

1. (Numeri di Fermat) Per ogni numero naturale n , si definisce l'ennesimo numero di Fermat come $F_n = 2^{2^n} + 1$; Far vedere che ogni divisore primo p di F_n soddisfa $p \equiv 1 \pmod{2^{n+1}}$.
2. (Logaritmo discreto) Sia p un numero primo.
 - (a) Sia $p = 41$. Determinare una radice primitiva \bar{g} in \mathbf{Z}_p^* .
 - (b) Sia g la radice primitiva modulo 41 calcolata nella parte (a). Calcolare $i \in \mathbf{Z}$ tale che $\bar{2} = \bar{g}^i$ in \mathbf{Z}_{41}^* .
 - (c) Per $\bar{a} \in \mathbf{Z}_p^*$, l'esponente j tale che $\bar{a} = \bar{g}^j$ in \mathbf{Z}_p^* , si dice *il logaritmo discreto* di $a \pmod{p}$ rispetto alla radice primitiva \bar{g} . Far vedere che il logaritmo discreto è ben definito modulo $p - 1$ e che il logaritmo di un prodotto è uguale alla somma dei logaritmi dei fattori $\pmod{p - 1}$.
3. Calcolare una radice primitiva g modulo 61. Calcolare i logaritmi discreti (rispetto alla radice primitiva g) $\log(2)$, $\log(47)$ e $\log(-1)$.
4. Sia p un numero primo e sia g una radice primitiva modulo p . Calcolare il logaritmo discreto di $\bar{-1} \in \mathbf{Z}_p^*$.
5. 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*.
6. Sia p un numero primo. Sia g una radice primitiva modulo p e sia \log_g il logaritmo discreto rispetto a g (cioè se $x \in \mathbf{Z}_p^*$ è uguale a g^i , allora $\log_g(x) = i$). Sia g' una seconda radice primitiva e sia $\log_{g'}$ il logaritmo discreto rispetto a g' . Far vedere che esiste $c \in \mathbf{Z}$ tale che per ogni $x \in \mathbf{Z}_p^*$ si ha che $\log_{g'}(x) = c \log_g(x)$.
7. Sia $p > 3$ un numero primo. Dimostrare:
 - (a) -1 è quadrato modulo p se e solo se $p \equiv 1 \pmod{4}$.
 - (b) -3 è quadrato modulo p se e solo se $p \equiv 1 \pmod{3}$. (Sugg: $T^2 + 3$ ha uno zero modulo p se e solo se $T^2 + T + 1$ ha uno zero modulo p .)
 - (c) Dedurre: 3 è quadrato modulo p se e solo se $p \equiv \pm 1 \pmod{12}$.
8. Sia $n \in \mathbf{Z}_{>0}$ non divisibile per 3.
 - (a) Dimostrare che $\bar{x} = \bar{1}$ è l'unico elemento di \mathbf{Z}_n che soddisfa $x^3 \equiv 1 \pmod{n}$, se e solo ogni divisore primo di n è congruo a $2 \pmod{3}$.
 - (b) Far vedere che il numero di $\bar{x} \in \mathbf{Z}_n$ con $x^3 \equiv 1 \pmod{n}$, è uguale a 3^t dove t è il numero di divisori primi di n che sono congrui a $1 \pmod{3}$.
9. Si p un numero primo dispari.
 - (a) Dimostrare che per ogni $\bar{x} \in \mathbf{Z}_p^*$ la classe $\bar{x}^{(p-1)/2}$ è uguale a $\pm \bar{1}$.
 - (b) Far vedere che $\bar{x} \in \mathbf{Z}_p^*$ è un *quadrato* se e solo se $\bar{x}^{(p-1)/2} = \bar{1}$.
 - (c) Quanti quadrati ci sono in \mathbf{Z}_p^* ?
10. Si p un numero primo e sia d un divisore di $p - 1$.
 - (a) Sia $W = \{\bar{x} \in \mathbf{Z}_p^* : \bar{x}^d = \bar{1}\}$. Quanti elementi ci sono in W ?
 - (b) Dimostrare che per ogni $\bar{x} \in \mathbf{Z}_p^*$ la classe $\bar{x}^{(p-1)/d}$ è un elemento di W .
 - (c) Far vedere che $\bar{x} \in \mathbf{Z}_p^*$ è una *d-esima potenza* se e solo se $\bar{x}^{(p-1)/d} = \bar{1}$.
 - (d) Quante *d-esime potenze* ci sono in \mathbf{Z}_p^* ?

PER IL SEGUENTE ESERCIZIO È UTILE UN COMPUTER.

11. Per i numeri primi 23, 191, 8761, 44000003, 280000000572000000077, calcolare una radice primitiva.