Equazioni diofantee

si cercano soluzioni intere

$55x + 59y = 1$

$x^6 - 1 = y^2 + 1$

$a^p = b! + p$

2 tipologie di tecniche

- Congruenze — $A = B$, ma mod m $A \not\equiv B$ (m)

- Disuguaglianze — se voglio $A = B$, ma trovo $A > 1000B$

voglio che A sia intero
ma trovo che $n < A < n+1$

Diofantee polinomali

$p(x_1, \dots, x_n) = 0$

$ax + by = c$ — se trovo che mod p, $p|a$, $p|b$
ma $p \nmid c$

$(a,b) \mid c$

altrimenti

$c=0$ — $ax + by = 0$ — ((x_0, y_0) sol $\Rightarrow$ $(\lambda x_0, \lambda y_0)$ sol)

$c=1$

se so risolvere questo caso so risolvere tutto

se (x_0, y_0) e (x_1, y_1) sono soluzioni
allora $ax_0 + by_0 = c$
e $ax_1 + by_1 = c$

$$a(x_0 - x_1) + b(y_0 - y_1) = 0$$

se (x_2, y_2) è soluzione con $c=1$ $\left(ax_2 + by_2 = 1\right)$

basta prendere (cx_2, cy_2) per ottenere 1 soluzione a $ax + by = c$

Per trovare soluzioni (con $c=1$) riduco il problema un po' alla volta:

$$5x - 7y = 1$$

$$5(x-y) - 2y = 1 \qquad x' := x - y$$

$$5x' - 2y = 1$$

$$x' + 2(2x' - y) = 1 \qquad y' := 2x' - y$$

$$x' + 2y' = 1 \qquad (1, 0) \text{ è soluz.}$$

Polinomi di grado 2
(lavoriamo solo con x, y)

L'idea di base è che possiamo semplificare la forma dell'equaz. mediante cambi di variabile affini:

$$\begin{cases} x' := \alpha x + \beta y + \gamma \\ y' := \delta x + \varepsilon y + \zeta \end{cases}$$

1) Caso degenere: $p(x,y) = p_1(x,y)\, p_2(x,y)$

per risolvere $p(x,y) = 0$
basta risolvere $p_1(x,y) = 0$
e $p_2(x,y) = 0$

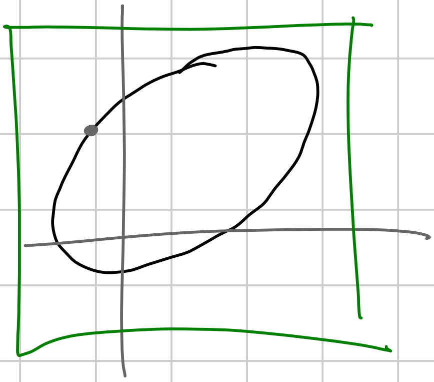
2) Caso ellisse: $\alpha x^2 + \beta y^2 = \gamma$ con $\alpha, \beta > 0$

$$2x^2 + y^2 = 2022$$

le soluzioni sono finite perché $x^2, y^2 \geq 0$

$\Rightarrow$ $2022 = 2x^2 + y^2 \geq 2x^2 \Rightarrow |x| \leq \sqrt{1011} < 1000$

$\geq y^2$ $\quad |y| \leq \sqrt{2022}$



3) Caso parabola $\quad \alpha x^2 + \beta y = \gamma$

$$y = \frac{\gamma - \alpha x^2}{\beta}$$

infinite soluzioni $(\forall x, \exists y)$

4) Caso iperbole $\quad \alpha x^2 - \beta y^2 = \gamma \quad \alpha, \beta > 0$

1) sottocaso: riesco ad assorbire α e β dentro x, y

$$x^2 - y^2 = \gamma'$$

$$(x-y)(x+y) = \gamma'$$

$$z_1 \cdot z_2 = \gamma'$$

ho finite soluzioni

(caso simile: $y \, \text{cose}(x) = \text{altro}(x)$

$$y = \frac{\text{altro}(x)}{\text{cose}(x)}$$

$$y = \text{intero}(x) + \frac{r}{\text{cose}(x)}$$

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

(di solito $|x+1| < |2x^2-7x+3| \Rightarrow \left|\frac{}{}\right| < 1$
$\Rightarrow x+1=0$)

