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

Esame: Appello B

MATRICOLA/IDENTIFICATIVO PERSONALE: .....

COGNOME: ..... **NOME:** .....

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

ESERCIZIO 1. **(a)** Enunciare il "Piccolo" Teorema di Fermat e la sua generalizzazione detta Teorema di Euler-Fermat.

(b) Dimostrare il Teorema di Euler-Fermat.

(c) Utilizzando il Teorema di Euler-Fermat, determinare un inverso aritmetico di 23 (mod 30).

(d) Determinare il più piccolo esponente intero positivo x tale che $23^x \equiv 1 \pmod{30}$ e mettere in relazione questo valore di x con $\varphi(30)$.

ESERCIZIO 2. Determinare tutte le (eventuali) soluzioni della congruenza polinomiale:

$$f(X) := X^5 + 15X^4 + X^3 + 18X^2 + 20X + 25 \equiv 0 \pmod{45 \quad (= 3^2 \cdot 5)}\,.$$

ESERCIZIO 3. (a) Determinare tutte le radici primitive (mod 17) e scrivere la tabella degli indici rispetto alla radice primitiva minima positiva (mod 17).

(b) Determinare le soluzioni (mod 16) della congruenza $5^X \equiv 13 \pmod{17}$.

ESERCIZIO 4. **(a)** Determinare per quali valori del parametro λ, $0 \leq \lambda \leq 16$ (notare che viene incluso nell'intervallo da prendere in considerazione anche il valore $\lambda = 0$), la seguente congruenza è risolubile:

$$7X^2 - 11X + \lambda \equiv 0 \pmod{17}.$$

(b) Per ogni valore di λ, $0 \leq \lambda \leq 16$, per il quale la congruenza in **(a)** è risolubile determinare tutte le sue soluzioni.

ESERCIZIO 5.

(a) Sia p un primo dispari, r una radice primitiva (mod p), e sia $a \in \mathbb{Z}$. Quando $a \neq 0$, dimostrare che l'equazione diofantea (in due inderminate):

$$X^5 - pY - a = 0$$

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

$$5T \equiv \mathrm{ind}_r(a) \pmod{(p-1)}.$$

(b) Determinare per quali valori di a, con $0 \leq a \leq 6$, l'equazione diofantea:

$$X^5 - 7Y - a = 0$$

è risolubile.

(c) Per il più piccolo valore positivo di a, con $1 \leq a \leq 6$, per il quale l'equazione diofantea:

$$X^5 - 7Y - a = 0$$

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

ESERCIZIO 6. Sia μ la funzione di Moebius:

(a) Dimostrare che se n è un intero positivo pari, allora $\mu(n)+\mu(n+1)+\mu(n+2) < 3$.

(b) Determinare il più piccolo intero positivo $n \in \mathbb{N}$ tale che $\mu(n) + \mu(n+1) + \mu(n+2) = 3$.

(c) Determinare $\sum_{k=1}^{\infty} \mu(k!)$.

SOLUZIONI

ESERCIZIO 1.

(c) Si noti che $\varphi(30) = 8$ e che $23^7 \equiv 17 \pmod{30}$, dove $7 = \varphi(30) - 1$.

(d) $x = 4$ (con $4 \mid \varphi(30) = 8$), infatti $23^4 \equiv 1 \pmod{30}$. Si noti anche che $23 \not\equiv 1$ e $23^2 \equiv 19 \not\equiv 1 \pmod{30}$.

ESERCIZIO 2.

$f(X) \equiv 0 \pmod 3$ ha come soluzione $x \equiv 2 \pmod 3$.
$f(X) \equiv 0 \pmod 9$ ha come soluzione $x \equiv 8 \pmod 9$.
$f(X) \equiv 0 \pmod 5$ ha come soluzioni $x \equiv 0, 1 \pmod 5$.
$f(X) \equiv 0 \pmod{3^2 \cdot 5}$ ha come soluzioni $x \equiv 26, 35 \pmod{45}$.

ESERCIZIO 3.

(a) Una radice primitiva è $r = 3$. Tutte le altre appartengono all'insieme $\{3^k \mid 1 \leq k \leq 16\,,\ \mathrm{MCD}(k, 16) = 1\} = \{3, 10, 5, 11, 14, 7, 12, 6\}$. (Si noti che $\varphi(16) = 8$.) Chiaramente $r = 3$ è la radice primitiva minima con:
$\mathrm{ind}_3(1) = 16$; $\mathrm{ind}_3(2) = 14$; $\mathrm{ind}_3(3) = 1$; $\mathrm{ind}_3(4) = 12$; $\mathrm{ind}_3(5) = 5$;
$\mathrm{ind}_3(6) = 15$; $\mathrm{ind}_3(7) = 11$; $\mathrm{ind}_3(8) = 10$; $\mathrm{ind}_3(9) = 2$; $\mathrm{ind}_3(10) = 3$;
$\mathrm{ind}_3(11) = 7$; $\mathrm{ind}_3(12) = 13$; $\mathrm{ind}_3(13) = 4$; $\mathrm{ind}_3(14) = 9$; $\mathrm{ind}_3(15) = 6$;
$\mathrm{ind}_3(16) = 8$.

