Università degli Studi di Roma Tre
Corso di Studi in Matematica, A.A. 2007/2008
TN1 - Introduzione alla Teoria dei Numeri
3 aprile 2008

1. Sia $p \equiv 1 \pmod 3$. Dimostrare le seguenti affermazioni:
   - esiste un elemento c tale che $p \nmid c$ e $\mathrm{ord}_p(c) = 3$;
   - $(2c+1)^2 \equiv -3 \pmod p$;
   - $\left(\frac{-3}{p}\right) = 1$ ovvero -3 è un residuo quadratico $\pmod p$.
2. Dimostrare che, per ogni $p \geq 3$ primo, si ha che:
$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$$
3. Sia $n \geq 4$ composto. Dimostrare che
$$(n-1)! \equiv 0 \pmod n$$
4. Sia p un primo. Dimostrare che esistono $x, y \in \mathbb{Z}$ tali che $p = x^2 + 2y^2$ se e soltanto se $p \equiv 1, 3 \pmod 8$
5. Siano p un primo dispari ed $a \in \mathbb{Z}$, con $p \nmid a$. Diciamo che a è un **residuo biquadratico** $\pmod p$ se la congruenza $X^4 \equiv a \pmod p$ è risolubile. Mostrare le seguenti affermazioni:
   - -1 è un r.bq. se e soltanto se $p \equiv 1 \pmod 8$;
   - se $p \equiv 3 \pmod 4$ allora a è un r.bq. se e soltanto se a è un r.q..
   - se $p \equiv 1 \pmod 4$, allora -4 è un r.bq.. Utilizzare le soluzioni della congruenza $X^2 \equiv -1 \pmod p$ per determinare le soluzioni della congruenza $X^4 \equiv -4 \pmod p$
6. Sia $p = 8k+1$ un primo e sia g una sua radice primitiva. Mostrare che le soluzioni della congruenza $X^2 \equiv \pm 2 \pmod p$ sono date da:
$$x \equiv \pm(g^{7k} \pm g^k) \pmod p$$
7. Siano p un primo ed $a \in \mathbb{Z}$. Definiamo $v_p(a) = k$ se e soltanto se $p^k | a$ e $p^{k+1} \nmid a$ (*valutazione p-adica*). Mostrare che $\left(\frac{a}{p}\right) = -1$ se e soltanto se $v_2(p-1) = v_2(\mathrm{ord}_p(a))$.

8. Sia p un primo dispari. Dimostrare che il più piccolo (positivo) non-r.q. è un primo.

9. Sia $t_k(n) = \#\{d : d|n \text{ e } d \equiv k \pmod 4\}$, e sia

$$s(n) = t_1(n) - t_3(n)$$

Dimostrare che:

- s è una funzione moltiplicativa
- esprime s in funzione di p^k, con p primo