2) Equazioni di Pell: $x^2-dy^2=\gamma$

ci sono casi in cui mod m non trovo soluzioni

$$x^2-3y^2=2$$

mod 3: $x^2 \equiv -1$ assurdo

se $\gamma=1$, ho sempre soluzioni

$\exists \infty$ infinite soluzioni, e si ottengono

$$x^2-dy^2=(x-\sqrt{d}y)(x+\sqrt{d}y)=1$$

trovata una soluzione non banale x_0, y_0

$$(x_0-\sqrt{d}y_0)^n = x_n-\sqrt{d}y_n \quad e \ (x_n, y_n)$$

$$(x_n-\sqrt{d}y_n)(x_n+\sqrt{d}y_n) = (x_0-\sqrt{d}y_0)^n \cdot (x_0+\sqrt{d}y_0)^n =$$

$$= (x_0^2-dy_0^2)^n = 1^n = 1$$

$\|$

$x_n^2-dy_n^2$

Equazioni polinomiali generiche di grado più alto

sono molto più difficili

$x^6 - 1 = y^2 + 1$ (se esiste una soluzione ovvia allora esiste una " " mod m $\forall m$)

proviamo mod p t.c. $6 | p-1$ $\quad x^6 = y^2+1$

tipo $p=7$

$x^6 \equiv 0, 1 \qquad y^2 \equiv \dots \equiv \begin{cases} 0 \\ 1 \\ 4 \\ 2 \end{cases}$

$y^2+2 \equiv \begin{cases} 2 \\ 3 \\ 6 \\ 4 \end{cases}$ assurdo mod 7.

Diofantee con esponenti.

Es: Trovare tutte le coppie (a,b) di interi non negativi t.c.

$$7^a - 5^b = 2$$

mod 5 : $2^a - 1 \equiv 2$ $\qquad b=0$ soluz con $a \equiv 3\ (4)$

$2^a \equiv 2$ $\qquad b>0$ $\qquad a \equiv 1\ (4)$

$(1,1)$ è soluzione!

mod 25, assumendo $b>1$ $\qquad 7^a \equiv 2\ (25)$

$7^0 \quad 7^1$

$1 \quad 7 \quad -1 \quad -7 \quad 1$

si ripetono mod 4. Assurdo mod 25

$\Rightarrow b \leq 1$

Es (IMO 2019.4) Trovare tutte le coppie di interi non negativi (k, n) t.c.

$$k! = (2^n - 2^0) \cdot (2^n - 2^1) \cdot \ldots \cdot (2^n - 2^{n-1})$$

Sol: Lavorare con le congruenze mi spinge a contare i fattori p in entrambi i termini.

$$p = 2: \quad v_2(k!) = \left\lfloor \frac{k}{2} \right\rfloor + \left\lfloor \frac{k}{4} \right\rfloor + \ldots + \left\lfloor \frac{k}{2^n} \right\rfloor$$

(Def: La "valutazione p-adica" $v_p(n)$ è l'esponente che compare nella fattor. di n sopra p.)

$$v_2(k!) < k$$
$$> k - \text{poco} \ldots$$

$$v_2\left((2^n - 2^0) \cdot \ldots \cdot (2^n - 2^{n-1})\right) = 0 + 1 + \ldots + (n-1) = \frac{(n-1)n}{2}$$

$$\Rightarrow k > v_2(k!) = \frac{(n-1)n}{2} \Rightarrow k > \frac{(n-1)n}{2}$$

$$\Rightarrow k! > \left(\frac{(n-1)n}{2}\right)!$$

sembra potenzialmente più grande di $(2^n-2^0)\cdot\ldots\cdot(2^n-2^{n-1})$

$$RHS < 2^n \cdot 2^n \cdot \ldots \cdot 2^n = 2^{n^2}$$

$$\left(\frac{(n-1)n}{2}\right)! > \left(\frac{\frac{(n-1)n}{2}}{4}\right)^{\frac{(n-1)n}{2}}$$ è vero per n un po' grande

