compito 9

1.) a) $9 = 4 \cdot 2 + 1$
$4 = 2 \cdot 2 + 0$
$\text{mcd}(4,9) = 1$

$1 = 9 - 4 \cdot 2$
$1 = 9 \cdot (1) + 4 \cdot (-2)$
$1 \equiv 4 \cdot (-2) \pmod 9$

un inverso è -2 $\quad -2 \equiv 7 \pmod 9$
l'inverso è 7.

b) $5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$
$\text{mcd}(5,3) = 1$

$1 = 3 - 2 \cdot 1$
$= 3 - (5 - 3 \cdot 1) \cdot 1$
$= 3 \cdot 2 - 5 \cdot 1$
$1 = 3 \cdot 2 + 5 \cdot (-1)$
$1 \equiv 3 \cdot 2 \pmod 5$

un inverso è 2
l'inverso è 2.

c) $144 = 19 \cdot 7 + 11$
$19 = 11 \cdot 1 + 8$
$11 = 8 \cdot 1 + 3$
$8 = 3 \cdot 2 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$
$\text{mcd}(144, 19) = 1$

$1 = 3 - 2 \cdot 1$
$= 3 - (8 - 3 \cdot 2) \cdot 1 = 3 \cdot 3 - 8 \cdot 1$
$= (11 - 8 \cdot 1) \cdot 3 - 8 \cdot 1 = 11 \cdot 3 - 8 \cdot 4$
$= 11 \cdot 3 - (19 - 11 \cdot 1) \cdot 4 = 11 \cdot 7 - 19 \cdot 4$
$= (144 - 19 \cdot 7) \cdot 7 - 19 \cdot 4 = 144 \cdot 7 - 19 \cdot 53$
$1 = 144 \cdot (7) + 19 \cdot (-53)$
$1 \equiv 19 \cdot (-53) \pmod{144}$

un inverso è -53
$-53 \equiv 91 \pmod{144}$
l'inverso è 91.

2.) a) $4x \equiv 5 \pmod 9$ $\quad \text{mcd}(4,9) = 1$ quindi 4 è invertibile modulo 9
un inverso di 4 (mod 9) è 7 quindi $x \equiv 35 \pmod 9$ cioè $x \equiv 8 \pmod 9$

b) $2x \equiv 7 \pmod{17}$ $\quad \text{mcd}(2,17) = 1$ quindi 2 è invertibile modulo 17
un inverso di 2 (mod 17) è 9 quindi $x \equiv 63 \pmod{17}$ cioè $x \equiv 12 \pmod{17}$.

c) $4x \equiv 2 \pmod 8$ $\quad \text{mcd}(4,8) = 4$ $4 \nmid 2$ quindi non ci sono soluzioni

d) $15x \equiv 9 \pmod{21}$ $\quad \text{mcd}(15,21) = 3$ $3 \mid 9$ ci sono soluzioni (e ci sono 3 modulo 21).

$21 = 15 \cdot 1 + 6$
$15 = 6 \cdot 2 + 3$
$6 = 3 \cdot 2 + 0$
$\text{mcd}(15,21) = 3$

$3 = 15 - 6 \cdot 2$
$= 15 - (21 - 15 \cdot 1) \cdot 2$
$= 15 \cdot 3 - 21 \cdot 2$
$3 = 15 \cdot (3) + 21 \cdot (-2)$

Consideriamo $15x + 21y = 9$

- omogeneo: $15x + 21y = 0$ $\quad$ $5x + 7y = 0$ $\quad$ sol $\begin{cases} x = 7h \\ y = -5h \end{cases}$ $h \in \mathbb{Z}$.

