



## Tavola n. 4.2 Contare gli invertibili quando $n$ è prodotto di due primi

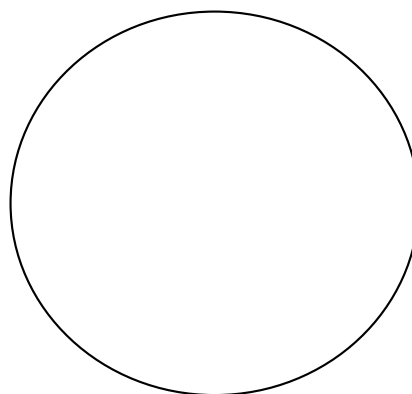
1. Quante sono le chiavi per cifrare con la moltiplicazione

$$p \mapsto \bar{a} \cdot \bar{p} \text{ modulo } 6?$$

Sono ....

Rappresenta  $\mathbf{Z}_6$  sul cerchio, mettendo in evidenza le classi invertibili.

Invertibile?	si	no
0		
1		
2		
3		
4		
5		



2. Fai l'elenco dei numeri  $a$  con  $0 < a < 15$  e tali che  $\text{MCD}(a, 3) > 1$ :  
 {.....}. Sono .....

Fai l'elenco dei numeri  $a$  con  $0 < a < 15$  e tali che  $\text{MCD}(a, 5) > 1$ :  
 {.....}. Sono .....

Fai l'elenco dei  $a$ , con  $0 < a < 15$ , tali che  $\text{MCD}(a, 15) > 1$ :  
 {.....}. Sono .....

Ricorda che gli invertibili in  $\mathbf{Z}_{15}$  sono i numeri  $a$  con  $0 < a < 15$  e tali che  $\text{MCD}(a, 15) = 1$ . A partire da quanto hai osservato, quanti sono gli invertibili in  $\mathbf{Z}_{15}$ ?

Sono .....

Ricorda che sono gli invertibili in  $\mathbf{Z}_{15}$

3. Sia  $n$  il prodotto di due primi distinti:

$$n = p q \text{ con } p \text{ e } q \text{ primi distinti}$$

a) Quanti sono i numeri  $a$  con  $0 < a < n$  che sono divisibili per  $p$ ?  
 Sono .....

b) Quanti sono i numeri  $a$  con  $0 < a < n$  che sono divisibili per  $q$ ?  
 Sono .....

c) Quanti sono i numeri  $a$ , con  $0 < a < n$ , che NON sono coprimi con  $n$ ?  
 Sono .....

d) Quanti sono gli elementi invertibili in  $\mathbf{Z}_n$ ? Sono .....