Stirling : $$n! \underset{4}{\approx} \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

il rapporto fra le due espressioni si avvicina arbitrariamente a 1 al crescere di n

ora dovrei avere, per n un po' grande

$$\frac{n^{n^2}}{8^n} \sim \left(\frac{(n-1)n}{8}\right)^{\frac{n(n-1)}{2}} < 2^{n^2}$$

In bella scriverò $$\left(\frac{(n-1)n}{2}\right)! > \left(\frac{(n-1)n}{8}\right)^{\frac{(n-1)n}{2}} \quad ? \quad \text{per } n>7$$

e $$2^{n^2} < \left(\frac{(n-1)n}{8}\right)^{\frac{(n-1)n}{2}} \quad \text{per } n>7$$

se trovo questo, trovo un assurdo per $n>7$ e quindi devo controllare solo i primi 7 casi

---

Es (IMO 2022 . 5) Trovare tutte le terne di interi >0 a, b, p t.c. p è primo e

$$a^p = b! + p$$

Sol: mod p : $a \equiv b!$

se $b \geq p$, si riduce a $a \equiv 0 \ (p)$

$\Rightarrow p \mid a$

mod p^2: $a^p \equiv b! + p$

se $b \geq 2p$ ottengo $a^p \equiv p \ (p^2)$

$\Rightarrow a^p \equiv 0 \ (p)$

$\Rightarrow p \mid a$

$\Rightarrow p^p \mid a^p$

$\Rightarrow a^p \equiv 0 \ (p^2)$

$\Rightarrow 0 \equiv p \ (p^2)$

assurdo

Ora so che $b < 2p$

distinguiamo 2 casi $b \geq p$ e $b < p$

se $b \geq p$, $p \mid a$ $a = pc$

$p^p c^p = b! + p$

$$\left(\text{se } b = p \qquad p^p c^p = p! + p \qquad p! < p^p \right)$$

se $c \geq 2$, $a > b$

$a^p \geq (2p)^p \overset{?}{>} (2p-1)! + p \geq b! + p$

$2p \cdot 2p \cdot \ldots \cdot 2p$

$(2p-1)(2p-2) \cdot \ldots 2 \cdot 1$

se $a \geq p^2$

$a^p \geq p^{2p} > (2p)! > (2p-1)! + p$

ora in effetti: $(2p-k)k < p^2$

$\Rightarrow a < p^2$
$(b < 2p)$

$a^p = b! + p$

sia $q \mid a$, mod q

$0 \equiv b! + p$

se $b \geq q$ avrei: $0 \equiv p \ (q) \Rightarrow q = p$

$p \mid a < p^2 \quad b < 2p$

ogni fattore di a diverso da p è $< p$

ma siamo nel caso $b \geq p$

Quindi $a = p^k$ ci sono i casi $a = 1$

$a = p$ (visto N1 Medim)

e rimane il caso $b < p$. (per casa)

Es : determinare tutte le terne (a,b,c) t.c. $\exists$ interi non nulli (λ, μ, ν) t.c. $\forall n > 0$

$$\lambda a^n + \mu b^n + \nu c^n = 0$$

Sol: A meno di rinominare, $|a| \geq |b|$, $|a| \geq |c|$

divido per a^n: $\lambda = -\mu\left(\frac{b}{a}\right)^n - \nu\left(\frac{c}{a}\right)^n$

se $|a| > |b|$ e $|a| > |c|$
allora esiste n t.c.