- particolare: $3 = 15 \cdot 3 + 21 \cdot (-2)$
$9 = 15 \cdot 9 + 21 \cdot (-6)$ $\quad$ sol. $\begin{cases} x_0 = 9 \\ y_0 = -6 \end{cases}$

sol. di $15x + 21y = 9$ sono $\begin{cases} x = 9 + 7h \\ y = -6 - 5h \end{cases}$ $h \in \mathbb{Z}$.

le sol. di $15x \equiv 9 \pmod{21}$ sono $x = 9 + 7h$, $h \in \mathbb{Z}$.

cioè $x \equiv 2 \pmod{21}$ o
$x \equiv 9 \pmod{21}$ o
$x \equiv 16 \pmod{21}$

3.) Dobbiamo risolvere il sistema $\begin{cases} x \equiv a_1 \pmod 4 \\ x \equiv a_2 \pmod 7 \end{cases}$ per (a_1, a_2) dati

mod 4: $\Pi_1 = 7$ $\quad 7 \equiv 3 \pmod 4$ $\quad 3 \cdot y_1 \equiv 1 \pmod 4$ $\quad y_1 = 3$

mod 7 $\quad \Pi_2 = 4$ $\quad 4 y_2 \equiv 1 \pmod 7$ $\quad y_2 = 2$

$x = a_1 \Pi_1 y_1 + a_2 \Pi_2 y_2 = a_1 \cdot 7 \cdot 3 + a_2 \cdot 4 \cdot 2 = a_1 \cdot 21 + a_2 \cdot 8$

a) $(0,0)$ $\quad x = 0 \cdot 21 + 0 \cdot 8 = 0$ $\quad x = 0$

b) $(3,1)$ $\quad x = 3 \cdot 21 + 1 \cdot 8 = 71 = 28 \cdot 2 + 15$ $\quad x = 15$

c) $(3,6)$ $\quad x = 3 \cdot 21 + 6 \cdot 8 = 111 = 28 \cdot 3 + 27$ $\quad x = 27$

d) $(3,5)$ $\quad x = 3 \cdot 21 + 5 \cdot 8 = 103 = 28 \cdot 3 + 19$ $\quad x = 19$

e) $(2,2)$ $\quad x = 2 \cdot 21 + 2 \cdot 8 = 58 = 28 \cdot 2 + 2$ $\quad x = 2$

f) $(1,1)$ $\quad x = 1 \cdot 21 + 1 \cdot 8 = 29 = 28 \cdot 1 + 1$ $\quad x = 1$

4.)

$0 : (0,0)$	$3 : (0,3)$	$6 : (0,1)$	$9 : (0,4)$	$12 : (0,2)$
$1 : (1,1)$	$4 : (1,4)$	$7 : (1,2)$	$10 : (1,0)$	$13 : (1,3)$
$2 : (2,2)$	$5 : (2,0)$	$8 : (2,3)$	$11 : (2,1)$	$14 : (2,4)$

5.)

a) $\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod{11} \end{cases}$ i moduli sono due a due relativamente primi. $m = 5 \cdot 7 \cdot 11 = 385$

modulo 5 $\quad \Pi_1 = 7 \cdot 11 = 77$ $\quad 77 \equiv 2 \pmod 5$ $\quad 2 \cdot y_1 \equiv 1 \pmod 5$ $\quad y_1 = 3$

modulo 7 $\quad \Pi_2 = 5 \cdot 11 = 55$ $\quad 55 \equiv 6 \pmod 7$ $\quad 6 y_2 \equiv 1 \pmod 7$ $\quad y_2 = 6$

modulo 11 $\quad \Pi_3 = 5 \cdot 7 = 35$ $\quad 35 \equiv 2 \pmod{11}$ $\quad 2 y_3 \equiv 1 \pmod{11}$ $\quad y_3 = 6$

$x = 1 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 3 \cdot 35 \cdot 6 = 231 + 660 + 630 = 1521$ $\quad 1521 \equiv 366 \pmod{385}$

quindi $x \equiv 366 \pmod{385}$ (controllo $366 \equiv 1 \pmod 5$, $366 \equiv 2 \pmod 7$, $366 \equiv 3 \pmod{11}$)

b) $\begin{cases} x \equiv 7 \pmod 5 \\ x \equiv 37 \pmod 7 \\ x \equiv 36 \pmod{11} \end{cases}$ $\quad 7 \equiv 2 \pmod 5$, $\quad 37 \equiv 2 \pmod 7$, $\quad 36 \equiv 3 \pmod{11}$ $\quad$ quindi il sistema è $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod{11} \end{cases}$

