

Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2013/2014
TN410 - Introduzione alla teoria dei numeri
Esercizi 7

1. Risolvere le seguenti congruenze quadratiche:
 - (a) $X^2 - 3X + 2 \equiv 0 \pmod{15}$;
 - (b) $X^2 + 3X + 1 \equiv 0 \pmod{21}$;
 - (c) $X^2 + 2X - 3 \equiv 0 \pmod{21}$;
 - (d) $5X^2 + 6X + 1 \equiv 0 \pmod{23}$.
2. Provare che la congruenza quadratica $6X^2 + 5X + 1 \equiv 0 \pmod{p}$ ha soluzioni per ogni primo p , sebbene l'equazione $6X^2 + 5X + 1 = 0$ non abbia soluzioni in \mathbb{Z} .
3. Studiare il gruppo dei residui quadratici Q_n per ogni $n \leq 17$.
4. Sapendo che 2 è una radice primitiva dell'unità modulo 29, elencare gli elementi di Q_{29} .
5. Siano p e q numeri primi dispari con $q = 4p + 1$. Provare che se a è un non-residuo quadratico di q , allora a è una radice primitiva dell'unità modulo q oppure $\text{ord}_q a = 4$.
6. Siano p un primo dispari ed a un residuo quadratico di p . Provare che:
 - (a) a non è una radice primitiva mod p ;
 - (b) l'intero $p - a$ è un residuo quadratico o un non-residuo quadratico di p rispettivamente se $p \equiv 1 \pmod{4}$ o $p \equiv 3 \pmod{4}$;
 - (c) Se $p \equiv 1 \pmod{4}$, allora $x \equiv \pm a^{(p+1)/4} \pmod{p}$ sono le soluzioni della congruenza $X^2 \equiv a \pmod{p}$.
7. Se $p = 2^k + 1$ è primo, provare che ogni non-residuo quadratico di p è una radice primitiva di p . (Sugg. : applicare il criterio di Eulero)
8. Sia p un primo dispari ed a un intero positivo $\leq p - 1$. Dimostrare che se $\left(\frac{a}{p}\right) = -1$, allora $\sum_{d|a} d^{\frac{p-1}{2}} \equiv 0 \pmod{p}$.
9. Sia p un primo dispari. Dimostrare che il prodotto dei residui quadratici di p in un assegnato sistema ridotto di residui modulo p è congruente modulo p a $-\left(\frac{-1}{p}\right)$.
10. Trovare il valore di $\left(\frac{7}{13}\right)$ usando il criterio di Eulero ed usando il lemma di Gauss.

11. Usando il lemma di Gauss, calcolare i seguenti simboli di Legendre:

$$\left(\frac{10}{23}\right), \left(\frac{5}{17}\right), \left(\frac{14}{23}\right).$$

12. Determinare per quali primi dispari p si ha che $-2 \in Q_p$.

13. Trovare il valore dei seguenti simboli di Legendre:

$$\left(\frac{2}{17}\right), \left(\frac{3}{31}\right), \left(\frac{13}{67}\right), \left(\frac{6}{113}\right), \left(\frac{-6}{317}\right), \left(\frac{-25}{337}\right).$$