$$\left|\frac{b}{a}\right|^n < \frac{1}{2022\mu}$$

$$\left|\frac{c}{a}\right|^n < \frac{1}{2022\nu}$$

$$\lambda = -\mu\left(\frac{b}{a}\right)^n - \nu\left(\frac{c}{a}\right)^n \leq \left|-\mu\left(\frac{b}{a}\right)^n - \nu\left(\frac{c}{a}\right)^n\right|$$

$$\text{dis. triangolare} \leq \left|\mu\left(\frac{b}{a}\right)^n\right| + \left|\nu\left(\frac{c}{a}\right)^n\right|$$

$$< \frac{1}{2022} + \frac{1}{2022}$$

$\Rightarrow \lambda = 0$ assurdo

$\Rightarrow |a| = |b|$

$$\lambda a^n \pm \mu a^n + \nu c^n = 0$$

$$(\lambda \pm \mu) a^n + \nu c^n = 0$$

come prima $\lambda \pm \mu = 0 \ \vee \ |a| = |c|$

.... $\Rightarrow$ l'unica possibilità $|a| = |b| = |c|$
oppure qualcuno fra $a, b, c = 0$

Es (BMO 2017.1) Trovare tutti gli interi non negativi (x,y) t.c.

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

Sol: mod $d | 42$: $x^3 + y^3 \equiv x^2 + y^2$

Oss: $(0,0)$ è soluzione
quindi le congruenze da sole non bastano

proviamo con qualche stima

$$x^3 + y^3 = (x+y)(x^2 - xy + y^2) \overset{?}{>} x^2 + 42xy + y^2$$

in effetti: $x^2 - xy + y^2 < x^2 + 42xy + y^2$

$\cancel{x}^2 - xy + y^2$

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

$$x^2 - xy + y^2 \overset{?}{\geq} c\,(x^2 + 42xy + y^2)$$

se $C = \frac{1}{42}$

$\frac{x^2 + y^2}{42} + xy$

se $C = \frac{1}{2 \cdot 42}$

ma $\frac{x^2 - xy + y^2}{2} \geq \frac{xy}{2}$

$\frac{x^2 + y^2}{2 \cdot 42} + \frac{xy}{2}$

$$\frac{x^2-xy+y^2}{2} \geq \frac{x^2+y^2}{2\cdot 42}$$

$$42x^2-42xy+42y^2 \geq x^2+y^2$$

$$41(x^2+y^2) \geq 42xy$$

quindi ora abbiamo

$$x^3+y^3 \geq (x+y)\ \frac{1}{C}(x^2+42xy+y^2) > x^2+42xy+y^2$$

se $x+y > C$

Abbiamo trovato che $x+y \leq C$

poiché $x, y \geq 0$ ho solo finiti casi da controllare.

(in realtà $C = 44$ dovrebbe funzionare)

Sol 2: Osserviamo che l'eq. è simmetrica in x, y

$\Rightarrow$ possiamo scrivere tutto in funzione di $x+y=s$ $xy=p$

$$x^3+y^3 = (x+y)(x^2-xy+y^2) = s\cdot(s^2-3p)$$

$$x^2+42xy+y^2 = s^2+40p$$

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

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

$$p = \frac{s^3-s^2}{40+3s} \in \mathbb{Z}$$

se p è intero anche $27p \in \mathbb{Z}$

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

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

$$\Rightarrow \underset{\mathbb{Z}}{\underset{\cap}{Q(s')}} + \frac{(-40)^3 - 3(-40)^2}{s'+40} \in \mathbb{Z}$$

$\Rightarrow$ è intero

$\Rightarrow s'+40$ è un divisore di $40^2 \cdot 43$

Esercizi: Parte 1 : 41, 46, 54, 56
Parte 2 N1 : 2
" N2 : 5
Foglio 21 N2B : tutti i pari

Correzione

Parte 1 : 56 $\qquad 3^y - 2^x = 41$

Sol: Provare con alcuni moduli

I moduli che hanno senso sono 3 (o potenze di 3)
e 2 (o potenze di 2)

In effetti: mod 3 $\Rightarrow$ x è pari
mod 4 $\Rightarrow$ y pari

$\Rightarrow \quad x = 2x' \quad y = 2y'$

$$(3^{y} - 2^{x})(3^{y} + 2^{x}) = 41$$
$$\underset{1}{\underset{\shortparallel}{(3^{y} - 2^{x})}} \qquad \underset{41}{\underset{\shortparallel}{(3^{y} + 2^{x})}}$$

Parte 2 N1.2

Trovare i primi p t.c. $x^2 + px - 444p = 0$ ha 2 soluzioni intere

Sol: $p(x-444) = -x^2$

$$p = \frac{-x^2}{x-444} \in \mathbb{Z}$$

$$\Rightarrow \quad x - 444 \mid 444^2$$ e qui rimangono finiti casi.