Dal calcolo di a) segue:
$x = 2 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 3 \cdot 35 \cdot 6 = 462 + 660 + 630 = 1752$, $\quad 1752 \equiv 212 \pmod{385}$,
quindi $x \equiv 212 \pmod{385}$ (fai i controlli!!)

c) $\begin{cases} 2x \equiv 3 \pmod 5 \\ 3x \equiv 6 \pmod 7 \end{cases}$ i moduli sono relativamente primi.

un inverso di 2 modulo 5 è 3 $\quad x \equiv 9 \pmod 5$ $\quad x \equiv 4 \pmod 5$

un inverso di 3 modulo 7 è 5 $\quad x \equiv 30 \pmod 7$ $\quad x \equiv 2 \pmod 7$

Il sistema è equivalente a $\begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$ $\quad m = 5 \cdot 7 = 35$

modulo 5: $\quad \Pi_1 = 7$ $\quad 7 \equiv 2 \pmod 5$ $\quad 2 \cdot y_1 \equiv 1 \pmod 5$ $\quad y_1 = 3$

modulo 7: $\quad \Pi_2 = 5$ $\quad 5 y_2 \equiv 1 \pmod 7$ $\quad y_2 = 3$

$x = 4 \cdot 7 \cdot 3 + 2 \cdot 5 \cdot 3 = 84 + 30 = 114$, $\quad 114 \equiv 9 \pmod{35}$, $\quad x \equiv 9 \pmod{35}$

(controllo: $2 \cdot 9 \equiv 18 \equiv 3 \pmod 5$, $\quad 3 \cdot 9 \equiv 27 \equiv 6 \pmod 7$ ok!)

d) $\begin{cases} x \equiv 347 \pmod{22} \\ 17x \equiv 77 \pmod{31} \\ x \equiv -300 \pmod{51} \end{cases}$ si osserva che i moduli sono due a due relativamente primi

$m = 22 \cdot 31 \cdot 51 = 34782$

$31 = 17 \cdot 1 + 14$ $\quad 1 = 3 - 2 \cdot 1$
$17 = 14 \cdot 1 + 3$ $\quad = 3 - (14 - 3 \cdot 4) \cdot 1 = 3 \cdot 5 - 14 \cdot 1$
$14 = 3 \cdot 4 + 2$ $\quad = (17 - 14 \cdot 1) \cdot 5 - 14 \cdot 1 = 17 \cdot 5 - 14 \cdot 6$
$3 = 2 \cdot 1 + 1$ $\quad = 17 \cdot 5 - (31 - 17 \cdot 1) \cdot 6 = 17 \cdot 11 - 31 \cdot 6$
$2 = 1 \cdot 2 + 0$ $\quad 1 = 17 \cdot 11 + 31 \cdot (-6)$ $\quad$ quindi $1 \equiv 17 \cdot 11 \pmod{31}$ un inverso di $17 \pmod{31}$ è 11

$\begin{cases} x \equiv 347 \pmod{22} \\ x \equiv 847 \pmod{31} \\ x \equiv -300 \pmod{51} \end{cases}$ cioè $\begin{cases} x \equiv 17 \pmod{22} \\ x \equiv 10 \pmod{31} \\ x \equiv 6 \pmod{51} \end{cases}$

modulo 22 $n_1 = 31 \cdot 51 = 1581$ $\quad 1581 \equiv 19 \pmod{22}$ $\quad 19\, y_1 \equiv 1 \pmod{22}$

$22 = 19 \cdot 1 + 3$ $\quad 1 = 19 - 3 \cdot 6$ $\quad 1 \equiv 19 \cdot 7 \pmod{22}$
$19 = 3 \cdot 6 + 1$ $\quad = 19 - (22 - 19 \cdot 1) \cdot 6 = 19 \cdot 7 - 22 \cdot 6$
$3 = 1 \cdot 3 + 0$ $\quad 1 = 19 \cdot 7 + 22 \cdot (-6)$ $\quad y_1 = 7$.

