1. Sia $p = 79$.
   (a) Determinare se $\bar{2}$ è una radice primitiva in $\mathbf{Z}_p^*$.
   (b) Verificare che $\bar{3}$ è una radice primitiva in $\mathbf{Z}_p^*$.

2. Trovare una radice primitiva $\bar{g}$ in $\mathbf{Z}_p^*$, per $p = 71$, 101, 113.

3. Sia p un numero primo e sia $\bar{g}$ una radice primitiva in $\mathbf{Z}_p^*$. Il *logaritmo discreto* $\log \bar{a}$ di $\bar{a} \in \mathbf{Z}_p^*$ in base $\bar{g}$ è un intero j tale che $\bar{g}^j = \bar{a}$ modulo p.
   (a) Verificare che il logaritmo discreto in base $\bar{g}$ è ben definito modulo $p-1$, ossia $\bar{g}^i = \bar{g}^j$ se e solo se $i \equiv j \mod p-1$.
   (b) Verificare che il logaritmo di un prodotto è uguale alla somma dei logaritmi dei fattori (modulo $p-1$).

4. Sia p un numero primo e siano $\bar{g}$ e $\bar{g}'$ due radici primitive in $\mathbf{Z}_p^*$. Siano $\log_g$ il logaritmo in base g e $\log_{g'}$ il logaritmo in base g'. Verificare che esiste $c \in \mathbf{Z}$ tale che $\log_g \bar{a} = c \log_{g'} \bar{a}$, per ogni $\bar{a} \in \mathbf{Z}_p^*$.

5. Sia p un numero primo e sia $\bar{g}$ una radice primitiva in $\mathbf{Z}_p^*$. Verificare che $\log \overline{-1} = \frac{p-1}{2}$.

6. Sia $p = 79$ e sia fissata la radice primitiva $\bar{g} = \bar{3}$. Calcolare $\log \overline{-1}$, $\log \bar{3}$, $\log \bar{2}$, $\log \bar{5}$, $\log \bar{7}$, $\log \overline{41}$, $\log \overline{43}$ in tale base.

7. Sia $p = 83$ e sia $\bar{g} = \bar{2}$.
   (a) Verificare che $\bar{2}$ è una radice primitiva in $\mathbf{Z}_p^*$.
   (b) Calcolare $\log \bar{7}$ in tale base.

8. Sia $p = 23$.
   (a) Determinare una radice primitiva $\bar{g} \in \mathbf{Z}_p^*$.
   (b) Calcolare $\log \bar{2}$ in tale base.

9. Sia $p = 59$.
   (a) Verificare che $\bar{2}$ è una radice primitiva in $\mathbf{Z}_p^*$.
   (b) Calcolare $\log \bar{3}$ in tale base.

10. Sia $p \neq 2$ un numero primo sia $\bar{g}$ una radice primitiva in $\mathbf{Z}_p^*$. Verificare che $\bar{x}$ è un quadrato in $\mathbf{Z}_p^*$ se e solo se il logaritmo discreto è pari.