Tutorato di TN1 - Teoria dei Numeri

a.a. 2006/2007
Gabriele Fusacchia e Valeria Pucci
17 Aprile 2007 - Tutorato VI

(1) Trovare l'ordine dei seguenti elementi:

(a) 2 (mod 15), (mod 17), (mod 19), (mod 23)

(b) 3 (mod 16), (mod 17), (mod 19), (mod 23)

(c) 5 (mod 16), (mod 17), (mod 19), (mod 23)

(2) Mostrare che 15 non ha radici primitive calcolando l'ordine di tutti gli elementi (mod 15).

(3) Siano $a, n, h, k \in \mathbb{Z}$, $n \geq 2$ e $h, k > 0$. Mostrare che:

(a) se $\mathrm{ord}_n\, a = hk$, allora $\mathrm{ord}_n(a^h) = k$

(b) se p è un primo dispari e $\mathrm{ord}_p\, a = 2k$, allora $a^k \equiv -1$

(c) se $\mathrm{ord}_n\, a = n - 1$, allora n è primo
(*si ricordi che* $\varphi(n) \leq n - 1$)

(d) se p è primo e $\mathrm{ord}_p\, a = 3$, allora $\mathrm{ord}_p(a + 1) = 6$
(*suggerimento: dimostrare che* $a^2 + a + 1 \equiv 0 \pmod{p}$)

(4) Sia p un primo dispari ed r una radice primitiva (mod p). Mostrare che:

(a) $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

(b) se $r' \not\equiv r \pmod{p}$ è un'altra radice primitiva (mod p), allora rr' non è mai una radice primitiva (mod p)

(c) se $a \in \mathbb{Z}$ è tale che $ar \equiv 1$, allora a è una radice primitiva (mod p)