

# ALLENAMENTI DI MATEMATICA

## TEORIA DEI NUMERI E ALGEBRA MODULARE

### SOLUZIONI DEGLI ESERCIZI

#### ES. 1

Vale la seguente catena di uguaglianze:

$$2^m 3^{2m} - 1 = (2 \cdot 3^2)^m - 1 = 18^m - 1$$

SERIE GEOMETRICA è il limite della successione delle somme parziali

$$S_m = \sum_{k=0}^m x^k = \frac{1-x^{m+1}}{1-x} \Rightarrow 1-x^{m+1} = (1-x) \sum_{k=0}^m x^k$$

cambiando i segni si ha:  $x^{m+1} - 1 = (x-1) \sum_{k=0}^m x^k$

Nel nostro caso:  $x = 18$  e  $m = n-1$

Quindi  $18^m - 1 = (18-1)(18^0 + 18^1 + \dots + 18^{m-1}) = 17 \cdot (1 + 18 + \dots + 18^{m-1})$

$$\Rightarrow 17 \mid (2^m 3^{2m} - 1).$$

#### ES. 2

Cond. nec. e suff. affinché  $ax + by + cz = d$  ammetta sol. intere

è che  $\text{MCD}(a, b, c) \mid d$ .

Qui  $\text{MCD}(6, 10, 15) = 1 \mid 1$  ok, ammette sol. intere.

L'eq. è  $6x + 10y - 15z = 1$ .

Divido i coeff di modulo maggiore per quello di mod minore  
cioè divido 15 e 10 per 6:

$$15 = 6 \cdot 2 + 3 = 3 \pmod{6}$$

$$10 = 6 \cdot 1 + 4 = 4 \pmod{6}$$

Riscrivo l'eq:  $6x + 4y - 3z = 1 \pmod{6}$

Divido ora 6 e 4 per 3:

$$6 = 3 \cdot 2 + 0 = 0 \pmod{3}$$

$$4 = 3 \cdot 1 + 1 = 1 \pmod{3}$$

$\pmod{3}$

Riscrivo l'eq:  $0x + y - 3z = 1 \Leftrightarrow y - 3z = 1$

Posso trovare una sol. particolare di questa eq:  $(0, 1, 0)$ .

Procedo a ritroso e adatto questa sol al passo precedente

modificando  $z$  che ha il coeff di modulo minore:  $(0, 1, 1)$

Infine selgo ancora di un passo e modifico la  $x$ :  $(1, 1, 1)$

La sol generale sarà:  $(1 + 10(-15)n, 1 + 6(-15)s, 1 + 6 \cdot 10t)$  con  $n + s + t = 0$ .

21

ES. 3

Se  $d|m$ , allora  $\frac{m}{d}$  è un intero e anch'esso divide  $m$ . Perciò ogni divisore di  $m$  è associato ad un altro. Quindi:  
 $m$  ha un numero dispari di divisori sse  $d = \frac{m}{d}$  per un certo  $d|m$  (cioè  $d$  è associato a  $\frac{m}{d}$  ma coincidono) sse  $m = d^2$  per un certo divisore di  $m$ , cioè  $m$  è un quadrato perfetto.

ES. 4

Consideriamo per esempio la 6<sup>a</sup> cella. La sua serratura verrà girata 4 volte, ai passaggi 1, 2, 3 e 6, essendo questi i divisori di 6, perciò alla fine sarà chiusa.

La serratura della nona cella sarà invece girata ai passaggi 1, 3 e 9 e perciò, alla fine del processo, sarà aperta.

Perciò basta individuare i numeri che abbiano un numero dispari di divisori. Dall'esercizio 3 sappiamo che un numero naturale  $n$  ha un numero dispari di divisori se e solo se è un quadrato perfetto. Quindi i quadrati perfetti hanno un numero dispari di divisori, gli altri un numero pari.

I quadrati perfetti compresi tra 1 e 50 sono: 1, 4, 9, 16, 25, 36, 49.

Di conseguenza, serreranno rilasciati solamente i prigionieri delle celle 1, 4, 9, 16, 25, 36, 49.

ES. 5

L'eq. è  $x^2 - y^2 = 2$  e cerco le sol. intere.

2 è un numero primo, si può scrivere solo come  $2 \cdot 1$ , pertanto

$$x^2 - y^2 = (x+y)(x-y) = 2 \cdot 1$$

Non è restrittivo supporre  $x, y \geq 0$ , infatti tutti gli altri casi si possono concludere o per simmetria o per cambio di c.c. a questo.

Vale  $x+y \geq x-y$ , quindi:

$$\begin{cases} x+y=2 \\ x-y=1 \end{cases} \Rightarrow x = \frac{3}{2} \text{ e } y = \frac{1}{2} \quad \nexists \text{ perché cerco degli interi}$$

Altro caso, per es.  $x \geq 0, y \leq 0$ , allora si avrebbe  $x-y \geq x+y$ .

Ma, in realtà basta porre  $x' = x$  e  $y' = -y$  che si ottiene  $x' \geq 0, y' \geq 0$  e  $x' + y' \geq x' - y'$  che è il caso spiegato.

Analogamente per gli altri casi non approfonditi.

ES. 6

Si ha  $m^2 + 3m + 5 = (m+7)(m-4) + 33$ , quindi  $11 \mid m^2 + 3m + 5$  se e solo se  $11 \mid (m+7)(m-4)$ .

Se  $11 \nmid (m+7)(m-4)$  allora  $11$  (e quindi  $121$ ) non divide  $m^2 + 3m + 5$ .

