TN1 - Introduzione alla teoria dei numeri - A.A. 2006/2007

Esercitazione in classe in preparazione della II Prova

ESERCIZIO 1. (a) Sia p un primo dispari, r una radice primitiva (mod p), e sia $a \in \mathbb{Z}$. Dimostrare che l'equazione diofantea (in due inderminate):

$$X^2 - pY - a = 0$$

è risolubile se e soltanto se è risolubile la congruenza lineare (in una indeterminata):

$$2T \equiv \mathrm{ind}_r(a) \pmod{(p-1)}.$$

(b) Determinare per quali valori di a, con $0 \leq a \leq 10$, l'equazione diofantea:

$$X^2 - 11Y - a = 0$$

è risolubile.

(c) Per il più grande valore di a, con $0 \leq a \leq 10$, per il quale l'equazione diofantea:

$$X^2 - 11Y - a = 0$$

è risolubile, determinare per quest'ultima tutte le (infinite) soluzioni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

ESERCIZIO 2. (a) Determinare per quali valori del parametro λ, $0 \leq \lambda \leq 13$, la seguente congruenza è risolubile:

$$X^2 + X + \lambda \equiv 0 \pmod{14}.$$

(b) Per ogni valore di λ per il quale la congruenza in **(a)** è risolubile determinarne tutte le sue soluzioni.

ESERCIZIO 3. (a) Sia p un primo ed $e \geq 1$ un intero. Dimostrare che la congruenza:

$$X^{p-1} \equiv 1 \pmod{p^e}$$

ha esattamente $p-1$ soluzioni $(\mathrm{mod}\, p^e)$, qualunque sia l'intero $e \geq 1$.

(b) Determinare le (quattro) soluzioni della congruenza

$$X^4 \equiv 1 \pmod{25}.$$

ESERCIZIO 4. (a) Per quali interi a, $1 \leq a \leq 14$, relativamente primi con 15 il seguente simbolo di Jacobi vale 1:

$$\left(\frac{a}{15}\right).$$

(b) Determinare per quali interi a, $1 \leq a \leq 14$, relativamente primi con 15 la congruenza quadratica $X^2 - a \equiv 0 \pmod{15}$ è risolubile.

ESERCIZIO 5. (a) Determinare quali dei seguenti numeri si possono scrivere come somma di due quadrati:

(1) 14210
(2) 910

(b) Scrivere tali numeri come somma di due quadrati in due modi diversi.

SOLUZIONI

Esercizio 1. (b) La congruenza $X^2 - a \equiv 0 \pmod{11}$ è risolubile per $a = 0, 1, 3, 4, 5, 9$.

(c) Per $a = 9$ le soluzioni della congruenza $X^2 - 9 \equiv 0 \pmod{11}$ sono date da 3 e 8 (mod 11). Quindi le soluzioni dell'equazione diofantea sono date da

$$\left\{ \left(3 + k \cdot 11, \frac{(3 + k \cdot 11)^2 - 9}{11} \right) \mid k \in \mathbb{Z} \right\} \text{ e } \left\{ \left(8 + h \cdot 11, \frac{(8 + h \cdot 11)^2 - 9}{11} \right) \mid h \in \mathbb{Z} \right\}.$$

Si noti che

$$\frac{(3 + k \cdot 11)^2 - 9}{11} = 6 \cdot k + 11 \cdot k^2 \in \mathbb{Z} \quad \text{e} \quad \frac{(8 + h \cdot 11)^2 - 9}{11} = 5 + 16 \cdot h + 11 \cdot h^2 \in \mathbb{Z}.$$

Esercizio 2. La congruenza $X^2 + X + \lambda \equiv 0 \pmod{2}$ è risolubile se e soltanto se λ è pari. Per ogni valore di λ pari, la congruenza ha come insieme di soluzioni $\{0, 1\} \pmod 2$.

