ARITMETICA MODULARE (O DELL'OROLOGIO) (1)

SI PUÒ APPLICARE A FENOMENI CHE HANNO UN ANDAMENTO CICLICO (PERIODICO).

AD ESEMPIO I GIORNI DELLA SETTIMANA:

OGGI È LUNEDÌ 12/12/2016

CHE GIORNO DELLA SETTIMANA SARÀ IL 13/05/2017?

DIC: 19 G; GEN: 31 G; FEB: 28 G; MAR: 31 G; APR: 30; MAGG: 13; = 152 G.

$152 : 7 = 21$

14

12

7

RESTO = 5 → SABATO

L'ESEMPIO CI FA CAPIRE CHE IN ALCUNI PROBLEMI LA SOLUZIONE PUÒ ESSERE FORNITA DA UNO STO DI UNA OPPORTUNA DIVISIONE.

NEL CASO DELLA SETTIMANA POSSIAMO SCRIVERE IN MODO OPPORTUNO:

-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
...	...	...	...	...	...	...

I NUMERI IN OGNI COLONNA SONO CARATTERIZZATI DALLO STESSO RESTO NELLA DIVISIONE PER 7

DEFINIZIONE DI CONGRUENZA MODULO m (mod m)

Dati due interi a e b diciamo che sono <u>congrui modulo m</u>, se il resto della loro divisione per m è lo stesso

Si scrive $a \equiv b \pmod m$

Esempio: $50 \equiv 18 \pmod 8$

Infatti: $50 : 8 = 6$ resto 2 (48) ; $18 : 8 = 2$ resto 2 (16)

$16 \equiv -4 \pmod 5$ Infatti: $16 : 5 = 3$ resto 1 (15) ; $-4 : 5 = -1$ resto $+1$ (-5)

PROPRIETÀ

$a \equiv b \pmod m \iff m \mid a-b$ (se e solo se)

$\Rightarrow$ $a = k_1 m + r$, $b = k_2 m + r$ $\rightarrow$

$\rightarrow a - b = k_1 m + r - k_2 m - r = (k_1 - k_2) m$

dunque $m \mid a-b$

$\Leftarrow$ $a - b = km \rightarrow a - b = (k_1 - k_2) m \rightarrow$

$\rightarrow a - b = k_1 m - k_2 m + (r - r) \rightarrow a = k_1 m + r$

$b = k_2 m + r$

ESEMPIO: $50 \equiv 18 \pmod 8 \rightarrow 50 - 18 = 32$

$8 \mid 32$

$16 \equiv -4 \pmod 5 \rightarrow 16 - (-4) = 20$

$5 \mid 20$

$a \equiv b \pmod m \Rightarrow \exists$ (esiste) $k \in$ (appartenente) $\mathbb{Z}$ tale che $a \equiv km + b$

DIMOSTRAZIONE:

$a = k_1 m + r$ e $b = k_2 m + r$ (stesso resto) $\rightarrow a - b = (\overbrace{k_1 - k_2}^{k}) b$

$a - b = km \rightarrow a = km + b$ e.v.d.

ESEMPIO: $\overset{a}{50} \equiv \overset{b}{18} \pmod{\overset{m}{8}}$

$50 - 18 = 32 \qquad 32 : 8 = 4 \rightarrow 50 - 18 = 4 \cdot 8$

$\overset{a}{50} = \overset{km}{4 \cdot 8} + \overset{b}{18}$

$16 \equiv -4 \pmod 5 \rightarrow 16 - (-4) = 20$

$20 : 5 = 4 \rightarrow 16 - (-4) = 4 \cdot 5 \rightarrow \overset{a}{16} = \overset{km}{4 \cdot 5} - \overset{b}{4}$

PROPRIETÀ

$a \equiv 0 \pmod m \iff m \mid a$

$\Rightarrow \quad a - 0 = km \rightarrow a = km$

$\Leftarrow \quad a = km \rightarrow a - 0 = km$

$10 \equiv 0 \pmod 5 \iff 5 \mid 10$

PER ABBREVIARE D'ORA IN POI INDICHEREMO CON LA NUOVA SCRITTURA $a \equiv b \pmod m$

$[a]_m \equiv [b]_m$.