Supp invece che  $11$  divide  $(m+7)(m-4)$ . Allora  $11 \mid (m+7)$  o  $11 \mid (m-4)$ .

Ma  $m+7 \equiv m-4 \pmod{11}$ , quindi  $11$  divide sia  $(m+7)$  che  $(m-4)$ ,

da cui  $121 \mid (m+7)(m-4)$ . D'altra parte  $121 \nmid 33$  perciò

$$121 \nmid ((m+7)(m-4) + 33) = m^2 + 3m + 5.$$

In ogni caso  $121 \nmid (m^2 + 3m + 5)$ .

ES. 7

Siano  $x_i$  l'età di Alice e  $y_i$  l'età di Barbara, con  $i$  che indica le varie tappe. Riscriviamo il problema con questa notazione:

"Quando Alice avrà  $(x_1)$  un anno meno di quelli che avrà Barbara  $(y_2)$  quando Alice avrà  $(x_2)$  metà degli anni di quanti ne avrà Barbara  $(y_3)$  quando Alice avrà  $(x_3)$  il doppio dell'età che ha Barbara ora  $(y_0)$ , Barbara avrà  $(y_4)$  il triplo degli anni che aveva Alice  $(x_4)$  quando Barbara aveva  $(y_4)$  l'età che ha Alice ora  $(x_0)$ ."

$$\Rightarrow \begin{cases} x_1 = y_2 - 1 \\ x_2 = \frac{1}{2} y_3 \\ x_3 = 2y_0 \\ y_1 = 3x_4 \\ y_4 = x_0 \end{cases}$$

Prendiamo ora  $a, b, c, d \in \mathbb{N}$  tali che:

$$\begin{aligned} x_1 &= x_0 + a & y_1 &= y_0 + a \\ x_2 &= x_0 + b & y_2 &= y_0 + b \\ x_3 &= x_0 + c & y_3 &= y_0 + c \\ x_4 &= x_0 + d & y_4 &= y_0 + d \end{aligned}$$

Riscriviamo il sistema (con  $x_0 = x$  e  $y_0 = y$ ):

$$\begin{cases} x + a = y + b - 1 \\ x + b = \frac{1}{2}(y + c) \\ x + c = 2y \\ y + a = 3(x + d) \\ y + d = x \end{cases} \Rightarrow \begin{cases} x + a - b & & = y - 1 \\ x & + b - \frac{1}{2}c & = \frac{1}{2}y \\ \frac{1}{2}x & + \frac{1}{2}c & = y \\ 3x - a & + 3d & = y \\ 3x & - 3d & = 3y \end{cases}$$

Sommando le eq del sist si ottiene:

$$\frac{17}{2}x = \frac{13}{2}y - 1 \quad \text{cioè} \quad -17x + 13y = 2$$

Poiché  $x, y \in \mathbb{Z}$  questa è un'eq diofantea lineare.

Pongo  $X = -x$  e  $Y = y$  e risolvo:  $17X + 13Y = 2$ .

$\text{MCD}(17, 13) = 1 \mid 2 \Rightarrow$  l'eq ammette sol. intere.

$$17 = 13 \cdot 1 + 4 \quad ; \quad 13 = 4 \cdot 3 + 1 \quad ; \quad 4 = 1 \cdot 4 + 0$$

48

$$\Rightarrow 1 = 13 - 4 \cdot 3 = 13 - 17 \cdot 3 + 13 \cdot 3 = 17(-3) + 13(4)$$

Moltiplico per 2 e trovo una sol (particolare):  $2 = 17(-6) + 13(8)$

$$(\bar{x}, \bar{y}) = (-6, 8)$$

Sol generiche in  $x$  e  $y$ :  $(x, y) = (-6 + 13h, 8 - 17h)$

Sol generiche in  $x$  e  $y$ :  $(x, y) = (6 - 13h, 8 - 17h)$

Poiché una delle due è una teenager, si ha necessariamente  $h = 1$ , da cui  $x = 19$  (Alice) e  $y = 25$  (Barbara).

### ES. 8

Supponiamo che 167 non sia primo, allora  $\exists m > 1$  che divide 167.

Quindi  $m$  e  $\frac{167}{m}$  dividono entrambi 167 e il più piccolo tra i due è al massimo  $\sqrt{167}$  e deve avere una fattorizzazione in fattori

primi minori o uguali a  $\sqrt{167}$ . Poiché  $\sqrt{167} < 13$ , si prova subito

che nessuno tra i primi 2, 3, 5, 7, 11 divide 167, il che va contro l'ipotesi che 167 non sia primo. Pertanto 167 è primo.

### ES. 9

$d = 1$ ,  $d = 3$ ,  $d = 9$  hanno le proprietà richieste. Ora dobbiamo mostrare che non ce ne sono altri.

Supponiamo che  $d$  sia un numero di  $k$  cifre t.c. se  $d$  divide un intero  $n$ ,  $d$  divide anche ogni intero  $m$  costituito dalle stesse cifre di  $n$ .

Allora esiste un numero a  $k+2$  cifre  $10a_1a_2\dots a_k$  che è divisibile per  $d$ . Per la proprietà appena enunciata, segue che anche i numeri  $a_1a_2\dots a_k10$  e  $a_1a_2\dots a_k01$  sono divisibili per  $d$ . Ma visto che  $a_1a_2\dots a_k10 - a_1a_2\dots a_k01 = 9$ ,  $d$  deve dividere 9. Pertanto  $d = 1, 3, 9$ .