Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2008/2009
TN1 - Introduzione alla teoria dei numeri
Tutorato 5 (2 aprile 2009)
Giacomo Milizia

1. Trovare le 4 radici primitive modulo 26 e le otto radici primitive modulo 25.
2. Trovare tutte le radici primitive modulo 3^2, 3^3, e 3^4.
3. Scrivere la tabella degli indici (mod 17) rispetto alla radice primitiva 3.
4. Trovare l'indice di 5 relativamente ad ognuna delle radici primitive di 26.
5. Con l'aiuto della tabella dell'esercizio 3, risolvere le seguenti congruenze:
   (a) $X^{12} \equiv 13 \pmod{17}$;
   (b) $9X^8 \equiv 8 \pmod{17}$;
   (c) $7^X \equiv 7 \pmod{17}$.
6. Usando la teoria degli indici,trovare il resto della divisione di $3^{24} \cdot 5^{13}$ per 17.
7. Siano p un primo dispari ed r una radice primitiva (mod p).
   (a) Provare che $\text{ind}_r(-1) = \text{ind}_r(p-1) = \frac{p-1}{2}$.
   (b) Provare che per ogni numero intero a tale che MCD(a,p)=1 si ha che
   $$\text{ind}_r(p-a) \equiv \text{ind}_r a + \frac{p-1}{2} \pmod{(p-1)}.$$
8. Sapendo che 2 è una radice primitiva modulo 13, stabilire per quali interi positivi a la conguenza $aX^4 \equiv 2 \pmod{13}$ è risolubile.
9. Sia p un numero primo dispari. Dimostrare che la congruenza
   $$X^4 \equiv -1 \ (\text{ mod } p)$$
   è risolubile se e solo se $p \equiv 1 \pmod{8}$.
10. Si consideri la congruenza $X^3 \equiv a \pmod{p}$, con $p \geqslant 5$ numero primo e a primo con p. Provare che:
    (a) Se $p \equiv 1 \pmod{6}$, allora la congruenza non ha soluzioni oppure ha tre soluzioni incongruenti modulo p.
    (b) Se $p \equiv 5 \pmod{6}$, allora la congruenza ha una sola soluzione modulo p.