Tutorato di TN1 - Teoria dei Numeri

Andrea Susa

15 aprile 2002

(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 gli ordini di tutti gli elementi (mod 15).

(3) Siano $a, n \in \mathbb{Z}$, $n \geq 2$, $h, k \in \mathbb{N}$. Mostrare le seguenti:
(a) se $ord_n(a) = hk$, allora $ord_n(a^h) = k$;
(b) se $p \geq 3$ primo e $ord_p(a) = 2k$, allora $a^k \equiv -1 \pmod{p}$;
(c) se esiste a tale che $ord_n(a) = n - 1$, allora n è primo;
(d) se p è primo e $ord_p(a) = 3$, allora $ord_p(a + 1) = 6$.

(4) Sia p un primo dispari e r una radice primitiva (mod p). Allora:
(a) $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$;
(b) se r_1 è un'altra radice primitiva (mod p), allora rr_1 **non è mai** una radice primitiva (mod p);
(c) se $a \in \mathbb{Z}$ è tale che $ar \equiv 1 \pmod{p}$, allora a è una radice primitiva (mod p);
(d) se $p \equiv 1 \pmod{4}$, allora $-r$ è ancora una radice primitiva (mod p);
(e) se $p \equiv 3 \pmod{4}$, allora $ord_p(-r) = \frac{p-1}{2}$, cioè $(-r)^2$ è una radice primitiva (mod p).