

1. Sia $p = 41$.
 - (a) Determinare una radice primitiva $\bar{g}$ in $\mathbf{Z}_p^*$.
 - (b) Sia g la radice primitiva modulo 41 calcolata nella parte (a). Calcolare $m \in \mathbf{Z}$ tale che $\bar{2} = \bar{g}^m$ in $\mathbf{Z}_{41}^*$.
2. Calcolare una radice primitiva g modulo 61. Calcolare i logaritmi discreti (rispetto alla radice primitiva g) $\log(2)$, $\log(47)$ e $\log(-1)$.
3. Sia $p = 61$. Fissiamo g una radice primitiva modulo 61; per $\log a$ intendiamo il logaritmo discreto di $a \in \mathbf{Z}_p^*$ rispetto a g .
 - (a) Dimostrare che $6 \log 2 = \log 3$;
 - (b) Dimostrare che $2 \log 2 + \log 3 + \log 5 = 30$.
 - (c) Dedurre che $\log 5 = 30 - 8 \log 2$.
4. Sia p un numero primo e sia g una radice primitiva modulo p . Calcolare il logaritmo discreto di $-1 \in \mathbf{Z}_p^*$.
5. Siano p, q due primi dispari distinti. Dimostrare che esiste $g \in \mathbf{Z}$ tale che g è radice primitiva sia modulo p che modulo q . Dimostrare che un tale elemento g *non* genera $\mathbf{Z}_{pq}^*$.
6. Sia p un primo e sia g una radice primitiva modulo p . Spiegare: per ogni $\bar{x} \in \mathbf{Z}_p^*$ si ha che $\bar{x}$ è quadrato in $\mathbf{Z}_p^*$ se e solo se il logaritmo discreto di $\bar{x}$ è *pari*.
7. Sia p un primo. Dimostrare che il numero di radici primitive $g \in \mathbf{Z}_p^*$ è uguale a $\varphi(p-1)$. Determinare tutte le radici primitive in $\mathbf{Z}_{13}^*$.
8. Sia p un primo. Sia “log” il logaritmo discreto rispetto alla radice primitiva $g \in \mathbf{Z}_p^*$.
 - (a) Dimostrare che la mappa $x \mapsto \log x$ induce un isomorfismo di gruppi $\mathbf{Z}_p^* \cong \mathbf{Z}_{p-1}$.
 - (b) Dimostrare che $x \in \mathbf{Z}_p^*$ è radice primitiva se e solo se $\text{mcd}(\log x, p-1) = 1$.
 - (c) Siano $a, b \in \mathbf{Z}_p^*$. Dimostrare che il rapporto $\log a / \log b$ non dipende dalla scelta di g .
9. Sia $p > 5$ un primo. Dimostrare che il periodo della frazione decimale di $1/p$ è uguale a $p-1$ se e solo se $10 \in \mathbf{Z}_p^*$ è una radice primitiva.
10. Sia $p > 2$ un primo. Dimostrare che il periodo della frazione *esadecimale* (cioè in base 16) di $1/p$ non ha mai lunghezza $p-1$.

PER I SEGUENTI ESERCIZI È UTILE UN COMPUTER.

11. Per i numeri primi $p = 23, 191, 8761, 44000003, 280000000572000000077$, calcolare una radice primitiva $g \in \mathbf{Z}_p^*$.
12. Sia $p = 44000003$. Calcolare il logaritmo discreto di $3 \in \mathbf{Z}_{44000003}^*$ rispetto alla radice primitiva g calcolato nell'esercizio 11,