modulo 31 $n_2 = 22 \cdot 51 = 1122$ $\quad 1122 \equiv 6 \pmod{31}$ $\quad 6\, y_2 \equiv 1 \pmod{31}$

$31 = 6 \cdot 5 + 1$ $\quad 1 = 31 - 6 \cdot 5$ $\quad 1 \equiv 6 \cdot (-5) \pmod{31}$
$6 = 1 \cdot 6 + 0$ $\quad 1 = 31 \cdot 1 + 6 \cdot (-5)$ $\quad y_2 = -5$

modulo 51 $n_3 = 22 \cdot 31 = 682$ $\quad 682 \equiv 19 \pmod{51}$ $\quad 19\, y_3 \equiv 1 \pmod{51}$

$51 = 19 \cdot 2 + 13$ $\quad 1 = 13 - 6 \cdot 2$ $\quad 1 \equiv 19 \cdot (-8) \pmod{51}$
$19 = 13 \cdot 1 + 6$ $\quad = 13 - (19 - 13 \cdot 1) \cdot 2 = 13 \cdot 3 - 19 \cdot 2$
$13 = 6 \cdot 2 + 1$ $\quad = (51 - 19 \cdot 2) \cdot 3 - 19 \cdot 2 = 51 \cdot 3 - 19 \cdot 8$ $\quad y_3 = -8$
$6 = 1 \cdot 6 + 0$ $\quad 1 = 51 \cdot 3 + 19 \cdot (-8)$

$x = 17 \cdot 1581 \cdot 7 + 10 \cdot 1122 \cdot (-5) + 6 \cdot 682 \cdot (-8) = 188139 - 56100 - 32736 = 99303$

$99303 \equiv 29739 \pmod{34782}$ $\quad x \equiv 29739 \pmod{34782}$. (fai i controlli!)

e) $\begin{cases} x \equiv 264 \pmod{16} \\ 17x \equiv 18 \pmod{27} \\ x \equiv -504 \pmod{31} \end{cases}$ si osserva che i moduli sono due a due relativamente primi

$m = 16 \cdot 27 \cdot 31 = 13392$

$27 = 17 \cdot 1 + 10$ $\quad 1 = 7 - 3 \cdot 2$ $\quad 1 \equiv 17 \cdot 8 \pmod{27}$
$17 = 10 \cdot 1 + 7$ $\quad = 7 - (10 - 7 \cdot 1) \cdot 2 = 7 \cdot 3 - 10 \cdot 2$ un inverso di $17 \pmod{27}$ è 8.
$10 = 7 \cdot 1 + 3$ $\quad = (17 - 10 \cdot 1) \cdot 3 - 10 \cdot 2 = 17 \cdot 3 - 10 \cdot 5$
$7 = 3 \cdot 2 + 1$ $\quad = 17 \cdot 3 - (27 - 17 \cdot 1) \cdot 5 = 17 \cdot 8 - 27 \cdot 5$
$3 = 1 \cdot 3 + 0$ $\quad 1 = 17 \cdot 8 + 27 \cdot (-5)$

$\begin{cases} x \equiv 264 \pmod{16} \\ x \equiv 144 \pmod{27} \\ x \equiv -504 \pmod{31} \end{cases}$ cioè $\begin{cases} x \equiv 8 \pmod{16} \\ x \equiv 9 \pmod{27} \\ x \equiv 18 \pmod{31} \end{cases}$

modulo 16: $n_1 = 27 \cdot 31 = 837$ $\quad 837 \equiv 5 \pmod{16}$ $\quad 5\, y_1 \equiv 1 \pmod{16}$

