## ESERCIZI SU DIVISIBILITÀ E CONGRUENZE

Nota bene: $b$ è l'opposto (additivo) di $a$ modulo $n$ se $a + b \equiv_n 0$;

$b$ è l'inverso (moltiplicativo) di $a$ modulo $n$ se $ab \equiv_n 1$.

(1) Trovare l'opposto additivo di 43 modulo 12.

(2) L'opposto additivo di $a$ modulo $n$ è uguale a

| | | |
|---|---|---|
| **V** | **F** | $a - n$; |
| **V** | **F** | $n - a$; |

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

| | | |
|---|---|---|
| **V** | **F** | 0; |
| **V** | **F** | 1; |

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

| | | |
|---|---|---|
| **V** | **F** | 0; |
| **V** | **F** | 1; |
| **V** | **F** | 2; |

(5) Determina gli elementi invertibili nelle classi resto modulo 12 e i rispettivi inversi.

(6) Se $a \equiv_n b$ allora

| | | |
|---|---|---|
| **V** | **F** | per ogni $k \in \mathbb{N}$ si ha $a^k \equiv_n b^k$; |
| **V** | **F** | per ogni $k \in \mathbb{N}$ si ha $k^a \equiv_n k^b$; |
| **V** | **F** | per ogni $k \in \mathbb{Z}$ si ha $ak \equiv_n bk$; |

(7) Se $a \equiv b \bmod (c)$ allora:

| | | |
|---|---|---|
| **V** | **F** | per ogni $x \in \mathbb{Z}$ vale $a + x \equiv b + x \bmod (c + x)$; |
| **V** | **F** | per ogni $x \in \mathbb{Z}$ vale $ax \equiv bx \bmod (cx)$; |

(8) Se $a, b, k$ sono interi non nulli e $n > 0$ allora:

| | | |
|---|---|---|
| **V** | **F** | se $ak \equiv_n bk$ allora $a \equiv_n b$. |

(9) Dimostrare che, se $c \neq 0$ e $ac \equiv bc$ modulo $(mc)$ allora $a \equiv b$ modulo $(c)$.

(10) La classe $14|_{60}$ è invertibile in $Z_{60}$? Se sí, qual è la classe inversa?

(11) 15 è invertibile modulo 17? Se Se sí, qual è l'inverso?

(12) Se $p$ è un numero primo e $a$ è un numero tale che $(a, p) = 1$ determina l'inverso di $a$ modulo $p$. (Suggerimento: riguardare il piccolo Teorema di Femat)

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

| | | |
|---|---|---|
| **V** | **F** | $-1$; |
| **V** | **F** | 34; |
| **V** | **F** | 1; |

(14) Sia $R$ la relazione binaria su $\mathbb{Z}$ definita da:

$$a \; R \; b \qquad \Leftrightarrow \qquad a_{|_b} \text{ è invertibile in } \mathbb{Z}_b \; .$$

Si ha:

| | | |
|---|---|---|
| **V** | **F** | $R$ è riflessiva; |
| **V** | **F** | $R$ è simmetrica; |
| **V** | **F** | $R$ è transitiva; |

(15) Calcolare $3^{24}$ modulo 23. (Ricorddarsi il Piccolo Teorema di Fermat).

(16) Sia $q = 47$. Se $\phi$ è la funzione di Eulero, determinare:
a) $\phi(q)$;
b) l'inverso di 3 modulo $\phi(q)$;
c) utilizzare la chiave pubblica $(3, 47)$ per cifrare il numero 7.

(17) Sia $q = 899 = 29 \times 31$. Se $\phi$ è la funzione di Eulero, determinare:
a) $\phi(q)$;
b) l'inverso di 11 modulo $\phi(q)$;

(18) Sia $q = 31$ e $t = 13$. Sapendo che la coppia $(13, 31)$ è la chiave privata, quale sarà la chiave pubblica del sistema $RSA$?

(19) Siano $a, n$ numeri naturali con $(a, n) = 1$ Dimostrare che:
a) se $a$ è dispari allora $(a, 2n) = 1$;
b) se $n$ dispari e $a$ è pari oppure se $n$ pari e $a$ è dispari, allora $(a + n, 2n) = 1$.

(20) Sia $\phi$ la funzione di Eulero. Dimostrare che $\phi(2n) = \phi(n)$, se $n$ è dispari, mentre $\phi(2n) = 2\phi(n)$ se $n$ è pari.
(suggerimento: usare l'esercizio precedente)