ISTITUZIONI DI ALGEBRA SUPERIORE

Claudia Malvenuto

Scheda di esercizi n. 7

1. Determinare i primi dispari per cui $(-3|p) = 1$ e quelli per cui $(-3|p) = -1$.

2. Dimostrare che 5 è un residuo quadratico per un primo dispari p se $p \equiv \pm 1 \pmod{10}$ e che 5 è un non residuo quadratico se $p \equiv \pm 3 \pmod{10}$.

3. Trovare la catena di congruenze (quadratica pura e poi lineare) equivalenti a $2x^2 + 3x - k \equiv 0 \pmod 5$ e determinare per quali valori di k esistono soluzioni della conguenza quadratica.

4. Se $x^2 \equiv a \pmod p$ ammette una soluzione x_1, mostrare che anche $x_2 = p - x_1$ è una soluzione. Se $a \not\equiv 0 \pmod p$ e p dispari, mostrare che $x_1 \not\equiv x_2 \pmod p$.

5. Se p è un primo dispari e se $(a|p) = 1$, mostrare che a è un residuo quadratico $\pmod{p^n}$ e che $x^2 \equiv a \pmod{p^n}$ ha *esattamente due* soluzioni. (Usare la riduzione delle congruenze $p^s \to p^{s-1}$ e l'induzione.)

6. Se a è dispari e $m \geq 3$, allora $x^2 \equiv a \pmod{2^m}$ è impossibile, a meno che $a \equiv 1 \pmod 8$.

7. Mostrare che $(-1|p) = +1$ se e solo se p è della forma $p = 4K + 1$.

8. Risolvere $x^2 \equiv 140 \pmod{221}$; $x^2 \equiv 65 \pmod{280}$; $x^2 \equiv 11 \pmod{101}$; $x^2 \equiv 33 \pmod{101}$.

9. Mostrare che per ogni primo $p > 3$ la somma dei residui quadratici modulo p è divisibile per p. (Suggerimento: usare l'identità: $1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6$.)

10. Trovare i valori di $(a|p)$ in ognuno dei 12 casi che si ottengono con $a = -1, 2, -2, 3$ e $p = 11, 13, 17$.

11. (a) Elencare i residui quadratici per ognuno dei primi $7, 11, 13, 17, 29, 37$.

    (b) Per ogni intero positivo n, si definisca $F(n)$ come il più piccolo valore di $|n^2 - 17x|$, per x che varia tra tutti gli interi. Dimostrare che $F(n)$ vale 0 oppure è una potenza di 2.

12. Dimostrare che se p è un primo dispari, allora $x^2 \equiv 2 \pmod{p}$ ha soluzioni se e solo se $p \equiv 1 \pmod{8}$ oppure se $p \equiv 7 \pmod{8}$.

13. Sia g una radice primitiva modulo un primo p dispari. Dimostrare che tutti i residui quadratici modulo p sono congruenti a $g^2, g^4, g^6, \ldots, g^{p-1}$ e che i non residui quadratici sono congruenti a $g, g^3, g^5, \ldots, g^{p-2}$. Questo dimostra (in un altro modo) che ci soo tanti residui quadratici quanti residui non quadratici.

14. Sia p un primo dispari. Dimostrare che se c'è un intero x tale che

$$p|(x^2 + 1) \text{ allora } p \equiv 1 \pmod{4};$$

$$p|(x^2 - 2) \text{ allora } p \equiv 1 \text{ oppure } 7 \pmod{8};$$

$$p|(x^2 + 2) \text{ allora } p \equiv 1 \text{ oppure } 3 \pmod{8};$$

$$p|(x^4 + 1) \text{ allora } p \equiv 1 \pmod{8};$$

    dimostrare inoltre che ci sono infiniti primi della forma $8n + 1$.

15. Trovare tuti i primi p tali che la congruenza $x^2 \equiv 13 \pmod{p}$ ammette soluzioni.

16. Trovare i primi q tali che $(5|q) = -1$.

17. Dimostrare che ci sono infiniti primi della forma $4n + 1$.

18. Valutare $(-23|83)$, $(51|71)$, $(71|73)$, $(-35|97)$.

19. Quali delle seguenti congruenze sono risolubili?

    (a) $x^2 \equiv 11 \pmod{61}$

    (b) $x^2 \equiv 42 \pmod{97}$

(c) $x^2 \equiv -43 \pmod{79}$

(d) $x^2 \equiv 31 \pmod{103}$

20. Sia k dispari. Dimostrare che $x^2 \equiv k \pmod{2}$ ha esattamente una soluzione. Inoltre, $x^2 \equiv k \pmod{2^2}$ ammette soluzioni se e solo se $k \equiv 1 \mod 4$, nel qual caso ci sono due soluzioni.