$16 = 5 \cdot 3 + 1$ $\quad 1 = 16 - 5 \cdot 3$ $\quad 1 \equiv 5 \cdot (-3) \pmod{16}$
$5 = 1 \cdot 5 + 0$ $\quad 1 = 16 + 5 \cdot (-3)$ $\quad y_1 = -3$

modulo 27 $n_2 = 16 \cdot 31 = 496$ $\quad 496 \equiv 10 \pmod{27}$ $\quad 10\, y_2 \equiv 1 \pmod{27}$

$27 = 10 \cdot 2 + 7$ $\quad 1 = 7 - 3 \cdot 2$ $\quad 1 \equiv 10 \cdot (-8) \pmod{27}$
$10 = 7 \cdot 1 + 3$ $\quad = 7 - (10 - 7 \cdot 1) \cdot 2 = 7 \cdot 3 - 10 \cdot 2$
$7 = 3 \cdot 2 + 1$ $\quad = (27 - 10 \cdot 2) \cdot 3 - 10 \cdot 2 = 27 \cdot 3 - 10 \cdot 8$ $\quad y_2 = -8$
$3 = 1 \cdot 3 + 0$ $\quad 1 = 27 \cdot 3 + 10 \cdot (-8)$

modulo 31 $n_3 = 16 \cdot 27 = 432$ $\quad 432 \equiv 29 \pmod{31}$ $\quad 29\, y_1 \equiv 1 \pmod{31}$

$31 = 29 \cdot 1 + 2$
$29 = 2 \cdot 14 + 1$
$2 = 1 \cdot 2 + 0$

$1 = 29 - 2 \cdot 14$
$= 29 - (31 - 29 \cdot 1) \cdot 14 = 29 \cdot 15 - 31 \cdot 14$
$1 = 29 \cdot 15 + 31 (-14)$

$1 \equiv 29 \cdot 15 \pmod{31}$
$y_3 = 15$

$x = 8 \cdot 837 \cdot (-3) + 9 \cdot 496 \cdot (-8) + 18 \cdot 432 \cdot 15 = -20088 - 35712 + 116640 = 60840$

$60840 \equiv 7272 \pmod{33912}$ $\quad x \equiv 7272 \pmod{33912}$.

f) $\begin{cases} 6x \equiv 0 \pmod{31} \\ 3x \equiv -89 \pmod{10} \\ 8x \equiv 123 \pmod{21} \end{cases}$ si osserva che i moduli sono due a due relativamente primi

$m = 31 \cdot 10 \cdot 21 = 6510$.

$31 = 6 \cdot 5 + 1$
$6 = 1 \cdot 6 + 0$
$\text{mcd}(31, 6) = 1$

$1 = 31 - 6 \cdot 5$
$1 = 31 \cdot 1 + 6 \cdot (-5)$
$1 \equiv 6 \cdot (-5) \pmod{31}$

un inverso di 6 modulo 31 è -5
$6x \equiv 0 \pmod{31}$
$x \equiv 0 \pmod{31}$.

$10 = 3 \cdot 3 + 1$
$3 = 1 \cdot 3 + 0$
$\text{mcd}(10, 3) = 1$

$1 = 10 - 3 \cdot 3$
$1 = 10 \cdot 1 + 3 \cdot (-3)$
$1 \equiv 3 \cdot (-3) \pmod{10}$

un inverso di 3 modulo 10 è -3
$3x \equiv -89 \pmod{10}$
$x \equiv 267 \pmod{10}$
$x \equiv 7 \pmod{10}$

$21 = 8 \cdot 2 + 5$
$8 = 5 \cdot 1 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$
$\text{mcd}(21, 8) = 1$

$1 = 3 - 2 \cdot 1$
$= 3 - (5 - 3 \cdot 1) \cdot 1 = 3 \cdot 2 - 5 \cdot 1$
$= (8 - 5 \cdot 1) \cdot 2 - 5 \cdot 1 = 8 \cdot 2 - 5 \cdot 3$
$= 8 \cdot 2 - (21 - 8 \cdot 2) \cdot 3 = 8 \cdot 8 - 21 \cdot 3$
$1 = 8 \cdot 8 + 21 (-3)$
$1 \equiv 8 \cdot 8 \pmod{21}$

un inverso di 8 modulo 21 è 8
$8x \equiv 123 \pmod{21}$
$x \equiv 984 \pmod{21}$
$x \equiv 18 \pmod{21}$

