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

Appello X

MATRICOLA/IDENTIFICATIVO PERSONALE: ....
COGNOME: .... **NOME:** ....

esercizio	1			2		3	4	5				6	
punteggio max	5	10	4	5	3	5	8	4	5	6	4	5	4
punteggio assegnato													
totale													

ESERCIZIO 1. **(a)** Enunciare il Teorema di Euler-Fermat di caratterizzazione degli interi che possono essere scritti come somma di due quadrati.

(b) Dimostrare che un primo dispari p si scrive come somma di due quadrati se e soltanto se $p \equiv 1 \pmod 4$.

(c) Determinare tutte le coppie di interi naturali $\{a, b\}$ tali che $325 = a^2 + b^2$.

ESERCIZIO 2. **(a)** Determinare per quali valori interi del parametro λ, $0 \leq \lambda \leq 21$, la seguente congruenza è risolubile:

$$X^2 + X + \lambda \equiv 0 \pmod{22}.$$

(b) Per il più piccolo valore positivo dell'intero λ ($\lambda \neq 0$) per il quale la congruenza in **(a)** è risolubile determinare tutte le sue soluzioni.

ESERCIZIO 3. Si consideri il seguente sistema di congruenze lineari in due indeterminate:

$$\begin{cases} 4X - \lambda Y \equiv 2 \pmod{15} \\ 17X + 7Y \equiv 7 \pmod{15}\,. \end{cases}$$

Determinare tutte le eventuali soluzioni del sistema $\pmod{15}$ al variare di λ, con $0 \leq \lambda \leq 2$.

ESERCIZIO 4. Sia p un primo dispari ed a un intero tale che $\mathrm{MCD}(a, p) = 1$. Dimostrare che:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

ESERCIZIO 5. **(a)** Determinare la più piccola radice primitiva positiva $r \pmod{13}$ ovviamente con $1 \leq r \leq 12$.

(b) Determinare la tabella degli indici rispetto alla radice primitiva positiva minima r modulo 13.

(c) Determinare per quali valori del parametro λ, $0 \leq \lambda \leq 12$, la seguente equazione diofantea è risolubile:

$$5X^4 - 13Y - \lambda = 0\,.$$

(d) Per il più piccolo valore di λ *positivo* $(\lambda \neq 0)$ per il quale l'equazione diofantea data in **(c)** è risolubile determinare tutte le infinite coppie $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ che sono soluzioni di tale equazione diofantea.
In particolare, per il più piccolo intero positivo $\bar{x}$ tale che $(\bar{x}, \bar{y})$ è soluzione, determinare esplicitamente $\bar{y}$.

ESERCIZIO 6. **(a)** Determinare per quali interi a, $1 \leq a \leq 13$, relativamente primi con 14, il seguente simbolo di Jacobi vale 1:

$$\left(\frac{a}{14}\right).$$

(b) Determinare per quali interi a, $1 \leq a \leq 13$, relativamente primi con 14 la congruenza quadratica $X^2 - a \equiv 0 \pmod{14}$ è risolubile.

Soluzioni

1. Per **(a)** e **(b)** vedere gli appunti del corso.
(c) $325 = 5^2 \cdot 13 = 1^2 + 18^2 = 6^2 + 17^2 = 10^2 + 15^2$

2. La congruenza data è risolubile per $\lambda = 0, \mathbf{2}, 10, 14, 16, 20$ ed ha come soluzioni rispettivamente
$\{0, 10, 11, 21\}$; $\mathbf{\{4, 6, 15, 17\}}$; $\{3, 7, 14, 18\}$; $\{5, 16\}$; $\{2, 8, 13, 19\}$; $\{1, 9, 12, 20\}$.

3. Il sistema dato è equivalente al sistema:

$$\begin{cases} \Delta_\lambda X \equiv a_\lambda \pmod{15} \\ \Delta_\lambda Y \equiv b_\lambda \pmod{15}, \end{cases}$$

dove $\Delta_\lambda = 28 + 17\lambda$, $a_\lambda = 14 + 7\lambda$ e $b_\lambda = b = 28 - 34$.