(b) Le soluzioni si ottengono dalle soluzioni della congruenza $\mathrm{ind}_3(5)X \equiv \mathrm{ind}_3(13) \pmod{16}$ ovvero $5X \equiv 4 \pmod{16}$. Tale congruenza ha un'unica soluzione $x \equiv 4 \pmod{16}$.

ESERCIZIO 4.

Sia $Y := 14X - 11$ e $\Delta_\lambda := 121 - 28\lambda \equiv 2 + 6\lambda \pmod{17}$. La congruenza data è equivalente alla congruenza:

$$Y^2 \equiv \Delta_\lambda \equiv 2 + 6\lambda \pmod{17}.$$

La congruenza nella incognita Y è risolubile per $\lambda = 0, 1, 4, 5, 6, 8, 11, 14, 16$ ed ha come insiemi di soluzioni, rispettivamente, i seguenti insiemi: $\{6, 11\}$, $\{5, 12\}$, $\{3, 14\}$, $\{7, 10\}$, $\{2, 15\}$, $\{4, 13\}$, $\{0\}$, $\{1, 16\}$, $\{8, 9\}$.

Pertanto, la congruenza data (nella incognita X) è risolubile per gli stessi valori di λ (cioè $\lambda = 0, 1, 4, 5, 6, 8, 11, 14, 16$) ed ha come insiemi di soluzioni, rispettivamente, i seguenti insiemi: $\{0, 4\}$, $\{6, 15\}$, $\{1, 3\}$, $\{10, 11\}$, $\{7, 14\}$, $\{9, 12\}$, $\{2\}$, $\{8, 13\}$, $\{5, 16\}$.

ESERCIZIO 5.

(b) Per ogni valore di a, con $0 \leq a \leq 6$, la congruenza $X^5 \equiv a \pmod 7$ è risolubile ed ammette un'unica soluzione. Precisamente:
$a = 0 \ \mapsto\ x \equiv 0 \pmod 7$;
$a = 1 \ \mapsto\ x \equiv 1 \pmod 7$;
$a = 2 \ \mapsto\ x \equiv 4 \pmod 7$;
$a = 3 \ \mapsto\ x \equiv 5 \pmod 7$;
$a = 4 \ \mapsto\ x \equiv 2 \pmod 7$;
$a = 5 \ \mapsto\ x \equiv 3 \pmod 7$;
$a = 6 \ \mapsto\ x \equiv 6 \pmod 7$.

Infatti è facile verificare che $r = 3$ è una radice primitiva (mod 7). Se $b := \mathrm{ind}_3(a)$ e $T := \mathrm{ind}_3(X)$, allora la congruenza $5T \equiv b \pmod 6$ è risolubile ed ammette un'unica soluzione per ogni valore di b, con $1 \leq b \leq 6$. Precisamente:

$b = 1 \ \mapsto \ t \equiv 5 \pmod 6$;
$b = 2 \ \mapsto \ t \equiv 4 \pmod 6$;
$b = 3 \ \mapsto \ t \equiv 3 \pmod 6$;
$b = 4 \ \mapsto \ t \equiv 2 \pmod 6$;
$b = 5 \ \mapsto \ t \equiv 1 \pmod 6$;
$b = 6 \ \mapsto \ t \equiv 0 \pmod 6$.

Infine si noti che:
$\mathrm{ind}_3(1) = 6$; $\mathrm{ind}_3(2) = 2$; $\mathrm{ind}_3(3) = 1$; $\mathrm{ind}_3(4) = 4$; $\mathrm{ind}_3(5) = 5$; $\mathrm{ind}_3(6) = 3$.

(c) Per $a = 1$, le (infinite) soluzioni dell'equazione diofantea data sono:

$$(x_\lambda,\ y_\lambda) = \left(1 + 7\lambda,\ \frac{(1+7\lambda)^5 - 1}{7}\right) \text{ al variare comunque di } \lambda \in \mathbb{Z}\,.$$

ESERCIZIO 6. (a) Se n è pari, esattamente uno fra n e $n+2$ è divisibile per 4, quindi almeno uno tra $\mu(n)$ e $\mu(n+2)$ è uguale a zero.

(b) $n = 33$ (osservare che necessariamente $n, n+1, n+2$ devono essere tutti e tre prodotto di un numero pari –in tal caso, due– di numeri primi).

(c) Se $k \geq 4$, $4 \mid k!$ e $\mu(k!) = 0$. Quindi $\sum_{k=1}^{\infty} \mu(k!) = \mu(1) + \mu(2) + \mu(6) = 1$.