Il sistema da risolvere è $\begin{cases} x \equiv 0 \pmod{31} \\ x \equiv 7 \pmod{10} \\ x \equiv 18 \pmod{21} \end{cases}$

modulo 31 $n_1 = 10 \cdot 21 = 210$ $\quad 210 \equiv 24 \pmod{31}$ $\quad 24\, y_1 \equiv 1 \pmod{31}$

$31 = 24 \cdot 1 + 7$
$24 = 7 \cdot 3 + 3$
$7 = 3 \cdot 2 + 1$
$3 = 1 \cdot 3 + 0$

$1 = 7 - 3 \cdot 2$
$= 7 - (24 - 7 \cdot 3) \cdot 2 = 7 \cdot 7 - 24 \cdot 2$
$= (31 - 24 \cdot 1) \cdot 7 - 24 \cdot 2 = 31 \cdot 7 - 24 \cdot 9$
$1 = 31 \cdot 7 + 24 (-9)$

$1 \equiv 24 \cdot (-9) \pmod{31}$
$y_1 = -9$

modulo 10 $n_2 = 31 \cdot 21 = 651$ $\quad 651 \equiv 1 \pmod{10}$ $\quad 1 \cdot y_2 \equiv 1 \pmod{10}$ $\quad y_2 = 1$.

modulo 21 $n_3 = 10 \cdot 31 = 310$ $\quad 310 \equiv 16 \pmod{21}$ $\quad 16\, y_3 \equiv 1 \pmod{21}$

$21 = 16 \cdot 1 + 5$
$16 = 5 \cdot 3 + 1$
$5 = 1 \cdot 5 + 0$

$1 = 16 - 5 \cdot 3$
$= 16 - (21 - 16 \cdot 1) \cdot 3 = 16 \cdot 4 - 21 \cdot 3$
$1 = 16 \cdot 4 + 21 \cdot (-3)$

$1 \equiv 16 \cdot 4 \pmod{21}$
$y_3 = 4$

$x = 0 \cdot 210 \cdot (-9) + 7 \cdot 651 \cdot 1 + 18 \cdot 310 \cdot 4 = 4557 + 22320 = 26877$

$26877 \equiv 837 \pmod{6510}$ $\quad x \equiv 837 \pmod{6510}$ (fai i conteggi)

6.)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

a) $p \longmapsto 21p + 2 \pmod{26}$ $\quad q = 21p + 2 \pmod{26}$ quindi $q - 2 \equiv 21p \pmod{26}$

$26 = 21 \cdot 5 + 5$ $\quad 1 = 21 - 5 \cdot 4$ $\quad 1 \equiv 21 \cdot 5 \pmod{26}$

$21 = 5 \cdot 4 + 1$ $\quad = 21 - (26 - 21 \cdot 1) \cdot 4 = 21 \cdot 5 - 26 \cdot 4$ un inverso di 21 modulo 26 è 5

$4 = 1 \cdot 4 + 0$ $\quad 1 = 21 \cdot 5 + 26(-4)$ $\quad 5(q-2) \equiv p \pmod{26}$

$q \longmapsto 5(q-2) \pmod{26}$

b) $P : 15 \longmapsto 5 \cdot 13 \equiv 65 \equiv 13 \pmod{26}$: N

$K : 10 \longmapsto 5 \cdot 8 \equiv 40 \equiv 14 \pmod{26}$: O

$Z : 25 \longmapsto 5 \cdot 23 \equiv 115 \equiv 11 \pmod{26}$: L

$Q : 16 \longmapsto 5 \cdot 14 \equiv 70 \equiv 18 \pmod{26}$: S

P K P Z K Q K

N O N L O S O

7.) $85 = 5 \cdot 17$

Quindi i primi p e q sono 5 e 17 $\quad (p-1)(q-1) = 4 \cdot 16 = 64$

$e = 43$ un inverso di 43 (mod 64):

