Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2010/2011
TN410 - Introduzione alla teoria dei numeri
Tutorato 4 (7 aprile 2011)
Giacomo Milizia

1. Trovare le due radici primitive modulo 10.
2. Trovare tutte le radici primitive modulo 3^2, 3^3, e 3^4.
3. Trovare le 6 radici primitive modulo 54 e le 12, radici primitive modulo 49.
4. Scrivere la tabella degli indici (mod 19) rispetto alla radice primitiva 2.
5. Trovare l'indice di 5 relativamente ad ognuna delle radici primitive di 38.
6. Con l'aiuto della tabella dell'esercizio 4, risolvere le seguenti congruenze:
   (a) $X^{12} \equiv 11 \pmod{19}$;
   (b) $X^8 \equiv 6 \pmod{19}$;
   (c) $X^9 \equiv 6 \pmod{19}$;
   (d) $14X^8 \equiv 3 \pmod{19}$;
   (e) $7^X \equiv 11 \pmod{19}$.
7. Provare che la congruenza $X^3 \equiv 3 \pmod{19}$ non ha soluzioni e che la congruenza $X^3 \equiv 12 \pmod{19}$ ha 3 soluzioni non congruenti.
8. Usando le proprietà degli indici, trovare il resto della divisione di $5^{174} \cdot 11^{29}$ per 19.
9. Siano p un primo dispari ed r una radice primitiva (mod p).
   (a) Provare che $\mathrm{ind}_r(-1) = \mathrm{ind}_r(p-1) = \frac{p-1}{2}$.
   (b) Provare che per ogni numero intero a tale che MCD(a, p)=1 si ha che
   $$\mathrm{ind}_r(p-a) \equiv \mathrm{ind}_r a + \frac{p-1}{2} \pmod{(p-1)}.$$
10. Sapendo che 2 è una radice primitiva modulo 13, stabilire per quali interi positivi a la conguenza $aX^4 \equiv 5 \pmod{13}$ è risolubile.
11. Sia p un numero primo dispari. Dimostrare che la congruenza
   $$X^4 \equiv -1 \pmod{p}$$
   è risolubile se e solo se $p \equiv 1 \pmod{8}$.
12. Stabilire se le due congruenze $X^5 \equiv 13 \pmod{23}$ e $X^7 \equiv 15 \pmod{29}$ sono risolubili.