

Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2011/2012
TN410 - Introduzione alla teoria dei numeri
Esercizi 4

1. Trovare gli ordini degli elementi di U_{20} e di U_{14} .
2. Verificare che 2 è una radice primitiva modulo 13; trovare tutte le radici primitive modulo 13.
3. Trovare una radice primitiva modulo 49.
4. Trovare tutte le radici primitive modulo n per $n = 19$ e 23 .
5. Sapendo che 2 è una radice primitiva modulo 37, trovare:
 - (a) tutti gli interi positivi minori di 37 di ordine 9 modulo 37;
 - (b) tutti gli interi positivi minori di 43 di ordine 18 modulo 37.
6. Sia p un numero primo dispari. Sia r una radice primitiva modulo p . Provare che:
 - (a) $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
 - (b) Se r' è un'altra radice primitiva modulo p , allora rr' non è una radice primitiva modulo p .
 - (c) Se r' è un numero intero tale che $rr' \equiv 1 \pmod{p}$, allora r' è una radice primitiva modulo p .
7. Provare che se $p > 3$ è un numero primo, allora le radici primitive mod p si possono raggruppare in coppie r, r' tali che $rr' \equiv 1 \pmod{p}$.
8. Sia r una radice primitiva modulo un numero primo dispari p . Provare che:
 - (a) Se $p \equiv 1 \pmod{4}$, allora anche $-r$ è una radice primitiva modulo p .
 - (b) Se $p \equiv 3 \pmod{4}$, allora $-r$ ha ordine $\frac{p-1}{2}$ modulo p .