La congruenza $X^2 + X + \lambda \equiv 0 \pmod{7}$ è risolubile se e soltanto se $\lambda \in \{0, 1, 2, 5, 7, 8, 9, 12\}$ (ed ha come insieme di soluzioni, rispettivamente, $\{0\}$, $\{2, 4\}$, $\{3\}$, $\{1, 5\}$, $\{0, 6\}$, $\{2, 4\}$, $\{3\}$, $\{1, 5\}$ (mod 7).

Pertanto la congruenza $X^2 + X + \lambda \equiv 0 \pmod{14}$ è risolubile se e soltanto se $\lambda \in \{0, 2, 8, 12\}$ ed ha come insieme di soluzioni, rispettivamente, $\{0, 6, 7, 13\}$, $\{3, 10\}$, $\{2, 4, 9, 11\}$, $\{1, 5, 8, 12\}$, (mod 14).

Esercizio 3. (b) La congruenza $X^4 - 1 \equiv 0 \pmod{5}$ ha come soluzioni 1, 2, 3, 4 (mod 5).

La congruenza $X^4 - 1 \equiv 0 \pmod{25}$ ha come soluzioni 1, 7, 18, 24 (mod 25).

Esercizio 4. (a)
$\left(\frac{1}{3}\right) = 1$, $\left(\frac{1}{5}\right) = 1$, $\left(\frac{1}{15}\right) = 1$ ◀ .
$\left(\frac{2}{3}\right) = -1$, $\left(\frac{2}{5}\right) = -1$, $\left(\frac{2}{15}\right) = 1$ ◁ .
$\left(\frac{4}{3}\right) = 1$, $\left(\frac{4}{5}\right) = 1$, $\left(\frac{4}{15}\right) = 1$ ◀ .
$\left(\frac{7}{3}\right) = 1$, $\left(\frac{7}{5}\right) = -1$, $\left(\frac{7}{15}\right) = -1$.
$\left(\frac{8}{3}\right) = -1$, $\left(\frac{8}{5}\right) = -1$, $\left(\frac{8}{15}\right) = 1$ ◁ .
$\left(\frac{11}{3}\right) = -1$, $\left(\frac{11}{5}\right) = 1$, $\left(\frac{8}{15}\right) = -1$.
$\left(\frac{13}{3}\right) = 1$, $\left(\frac{13}{5}\right) = -1$, $\left(\frac{13}{15}\right) = -1$.
$\left(\frac{14}{3}\right) = -1$, $\left(\frac{14}{5}\right) = 1$, $\left(\frac{14}{15}\right) = -1$.

(b) Se $1 \leq a \leq 14$ e $\mathrm{MCD}(a, 15) = 1$, da quanto sopra si ricava che $X^2 - a \equiv 0 \pmod{15}$ è risolubile se e soltanto se $a = 1, 4 \pmod{15}$.

Per $a = 1$, l'insieme delle soluzioni (mod 15) è dato da $\{1, 4, 11, 14\}$.

Per $a = 4$, l'insieme delle soluzioni (mod 15) è dato da $\{2, 7, 8, 13\}$.

Si noti anche che la congruenza $X^2 - a \equiv 0 \pmod{15}$ è anche risolubile per altri valori di a non relativamente primi con 15.

Per $a = 0$, l'insieme delle soluzioni (mod 15) è dato da $\{0\}$.

Per $a = 6$, l'insieme delle soluzioni (mod 15) è dato da $\{6, 9\}$.

Per $a = 9$, l'insieme delle soluzioni (mod 15) è dato da $\{3, 12\}$.

Per $a = 0$, l'insieme delle soluzioni (mod 15) è dato da $\{5, 10\}$.

Esercizio 5.

$14210 = 2 \cdot 5 \cdot 7^2 \cdot 29$ è somma di due quadrati perché $5 \equiv 29 \equiv 1$ modulo 4. $14210 = 91^2 + 77^2 = 119^2 + 7^2$.

$910 = 13 \cdot 7 \cdot 5 \cdot 2$ non è somma di due quadrati perché $7 \not\equiv 1$ modulo 4.