$64 = 43 \cdot 1 + 21$ $\quad 1 = 43 - 21 \cdot 2$ $\quad 1 \equiv 43 \cdot 3 \pmod{64}$

$43 = 21 \cdot 2 + 1$ $\quad = 43 - (64 - 43 \cdot 1) \cdot 2 = 43 \cdot 3 - 64 \cdot 2$ un inverso di 43 (mod 64) è 3

$21 = 1 \cdot 21 + 0$ $\quad 1 = 43 \cdot 3 + 64 \cdot (-2)$ d'inverso di 43 (mod 64) è 3

$d = 3$

La funzione di codificazione: $x \longmapsto x^{43} \pmod{85}$

La funzione di decodificazione $x \longmapsto x^{3} \pmod{85}$.

$(59)^3 = 205379 = 85 \cdot 2416 + 19$ $\quad (59)^3 \equiv 19 \pmod{85}$: 19 S

$(60)^3 = 216000 = 85 \cdot 2541 + 15$ $\quad (60)^3 \equiv 15 \pmod{85}$: 15 O

$(00)^3 = 0$ $\quad (0)^3 \equiv 0 \pmod{85}$: 0 spazio

$(56)^3 = 175616 = 85 \cdot 2066 + 6$ $\quad (56)^3 \equiv 6 \pmod{85}$: 6 F

$(01)^3 = 1$ $\quad (1)^3 \equiv 1 \pmod{85}$: 1 A

$(52)^3 = 140608 = 85 \cdot 1654 + 18$ $\quad (52)^3 \equiv 18 \pmod{85}$: 18 R

$(23)^3 = 12167 = 85 \cdot 143 + 12$ $\quad (23)^3 \equiv 12 \pmod{85}$: 12 L

$(60)^3 = 216000 = 85 \cdot 2541 + 15$ $\quad (60)^3 \equiv 15 \pmod{85}$: 15 O

8.) inizio alle 7:00

finisce dopo le 22:00. Quindi almeno 15 ore $\quad 15 \times 60 = 900$ minuti

a) $900 = 48 \cdot 18 + 36$. quindi l'ultima volta che era all'autostazione erano 36 minuti prima delle 22:00 cioè alle 21:24

Si osserva che pullman A fa 18 turni e finisce alle 22:12

$900 = 57 \cdot 15 + 45$ quindi pullman B fa 16 turni e finisce alle 22:12

Quindi nessun problema con i sindacati.

b) Sia z il numero di minuti dopo le 7:00

sono arrivato con pullman B, quindi $z \equiv 0 \pmod{57}$

Fra 6 minuti arriva pullman A, quindi $z+6 \equiv 0 \pmod{48}$

da risolvere: $\begin{cases} z \equiv 0 \pmod{57} \\ z \equiv -6 \pmod{48} \end{cases}$

$57 = 48 \cdot 1 + 9$
$48 = 9 \cdot 5 + 3$
$9 = 3 \cdot 3 + 0$
$\text{mcd}(57, 48) = 3$

non si può usare il teorema cinese dei resti!!

Pullman A fa 19 turni; Pullman B fa 16 turni

Quindi $z = 57k$ per certo $0 \le k \le 16$

$z+6 = 48\ell$ per certo $0 \le \ell \le 19$ $\quad 57k + 6 = 48\ell$

quindi cerco le soluzioni di $48x - 57y = 6$ con $0 \le x \le 19$ e $0 \le y \le 16$

$\text{mcd}(57, 48) = 3$ $\quad 3 \mid 6$ ci sono soluzioni

omogeneo: $48x - 57y = 0$ $\quad 16x - 19y = 0$ $\quad$ sol. $\begin{cases} \hat{x} = 19n \\ \hat{y} = 16n \end{cases}$ $n \in \mathbb{Z}$.

particolare $\quad 3 = 48 - 9 \cdot 5$
$= 48 - (57 - 48 \cdot 1) \cdot 5 = 48 \cdot 6 - 57 \cdot 5$
$3 = 48 \cdot 6 - 57 \cdot 5$
$6 = 48 \cdot 12 - 57 \cdot 10$ $\quad$ una sol. $\begin{cases} x_0 = 12 \\ y_0 = 10 \end{cases}$

le soluzioni di $48x - 57y = 6$ sono $\begin{cases} x = 12 + 19n \\ y = 10 + 16n \end{cases}$ $n \in \mathbb{Z}$.

