Teoria dei Numeri 1 - Basic

Note Title 9/5/2017

Tess

Equazioni diofantee

trovare le soluzioni intere $3a - 2b = 1$

$a^n + b^n = c^n$

- Disuguaglianze
- Congruenze

Testo: $A = B$, riesco a dimostrare $A > B \cdot 1000$

allora non ci sono soluzioni

oppure

A è dispari, B è pari, dunque niente soluzioni

Disuguaglianze

Es: $a^n + b^n + c^n = 0$ per infiniti $n > 0$ interi e dispari

determinare tutti i possibili valori di a, b, c

Oss: posso prendere la variabile non più piccola e chiamarla wlog "a",

$a^n = -b^n - c^n$

$1 = -\left(\frac{b}{a}\right)^n - \left(\frac{c}{a}\right)^n$

$|a| \geq |b| \quad |a| \geq |c|$

$\left|\frac{b}{a}\right|, \left|\frac{c}{a}\right| \leq 1$ se non avessi nessuna =

se $\left|\frac{b}{a}\right| \leq 0{,}999$

$\left|\frac{b}{a}\right|^n \leq 0{,}00001$ (per n abbastanza grande)

$$\left|-\left(\frac{b}{a}\right)^n - \left(\frac{c}{a}\right)^n\right| \leq \left|\left(\frac{b}{a}\right)\right|^n + \left|\left(\frac{c}{a}\right)\right|^n \leq 0{,}00002 < 1$$

$\Rightarrow$ wlog $|a| = |b|$, allora il problema è finito

non posso avere $a=b$, quindi $a=-b$

quindi $c=0$.

TST 2014 6, siano a, b, c; p, q, r interi positivi

t.c. $a^p + b^q + c^r = a^q + b^r + c^p = a^r + b^p + c^q$

Tesi: $a=b=c$ oppure $p=q=r$

Sol: wlog $a \geq b \geq c$, $p \geq q$, $p \geq r$

without loss of generality

Ci sono 2 casi $q \geq r$, $q < r$

Caso $q \geq r$: Idea: $a^p + b^q + c^r$ sembra il membro più grande

$$a^p + b^q + c^r \overset{?}{\geq} a^q + b^r + c^p$$

Hope

$q = r + x \quad x \geq 0$; $p = r + x + y \quad y \geq 0$

$$\boxed{a^{r+x}(a^y - 1) + b^r(b^x - 1)} \overset{?}{\geq} \boxed{c^r(c^{x+y} - 1)}$$

$a^r \geq c^r \qquad b^r \geq c^r$

$\boxed{} \underset{\Uparrow}{\geq} c^r \cdot a^x(a^y-1) + c^r(b^x-1) \underset{\Uparrow}{\overset{?}{\geq}} \boxed{}$

è vera — la nuova speranza

$$a^x(a^y-1) + b^x \geq c^{x+y}$$ ...finite i dettagli.

Disuguaglianze 2.0

Se $0 < x < 1$ allora x non è intero

Es: determinare tutti gli interi n t.c.

$\frac{2017}{n+3}$ è intero

Oss: se $n \gg 0$ allora $0 < \frac{2017}{n+3} < 1$

se $n \ll 0$ " $-1 < \frac{2017}{n+3} < 0$

Es: T1 n° 13 quanti sono gli n t.c.

$n^2 + 85n + 2017$ è $\square$

Sol: $n^2 + 85n + 2017 = a^2$

$(n+44+b)^2$

" $= (n+b)^2$ (ora cerco b)

$$85n + 2017 = 2nb + b^2$$

$$n = \frac{2017 - b^2}{2b - 85} \in \mathbb{Z}$$

allora

$$4n = \frac{4 \cdot 2017 - (2b)^2}{2b - 85}$$ è intero

$$4n = Q(2b) + \frac{4\cdot 2017 - (85)^2}{2b-85} \qquad \square$$

Es: Cesenatico2 Dimostrare che esistono, fissato $n \in \mathbb{Z}$, solo finite terne di interi (a,b,c) t.c.

$$\begin{cases} a+b-c=n \\ a^2+b^2-c^2=n \end{cases}$$

Sol: $a = n-b+c$

$$n^2+b^2+\cancel{c^2}-2nb+2nc-2bc+b^2-\cancel{c^2}=n$$

$$b^2-bc-nb+nc+\frac{n^2-n}{2}=0$$

ora $c = \dfrac{b^2-nb+\frac{n^2-n}{2}}{b-n} \in \mathbb{Z}$

$c-b = \dfrac{\frac{n^2-n}{2}}{b-n} \in \mathbb{Z}$ ho solo finite possibilità per b

---

$$c = a+b-n$$

$$a^2+b^2-(a+b-n)^2 = n$$

$$-n^2-2ab+2an+2bn = n$$

$$-2(a-n)(b-n)+n^2=n$$

$$(a-n)(b-n) = \frac{n^2-n}{2} \qquad \text{....fine}$$

$$a-c = n-b$$

$$a^2-c^2 = n-b^2$$

$$a+c = \frac{n-b^2}{n-b} = Q(b) + \frac{n-n^2}{n-b} \qquad \text{....fine.}$$

Congruenze

$a \mid b$ "a divide b" $\exists\, c \in \mathbb{Z}$ t.c. $b = ac$

$(n \mid 0 \;,\; 1 \mid n \;,\; -1 \mid n)$

p è un numero primo quando

$p > 1$ intero, $\quad p = ab \Rightarrow p = a \vee p = b$

$p \mid ab \Rightarrow p \mid a \vee p \mid b$

Dato n intero $a \equiv b$ è una relazione di equivalenza

$\Leftrightarrow n \mid a - b$

$\Leftrightarrow$ il resto della divisione tra a e n
e " b e n
è lo stesso

si usa lavorare con dei rappresentanti:

$0, \dots, n-1$ oppure $-\left\lfloor \frac{n}{2} \right\rfloor, \dots, \left\lceil \frac{n}{2} \right\rceil$

a meno di off by 1

Le operazioni vengono rispettate!

- se $a \equiv b$ e $c \equiv d \Rightarrow a + c \equiv b + d$

- " $\Rightarrow ac \equiv bd$

Non è vero che: $\cancel{\frac{a}{c} \equiv \frac{b}{d}}$

$\cancel{a^c \equiv b^d}$

Es: $5a \equiv 5b \quad (6)$

$\Rightarrow a \equiv b \quad (6)$

infatti moltiplicando per 5 entrambi i membri

ottengo, $25 \equiv 1 \quad (6)$

Es: $5a \equiv 5b \quad (10)$

$\cancel{\Rightarrow} \; a \equiv b \quad (10)$

$\Rightarrow a \equiv b \quad \left(\frac{10}{5}\right)$

In generale, per dividere per a, cerchiamo un intero b t.c. $a \cdot b \equiv 1 \quad (n)$

$\Longleftrightarrow \quad n \mid ab - 1 \Longleftrightarrow \exists\, k$ t.c. $ab + nk = 1$

"si può dividere per a mod n" $\Leftrightarrow \exists\, b, k$ t.c. $ab + nk = 1$

$\Leftrightarrow \quad ax + ny = 1$ ha soluzioni intere.

Oss: se $d \mid a$, $d \mid n \Rightarrow d \mid 1 \Rightarrow d = \pm 1$

deve essere $(a, n) = 1$

$(\,\mathrm{MCD}(a, n) = 1\,)$

Oss. generalizzante: se avessi avuto questa diofantea

$ax + by = c$, la condizione sarebbe stata

$(a, b) \mid c$

Th (Bezout): se $(a,b) \mid c \Rightarrow \exists\, x, y$ interi

t.c. $ax + by = c$

Dim: intanto se so risolvere per $c = 1$, so risolvere

tutto: siano x_0, y_0 soluzioni $ax_0 + by_0 = 1$

allora cx_0, cy_0 " $ax + bx = c$

si dimostra per induzione estesa su $|a| + |b|$

si usa la divisione euclidea

$a = qb + r$ con $0 \le r < b$

$ax + by = 1$

$(qb + r)x + by = 1$

$rx + b(y - qx) = 1$

è del tipo $ax + by = 1$ con $a \leftarrow r$, $b \leftarrow b$

Per ipotesi induttiva $\exists\, x_0, y_0$ t.c.

$rx_0 + by_0 = 1$

ma allora ponendo $x = x_0$, $y = y_0 + qx_0$, risolvo

l'equazione di partenza

Attenzione al P.B: è quando $a=0 \vee b=0$

Th (Wilson): $(p-1)! \equiv -1 \quad (p)$

Dim: $1 \cdot 2 \cdot 3 \cdot \_\_\_\_ \cdot (p-2) \cdot (p-1) = (p-1)!$

Oss: posso accoppiare elementi inversi

Verifica 1: $a \not\equiv b \Rightarrow a^{-1} \not\equiv b^{-1}$

sono gli inversi moltipl.

$$a^{-1} \equiv b^{-1}$$
$$\Rightarrow a a^{-1} \equiv a b^{-1}$$
$$\Rightarrow 1 \equiv a b^{-1}$$
$$\Rightarrow b \equiv a (b^{-1} b)$$

Verifica 0: se x, y sono entrambi inversi di a

$$\Rightarrow x \equiv y$$

Verifica 2: $a \not\equiv a^{-1}$ tranne che se

$$a \equiv a^{-1} \Leftrightarrow a^2 \equiv 1$$
$$(a-1)(a+1) \equiv 0 \quad (p)$$
$$\Rightarrow p \mid (a-1)(a+1)$$
$$\Rightarrow a \equiv 1 \quad \vee \quad a \equiv -1$$

Ora tutto si semplifica e ottengo

$$(p-1)! \equiv (p-1) 1$$

Residui di quadrati o di potenze

Es: mod 3 : $0, 1, 2$

$\square$: $0, 1, 1$ $\Rightarrow$ $3a - 1 = b^2$

Verificate per esercizio che non tutte le classi di resto sono possibili come residui quadratici mod 4, 5, 7, 8

Es: mod 7 : $0, 1, 2, 3, 4, 5, 6$

$\square$: $0, 1, 1, -1, 1, -1, -1$

Es (IMO 2017.1) : a_0 fissato

e $a_{n+1} = \begin{cases} \sqrt{a_n} & \text{se } a_n \text{ è } \square \\ a_n + 3 & \text{altrimenti} \end{cases}$

Sol: Oss: la congruenza mod 3 gioca un ruolo importante

Oss: se $a_0 \equiv 0 \ (3) \Rightarrow a_n \equiv 0 \ (3)$

(induzione di 1 riga)

Oss: se applico (definit.) solo la seconda mossa allora a_0 non soddisfa la tesi

Per esempio $a_0 \equiv -1 \ (3)$

Rimane $a_0 \equiv 1$

Per induzione su a_0, mi riconduco sempre al caso $a_0 \equiv -1$ ($a_n \equiv -1$)

Esercizi:

P. 10 : 40, 41 (42, 43) 46, 49, 55

P. 42 : 2, 3, 6, 8

Bonus 1 : trovare tutte le terne (a,b,c) di razionali t.c.
$$7 = a^2+b^2+c^2$$

Bonus 42: $x, y > 0$ interi, risolvere
$$x^3+y^3 = x^2+42xy+y^2$$

Hint: - trovare bound dall'alto
- semplificare i casi con accortezze.

Correzione

es 40 $\quad (x-y)(x+y) = 2000$

oss: $x-y \equiv x+y \ (2)$

$(a - \dots)(b - \dots) = \dots$

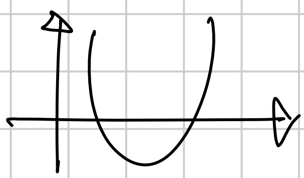
$(n+2)(m-1) = \dots$

es 41 $\quad \dfrac{n+7}{2n+1} \in \mathbb{Z} \iff \dfrac{2n+14}{2n+1} \in \mathbb{Z}$

$\iff \dfrac{13}{2n+1} \in \mathbb{Z}$

$-1 \overset{?}{<} \dfrac{3(5-n)}{2n^2+1} \overset{?}{<} 1$, stare attenti al caso $=0$

$-2n^2-1 < 15-3n$, $\quad P(n) > 0$



es 46: $5x + 8y = 22$ $\quad (-3, 2) = 1 \longrightarrow (-66, 44)$

$+n8 \quad -n5$

$5x + 3y = 1 \quad (-1, 2)$

$2x + 3y = 1 \quad (-1, 1)$

guardare le sol. di → $5x + 8y = 0 \quad (8n, -5n)$

es 49: $24 \mid n(n^2-1)(5n+2)$

$3 \mid (n^3 - n)$

$8 \mid$ $\quad$ $n = 0, 1$ $\quad$ guardo n mod 2

$n(n-1) \cdot (n+1)(5n+2)$

meglio guardare n mod 4 (meno casi)

es 55: $3^y - x^2 = 41$

mod 4: $(-1)^y - x^2 \equiv 1$

-1	0	$\equiv -1$
-1	-1	-2
1	0	1
1	-1	0

$2 \mid y$ $\quad (3^{y/2} - x)(3^{y/2} + x) = p$ .....

