Teoria dei numeri

Note Title 01/11/2019

$\mathbb{Z} = \{\dots -2, -1, 0, 1, 2 \dots\}$ (interi)

$\underbrace{}_{\text{naturali } \mathbb{N}}$

Problema. Quante sol (x, y) INTERE di

equazione di Fantea → $x^2 - y^2 = 2019$

$(x+y)(x-y) = 3 \cdot 673$

IDEA: fattorizzare!

per ogni valore ho una soluzione (x,y) diversa

± 1	± 2019
± 3	± 673
± 673	± 3
± 2019	± 1

→ $x = \pm 1010$ $y = \dots$

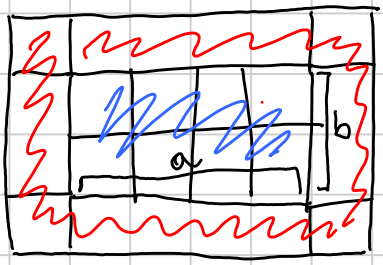
Ho trovato 8 soluzioni intere!

Problema bis $2020 = 2^2 \cdot 5 \cdot 101$

Che valori può prendere $(x+y)$? $\pm 2, \pm 2\cdot 5, \pm 2\cdot 101, \pm 2\cdot 5\cdot 101$

[# divisori di un numero $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ è $(e_1+1)(e_2+1)\dots(e_k+1)$]

Problema ter $x^2 - y^2 = 2022$ NON ha soluzioni!



Trovare tutti gli a, b interi ($a, b \geq 1$) t.c. area = perimetro

$ab = 2a + 2b + 4$

IDEA: Guardare i casi "grandi"

IDEA: dividere in casi

(ad es: $a \geq b$, a pari - vs - dispari, a, b coprimi ecc...)

assumo $a \geq b$ $\quad 2a + 2b + 4 \leq 4a + 4 \quad \Rightarrow b \leq 5$

$ab \leq 4a + 4$

[oppure $6a \leq ab \leq 4a + 4$, $2a \leq 4 \to a \leq 2$]

Adesso faccio i casi! $b = 1, 2, 3, 4, 5$

Per quali valori interi di b $\left(\frac{b^2+3b-1}{b-4}\right)^{\star}$ è intero?

(equivalentemente: $b-4 \mid b^2+3b-1$ ← "divide")

$$\frac{b^2+3b-1}{b-4} = \frac{\overbrace{(b-4)b}^{b^2-4b} + 7b - 1}{b-4} = b + \frac{7b-1}{b-4} = b + \frac{7(b-4)+27}{b-4}$$

$$= b + 7 + \frac{27}{b-4}$$

$\star$ è intero $\Leftrightarrow$ $\frac{7b-1}{b-4}$ è intero $\Leftrightarrow$ $b-4 \mid 27$

$\rightarrow$ guardo i divisori di 27, so quali sono!

NOTA: $d \mid a$, $d \mid a+b \Rightarrow d \mid b$

$d \mid a$, $d \mid b \Rightarrow d \mid na+mb \ \forall\, n, m$ interi

---

Quanto vale al max [MCD] $(n^2+100, (n+1)^2+100)$?

(spesso non si scrive)

n intero ≥ 0

NOTA $(a,b) = (a, a-b)$

$= (a, a-kb)$

$\Leftarrow$ [$(a,b) \mid (a, a-b)$ e $(a, a-b) \mid (a,b)$]

$$(n^2+100, (n+1)^2+100) = (2n+1, n^2+100) =$$
$$= (2n+1, 2n^2+200) =$$
$$= (2n+1, 200-n) =$$
$$= (2n+1, 400-2n) =$$
$$= (2n+1, 401)$$

L'MCD dell'inizio divide 401; la risposta è 401, effettivamente viene per $n=200$.

Ho un metodo per calcolare il MCD: algoritmo di Euclide

Basato su "divisione euclidea": a, b interi >0

DIVISIONE EUCLIDEA: $b = aq + r$, dove $0 \leq r \leq a-1$

$(a,b) = (a,r)$

$b > a$ $\quad b = aq + r$

Esempio:

$$(70,13) = (13\cdot 5+5, 13) =$$
$$= (5,13) = (5, 5\cdot 2+3) =$$
$$= (5,3) = (3\cdot 1+2, 3) =$$
$$= (2,3) = (2, 3 = 2\cdot 1+1) =$$
$$= (2,1) = 1$$

"intere (x,y)"

Domanda: che soluzioni ha un'equazione della forma $ax+by=c$? a,b,c interi

NOTA: dati a,b, perché ci sia soluzione dev'essere $(a,b) \mid c$.

Teorema [Bézout]: Se $(a,b) \mid c$ allora esiste una soluzione intera (x,y)

Suppongo $(a,b)=1$ ("primi fra loro") e $c=1$

ESEMPIO: $70x + 13y = 1$

$$1 = 3 - 2\cdot 1 = 3 - (5 - 3\cdot 1) = 2\cdot 3 - 5 =$$
$$= 2(13 - 5\cdot 2) - 5 =$$
$$= 2\cdot 13 - 5\cdot 5 =$$
$$= 2\cdot 13 - 5\cdot(70 - 13\cdot 5) =$$
$$= 27\cdot 13 - 5\cdot 70$$

Abbiamo trovato la soluzione $x=-5$ $y=27$

NOTA: se c'è una soluzione ce ne sono infinite!

$3^a - 2^b = 1$ quali soluzioni (a,b) intere non negative?

Provare casi "piccoli"!

$(1,1)$ è soluzione e $(2,3)$ è soluzione.

modulo 3: se $a \geq 1$ allora $3^a \equiv 0 (3)$, devo avere $(-1)^b \equiv -1 (3)$

$\Rightarrow$ ho scoperto che b deve essere dispari.

→ devo risolvere $3^a - 2^{2k+1} = 1$

→ posso provare a risolvere $3^a = 2^{2k+1} + 1 =$
$= (2+1)(2^{2k} - 2^{2k-1} + \dots)$

↑ dev'essere una potenza di 3

proviamo mod 4 : o $b = 1$ (poi lo faccio) o $3^a \equiv (-1)^a \equiv 1 (4)$
⇒ a pari! $3^{2k} - 2^b = 1$: devo risolvere
$(3^k + 1)(3^k - 1) = 2^b$

$MCD(3^k+1, 3^k-1) =$
$= (3^k+1, 2) \mid 2$

risolvo $3^k + 1 = 2^i$ $\quad 3^k - 1 = 2^j$ $\quad j < i$
devo avere $3^k - 1 = 1$ o 2

soluzione $k = 1$
⇒ $a = 2k = 2$, $b = 3$

↝ trovo tutte le soluzioni.

Qual è il MCD di tutti i numeri della forma $3n^5 + 5n^3 - 8n$ per $n > 1$ interi?

$o(3) \equiv 5n - 8n (3) \equiv$
$o(5) \equiv 3n - 8n (5) \equiv$

$n(3n^4 + 5n^2 - 8) = n(3n^2 + 8)(n^2 - 1) =$
$= n(3n^2 + 8)(n+1)(n-1)$

ottima idea!

è sempre divisibile per 3 e anche per 4!
In effetti c'è anche 5!
Poi basta trovare due numeri che abbiano MCD 120.

Piccolo teorema di Fermat: p primo, allora $\forall a \; a^p \equiv a (p)$
p primo, allora $\begin{cases} o \; a \equiv 0 (p) \\ o \; a^{p-1} \equiv 1 (p) \end{cases}$ [ordine di a mod p - cioè $\min n \mid a^n \equiv 1 (p)$ è un divisore di $p-1$]

PROBLEMI:

- p, q primi; se $p+q^2$ è un quadrato perfetto p^2+q^n NON lo è per nessun n.
- Dimostrare che $21n+4 / 14n+3$ non è mai intero
- Risolvere negli interi: $x^2+x+1=y^2$, $p^a+36=b^2$ (p primo, $a,b \geq 0$), $9^a-7^a=2^b$, $a,b \geq 0$,

$x^2+1 \equiv 0 \ (p)$ dove p primo è $\equiv 3 \ (4)$, $x^3+2y^3+4z^3=0$

- Dimostrare che $a^p \equiv a \ (p)$ (p primo) per induzione su a
- Qual è la più grande somma che NON si può spendere con monete di valore 7 e 16?

- Considera la successione a_n definita per $n \geq 10$ da $a_{n+1} = a_n + n$, $a_{10} = 10$; qual è il più grande $n \leq 100$ per cui $99 \mid a_n$.
- Se $13a \equiv 1 \bmod 99$ allora a cosa è $\equiv a \bmod 99$?

$$\frac{21n+4}{14n+3} = \frac{(14n+3)+(7n+1)}{14n+3} = 1 + \frac{7n+1}{14n+3}$$

$$14n+3 \mid 7n+1$$

$$\Longleftrightarrow \quad 14n+3 \mid 14n+2$$

$$14n+3 \mid -1$$

2) $13a \equiv 1 \ (99) \rightsquigarrow 99 \mid 13a-1$

$$13a-1 = 99b$$

$$\rightsquigarrow 13a - 99b = 1,$$

ha sol. solo quand $(13,-99) \mid 1$

$$99 = 99 \cdot 1 + 13 \cdot 0$$
$$13 = 99 \cdot 0 + 13 \cdot 1$$

$$8 = 99 \cdot 1 + 13 \cdot -7$$
$$5 = 99 \cdot -1 + 13 \cdot 8$$
$$3 = 99 \cdot 2 + 13 \cdot -15$$
$$2 = 99 \cdot -3 + 13 \cdot 23$$
$$1 = 99 \cdot 5 + 13 \cdot -38$$

Algoritmo di Euclide

$a \equiv -38 \bmod 99$

$13a \equiv 1 \bmod 99$

$$1 = 99a_1 + 13b_1$$
$$1 = 99a_2 + 13b_2 \quad \ominus$$

$$0 = 99(a_1 - a_2) + 13(b_1 - b_2)$$

$\Longrightarrow$?? $\boxed{13 \mid a_1 - a_2}$

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

$x^2 < x^2 + x + 1 < (x+1)^2$

$(x-1)^2 < x^2 + x + 1 < (x+1)^2$

x^2

mi serve che $x^2 + x + 1 > 0$ per $x \leq 0$

$x^2 + x + 1 < x^2 + 2x + 1$

0 1 4 9

$x^2 = x^2 + x + 1 \longrightarrow \boxed{x = -1,\ y = 1}$

99

13

MENSA!