Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2008/2009
TN1 - Introduzione alla teoria dei numeri
Tutorato 4 (26 marzo 2009)
Giacomo Milizia

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 modulo 11; trovare tutte le radici primitive modulo 11.
4. Verificare che 2 è una radice primitiva modulo 25.
5. Trovare tutte le radici primitive modulo n per $n = 29$ e 31.
6. Sapendo che 3 è una radice primitiva modulo 43, trovare:
   (a) tutti gli interi positivi minori di 43 di ordine 6 modulo 43;
   (b) tutti gli interi positivi minori di 43 di ordine 21 modulo 43.
7. Sapendo che 2 è una radice primitiva modulo 61, trovare tutti gli interi positivi minori di 61 di ordine 4 modulo 61.
8. 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.
9. 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.
10. Sia p un numero primo. Dimostrare che il prodotto delle $\varphi(p-1)$ radici primitive modulo p è congruente modulo p a $(-1)^{\varphi(p-1)}$.