OPERAZIONI E CONGRUENZE.

SOMMA (LA DIMOSTRAZIONE È A PAG. 6)

SE $[a]_m \equiv [a']_m$ e $[b]_m \equiv [b']_m \Rightarrow [a+b]_m \equiv [a'+b']_m$

ESEMPIO:

$[\overset{a}{17}]_5 \equiv [\overset{a'}{7}]_5$ (Resto 2) $[\overset{b}{18}]_5 \equiv [\overset{b'}{8}]_5$ (Resto 3)

$[\overset{a}{17}+\overset{b}{18}]_5 \equiv [\overset{a'}{7}+\overset{b'}{8}]_5 \Rightarrow [35]_5 \equiv [15]_5$ (Resto 0)

N.B. La somma dei resti iniziali è $3+2=[5]_5 \equiv [0]_5$

Questo vuol dire che in una somma, anche tra più di due numeri, ai fini della congruenza possiamo sostituire i numeri (addendi) iniziali con altri con i quali sia più semplice fare calcoli. (dei resti)

ESEMPIO: Per quali $n \in \mathbb{N}$ la somma dei primi n numeri naturali è multiplo di 3?

Sia $S_n = 1+2+3+\dots+n$ la successione dei primi n numeri naturali.

$S_1 = 1$, $S_2 = 1+2 = 3$, $S_3 = 1+2+3 = 6$

$S_4 = 1+2+3+4 = 10$ $S_5 = 1+2+3+4+5 = 15$ $S_6 = 1+2+3+4+5+6 = 21$

$S_7 = 28$ $S_8 = 36$ $S_9 = 45$

Se ragioniamo modulo 3

$S_1, S_4, S_7, S_{10}, \ldots \to [1]_3$

$S_2, S_5, S_8, S_{11}, \ldots \to [0]_3$

$S_3, S_6, S_9, S_{12}, \ldots \to [0]_3$

~~Ma~~ $n = 2, 5, 8, 11 \to [n]_3 = [2]_3$

quindi: $n = 3, 6, 9, 12 \to [n]_3 = [0]_3$

sono gli n soluzione del problema.

Potevamo applicare il teorema delle somme.

Dopo aver notato che modulo 3 i naturali si possono scrivere con 3 classi di resto:

$\ldots -3, [0], 3, 6, \ldots$ CLASSE DI RESTO $\underline{0}$

$\ldots -2, [1], 4, 7, \ldots$ CLASSE DI RESTO $\underline{1}$

$\ldots [-1], 2, 5, 8, \ldots$ CLASSE DI RESTO $\underline{-1}$

$[2]_3 \equiv [-1]_3$

MASCHERIAMO -1

PERCHÉ CI CONVIENE

ALLORA $1+2+3+4+5+6+\ldots \equiv 1+(-1)+0+1+(-1)+0+\ldots$

QUINDI:

$n = 1 \to [S_1]_3 \equiv [1]_3$

$n = 2 \to [S_2]_3 \equiv [0]_3$

$n = 3 \to [S_3]_3 \equiv [0]_3 \Rightarrow$ SOLUZIONI.

