Bollettino
Unione Matematica Italiana

Antonio Battaglia

Un caso d'impossibilità dell'equazione indeterminata: $x^{2n} + y^{2n} = z^2$.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **12** (1957), n.4, p. 689–694.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1957_3_12_4_689_0>

Bollettino dell'Unione Matematica Italiana, Zanichelli, 1957.

Un caso d'impossibilità dell'equazione indeterminata: $x^{2n} + y^{2n} = z^2$.

Nota di ANTONIO BATTAGLIA (a Crotone)

Sunto. - *Si dimostra che l'equazione indeterminata* $x^{2n} + y^{2n} = z^2$ *non ha soluzioni in numeri interi se* n *è primo, quando* z *è primo con* n *ed è* $x^2 + y^2 = P^{2c}$ *con* P *primo,* c *intero positivo.*

Summary. - *The purpose of this paper is to demonstrate that diophantine equation* $x^{2n} + y^{2n} = z^2$ *is impossible if* n *is a prime number non comprised* 3, *when is satisfied the condition:* $x^2 + y^2 = P^{2c}$, P *a prime number,* c *a positive integer.*

1. È facile vedere che basta limitarsi al caso in cui x, y. z son primi tra di loro, infatti sia d il massimo comun divisore di x ed y, posto $x = dx_1$, $y = dy_1$ l'equazione

$$x^{2n} + y^{2n} = z^2 \tag{1}$$

si scrive

$$x_1^{2n} + y_1^{2n} = \left(\frac{z}{d^n}\right)^2;$$

ponendo $\frac{z}{d^n} = z$, si ha

$$z_1^{2n} + y_1^{2n} = z_1^2$$

che è della stessa forma di (1).

2. Si può vedere che x ed y non possono essere entrambi dispari perchè il primo membro di (1) avrebbe in questa ipotesi la forma $4h + 2$ che non si può attribuire a z^2 pari, consegue che x è pari, y e z dispari.

3. Dimostriamo che i numeri

$$x^2 + y^2 \text{ e } (x^2)^{n-1} - (x^2)^{n-2}y^2 + (x^2)^{n-3}(y^2)^2 - \dots + (y^2)^{n-1}$$

fattori di $x^{2n} + y^{2n}$ son primi tra di loro quando z è primo con n. Supponiamo $n = 5$; per una ben nota formula di WARING si ha:

$$\begin{aligned}(x^2)^5 + (y^2)^5 &= (x^2 + y^2)^5 - 5x^2y^2(x^2 + y^2)^3 + 5(x^2)^2(y^2)^2(x^2 + y^2) = \\ &= (x^2 + y^2)[(x^2 + y^2)^4 - 5x^2y^2(x^2 + y^2)^2 + 5(x^2)^2(y^2)^2],\end{aligned}$$

ma è anche:

$$(x^2)^5 + (y^2)^5 = (x^2 + y^2)[(x^2)^4 - (x^2)^3 y^2 + (x^2)^2(y^2)^2 - x^2(y^2)^3 + (y^2)^4],$$

si ha pertanto:

$$(x^2)^4 - (x^2)^3 y^2 + (x^2)^2(y^2)^2 - x^2(y^2)^3 + (y^2)^4 = (x^2 + y^2)^4 - \\ - 5x^2y^2(x^2 + y^2)^2 + 5(x^2)^2(y^2)^2, \tag{2}$$

il secondo membro di quest'eguaglianza è un numero primo con $x^2 + y^2$ perchè il numero $x^2 + y^2$ è primo con x ed y primi tra di loro ed è primo con 5 perchè nella (1) z è supposto primo con n, consegue che anche il primo membro di (2) è un numero primo con $x^2 + y^2$; questa conclusione è valida per n primo qualsiasi perchè l'espressione di $x^{2n} + y^{2n}$ per mezzo di $x^2 + y^2$ e x^2y^2 data dalla formola di WARING contiene il fattore $x^2 + y^2$ in tutti i termini quando n è dispari. Posto pertanto nella (1) $z = tu$ con t ed u primi tra di loro si ha:

$$x^2 + y^2 = u^2,\ (x^2)^{n-1} - (x^2)^{n-2}y^2 + \ldots + (y^2)^{n-1} = t^2. \tag{3}$$

È evidente che non può essere $u = 1$ e quindi nemmeno $t = 1$, perchè, com'è facile dimostrare, è $t^2 > u^2$.

