

Equazioni diofantee

Un'equazione dove cerchiamo soluzioni intere

- Esempi:
- trovare tutte le coppie $m, n \in \mathbb{Z}$ t.c. $m(n+3) = n^2 + 2026$
 - " $x, y \in \mathbb{Z}_{>0}$ t.c. $x^3 + y^3 = x^2 + 42xy + y^2$
 - dimostrare che $\forall n \in \mathbb{Z}$ esistono solo finite terne $a, b, c \in \mathbb{Z}$ t.c.
$$\begin{cases} a+b+c=n \\ a^2+b^2+c^2=n \end{cases}$$
 - trovare tutte le coppie $a, b \in \mathbb{Z}_{>0}$ t.c. $9^a - 7^b = 2^b$

Esistono soltanto due macro categorie di tecniche

Congruenze

$$LHS \not\equiv RHS \pmod{m}$$

$\Rightarrow \nexists$ soluzioni

Disuguaglianze

$$LHS > 1000 RHS$$

$\Rightarrow \nexists$ soluzioni

($\nexists$ interi fra 0 e 1

oppure stringere fra due quadrati)

(se $a|b \Rightarrow \frac{b}{a} = 0 \leq |b|$)

Es $p^2 + 36 = b^2 \quad a, b \in \mathbb{Z}, p \text{ primo} \quad (a \geq 0)$

$$p^2 = b^2 - 36 = (b-6)(b+6)$$

$$\Rightarrow p|b-6 \vee p|b+6$$

• supponiamo che $p|b-6$ e $p|b+6 \Rightarrow p|(b+6) - (b-6) = 12$

$$\Rightarrow p=2, 3$$

$$p \mid z \quad z^2 = (b-r)(b+r) \\ \text{mod } p^2$$

In realtà, abbiamo una struttura ancora più rigida

$$\begin{aligned} b-r &\mid p^2 &\Rightarrow b-r &= \pm p^x \\ b+r &\mid p^2 &b+r &= \pm p^{2-x} \end{aligned}$$

$$12 = \pm p^x \pm p^{2-x}$$

se $x \leq 2-x$, posso raccogliere p^x

$$\Rightarrow p^x \mid 12 \Rightarrow \begin{aligned} p &= 2 \\ x &\leq 2 \end{aligned}$$

$$\vee \\ p = 3 \\ x \leq 1$$

$$\vee \\ x = 0$$

$$b-r = \pm 1$$

Es: EGMO 2013. 4

Trovare tutti gli interi $a, b \in \mathbb{Z}^+$, $p(n) := \frac{n^5 + a}{b}$ è intero per 3 valori interi consecutivi di n .

$$\text{Sol: } \begin{cases} n^5 + a \equiv 0 & (\text{mod } b) \\ (n-1)^5 + a \equiv 0 & (1) \\ (n+1)^5 + a \equiv 0 & (b) \end{cases}$$

$$\begin{cases} a \equiv -n^5 \\ (n-1)^5 - n^5 \equiv 0 \\ (n+1)^5 - n^5 \equiv 0 \end{cases}$$

$$\begin{cases} a \equiv -n^5 \\ -5n^4 + 10n^3 - 10n^2 + 5n - 1 \equiv 0 \\ 5n^4 + 10n^3 + 10n^2 + 5n + 1 \equiv 0 \end{cases}$$

$$\text{se } b \mid n_1$$

$$b \mid n_2$$

$$\Rightarrow b \mid (n_1, n_2)$$

$$\begin{cases} 20n^3 + 10n \equiv 0 \\ -5n^4 + 10n^3 - 10n^2 + 5n - 1 \equiv 0 \end{cases} \quad \bullet 9$$

$$\begin{cases} 20n^3 + 10n \equiv 0 \\ 40n^3 - 30n^2 + 20n - 4 \equiv 0 \end{cases}$$

$$\begin{cases} 20n^3 + 10n \\ + 30n^2 + 4 \equiv 0 \end{cases}$$

$$\begin{cases} 60n^3 + 30n - 60n^2 - 8n \equiv 0 \\ 30n^2 + 4 \equiv 0 \end{cases}$$

