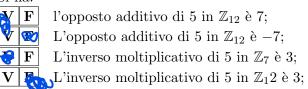
## ESERCIZI SU CONGRUENZE

(1) Si ha:

$$V$$
 |  $15 + 27 = 0 \text{ modulo } 14;$  |  $40\%14 = 12$  |  $15 - 27 = 0 \text{ modulo } 14;$  |  $12\%14 = 12 = -2$  |  $15^{342} = 1 \text{ modulo } 14.$ 

(2) Si ha:



(3) L'opposto additivo di a in  $\mathbb{Z}_n$  è uguale a

$$\begin{array}{|c|c|c|} \hline \mathbf{V} & a - n; \\ \hline \bullet & \mathbf{F} & n - a; \\ \hline \end{array}$$

(4) il numero 35724123 è congruo modulo 3 a:

(5) Trovare il resto nella divisione per 11 dei seguenti numeri (riducendo modulo 11):

```
154387, \qquad 12\%11=1; \ 10\%11=10=-1; \ 22\%11=0; \ 9\%11=9=-2 \\ 12^{83}-10^{34}+22^{1234}-9^5. \qquad 1^{83}-(-1)^{34}+0-(-2)^{5}=1-1+0+32=32\ \%\ 11=10=-1
```

(6)il numero  $52381^{1934}$ è congruo modulo 9 a:

(7) Siano a,b numeri interi e  $n \geq 1$ . Se MCD(a,n) = 1 e MCD(b,n) = 1 allora

```
\mathbf{V} \mid \mathbf{F} \mid MCD(ab, n) = 1;

\mathbf{V} \mid \mathbf{F} \mid MCD(ab, n) = 1 \text{ solo se } n \text{ è primo};
```

(8) Gli elementi invertibili in  $\mathbb{Z}_{12}$  sono:

$\mathbf{V}   \mathbf{F}$	1, 3, 7;
$\mathbf{V}   \mathbf{F}$	0, 5, 7, 11;
$\mathbf{V}   \mathbf{F}$	1, 5, 7, 11;

(9) Il numero  $34^{17}$ è congruo modulo 7 a

$\mathbf{V}$	$\mathbf{F}$	-1;
$\mathbf{V}$	$\mathbf{F}$	34
$\mathbf{V}$	$\mathbf{F}$	1;

- (10) Qual è l'opposto di 34 modulo 55?
- (11) Esprimere il massimo comun divisore di 34 e 55 come combinazione lineare dei due numeri, Qual è l'inverso moltiplicativo di di 34 modulo 55?
- (12) 7 è invertibile modulo 15? Se sì, qual è il suo inverso?
- (13) 15 è invertibile modulo 17? Se Se sí, qual è l'inverso?
- (14) Trovare tutti i numeri in  $\{0, 1, 2, \dots, 13\}$  che sono invertibili modulo 14 e per ciascuno di essi determinare l'inverso moltiplicativo.
- (15) Dimostrare che per ogni n > 1 il numero n 1 è invertibile modulo n e il suo inverso è n 1 stesso.
- (16) Trovare le soluzioni delle equazioni sottostanti, nell'insieme numerico indicato:

$$5x = 4 \quad \text{in } \mathbb{Z}_6$$

$$6x = -2 \quad \text{in } \mathbb{Z}_7$$

- (17) Dimostrare che se p è un numero primo e a è un numero tale che 0 < a < p, allora a è invertibile modulo p.
- (18) Dimostrare che, per ogni k, fra k numeri consecutivi ne esiste sempre uno divisibile per k. (suggerimento: considerare i possibili resti nella divisione per k).