4. La (1), posto $x^n = X$, $y^n = Y$ si scrive:

$$X^2 + Y^2 = z^2$$

nella quale, per l'ipotesi fatta, X, Y e z son primi tra di loro; essa è la ben nota equazione pitagorica e si sa che tutte le soluzioni in numeri interi primi tra di loro, sono dati dalle formole:

$$X = 2\lambda\mu, \qquad Y = \lambda^2 - \mu^2, \qquad z = \lambda^2 + \mu^2, \tag{4}$$

nelle quali λ e μ son primi tra di loro e di parità diversa; consegue che:

$$x^n = 2\lambda\mu, \qquad y^n = \lambda^2 - \mu^2, \qquad z = \lambda^2 + \mu^2. \tag{5}$$

5. Essendo

$$z = tu \tag{6}$$

abbiamo per la (4):

$$\lambda^2 + \mu^2 = tu;$$

questa dice che t divide la somma dei quadrati di due numeri interi primi tra di loro e quindi anch'esso è somma di due quadrati:

$$t = p^2 + q^2. \tag{7}$$

6. Abbiamo dimostrato al n. 3 che dev'essere

$$x^2 + y^2 = u^2\,;$$

da questa (equazione pitagorica) si deduce che è necessariamente:

$$x = 2\alpha\beta, \quad y = \alpha^2 - \beta^2, \quad u = \alpha^2 + \beta^2 \tag{8}$$

con α e β interi di parità diversa per x, y ed u primi tra di loro (*).

7. Dalla (6), per (4), (7) e (8) si ottiene l'eguaglianza:

$$(\alpha^2 + \beta^2)(p^2 + q^2) = \lambda^2 + \mu^2\,. \tag{9}$$

È noto che il prodotto di due somme di due quadrati è una somma di due quadrati in quattro modi diversi; cosicchè possiamo scrivere:

$$\begin{aligned}(\alpha^2 + \beta^2)(p^2 + q^2) &= (\alpha p + \beta q)^2 + (\alpha q - \beta p)^2 \\ &= (\alpha p - \beta q)^2 + (\alpha q + \beta p)^2 \\ &= (\alpha p + \beta q)^2 + (\beta p - \alpha q)^2 \\ &= (\beta q - \alpha p)^2 + (\alpha q + \beta p)^2\,.\end{aligned} \tag{10}$$

8. Qui è necessaria un'osservazione importante per il seguito; se l'equazione

$$x^{2n} + y^{2n} = z^2 \tag{1}$$

è soddisfatta da:

$$x^n = 2\lambda\mu, \quad y^n = \lambda^2 - \mu^2, \quad z = \lambda^2 + \mu^2$$

per $\lambda = a_1$ e $\mu = b_1$, essa è soddisfatta anche ponendo invece $\lambda = b_1$ e $\mu = a_1$, cioè scambiando i valori di λ e μ; infatti le due terne di numeri:

$$\begin{matrix} 2a_1b_1 & a_1^2 - b_1^2 & a_1^2 + b_1^2 \\ 2a_1b_1 & b_1^2 - a_1^2 & a_1^2 + b_1^2 \end{matrix}$$

differiscono solamente per il segno di y^n e quindi se la (1) è verificata dalla prima terna, è verificata anche dalla seconda e viceversa; si può quindi ragionare indifferentemente sopra una qualsiasi di esse; noi utilizzeremo quella che ci permette di giungere a delle conclusioni. Essendo n dispari, se cambia segno y^n significa che cambia segno y, il che equivale a dire che nelle (8) vengono scambiati i valori di α e β come sono stati scambiati i valori di λ e μ.

(*) Abbiamo supposto $u = P^c$ con P primo, siccome esiste una sola partizione di P nella somma di due quadrati anche per u si ha la sola partizione: $\alpha^2 + \beta^2$.

9. Consideriamo ora l'equazione

$$x^{2n} + y^{2n} = z^2 \tag{1}$$

quando n è primo della forma $4k - 1$; in questo caso z è necessariamente primo con n; infatti se n fosse fattore primo di z esso dovrebbe dividere $(x^n)^2 + (y^n)^2$ cioè la somma dei quadrati di due numeri primi tra di loro e quindi anch'esso una somma di due quadrati ciò che non è mai per numeri primi della forma $4k - 1$. Supponiamo che la (1) ammetta una soluzione $\overline{x}$, $\overline{y}$, $\overline{z}$ con

$$\overline{z} = \lambda^2 + \mu^2$$

nella quale λ *e* μ *hanno determinati valori interi in corrispondenza dei quali* α, β, p *e* q *hanno anch'essi determinati valori interi.*

La (9) dice che $\lambda^2 + \mu^2$ deve coincidere con una delle somme di quadrati che figurano a secondo membro delle (10); basta considerare la prima e la seconda, perchè la terza e la quarta danno gli stessi valori di λ^2 e μ^2 (cambiando segno λ o μ cambia solamente il segno di x^n).

Poniamo:

$$(\alpha p + \beta q)^2 + (\alpha q - \beta p)^2 = \lambda^2 + \mu^2$$

e quindi

$$\lambda = \alpha p + \beta q, \qquad \mu = \alpha q - \beta p \tag{11}$$

oppure

$$\lambda = \alpha q - \beta p, \qquad \mu = \alpha p + \beta q\,. \tag{12}$$

I valori di x^n, y^n, z che si ottengono prendendo le (11) differiscono da quelli che si ottengono prendendo le (12) solamente per il segno di y^n, dunque per quanto abbiamo detto al n. 9 basta considerare le (12); ponendo invece:

$$(\alpha p - \beta q)^2 + (\alpha q + \beta p)^2 = \lambda^2 + \mu^2$$

e quindi

$$\lambda = \alpha p - \beta q, \qquad \mu = \alpha q + \beta q \tag{13}$$

oppure

$$\lambda = \alpha q + \beta p, \qquad \mu = \alpha p - \beta q \tag{14}$$

basta considerare le (13).