$n = 4 \to [S_4]_3 \equiv [1]_3$ $\quad n = 2, 5, 8 \to [n]_3 \equiv [2]_3$

$n = 5 \to [S_5]_3 \equiv [0]_3$ $\quad n = 3, 6, 9 \to [n]_3 \equiv [0]_3$

$n = 6 \to [S_6]_3 \equiv [0]_3$

$\vdots$

PRODOTTO

Se $[a]_m \equiv [a']_m$ e $[b]_m \equiv [b']_m \rightarrow [a \cdot b]_m \equiv [a' b']_m$

ESEMPIO:

$[17]_5 \equiv [7]_5$ e $[18]_5 \equiv [8]_5$

$\downarrow R=2$ $\quad\quad$ $\downarrow R=3$

$[17 \cdot 18]_5 \equiv [7 \cdot 8]_5 \rightarrow [306]_5 \equiv [56]_5$ CON $R=1$

$R=1$ perché 2 e 3 (i resti iniziali) danno come prodotto $2 \cdot 3 = 6$ che $[6]_5 \equiv [1]_5$

DIMOSTRAZIONE:

Se $[a]_m \equiv [a']_m$ e $[b]_m \equiv [b']_m \Rightarrow$

$\Rightarrow m \mid (a-a')$ e $m \mid (b-b') \Rightarrow$ COMBINAZIONE LINEARE

$m \mid b \cdot (a-a') + a'(b-b') \Rightarrow m \mid b \cdot a - b a' + a' b - a' b'$

$m \mid ab - a' b' \Rightarrow [a \cdot b]_m \equiv [a' b']_m$ C.V.D.

DIMOSTRAZIONE DELLA SOMMA

Se $[a]_m \equiv [a']_m$ e $[b]_m \equiv [b']_m \Rightarrow$

$\Rightarrow m \mid (a-a')$ e $m \mid (b-b') \Rightarrow m \mid (a-a') + (b-b') \Rightarrow$

$\Rightarrow m \mid (a+b) - (a'+b') \Rightarrow [a+b]_m \equiv [a'+b']_m$ C.V.D.

DIVISIONE

LA DIVISIONE È INVECE PROBLEMATICA.

Esempio:

$[18]_3 \equiv [6]_3$ ma dividendo per 6

$[3]_3 \equiv [1]_3$ è falso!!!

$\downarrow$

$[0]_3$

Questo accade perché quando dividiamo per 6 eliminiamo il fattore decisivo per la divisibilità per 3!!!

PERÒ: $18 = \overset{k\cdot a}{6\cdot 3}$ $\quad 6 = \overset{k\cdot b}{6\cdot 1}$

$m = 3$; $k = 6$ $\quad MCD(k, m) = 3$

Sia $m' = \frac{m}{MCD} = \frac{3}{3} = 1$

Allora $[18]_3 \equiv [6]_3 \Rightarrow$ (Dividendo per 6 a e b)

$a \qquad b$

$[3]_1 \equiv [1]_1$ avendo sostituito m con m'.

PROBLEMA: LA SOMMA DEI QUADRATI DI TRE NUMERI DISPARI CONSECUTIVI È UN NUMERO DI 4 CIFRE TUTTE UGUALI TRA LORO. TROVA I TRE NUMERI.

Sia n il numero centrale della terna, gli altri due saranno $(n-2)$ e $(n+2)$

Allora: $(n-2)^2 + n^2 + (n+2)^2 \overset{*}{=} aaaa = 1111\cdot a$

$n^2 + 4 - 4n + n^2 + n^2 + 4 + 4n = 1111\cdot a \rightarrow 3n^2 + 8 = 1111\cdot a$

$3n^2+8 = 1111\cdot a$ (equazione diofantea)

Ragioniamo modulo 3! (Dispari?)

$3n^2$ è divisibile per 3, mentre 8 fa parte della classe di resto 2, quindi

$[3n_2+8]_3 \equiv [2]_3$ (Da notare come questo modo di ragionare ci consente di sostituire, ai fini della congruenza, un polinomio con un numero)

mentre $[1111]_3 \equiv [1]_3$

Ma allora se $[1111\cdot a]_3 \equiv [2]_3$ deve essere

allora (prodotto dei resti) $[a]_3 \equiv [2]_3 \to a = 2, 5, 8$???

Quale di questi valori di a è corretto?

Ragioniamo modulo 2!?

