Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2002/2003
TN 1
Esercizi per casa, II prova (7 aprile 2003)

1. Dimostrare che se $n = 2^k$, con $k \geq 3$, non esistono radici primitive (mod n).

2. Dimostrare che:

(i) Se $r, s \geq 3$ e $MCD(r, s) = 1$ non esistono radici primitive (mod rs).

(ii) Se $n = pq$, con p, q primi dispari, non esistono radici primitive (mod n).

(iii) se $n = 2^e p^k$ con $e \geq 2$, $k \geq 1$, p primo dispari, non esistono radici primitive (mod n).

3. Sia p un primo dispari. Dimostrare che:

(i) Esiste sempre una radice primitiva r (mod p) tale che $r^{p-1} \not\equiv 1 \pmod{p^2}$.

(ii) Se r è una radice primitiva (mod p), allora r oppure $r + p$ è una radice primitiva (mod p^2).

(iii) Se r è una radice primitiva (mod p) e se $r^{p-1} \not\equiv 1 \pmod{p^2}$, allora $r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$, per ogni $k \geq 2$.

(iv) Se r è una radice primitiva (mod p) e se $r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$, allora r è una radice primitiva (mod p^k).

4. Sia p un primo dispari e $k \geq 1$. Dimostrare che:

(i) Esiste sempre una radice primitiva r(mod p^k) con $r \equiv 1 \pmod 2$.

(ii) Se r è una radice primitiva (mod p^k), e se $r \equiv 1 \bmod 2$ allora r è anche una radice primitiva (mod $2p^k$).