$$\begin{cases} 22n \equiv 0 \\ 30n^2 + 4 \equiv 0 \end{cases}$$

$$\begin{cases} 22n \equiv 0 & \leftarrow 11 \text{ è coprimo} \\ 8n^2 + 4 \equiv 0 \end{cases}$$

$$88n^2 + 44 - 88n^2 \equiv 0$$

$$\rightarrow 44 \equiv 0 \Rightarrow 6 \mid 44 \quad \text{solo finiti casi}$$

(ma sono ancora tanti,

si possono ridurre usando altre congruenze

ad esempio mod 2 $\Rightarrow b$ non era pari.

$$\Rightarrow b \mid 11)$$

$$m(n+3) = n^4 + 2026$$

$$\exists m = \frac{n^4 + 2026}{n+3}$$

se $\rightarrow$ è intero, allora anche $m - n^3 \in \mathbb{Z}$

$$m - n^3 = \frac{n^4 + 2026 - n^3(n+3)}{n+3} = \frac{-3n^3 + 2026}{n+3}$$

$$m + 3n^2 = \frac{-3n^3 + 2026 + 3n^3(n+3)}{n+3} = \frac{9n^2 + 2026}{n+3}$$

$\vdots$

$$\frac{R(n)}{n+3} \in \mathbb{Z}$$

$$\frac{81 + 2026}{n+3}$$

$\Rightarrow$ ora si controllano tutti i divisori di $81 + 2026$

(compresi quelli negativi)

Se il denominatore non fosse monico?

$$\frac{n^2 + 2026}{2n+1} \in \mathbb{Z} \Rightarrow \frac{2n^2 + 2 \cdot 2026}{2n+1} \in \mathbb{Z}$$

Cosa sarebbe accaduto nel caso di polinomi al denominatore di grado > 1

Alla fine abbiamo una forma più complicata come

$$\frac{n+7}{n^2-3n+1} \in \mathbb{Z}$$

$$\text{Se } n^2-3n+1 \mid n+7 \Rightarrow |n^2-3n+1| \leq |n+7| \quad \forall n+7 \neq 0$$

solamente finiti n soddisfano

$$\begin{cases} n^2-3n+1-n-7 \leq 0 \\ n^2-3n+1+n+7 \leq 0 \end{cases}$$

solo finiti n da controllare

Casistica di equazioni polinomiali

1° grado: trovare tutt. gli interi x, y t.c. $ax+by=c$
(a, b, c sono interi fissati)

1 caso $c=0$ $ax = -by \Rightarrow b \mid ax \Rightarrow \frac{b}{(a,b)} \mid x$
(il caso omogeneo) $a \mid by \Rightarrow \frac{a}{(a,b)} \mid y$

$$\exists k \in \mathbb{Z}: x = k \cdot \frac{b}{(a,b)} \quad \frac{abk}{(a,b)} = -by$$
$$y = -\frac{ak}{(a,b)}$$

2 caso $c=1$, qui potrei non avere soluzioni
 $ax+by=1$ se $\exists p \mid a, b$
assurdo mod p

alternat: $(a,b)=1$

esiste una soluzione (x_0, y_0)

come sono fatte le altre soluzioni?

$$ax + by = 1$$

$$ax_0 + by_0 = 1$$

$$a(x-x_0) + b(y-y_0) = 0$$

$\underbrace{\hspace{1cm}}_{x'} \quad \underbrace{\hspace{1cm}}_{y'}$

$\Rightarrow (x', y')$ è soluzione dell'omogenea

È utile ridurre con l'algoritmo di Euclide

eg:

$$27x + 64y = 1$$

$$64 = 2 \cdot 27 + 10$$

$$27x + 27 \cdot 2y + 10y = 1$$

$$27(x+2y) + 10y = 1$$

$$x' = x + 2y$$

$$27x' + 10y = 1$$

$$27 = 2 \cdot 10 + 7$$

$$x = 19$$

$$3 = x - 16$$

$$7x' + 10 \cdot 2x' + 10y = 1$$

$$7x' + 10(2x' + y) = 1$$

$$y' = 2x' + y$$

$$7x' + 10y' = 1$$

$$10 = 7 + 3$$

$$y = -8$$

$$-2 = 6 + y$$

$$7(x' + y') + 3y' = 1$$

$$x'' = x' + y'$$

$$7x'' + 3y' = 1$$

$$1 = x' + (-2)$$

$$x'' = 1 \quad y' = -2$$

$$x' = 3$$

se non lo vedeva fino alla fine

sarà arrivato a

$$1 \cdot x''' + 0y''' = 1$$

Se c è generico, che si fa?

sì, moltiplicare x_0 e y_0 per c

trovati con $c=1$

$$ax_0 + by_0 = 1$$

$$a(cx_0) + b(cy_0) = c$$

2° grado

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

si può fare una classificazione guardando il termine di grado massimo

$$ax^2 + bxy + cy^2 = 0$$

in $\mathbb{C}$, se $y \neq 0$

$$a\left(\frac{x}{y}\right)^2 + b\left(\frac{x}{y}\right) + c = 0$$

$t = \frac{x}{y}$ è quadratica in t

$$f(x, y)^2 = g(x, y)$$

$$w = f(x, y)$$

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

$\forall$ scelta di $w \exists!$ soluzione in z

se le due radici sono complesse coniugate

$$ax^2 + bxy + cy^2 = \alpha w^2 + \beta z^2$$

$$\alpha, \beta > 0$$

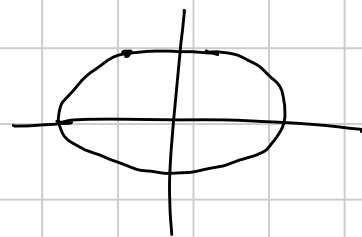
ho un'ellisse (dal punto di vista reale)

$$\alpha w^2 + \beta z^2 = \gamma \quad (\alpha, \beta, \gamma > 0)$$

$$\alpha w^2 < \gamma \quad |w| < \sqrt{\frac{\gamma}{\alpha}}$$

$$|z| < \sqrt{\frac{\gamma}{\beta}}$$

ho solo finiti casi da controllare



Nell'ultimo caso le radici sono reali:

e ho una forma del tipo $\alpha w^2 - \beta z^2 = \gamma \quad (\alpha, \beta > 0)$

$$(\alpha w)^2 - \alpha \beta z^2 = \alpha \gamma$$

$$(w - \sqrt{\beta'} z)(w + \sqrt{\beta'} z)$$

$$w^2 - \beta' z^2 = \gamma'$$

$$x^2 - y^2 = 2026$$

(è il caso in cui β' è un quadrato)

$$x - y = \frac{2026}{x + y}$$

Altimenti: β' non è un quadrato
e ottengo equazione di Pell
(d libero da quadrati)

$$x^2 - dy^2 = c$$

Se $c = 1$, $\exists$ infinite soluzioni

Se $c \neq 1$ $\left\{ \begin{array}{l} \nexists \text{ soluzioni per qualche congruenza} \\ \exists \text{ infinite soluzioni} \end{array} \right.$

$$x, y \in \mathbb{Z}_{>0} \text{ t.c. } x^3 + y^3 = x^2 + 42xy + y^2$$

Sol: dato che $x, y > 0$, per x, y abbastanza grandi m. aspetto che
LHS > RHS

$$x^3 + y^3 \stackrel{?}{>} (x^2 + 42xy + y^2)(x+y)c$$

dovrebbe $\exists c > 0$ t.c.