Possiamo anche osservare che mod p, $0 \equiv x^2$

$\Rightarrow \quad p \mid x \quad x = py$

$$p^2 y^2 + p^2 y - 444p = 0$$

$$p(y^2 + y) - 444 = 0$$

$\Rightarrow \quad p \mid 444$ ho ancora meno casi.

Foglio 2021 N2 B Es 2 trovare tutte le terne x, y, z di interi t.c.

$$2x + 3y + 5z = 7$$

Sol: cerco prima soluzioni alla omogenea associata

$$2x+3y+5z=0$$

$(3,-2,0)$, $(5,0,-2)$ sono soluzioni

$(-1,-1,1)$ è soluzione

ora $(-\lambda,-\lambda,\lambda)$ è soluzione

e anche $(3\mu,-2\mu,0)$ è soluzione

$(3\mu-\lambda,\ -2\mu-\lambda,\ \lambda)$ è soluzione

Vediamo se sono tutte:

vogliamo trovare λ,μ $\forall (x,y,z)$ soluzione in modo che

$$(3\mu-\lambda,\ -2\mu-\lambda,\ \lambda)=(x,y,z)$$

Allora scelgo $\lambda=z$

vorrei $\mu=\dfrac{x+z}{3}$? posso farla $\iff x+z\equiv 0\ (3)$

$$2x+3y+5z=0$$

$$2(x+z)+3y+3z=0 \qquad \text{mod } 3$$

$$2(x+z)\equiv 0$$

$$(x+z)\equiv 0$$

e ora controllo che y sia della forma giusta...

Per concludere devo trovare 1 soluzione al caso in cui il termine noto $=7$ (x_0,y_0,z_0)

ora, tutte le soluzioni sono della forma

$$(x_0,y_0,z_0)+(3\mu-\lambda,\ -2\mu-\lambda,\ \lambda).$$

Es 4 : $3y^2 = x^2 + x + 1$

Sol: $12y^2 = 4x^2 + 4x + 4$

$3(2y)^2 = (2x+1)^2 + 3$

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

$x^2 - 3y^2 = -3$

Equazione di Pell che ha $(0, 1)$ come soluzione
allora ha infinite soluzioni.

Risolvo prima $x^2 - 3y^2 = 1$

$(2, 1)$ è soluzione

$(2+\sqrt{3})^n = (a_n + b_n\sqrt{3}) \qquad (a_n, b_n)$ è soluzione
(e sono tutte)

tutte le soluzioni sono della forma

$$(0 + 1\sqrt{3}) \cdot (2+\sqrt{3})^n = x_n + y_n\sqrt{3}$$

sono soluzioni perché

$$\left(\sqrt{3} \cdot (2+\sqrt{3})^n\right) \cdot \left(-\sqrt{3} \cdot (2-\sqrt{3})^n\right) =$$

$$\left(\sqrt{3} \cdot (-\sqrt{3})\right) \left((2+\sqrt{3})(2-\sqrt{3})\right)^n =$$

$$-3 \cdot 1^n = -3$$

$3y^2 = 2x^2 + x + 1$

mod 3 $\quad 0 \equiv 2x^2 + x + 1$

assurdo.

mod 3

x	$2x^2+x+1$
0	1
1	1
2	2

Es 14 Dim. che $\forall n$ $\exists$ solo finite coppie (x,y) t.c.

$$x^6 - yx^5 + 11(x^5 - yx^4) + \ldots = n$$

Sol: osserviamo che y compare al massimo in grado 1

$$y\,P(x) = Q(x) + n$$

$$y = \frac{Q(x)+n}{P(x)} \in \mathbb{Z}$$

$P(x) \mid Q(x)+n$ come polinomi a coeff. interi

oppure $p(x) \nmid$ " e quindi: