Stage di TERNI - (25/01/2011)

Titolo nota 25/01/2011

ARITMETICA II

Trovare x, k interi t.c. $k<0$

1) $x^2+100k=27$

$100k$ è pari $\quad 27$ è dispari $\Rightarrow x^2$ dispari

$\Rightarrow x$ dispari

$x=2n+1 \qquad (2n+1)^2+100k=27$

$$\overbrace{4n^2+4n+1}+100k=27$$

$$4n^2+4n+100k=26$$

$$\underset{2}{\cancel{4}}\underbrace{(n^2+n+25k)}_{\text{intero impossibile}}=\underset{13}{\cancel{26}}$$

2) $x^2+4k=27 \dashrightarrow 4(n^2+n+k)=26$

impossibile

3) $x^2+4k=5 \dashrightarrow 4(n^2+n+k)=5-1=4$

si risolve

$(1+4=5$

$\quad \| $

$1^2+4\cdot 1=5)$

4) $x^2+4k=4h-1$

impossibile.

$$a^2+3b^2=113$$

→ a pari, b dispari I

→ a dispari, b pari II

I $a=2c \qquad b=2d+1$

$$4c^2+3(4d^2+4d+1)=113$$

$$4c^2+12d^2+12d=110$$

$$4(c^2+3d^2+3d)=110$$

impossib.

II $a=2c+1$

$b=2d$

$$4c^2+4c+1+12d^2=113$$

$$\cancel{4}(c^2+c+3d^2)=\cancel{112}\ 28$$

$$c^2+c+3d^2=28$$

$d=2e \qquad c^2+c+12e^2=28$

$$12e^2-28=-c^2-c$$

$c=4k$

$c+1=4K$ ... è un casino ...

+	P	D
P	P	D
D	D	P

$2k \qquad 2k+1$

+	B	C
B	B	C
C	C	boh...

$3k \qquad 3k+1 \qquad 3k+2$

		B	S	A
0	B	B	S	A
1	S	S	A	B
2	A	A	B	S

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$$a^2 + \underbrace{3b^2}_{} = \underbrace{113}_{3k+2}$$

$$A + B = A$$

$$a^2 + 3b^2 = 113 \Rightarrow a^2 = 3k+2$$

$\Rightarrow$ a non è div. per 3

$\Rightarrow$ $a = 3c+1$ oppure $a = 3c+2$

ma in entrambi i casi

$a^2 = 3h+1 \Rightarrow$ è impossibile

$a^2 = 3k+2$

(i) $a = 3c+1$

$a^2 = 9c^2+6c+1 =$
$= 3(3c^2+2c)+1$ S

(ii) $a = 3c+2$

$a^2 = 9c^2+12c+4 =$
$= 3(c^2+4c+1)+1$ S

×	P	D
P	P	P
D	P	D

×	B	S	A
B	B	B	B
S	B	S	A
A	B	A	S

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

•) se n è dispari, n^2 è $4k+1$

•) se n non è mult di 3, n^2 è $3k+1$

•) se n non è multiplo di 7, n^3 è $7k \pm 1$

---

m un intero fissato. Due interi a, b si dicono CONGRUI MODULO m se

$$\odot \quad a - b = km$$

ovvero se $\odot$ $a-b$ è divisibile per m

ovvero se $\odot$ $a = hm + b$

ovvero se $\odot$ a, b hanno lo stesso resto quando li divido per m

ovvero se $\odot$ $a = x m + y$ $\quad b = z \cdot m + y$ $\quad x, y, z$ interi

Questo si scrive $a \equiv b \pmod{m}$

o più semplicemente $a \equiv b \ (m)$

<u>Es</u>: $35 \overset{?}{\equiv} 24 \ (11)$ sì

$111111 \equiv 0 \ (3)$ sì

$11111 \equiv 2 \ (3)$ $\qquad 11111 \equiv 5 \ (9)$

$12133 \equiv 0 \quad (11) \qquad 31492 \equiv 10 \ (11)$

<u>Proprietà</u>: $a \equiv b \ (m) \qquad c \equiv d \ (m)$

1) $a+c \equiv b+d \ (m)$

$a-b = km \qquad c-d = hm$

1bis) $a-c \equiv b-d \ (m)$

$(a+c)-(b+d) = (k+h)m$

2) $ac \equiv bd \ (m)$

$a = km+b \qquad c = hm+d$

$$ac = \underbrace{m^2kh + m(kd+hb)}_{m \cdot \text{ROBA}} + bd$$

<u>Es</u>: $22 \equiv 12 \ (10) \qquad 2 \equiv 2 \ (10)$

$11 \not\equiv 6 \ (10)$

<u>Es +</u>: $22 \equiv 12 \ (10)$

$22 - 12 = 10 \cdot 1$

$11 - 6 = 5 \cdot 1 \rightarrow$ è una congruenza modulo 5

Es: $16 \equiv 2 \quad (7) \qquad 16-2 = 7 \cdot 2$

$8 \equiv 1 \quad (7) \longleftarrow \quad 8-1 = 7$

Es: $16 \equiv 30 \quad (7)$

$8 \equiv 15 \quad (7)$

In generale: $a \equiv b \quad (m)$ se a, b sono multipli di un certo n

e $MCD(n, m) = 1$

allora $\frac{a}{n} \equiv \frac{b}{n} \quad (m)$

Es: $50 \equiv -10 \quad (12)$

$\cancel{50} - (-\cancel{10}) = \cancel{5} \cdot \cancel{12}^{6}$ non posso dividere.

$5 - (-1) = 6$

Oss: modulo un numero primo $= p$ posso dividere posso dividere per qualunque numero a parte i multipli di p

— ooo —

$2x + 1 \equiv 0 \quad (7)$

$2x \equiv -1 \quad (7)$

$$4(2x) \equiv -4 \quad (7)$$

$$\underset{\overset{\shortparallel}{0}}{7} + x \equiv \underset{\overset{\shortparallel}{0}}{-4+7} \quad (7)$$

$$x \equiv 3 \quad (7) \longrightarrow \boxed{7k+3}$$

<u>Es</u>: Carlo inizia ad andare in palestra un Lunedì e poi ci va ogni 4 giorni. Quando sarà la prima volta che ci va di Sabato?

Dom	Lun	Mar	Mer	Gio	Ven	Sab
0	1	2	3	4	5	6

$$1 + 4x \equiv 6 \quad (7)$$

$$4x \equiv 5 \quad (7)$$

$$2 \cdot 4x \equiv 10 \quad (7)$$

$$x \equiv 3 \quad (7) \longrightarrow$$

$x = 7k+3$

La prima volta che Sabato è per $x=3$

$\Rightarrow$ è la 4ª volta che va in palestra.

— o —

$$4x \equiv 0 \quad (16)$$

x	$4x$	x	$4x$
0	0	8	0
1	4	9	4
2	8	10	8
3	12	11	12
4	0	12	0
5	4	13	4
6	8	14	8
7	12	15	12

$x \equiv 0, 4, 8, 12 \quad (16)$

<u>Es:</u> $2x \equiv 1 \quad (8)$

$\Downarrow$

impossibile

x	$2x$
0	0
1	2
2	4
3	6
4	0

x	$2x$
5	2
6	4
7	6

<u>Come si fa:</u> $ax + b \equiv 0 \quad (m)$

- <u>Se</u> $MCD(a, m) = 1$ <u>allora</u> posso trovare c tale che $ac \equiv 1 \ (m)$

$2x \equiv 5 \ (7)$

$\Rightarrow x \equiv -bc \quad (m)$

- <u>Se</u> $MCD(a, m) = d > 1$ <u>allora</u>:

(i) d divide anche b

$2x \equiv 4 \ (8) \leftarrow$ allora divido <u>TUTTO</u>

$$\frac{a}{d}x + \frac{b}{d} \equiv 0 \quad \left(\frac{m}{d}\right)$$

$2x \equiv 1 \ (8)$ ← (ii) Se d non divide b allora è <u>impossibile</u>

<u>Oss</u>: quadrati modulo 4

x	x^2
0	0
1	1
2	0
3	1

mod 4

cubi modulo 7

$6 \equiv -1 \ (7)$

$7k \pm 1$

x	x^3
0	0
1	1
2	1
3	6

x	x^3
4	1
5	6
6	6

<u>Esercizi</u>

1) Risolvere le seguenti equazioni:

(i) $4x - 2 \equiv 0 \ (13)$ (ii) $2x - 8 \equiv 0 \ (17)$

(iii) $6x - 3 \equiv 0 \ (12)$ (iv) $7x - 2 \equiv 0 \ (21)$

2) Trovare i numeri interi n con $0 \leq n \leq 100$ tali che $3n^2 + 2n - 1$ è multiplo di 13

3) Trovare x, y interi t.c. $x^3 + y^3 = 710$

4) Trovare il più piccolo $x > 0$ che ha resto 2 se diviso per 7

e resto 5 se divido per 11

1) (i) $4x-2 \equiv 0 \ (13)$ $\qquad MCD(2,13)=1$

$\Downarrow$

$2x-1 \equiv 0 \ (13)$ $\qquad$ posso dividere per 2

$2x \equiv 1 \ (13)$

$13+1=2\cdot 7 \rightarrow 1 \equiv 2\cdot 7 \ (13)$

$x \equiv 7 \ (13)$

(ii) $2x-8 \equiv 0 \ (17)$ $\qquad MCD(2,17)=1$

$x \equiv 4 \ (17)$

(iii) $6x-3 \equiv 0 \ (12)$ $\qquad 6x-3=12k$

$MCD(6,12)$ deve $\qquad 2x-1=4k$ impossibile

dividere 3, ma non è vero

(iv) $7x-2 \equiv 0 \ (21)$ $\qquad MCD(7,21)=7$ non divide 2.

2) $3n^2+2n-1 \equiv 0 \ (13)$

$\parallel$

$3(n+1)(n-\frac{1}{3}) = (n+1)(3n-1) \equiv 0 \ (13)$

13 divide $(n+1)(3n-1) \Rightarrow$ 13 divide $n+1$

o

13 divide $3n-1$

$n+1 \equiv 0 \ (13)$ $\quad n \equiv -1 \ (13)$ $\qquad n=13k+12$

$3n-1 \equiv 0 \ (13) \quad 3n \equiv 1 \ (13) \quad -4 \cdot 3n \equiv -4 \ (13)$

$-12n \equiv -4 \ (13) \quad n \equiv -4 \ (13) \quad n = 13h - 4$

3) $x^3 + y^3 = 710$ $\quad x^3, y^3$ modulo 7 possono essere $\begin{cases} 0 \\ 1 \\ -1 \end{cases}$

$$x^3 + y^3 \equiv \begin{cases} 0+0 \\ 0+1 \\ 0-1 \\ 1+1 \\ 1-1 \\ -1-1 \end{cases} \equiv \begin{cases} 0 \\ 1 \\ -1 \\ 2 \\ 0 \\ -2 \end{cases} \equiv \begin{cases} 0 \\ 1 \\ 6 \\ 2 \\ 0 \\ 5 \end{cases} \not\equiv 3 \ (7)$$

$710 \equiv 3 \ (7)$ $\quad \Rightarrow$ non esistono.

4)

$$\begin{cases} x \equiv 2 \ (7) \\ x \equiv 5 \ (11) \end{cases} \rightsquigarrow \begin{cases} x = 7k + 2 \\ 7k + 2 \equiv 5 \ (11) \end{cases}$$

$7k \equiv 3 \ (11) \quad k = 11h + 2$

$-3 \cdot 7k \equiv -9 \ (11) \quad x = 77h + 14 + 2 =$

$k \equiv 2 \ (11) \quad = 77h + 16$

$h = 0 \Rightarrow x = 16$