Il sistema è risolubile per ogni valore di λ eccetto per $\lambda \equiv 1 \pmod{15}$. Le soluzioni sono date da

$\lambda \equiv 0 \quad \rightsquigarrow \quad \{(8, 3)\} \pmod{15}$
$\lambda \equiv 2 \quad \rightsquigarrow \quad \{(14, 12)\} \pmod{15}$
$\lambda \equiv 3 \quad \rightsquigarrow \quad \{(5, 6)\} \pmod{15}$
$\lambda \equiv 4 \quad \rightsquigarrow \quad \{(2, 4), (7, 9), (12, 14)\} \pmod{15}$
$\lambda \equiv 5 \quad \rightsquigarrow \quad \{(8, 3)\} \pmod{15}$
$\lambda \equiv 6 \quad \rightsquigarrow \quad \{(2, 0)\} \pmod{15}$
$\lambda \equiv 7 \quad \rightsquigarrow \quad \{(4, 2), (9, 7), (14, 12)\} \pmod{15}$
$\lambda \equiv 8 \quad \rightsquigarrow \quad \{(5, 6)\} \pmod{15}$
$\lambda \equiv 9 \quad \rightsquigarrow \quad \{(2, 9)\} \pmod{15}$
$\lambda \equiv 10 \quad \rightsquigarrow \quad \{(3, 3), (8, 8), (13, 13)\} \pmod{15}$
$\lambda \equiv 11 \quad \rightsquigarrow \quad \{(2, 0)\} \pmod{15}$
$\lambda \equiv 12 \quad \rightsquigarrow \quad \{(14, 12)\} \pmod{15}$
$\lambda \equiv 13 \quad \rightsquigarrow \quad \{(0, 1), (5, 6), (10, 11)\} \pmod{15}$
$\lambda \equiv 14 \quad \rightsquigarrow \quad \{(2, 9)\} \pmod{15}$.

4. Vedere gli appunti del corso.

5. (a) $r = 2$. le altre radici primitive sono date da r^k, con $\mathrm{MCD}(k, 12) = 1$, e cioè sono date rispettivamente da: $2^5 \equiv 6, 2^7 \equiv 11, 2^{11} \equiv 7 \pmod{13}$.

(b) $(a, \mathrm{ind}_2(a))$ = (2, 1), (4, 2), (8, 3), (3, 4) (6, 5), (12, 6), (11, 7), (9, 8), (5, 9), (10, 10), (7, 11), (1, 12).

(c) per $\lambda \neq 0$, la congruenza $5X^4 - \lambda \equiv 0 \pmod{13}$ se e soltanto se MCD(4, 12) = 4 divide $\mathrm{ind}_2(8\lambda)$ (dove 8 è l'inverso aritmetico di 5 (mod 13)). Cioè $8\lambda \equiv 1, 3, 9$ (mod 13) ovvero $\lambda \equiv 5, 2, 6$ (mod 13)

In conclusione, la conguenza sopra considerata è risolubile per $\lambda = 0, \mathbf{2}, 5, 6$, ed ha per soluzioni (nella indeterminata X), rispettivamente, da:
$\{0\}$;
$\mathbf{\{2, 3, 10, 11\}}$;
$\{1, 5, 8, 12\}$;
$\{4, 6, 7, 9\}$.

(d) Le soluzioni dell'equazione diofantea sono date dalle seguenti coppie al variare di $k \in \mathbb{Z}$:
$x_{k,1} = 2 + k \cdot 13$, $y_{k,1} = \frac{5(2+k\cdot 13)^4 - 2}{13}$;
$x_{k,2} == 3 + k \cdot 13$, $y_{k,1} = \frac{5(3+k\cdot 13)^4 - 2}{13}$;
$x_{k,3} == 10 + k \cdot 13$, $y_{k,1} = \frac{5(10+k\cdot 13)^4 - 2}{13}$;

$x_{k,4} == 11 + k \cdot 13$, $y_{k,1} = \frac{5(11+k\cdot 13)^4-2}{13}$.

6. (a) $\left(\frac{1}{14}\right) = 1$, $\left(\frac{3}{14}\right) = -1$ (perché $\left(\frac{3}{7}\right) = -1$), $\left(\frac{5}{14}\right) = -1$ (perché $\left(\frac{5}{7}\right) = -1$), $\left(\frac{9}{14}\right) = 1$ (perché 9 è un quadrato), $\left(\frac{11}{14}\right) = 1$, $\left(\frac{13}{14}\right) = -1$ (perché $\left(\frac{6}{7}\right) = -1$).

(b) È risolubile anche per valori di a con $\mathrm{MCD}(a, 14) \neq 1$. Precisamente, per

$a = 0 \rightsquigarrow 0 \pmod{14}$

$a = 1 \rightsquigarrow 1, 13 \pmod{14}$ (N.B. simbolo di Jacobi = 1)

$a = 2 \rightsquigarrow 4, 10 \pmod{14}$

$a = 4 \rightsquigarrow 2, 12 \pmod{14}$

$a = 7 \rightsquigarrow 7 \pmod{14}$

$a = 8 \rightsquigarrow 6, 8 \pmod{14}$

$a = 9 \rightsquigarrow 3, 11 \pmod{14}$ (N.B. simbolo di Jacobi = 1)

$a = 11 \rightsquigarrow 5, 9 \pmod{14}$ (N.B. simbolo di Jacobi = 1).