L. PARMEGGIANI 5/3/2019

ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)

Corso di Laurea: Informatica

SVOLGIMENTO DEGLI ESERCIZI PER CASA 1 (2^A PARTE)

$\boxed{4}$ In tutti i casi considerati nell'Esercizio 2, indicando con d il massimo comun divisore positivo di a e b, si trovino $m, n \in \mathbb{Z}$ tali che $d = ma + nb$.

1) $a = 126$, $b = 56$, $d = 14$

$$\underbrace{126}_{a} = \underbrace{56}_{b} \cdot 2 + \underbrace{14}_{d} \Rightarrow 14 = 126 - 56 \cdot 2$$

$$\Rightarrow \begin{cases} m = 1 \\ n = -2 \end{cases}$$

2) $a = 234$, $b = 273$, $d = 39$

$$\underbrace{273}_{b} = \underbrace{234}_{a} \cdot 1 + \underbrace{39}_{d} \Rightarrow 39 = 273 - 234$$

$$\Rightarrow \begin{cases} m = -1 \\ n = 1 \end{cases}$$

3) $a = -168$, $b = 180$, $d = 12$

$$180 = 168 \cdot 1 + 12$$

$$\Rightarrow \underbrace{180}_{b} = \underbrace{(-168)}_{a} \cdot (-1) + \underbrace{12}_{d} \Rightarrow 12 = 180 + (-168)$$

$$\Rightarrow \begin{cases} m = 1 \\ n = 1 \end{cases}$$

4) $a = 231$, $b = 165$, $d = 33$

$$231 = 165 \cdot 1 + 66 \Rightarrow \boxed{66 = 231 - 165}$$

$$165 = 66 \cdot 2 + \underbrace{33}_{d} \Rightarrow 33 = 165 - 66 \cdot 2 =$$

$$= 165 - (231 - 165) \cdot 2 =$$

$$= 165 - 231 \cdot 2 + 165 \cdot 2 =$$

$$= 165 \cdot 3 - 231 \cdot 2$$

$$\Longrightarrow \underbrace{33}_{d} = \underbrace{165}_{b}\cdot 3 + \underbrace{231}_{a}\cdot(-2)$$

$$\Longrightarrow \begin{cases} m = -2 \\ n = 3 \end{cases}$$

5) $a = -136$, $b = 48$, $d = 8$

$$136 = 48\cdot 2 + 40 \Longrightarrow \boxed{40 = 136 - 48\cdot 2}$$

$$48 = 40\cdot 1 + \underbrace{8}_{d} \Longrightarrow 8 = 48 - 40 = 48 - (136 - 48\cdot 2) = 48 - 136 + 48\cdot 2 = 48\cdot 3 - 136$$

$$\Longrightarrow \underbrace{8}_{d} = \underbrace{48}_{b}\cdot 3 + \underbrace{(-136)}_{a}$$

$$\Longrightarrow \begin{cases} m = 1 \\ n = 3 \end{cases}$$

6) $a = -208$, $b = 286$, $d = 26$

$$286 = 208\cdot 1 + 78 \Longrightarrow \boxed{78 = 286 - 208}$$

$$208 = 78\cdot 2 + 52 \Longrightarrow \boxed{52 = 208 - 78\cdot 2}$$

$$78 = 52\cdot 1 + \underbrace{26}_{d} \Longrightarrow 26 = 78 - 52 = 78 - (208 - 78\cdot 2) = 78 - 208 + 78\cdot 2 = 78\cdot 3 - 208 = (286 - 208)\cdot 3 - 208 = 286\cdot 3 - 208\cdot 3 - 208 = 286\cdot 3 - 208\cdot 4$$

a

$$\Longrightarrow \begin{cases} m = 4 \\ n = 3 \end{cases}$$

7) $a=132,\ b=180,\ d=12$

$$180 = 132+48 \Rightarrow \boxed{48 = 180-132}$$
$$132 = 48\cdot 2+36 \Rightarrow \boxed{36 = 132-48\cdot 2}$$
$$48 = 36\cdot 1+\underbrace{12}_{d} \Rightarrow 12 = 48-36 =$$
$$= 48-(132-48\cdot 2) =$$
$$= 48-132+48\cdot 2 =$$
$$= 48\cdot 3-132 =$$
$$= (180-132)\cdot 3-132 =$$
$$= 180\cdot 3-132\cdot 3-132 =$$
$$= 180\cdot 3-132\cdot 4$$

$$\Rightarrow \underbrace{12}_{d} = \underbrace{180}_{b}\cdot 3-\underbrace{132}_{a}\cdot 4$$

$$\Rightarrow \begin{cases} m=-4 \\ n=3 \end{cases}$$

$\boxed{5}$ Si dica quali delle seguenti congruenze sono vere e quali false:

1) $132 \equiv 8 \bmod 9$ FALSA : $132 = 9\cdot 14+6$
$\Rightarrow 132 \equiv 6 \bmod 9$

2) $132 \equiv 1 \bmod 11$ FALSA : $132 = 11\cdot 12+0$
$\Rightarrow 132 \equiv 0 \bmod 11$

3) $132 \equiv 0 \bmod 12$ $\boxed{\text{VERA}}$ $132 = 12\cdot 11+0$
$\Rightarrow 132 \equiv 0 \bmod 12$

4) $132 \equiv 4 \bmod 13$ FALSA : $132 = 13\cdot 10+2$
$\Rightarrow 132 \equiv 2 \bmod 13$

$\boxed{6}$ Si calcolino le tavole dell'addizione e della moltiplicazione per $\mathbb{Z}_3$ e per $\mathbb{Z}_6$.

$\mathbb{Z}_3$

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

$\mathbb{Z}_3$

$\cdot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

$\mathbb{Z}_6$

$+$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_4$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

$\mathbb{Z}_6$

$\cdot$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$