$\forall x, y \in \mathbb{R}_{>0}$

$$x^3 + y^3 = (x+y)(x^2 - xy + y^2)$$

$$x^2 - xy + y^2 \stackrel{?}{>} (x^2 + 42xy + y^2)c$$

$$(1-c)(x^2 + y^2) \stackrel{?}{>} (1 + 42c)xy$$

$$x^2 + y^2 \geq 2xy$$

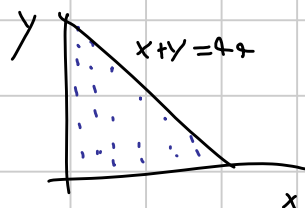
$$\frac{1+42c}{1-c} = 2 \quad \text{funzione}$$

$$c = \frac{1}{49}$$

$$x^3 + y^3 \geq (x^2 + 42xy + y^2) \frac{x+y}{49} > x^2 + 42xy + y^2$$

non appena $x+y > 49$

il problema è finito a meno di controllare finiti casi



Con qualche congruenza, i casi diventano pochi

Alt₁₂ soluzione:

$$x^3 + y^3 = x^2 + 42xy + y^2$$

↓

$$s(x^2 - xy + y^2) = s^2 + 40p$$

$$s(s^2 - 3p) = s^2 + 40p$$

$$p = \frac{p(s)}{q(s)} = \frac{s^3 - s^2}{3s + 40}$$

$$s^3 - s^2 = 40p + 3sp$$

$$\in \mathbb{Z} \Rightarrow 27p \in \mathbb{Z}$$

$$\Rightarrow \frac{27s^3 - 27s^2}{3s + 40} \in \mathbb{Z}$$

$$z = 3s$$

$$\Rightarrow \frac{z^3 - 3z^2}{z + 40} \in \mathbb{Z}$$

$$\Rightarrow \frac{(-40)^3 - 3(-40)^2}{z + 40} \in \mathbb{Z}$$

$$\frac{40^2 \cdot (40 + 3)}{z + 40} \in \mathbb{Z}$$

$$z > 0 \quad z + 40 > 40$$

$$3|z \Rightarrow z + 40 \equiv 1 \pmod{3}$$

Esercizi

$$1 \quad n, m \in \mathbb{Z}, \quad n^2 - 6n = m^2 + m - 12$$

$$2 \quad a, b, c, p, q, r \in \mathbb{Z}_{>0} \quad a^p + b^q + c^r = a^q + b^r + c^p = a^r + b^p + c^q \Rightarrow 1 \text{ o } a=b=c \text{ o } p=q=r$$

$$3 \quad p \text{ primo, quando } x^2 + px - 99 + p = 0 \text{ ha radici intere?}$$

$$4 \quad x, y, z \in \mathbb{Q}, \quad x^2 + y^2 + z^2 = 7$$

$$5 \quad a, b, c, d \in \mathbb{Z}, \quad a^3 + 2b^3 = 2014(c^3 + 2d^3)$$

$$6 \quad \text{per quanti } n \quad n^2 + 85n + 2017 \text{ è un quadrato?}$$

$$7 \quad a, b \in \mathbb{Z}_{>0} \quad 9^a - 7^a = 2^b$$

$$8 \quad x, y \in \mathbb{Z}_{>0} \quad 3^x - y^2 = 41$$

$$9 \quad \text{trovare tutte le } f: \mathbb{Z}_{>0} \rightarrow \mathbb{Z}_{>0} \text{ t.c. } n + f(m) \mid f(n) + n f(m) \quad \forall n, m \in \mathbb{Z}_{>0}$$

$$10 \quad \forall n \exists \text{ solo finiti } a, b, c \in \mathbb{Z} \text{ t.c. } \begin{cases} a+b-c=n \\ a^2+b^2-c^2=n \end{cases}$$

$$11 \quad x, y \in \mathbb{Z}_{>0}, p \text{ primo} \quad x^3 + y^3 = p(xy + p) \quad (\text{RMM 2023.1})$$

$$12 \quad x, y \geq 0 \quad 1 + 2^x + 2^{2x+1} = y^2 \quad (\text{IMO 2006.4})$$