Però $0 \le x \le 19$ e $0 \le y \le 16$ quindi $n = 0$ e $\begin{cases} x = 12 \\ y = 10 \end{cases}$

Quindi dopo 10 turni con pullman B mi trovo all'autostazione e devo aspettare 6 minuti per pullman A. cioè $57 \cdot 10 = 570 = 60 \cdot 9 + 30$

Alle 16:30.

c) cerchiamo soluzioni di $48x - 57y = T$ dove T è il tempo da aspettare (se T è negativo vuole dire che sono arrivato con A e aspetto B)

$\text{mcd}(48, 57) = 3$ quindi $3 \mid T$.

1) $|T| = 0$ allora $\begin{cases} x = 19n \\ y = 16n \end{cases}$ $n \in \mathbb{Z}$ ma $0 < x < 19$ non è possibile.

2) $|T| = 3$ $\quad 3 = 48 \cdot 6 - 57 \cdot 5$ quindi $\begin{cases} x = 6 + 19n \\ y = 5 + 16n \end{cases}$ $n \in \mathbb{Z}$.

c'è un unica possibilità: $n = 0$: $x = 6$, $y = 5$ cioè 6 turni di pullman A : 5 pullman B

$6 \cdot 48 = 288 = 4 \cdot 60 + 48$ $\quad$ ore 11:48 $\quad$ pullman A
$5 \cdot 57 = 285 = 4 \cdot 60 + 45$ $\quad$ ore 11:45 $\quad$ pullman B

$-3 = 48 \cdot (-6) - 57 \cdot (-5)$ quindi $\begin{cases} x = -6 + 19n \\ y = -5 + 16n \end{cases}$ $n \in \mathbb{Z}$

c'è un unica possibilità $n = 1$ $\quad x = 13$ $\quad y = 11$ cioè 13 turni pullman A, 11 pullman B

$13 \cdot 48 = 624 = 10 \cdot 60 + 24$ $\quad$ ore 17:24 $\quad$ pullman A
$11 \cdot 57 = 627 = 10 \cdot 60 + 27$ $\quad$ ore 17:27 $\quad$ pullman B

Quindi ci sono due possibilità di aspettare 3 minuti

9.) $\left\lceil \frac{677}{38} \right\rceil = 18$

10.) Siano (a,b) e (c,d) due punti nel piano. Allora il punto intermedio sulla retta è $\left(\frac{1}{2}(a+c), \frac{1}{2}(b+d)\right)$. se $a,b,c,d \in \mathbb{Z}$ allora $\frac{1}{2}(a+c) \in \mathbb{Z}$ se e solo se $a \equiv c \pmod 2$, e $\frac{1}{2}(b+d) \in \mathbb{Z}$ se e solo se $b \equiv d \pmod 2$. Per ogni punto (a,b) con $a \in \mathbb{Z}$ e $b \in \mathbb{Z}$ vale $(a \pmod 2, b \pmod 2) \in \{(0,0),(1,0),(0,1),(1,1)\}$.

Dato 5 punti (x_i, y_i) $i \in \{1, \dots, 5\}$ con $x_i, y_i \in \mathbb{Z}$.

Allora esistono $i,j \in \{1, \dots 5\}$ con $(x_i \pmod 2, y_i \pmod 2) = (x_j \pmod 2, y_j \pmod 2)$ cioè $x_i \equiv x_j \pmod 2$ e $y_i \equiv y_j \pmod 2$. Quindi il punto intermedio sulla retta di (x_i, y_i) e (x_j, y_j) ha coordinate intere.