$ e quindi si può risalire nella catena di trasformazioni lineari alle soluzioni intere della equazione di partenza oppure al terzo passo si stabilisce che l'equazione è priva di soluzioni primitive. Il metodo di Lagrange è valido per una equazione trinomia però.

Esempio

$$234x^2 - 18y^2 - 2z^2 = 0$$

Dividendola per 2 la rimettiamo nella forma del primo passo di cui sopra:

$$z^2 = 117x^2 - 9y^2 \quad (5)$$

Operiamo la trasformazione lineare:

$$x' = 1/3 x$$

$$y' = 1/3 y$$

$$z' = z$$

Otteniamo:

$$z'^2 = 13x'^2 - y'^2 \quad (6)$$

Se (m,n,p) è soluzione della (6) allora $(3m,n,p)$ è soluzione della (5). Viceversa se (α,β,γ) sono soluzione della (5) allora $(\alpha/3,\beta/3,\gamma)$ sono soluzioni della (6).

Il secondo passo non è vero e dobbiamo passare al terzo passo. La (6) la rimettiamo in una forma equivalente in modo da garantire che $|A| \leq |B|$:

$$z'^2 = -x'^2 + 13y'^2 \quad (7)$$

Controllando l'equazione ottenuta risulta che $A = -1$ $B=13$, ora -1 è un residuo quadratico modulo 13.

Difatti il concetto di residuo quadratico è che $A = c^2 \pmod B$, il che equivalente alle seguenti due forme

$$A - c^2 = 0 \pmod B$$

$$A - c^2 = kB$$

Se usiamo la seconda forma troviamo subito $-1 - 5^2 = 2 \cdot 13$ oppure $-26 \pmod{13} = 0 \pmod{13}$. Per cui non possiamo concludere ancora che non ammette soluzioni primitive e dobbiamo applicare anche il quarto passo.

Possiamo pensare di applicare una trasformazione lineare del tipo:

$$x' = (5/26)X + (1/26)Z$$

$$y' = (1/13)Y$$

$$z' = (5/26)Z - (1/26)X$$

Effettuando le sostituzioni nella (7) otteniamo:

$$Z^2/26 = -X^2/26 + Y^2/13$$

Da cui moltiplicando per 26 si ottiene (possiamo anche cambiare le variabili in x,y,z, perché non ci interessano i valori delle soluzioni ma solo se l'equazione ammette soluzioni):

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

Qui $|B'| < |B|$.

Ora per questa equazione occorre iterare il passo 2 e così via (*metodo a discesa* introdotto da Fermat: uno dei più grandi contributi alla teoria dei numeri). lasciamo al lettore il prosieguo, si arriva a $B = 1$.

Legendre

Il metodo di Lagrange stabilisce se un'equazione trinomia ammette soluzioni intere e permette con un procedimento a ritroso di trovarle. Tale metodo non stabilisce però a partire dai coefficienti a,b,c se l'equazione è risolvibile.

Legendre formulò prima il **Teorema 1**: *“Sano a,b,c coefficienti non tutti dello stesso segno, che abc sia non nullo e privo di quadrati, allora l'equazione trinomia $ax^2 + by^2 + cz^2 = 0$ ammette una soluzione intera non banale se e solo se $-bc$, $-ca$ e $-ab$ sono residui quadratici modulo $|a|$, modulo $|b|$, modulo $|c|$ rispettivamente”.*

Una seconda formulazione è il seguente **Teorema 2**: *“Sano a,b,c interi non tutti dello stesso segno, non nulli e privi di quadrati; allora l'equazione trinomia $ax^2 + by^2 + cz^2 = 0$ ammette una soluzione intera non banale se e solo le congruenze $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p^n}$ hanno soluzioni proprie per ogni potenza p^n di ogni primo p.”*

In sintesi il teorema 2 afferma che un'equazione trinomia di secondo grado ha soluzioni primitive se e solo se ha una soluzione reale (con a,b,c, non dello stesso segno) e le congruenze associate hanno soluzioni primitive. Questo alla fine è vero anche per le forme quadratiche non degeneri con un numero qualsiasi di variabili (Teorema di Hasse).

Equazioni trinomie di terzo grado

La congettura è interessata ad equazioni tali che $n = k$, di qualsiasi grado $n=1,2,3,4,5,\dots$; quindi nel caso della equazione trinomia interessa un'equazione trinomia di terzo grado:

$$x^3 + y^3 + z^3 = 0$$

Le congruenze associate all'equazione hanno soluzioni primitive, per cui l'equazione ha soluzioni; occorre solo verificare di che tipo: solo intere banali oppure anche intere non banali.

Equazioni di quinto grado

Sperimentalmente con un algoritmo in PARI/GP (vedi Appendice) si è verificata la congettura EUTF con una equazione di quinto grado in un intervallo numerico (-100,100) per le tre situazioni $n < k$, $n = k$, $n > k$ sia in termini di ricerca di soluzioni intere dell'equazione sia delle soluzioni intere della congruenza (modulo 10) associate all'equazione:

$$x_1^n + x_2^n + x_3^n + x_4^n + x_5^n = 0$$

Il risultato è nella tabellina seguente.

n vs k	Soluzioni intere equazione	Soluzioni intere congr. mod 10
n=4 k=5	NO	SI
n=5 k=5	SI	SI
n=6 k=5	NO	SI

La tabella porta anche ad una ulteriore possibile **Congettura n = k**: "Per $n = k$ se la congruenza associata all'equazione $x_1^n + x_2^n + x_3^n + x_4^n + \dots + x_k^n = 0$ ammette soluzioni intere allora anche l'equazione ammette soluzioni intere".

Conclusioni

L'articolo ha cercato di dare delle evidenze sulla veridicità della congettura EUTF e sulla congettura $n=k$.

APPENDICE

L'algoritmo presentato sfrutta l'algoritmo di Newton per la radice n-esima.

```
PATHLOG="J:\\Work\\MAT\\SRCPARI\\anum";
```

```
myfile = Str(PATHLOG, "\\list5.txt");
```

```
f(x,n,N)=local(); {
```

```
o=x^n-N;
```

```
return(o);
```

```
}
```

```
f1(x,n)=local(); {
```

```
o=n*x^(n-1);
```

```
return(o);
```

```
}
```

```
/*
```

```
* Algorithm of Newton for n-th root
```

```
* N: number
```

```
* n: exponent of the root
```

```
* x0: start value example 1.5
```

```
* c : number of the iterations
```

```
*/
```

```

Newt(x0, n, N, c=10) = local(i=0); {
x = x0;
if( c > 1,
for(i=2,c,
a = f(x, n, N)/f1(x,n);
x = x - a;
);
);
return(x);
}

/*
* It searches in a interval negative to positive (an, ap)
* solutions trivial and not trivial. It marks with '*'
* the solutions not trivial and returns their total.
*
*/

S5(an, ap, n, mod=0, h=10) = local(bn=0,bp=0,i=0, j=0,k=0, l=0, m=0, tot=0); {
if( mod == 1,
myfile = Str(PATHLOG, "\\list5Mod.txt");
);
if( mod == 0,
myfile = Str(PATHLOG, "\\list5.txt");
);
print("pow : ", n);
write(myfile, "pow : ", n, " an = ", an, " ap = ", ap, " h = ", h, " mod = ", mod);
for( i = an, ap,
for( j = an, ap,
for( k = an, ap,
for( l = an, ap,

```


This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.