Es 2: per quali p, $x^2 + px - 444p$ ha sol. intere

$\Rightarrow \Delta = \square$

$\Delta = p^2 + 4 \cdot 444p = a^2$

mod p, $a^2 \equiv 0 \Rightarrow a \equiv 0 \Rightarrow a = pb$

$$p + 4\cdot 444 = pb^2$$

mod p, $\quad p \mid 4\cdot 444$ ...

Es 3

trovare a t.c. $\quad 59 \mid 2002a+3$

$$2002a + 3 \equiv 0$$
$$-4a \equiv -3$$
$$4a \equiv 3$$

$$15 \cdot 4 \equiv 60 \equiv 1 \quad (59)$$
$$a \equiv 3 \cdot 15$$

Es 6:

$$MCD\left(\{ p^4 - q^4, \; p, q > 10 \text{ primi} \}\right)$$

provo con $p = 13$, $q = 11$
e ottengo $\quad 2 \cdot 24 \cdot 290 = 2^5 \cdot 3 \cdot 5 \cdot 29$

se scelgo $p = 29 \quad q \neq 29$, il 29 sparisce!

neanche 2^5 è il bound corretto

$2^4 \cdot 3 \cdot 5$,

$$(p-q)(p+q)(p^2+q^2)$$

mod 3 $\qquad p, q \equiv 1, 2$

mod 5 $\qquad$ non sono tanti casi

(p,q)

q \ p	1	2	3	4
4	✓	×	×	✓
3	✓	✓	✓	×
2	✓	✓	×	×
1	✓	×	×	×

Es 8

$$\max\{(100 + \underset{\overset{\shortparallel}{d_n}}{n^2}, 100 + n^2 + 2n + 1)\} = ?$$

$$(100 + n^2, 100 + n^2 + 2n + 1) =$$
$$(100 + n^2, \; 2n + 1) =$$
$$(4 \cdot 100 + (2n)^2, \; 2n+1) =$$

$(401 \quad , 2n+1) \mid 401$

$d_n \leq 401$, provo $n=200$ per vedere che $d_n = 401$

Bonus 1 $\quad a^2+b^2+c^2 = 7d^2$ (assumo $MCD=1$, a meno di semplif.)

↳ perché $d \neq 0$

mod 4 ci sono 2 r.q.

mod 8 " 3 r.q. → 0, 1, 4

$a^2+b^2+c^2+d^2 \equiv 0$

$\Rightarrow a, b, c, d$ sono pari

ma avevo assunto $(a,b,c,d)=1$

Bonus 42 (BMO 2017.1) $\quad x, y > 0$

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

uso disug. cerco di dire che LHS > RHS

$$RHS = (x+y)^2+40xy \leq (x+y)^2+40\left(\frac{x+y}{2}\right)^2$$
$$= 11(x+y)^2$$

ora so che vale la dis.

$$x^3+y^3 \leq 11 \cdot (x+y)^2$$

$$\frac{1}{4}(x+y)^2 \overset{?}{\leq} x^2-xy+y^2 \leq 11 \cdot (x+y)$$

$$x^2+2xy+y^2 \leq 4x^2-4xy+4y^2$$
$$6xy \leq 3x^2+3y^2 \checkmark$$

Quindi ho che

$$\frac{1}{4}(x+y)^2 \leq 11 \cdot (x+y)$$

$$\Rightarrow \quad x+y \leq 44$$

$0 < x$, $0 < y$, $x+y \leq 44$

Ora, per diminuire i casi, uso <u>congruenze</u>

Metodo alternativo:

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

$s = x+y$, $p = xy$

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

$$p = \frac{s^3-s^2}{3s-40} \quad \ldots \text{ fine!}$$