

Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2007/2008
TN1 - Introduzione alla teoria dei numeri
Tutorato 3 (14 marzo 2007)
Micaela De Santis

1. Verificare che ciascuna delle congruenze polinomiali
 - (a) $X^2 \equiv 1 \pmod{15}$
 - (b) $X^2 \equiv -1 \pmod{65}$
 - (c) $X^2 \equiv -2 \pmod{33}$ha 4 soluzioni non congruenti.
2. Trovare gli ordini degli elementi di U_{18} e di U_{15} .
3. Verificare che 2 è una radice primitiva mod (11); trovare tutte le radici primitive mod (11).
4. Verificare che 2 è una radice primitiva mod (25).
5. Trovare tutte le radici primitive mod (n) per $n = 23, 29$ e 31 .
6. Sapendo che 3 è una radice primitiva mod (43), trovare:
 - (a) tutti gli interi positivi minori di 43 di ordine 6 mod (43);
 - (b) tutti gli interi positivi minori di 43 di ordine 21 mod (43).
7. Trovare tutti gli interi positivi minori di 61 di ordine 4 mod (61).
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 mod (p).
 - (b) Se $p \equiv 3 \pmod{4}$, allora $-r$ ha ordine $\frac{p-1}{2}$ mod (p).
9. Sia p un numero primo. Dimostrare che il prodotto delle $\varphi(p-1)$ radici primitive modulo p è congruente modulo p a $(-1)^{\varphi(p-1)}$.