10. Considerando le (12) si ha:

$$\lambda^2 - \mu^2 = (q^2 - p^2)(\alpha^2 - \beta^2) - 2pq2\alpha\beta$$
$$2\lambda\mu = 2pq(\alpha^2 - \beta^2) + (q^2 - p^2)2\alpha\beta\,;$$

queste per le (4) e le (8) divengono:

$$y^n = (q^2 - p^2)y - 2pqx$$
$$x^n = 2pqy + (q^2 - p^2)x,$$

moltiplicando la prima per y, la seconda per x e sommando si ottiene

$$x^{n+1} + y^{n+1} = (q^2 - p^2)(x^2 + y^2)$$

ed essendo $n = 4k - 1$ si ha;

$$x^{4k} + y^{4k} = (q^2 - p^2)(x^2 + y^2)$$

ossia

(15) $$(x^2)^{2k} + (y^2)^{2k} = (q^2 - p^2)(x^2 + y^2);$$

quest' eguaglianza non sussiste per valori interi di x, y, p, q; infatti detto Q il quoziente di $(x^2)^{2k} + (y^2)^{2k}$ per $x^2 + y^2$ si ha:

$$(x^2)^{2k} + (y^2)^{2k} = (x^2 + y^2)Q + 2(y^2)^{2k}$$

e quindi la (15) si scrive:

(16) $$(x^2 + y^2)Q + 2(y^2)^{2k} = (q^2 - p^2)(x^2 + y^2);$$

quest' eguaglianza non sussiste per valori interi di p, q, x, y. Infatti Q è un polinomio in x ed y a coefficienti interi che per valori interi di x ed y dà numeri interi; il primo membro di (16) è allora un numero intero primo con $x^2 + y^2$ essendo $2(y^2)^{2m}$ anch' esso primo con $x^2 + y^2$ il quale è dispari con x ed y primi tra di loro.

Considerando le (13) si perviene all' eguaglianza:

(17) $$(x^2)^{2k} + (y^2)^{2k} = (p^2 - q^2)(x^2 + y^2)$$

anch' essa inammissibile.

Si può concludere pertanto che *l' equazione*

$$x^{2n} + y^{2n} = z^2,$$

dalla quale discendono le (15) e (17), non sussiste per valori interi di x, y, z *quando* n *è primo della forma* $4k - 1$ *ed è* $x^2 + y^2 = P^{2c}$ *con* P *primo,* c *intero positivo.*

11. Supponiamo ora che nell' equazione

(1) $$x^{2n} + y^{2n} = z^2$$

n sia della forma $4k + 1$. Ripetendo le osservazioni che abbiamo esposto al n. 10, consideriamo quì, com' è sufficiente, le (11) e le (14).

Per le (11) si ha:

$$\lambda^2 - \mu^2 = (p^2 - q^2)(\alpha^2 - \beta^2) + 2pq \cdot 2\alpha\beta$$
$$2\lambda\mu = 2pq(\alpha^2 - \beta^2) - (p^2 - q^2)2\alpha\beta$$

che per le (4) e le (8) si scrivono:

$$y^n = (p^2 - q^2)y + 2pqx$$
$$x^n = 2pqy - (p^2 - q^2)x;$$

moltiplicando la prima per x, la seconda per y e sommando si ha:

$$xy(x^{n-1} + y^{n-1}) = 2pq(x^2 + y^2)$$

ed essendo $n = 4k + 1$:

$$xy(x^{4k} + y^{4k}) = 2pq(x^2 + y^2), \tag{18}$$

è facile vedere che quest'eguaglianza è inammissibile: infatti $x^2 + y^2$ è primo con x e con y perchè x ed y son primi tra di loro; inoltre, $x^2 + y^2$ è primo con $x^{4k} + y^{4k}$ come si dimostra con il procedimento adoperato per la (15). Considerando le (14) si perviene di nuovo all'eguaglianza (18).

Consegue che la (1) *non ha soluzioni in numeri interi* x, y, z *quando* n *è primo della forma* 4k + 1 *nel caso in cui* z *è primo con* n *ed è* $\mathrm{x}^2 + \mathrm{y}^2 = \mathrm{P}^{2c}$ *con* P *primo*, c *intero positvo.*

12. È evidente che la dimostrazione sopra esposta vale tanto nel caso in cui x ed y sono entrambi primi con n che nel caso di x od y divisibile per n.

In altra nota esporrò un'indagine analoga quando z contiene il fattore primo n.