Soluzioni

$$n, m \in \mathbb{Z}, \quad n^2 - 6n = m^2 + m - 12 \quad n^2 - m^2 - 6n - m + 12 = 0$$

oss: è quadratica, è iperbole $(n^2 - m^2)$

e si fattorizza negli interi $((n-m)(n+m))$

$$xy = C$$

$$x = n - m + c_1$$

$$y = n + m + c_2$$

$$xy = n^2 - m^2 + c_1 n + c_1 m + c_2 n - c_2 m + c_1 c_2 - C = 0$$

$$c_1 + c_2 = -6$$

$$c_1 = -\frac{7}{2}$$

$$\frac{35}{4} - C = 12$$

$$c_1 - c_2 = -1$$

$$c_2 = -\frac{5}{2}$$

$$4C = -13$$

$$(2x)(2y) = 4C$$

$$(2n - 2m - 7)(2n + 2m - 5) = -13$$

α

β

$$\alpha = \begin{pmatrix} 1 & -1 & 13 & -13 \\ -13 & 13 & -1 & 1 \end{pmatrix}$$

2 $a, b, c, p, q, r \in \mathbb{Z}_{>0}$ $a^p + b^q + c^r = a^q + b^r + c^p = a^r + b^p + c^q \Rightarrow 1$ m $a=b=c$
 $p=q=r$

Proviamo a usare le disuguaglianze

supponiamo $a > b, c$ $p > q, r$

il termine 2^p sembra p.u. grande di tutt. gl. altri 8 scritti

spero sia vero che $2^r + b^q + c^r > 2^q + b^r + c^p$
 $> 2^r + b^p + c^q$

spero sia vero che $2^p \gg 2^q + b^r + c^p$

$$\begin{array}{cc} p \geq q+1 & p \geq r+1 \\ 2 \geq b+1 & 2 \geq c+1 \end{array} \quad 2^{p-1} \underbrace{(2-1)}_{\substack{\geq 2 \\ \text{size}}} \geq b^r + c^p$$

varri:
tanto

Se $b_{sse} \quad 2^p > b^r$
 $2^r > c^p$

$$\begin{aligned} C &\leq 2-1 \\ C^p &\leq (2-1)^p \\ &\leq 2^p - p2^{p-1} \end{aligned}$$

$$2^p \geq \underbrace{2^q + b^r + c^p}$$

$$\leq 2^q + 2^r + 2^p - p2^{p-1} \leq 2^{p-1} + 2^{p-1} - p2^{p-1}$$

$$p a^{p-1} \geq a^q + b^r$$

$$2^a \leq 2^{p-1}$$

6 7 8

$$r \leq p-1$$

$$x, y \in \mathbb{Z}_{>0}, p \text{ primo}$$

$$x^3 + y^3 = p(xy + p)$$

(RMM 2023.1)

Sol: è simmetrico in x, y

$$s = x + y$$

$$q = xy$$

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

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

$$q = \frac{s^3 - p^2}{p + 3s}$$

$$27q = \frac{(3s)^3 - 27p^2}{p + 3s} \in \mathbb{Z} \Leftrightarrow \frac{-p^3 - 27p^2}{p + 3s} \in \mathbb{Z}$$

$$3s + p \mid p^2(p + 27)$$

$$p \mid s \vee p \mid s^2 - 3q$$

↑

in questo caso $(s, p) = 1$

$$\Rightarrow 3s + p \mid p + 27$$

$$3s + p \leq p + 27$$

$$s \leq 9$$

$$12 \quad x, y \geq 0$$

$$1 + 2^x + 2^{2x+1} = y^2$$

(IMO 2005.4)

Sol

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

$$= (y-1)(y+1)$$

y è dispar.

$$y = 2z + 1 \quad 2z(2z + 2)$$

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

Due casi $2^{x-2} \mid z$

$$2^{x-2} \mid z+1$$

$$w = 2^{x-2}$$

$$1 + 8w = 1 + 2^{x+1}$$

$$w \mid z$$

$$z = kw$$

$$\cancel{u}(1+8w) = k\cancel{u}(ku+1)$$

$$1+8w = k^2w + k \geq k^2w + 1$$

$$8 \geq k^2 \quad k=1, 2$$

Fare anche l'altro caso (che porta a soluzione!)