Bollettino Unione Matematica Italiana

Giovanni Vacca

Equazioni indeterminate in numeri interi. Osservazioni sull'ultimo teorema di Fermat

Bollettino dell'Unione Matematica Italiana, Serie 1, Vol. **1** (1922), n.2-3, p. 44–47.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1922_1_1_2-3_44_1>

Equazioni indeterminate in numeri interi. Osservazioni sull'ultimo teorema di Fermat.

Nota di GIOVANNI VACCA

Scopo di questa nota è quello di offrire alcuni risultati assai semplici, forse finora inosservati, i quali aprono la via a nuove ricerche di carattere assai generale.

1. Una classe molto estesa di equazioni indeterminate, aventi almeno una soluzione, del tipo:

(1) $$Fa + Fb = Fc$$

dove a, b, c sono interi ed F una funzione a valori interi [1], si ottiene supponendo:

$$(2) \qquad Fx = fx(ga + gb - gc) - gx(fa + fb - fc)$$

dove fx, gx sono funzioni completamente arbitrarie. Qualunque esse siano, si ha sempre: $Fa + Fb = Fc$.

Se per esempio, nella (1) si pone: $gx = 1$, $fx = x^2 + 1$, si ha: $Fx = x^2 - (a^2 + b^2 - c^2)$, che dà soluzioni ovvie.

2. È interessante cercare la soluzione della (1) quando si ponga $Fx = x^3 + k$ dove k è un numero intero, ovvero cercare le soluzioni intere della:

$$(3) \qquad a^3 + b^3 = c^3 - k.$$

Questa equazione non ha alcuna soluzione per $k = 4$, $k = 5$, come si vede facilmente, osservando che ogni cubo è della forma $9n$ ovvero $9n + 1$.

Il caso $k = 0$ conduce alla impossibilità dimostrata da FERMAT. Se è impossibile la (3) quando k è della forma $9n \pm 4$, è invece possibile se k è di una delle forme $9n \pm 1$, ± 2, ± 3. Ma non sembra facile dimostrare che esistano effettivamente soluzioni per ognuno di tali valori di k.

Analogamente si vede subito che l'equazione $a^4 + b^4 = c^4 - k$ è insolubile in numeri interi se k è un intero della forma $16n + r$, dove r è un intero compreso tra 3 e 13, perchè ogni potenza quarta di un numero intero ha una delle forme $16n$, $16n + 1$.

3. Si possono facilmente trovare funzioni intere di qualsivoglia grado, per le quali la (1) ha sempre una soluzione.

Basta osservare che se n è un intero positivo, se si pone:

$$Fx = \frac{(x + n)!}{x!},$$

la (1) è risolubile ponendo $a = b = n - 1$, $c = n$.

Quindi, mentre è impossibile trovare un cubo somma di due cubi, è invece possibile trovare un numero piramidale, somma di due piramidali. Oltre alla soluzione precedente, data dalla identità:

$$3 \cdot 4 \cdot 5 + 3 \cdot 4 \cdot 5 = 4 \cdot 5 \cdot 6,$$

[1] Seguendo l'uso dei classici, LAGRANGE, GAUSS, etc. se f è un segno di funzione, scriverò fx invece di $f(x)$, notazione oggi più usata, ma non soddisfacente.

se ne hanno però altre; per esempio:

$$8 \cdot 9 \cdot 10 + 14 \cdot 15 \cdot 16 = 15 \cdot 16 \cdot 17.$$

4. Si possono pure trovare altre funzioni di qualsivoglia grado per cui la (1) non ha alcuna soluzione. Se si pone, essendo sempre n un numero intero positivo, $Fx = \frac{(x+n)!}{x!} + k$, dove k è un numero intero positivo, minore di $n! - 1$, la (1) è sempre insolubile in numeri interi, come appare osservando che $Fa + Fb - Fc - k$ è divisibile per $n!$ mentre k non lo è.

Si vede così che mentre è difficilissimo stabilire l'esistenza o la non esistenza di soluzioni della (1) per alcune espressioni della F per mezzo di polinomi di grado n, a coefficienti interi, è invece facilissimo risolvere tale problema allorchè questi polinomî hanno forme speciali.

5. Un'altra estensione dell'ultimo teorema di FERMAT è suggerita da una ricerca iniziata molti anni or sono da ANGELO GENOCCHI, ma passata inosservata.

L'equazione $a^3 + b^3 = c^3$, impossibile in numeri razionali, è invece possibile se si scelgono a, b, c tra i numeri della forma $p + \sqrt{q}$, dove p, q sono interi. Così ad esempio:

$$(9 + \sqrt{5})^3 + (9 - \sqrt{5})^3 = 12^3; \quad (\sqrt{85} - 1)^3 + 8^3 = (\sqrt{85} + 1)^3, \text{ etc.}$$

Invece GENOCCHI ha dimostrato [1] (partendo da un risultato di LAMÉ) che l'equazione $a^7 + b^7 = c^7$ è impossibile anche se si cerchino i numeri a, b, c tra le radici delle equazioni di terzo grado a coefficienti razionali.

Ma questa equazione è ovviamente possibile ricercando a, b, c tra i numeri che si ottengono risolvendo successivamente un'equazione di secondo grado e poi una di terzo grado, a coefficienti razionali. (Si ottengono considerando l'equazione indeterminata in numeri razionali: $(a+1)^7 - (a-1)^7 = b^7$).

Parimenti $a^5 + b^5 = c^5$ è risolubile quando si cerchino a, b, c tra le radici di una equazione di quarto grado a coefficienti razionali, risolubile per mezzo di due equazioni di secondo grado.

Si può quindi indurre che se n è un numero primo, l'equazione $a^n + b^n = c^n$ si possa risolvere soltanto cercando a, b, c tra

[1] A. GENOCCHI: *Dei congrui di Leonardo Pisano*, (estr. dal *Cimento*, vol. VI, fasc. 8), Torino, 1855, pag. 12, nota.

le radici di una equazione a coefficienti razionali di grado $n-1$, e che inoltre le radici di questa equazione si possano ottenere risolvendo successivamente α equazioni di grado p, β equazioni di grado q, etc. dove si supponga $n-1$ decomposto nei suoi fattori primi: $n-1=p^\alpha q^\beta \ldots$.

Resta da indagare se, come accade per $n=3$, $n=5$, $n=7$, $n=11$, questo sistema di equazioni sia irriducibile, come accade nella teoria della divisione del circolo, come è stato dimostrato da Gauss.

Si avrebbe allora la dimostrazione di un teorema assai più preciso e comprensivo di quello enunciato da Fermat.

Firenze, 14 ottobre 1922.