Poiché n è dispari $\to 3n^2+8$ è dispari,

ma allora poiché 1111 è dispari $\to a$ è dispari

$\to a = 5$ (Si poteva anche solo provare sostituendo $a = 2, 5, 8$ nell'equazione $3n^2+8 = 1111\cdot a$).

ATTENZIONE!

Se $a = b \Rightarrow [a]_m = [b]_m$

MA SE $[a]_m \equiv [b]_m \not\Rightarrow a = b$ naturalmente

(È ANCHE VERO CHE SE $[a]_m \neq [b]_m \Rightarrow a \neq b$)

DICIAMO CHE LA CONDIZIONE DI CONGRUENZA È NECESSARIA MA NON SUFFICIENTE PERCHÉ $a = b$.

Quindi noi sappiamo che per $e=5$

$3n^2+8 \equiv eeae$ → sia modulo 3 che modulo 2 ma non sappiamo se

$3n^2+8 = eeae = 5555$

Risolviamo $3n^2+8 = 5555 \rightarrow 3n^2 = 5547$

$n^2 = \frac{5547}{3} = 1849$

$n = 43 \rightarrow \underline{41,43,45}$

è la terna cercata.

$\sqrt{18.49}\,|\,43$

16 | 83×3

249

249

//

PROBLEMA: RISOLVERE LA SEGUENTE EQUAZIONE DIOFANTEA: $x^2+y^2+z^2 = 4^n$

con $x, y, z \in \mathbb{N}$

Parentesi esemplificative:

$x=60 \; ; \; y=40 \; ; \; z=70$

$x = 2^2 \cdot 3 \cdot 5 \; ; \; y = 2^3 \cdot 5^1 \; ; \; z = 2^1 \cdot 7^1 \cdot 5^1 \rightarrow MCD = 2^1 \cdot 5^1$

la più grande potenza di 2 che divide tutti e tre i numeri è 2^1 (che è anche la potenza di 2 che si trova in MCD)

Quindi $x = 2^1 \cdot 30 \; ; \; y = 2^1 \cdot 20 \; ; \; z = 2^1 \cdot 35$

In questo modo i tre numeri x, y, z che erano tutti e tre pari si trasformano nel prodotto di una potenza di 2 per tre numeri che non sono tutti e tre pari. (OSSERVAZIONE)

Quindi poniamo $x = 2^\alpha \cdot a$, $y = 2^\alpha \cdot b$, $z = 2^\alpha \cdot c$ dove 2^α è la potenza di 2 che compare in $MCD(x, y, z)$.

Sostituendo nell'equazione iniziale:

$(2^\alpha)^2 a^2 + (2^\alpha)^2 \cdot b^2 + (2^\alpha)^2 \cdot c^2 = 4^n$

Dividendo per $(2^\alpha)^2 = 2^{2\alpha} = 4^\alpha$ otteniamo:

$$a^2 + b^2 + c^2 = \frac{4^n}{4^\alpha} = 4^{n-\alpha}$$

ma $a^2 + b^2 + c^2 \in \mathbb{N}$ e $a^2 + b^2 + c^2 \geq 3$

Dunque $n > \alpha \rightarrow 4^{n-\alpha}$ è multiplo di 4,

dunque pari.

Per l'osservazione di pagina 9 i tre numeri a, b, c non possono essere tutti e tre pari, dunque due di loro devono essere dispari.

Ragionando modulo 4 sui quadrati:

Dato un numero pari $2m \rightarrow [(2m)^2]_4 \equiv [4m^2] \equiv [0]_4$

" " dispari $[(2m+1)^2]_4 \equiv [4m^2 + 4m + 1]_4 \equiv [1]_4$

Dunque $[a^2 + b^2 + c^2]_4 \equiv [1]_4 + [1]_4 + [0]_4 = [2]_4$

MA $[4^{n-\alpha}]_4 \equiv [0]_4 \rightarrow$ Dunque L'EQUAZIONE È IMPOSSIBILE ($[a]_m \neq [b]_m \Rightarrow a \neq b$)