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

Esame: Appello A

MATRICOLA/IDENTIFICATIVO PERSONALE: .....

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

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

ESERCIZIO 1. **(a)** Enunciare e dimostrare il Teorema di Lagrange relativo a congruenze del tipo:

$$f(X) \equiv 0 \pmod{p}$$

dove $f(X) \in \mathbb{Z}[X]$ è un polinomio non nullo e p è un intero primo.

(b) Determinare il numero massimo di soluzioni incongruenti (mod 17) della congruenza

$$X^{35} + X^{17} + X - 1 \equiv 0 \pmod{17}\,.$$

ESERCIZIO 2. Calcolare le eventuali soluzioni (mod 19) del seguente sistema di congruenze lineari in due indeterminate:

$$\begin{cases} 7X + 5Y \equiv 17 \pmod{19} \\ 6X - 11Y \equiv 3 \pmod{19}\,. \end{cases}$$

ESERCIZIO 3. **(a)** Determinare tutte le radici primitive (mod 19) e scrivere la tabella degli indici rispetto alla radice primitiva minima positiva (mod 19).

(b) Determinare le soluzioni (mod 19) della congruenza $7X^7 \equiv 2 \pmod{19}$.

(c) Determinare le soluzioni (mod 18) della congruenza $5^X \equiv 9 \pmod{19}$.

ESERCIZIO 4. **(a)** Determinare per quali valori del parametro λ, $0 \leq \lambda \leq 21$, la seguente congruenza è risolubile:

$$5X^2 + X + \lambda \equiv 0 \pmod{22}.$$

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

ESERCIZIO 5. **(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, $1 \leq a \leq 14$, relativamente primi con 14 la congruenza quadratica $X^2 - a \equiv 0 \pmod{14}$ è risolubile.

ESERCIZIO 6. **(a)** Sia f una funzione aritmetica, e sia $F(n) := \sum_{d|n} f(d)$, per ogni $n \in \mathbb{N}$. Dimostrare che F è moltiplicativa se e soltanto se f è moltiplicativa.

(b) Dimostrare che, per ogni intero $k \geq 1$, la funzione

$$\sigma^k(n) := \sum_{d|n} d^k$$

è una funzione moltiplicativa.

ESERCIZIO 1: Soluzione. (b) La congruenza data è equivalente a $X^3+2X-1 \equiv 0 \pmod{17}$ (applicazione del "Piccolo" Teorema di Fermat) che ha esattamente tre soluzioni: 8, 12, 14 (mod 17).

ESERCIZIO 2: Soluzione. Il discriminante $\Delta = -107 \equiv 7 \pmod{19}$. Il sistema dato e equivalente al sistema

$$\begin{cases} \Delta \cdot X \equiv 7 \pmod{19} \\ \Delta \cdot Y \equiv 14 \pmod{19}\,. \end{cases}$$

Essendo l'inverso aritmetico di $\Delta = 7$ uguale ad 11 (mod 19), il sistema ammette un'unica soluzione che è data da $(x, y) = (1, 2) \pmod{19}$.

ESERCIZIO 3: Soluzione.

(a) Una radice primitiva è $r = 2$. Tutte le altre appartengono all'insieme $\{2^k \mid 1 \leq k \leq 18\,,\ \mathrm{MCD}(k, 18) = 1\} = \{2, 13, 14, 15, 3, 10\}$. Chiaramente $r = 2$ è la radice primitiva minima con:
$\mathrm{ind}_2(1) = 18$; $\mathrm{ind}_2(2) = 1$; $\mathrm{ind}_2(3) = 13$; $\mathrm{ind}_2(4) = 2$; $\mathrm{ind}_2(5) = 16$;
$\mathrm{ind}_2(6) = 14$; $\mathrm{ind}_2(7) = 6$; $\mathrm{ind}_2(8) = 3$; $\mathrm{ind}_2(9) = 8$; $\mathrm{ind}_2(10) = 17$;
$\mathrm{ind}_2(11) = 12$; $\mathrm{ind}_2(12) = 15$; $\mathrm{ind}_2(13) = 5$; $\mathrm{ind}_2(14) = 7$; $\mathrm{ind}_2(15) = 11$;
$\mathrm{ind}_2(16) = 4$; $\mathrm{ind}_2(17) = 10$; $\mathrm{ind}_2(18) = 9$.

(b) La congruenza data è equivalente a $X^7 \equiv 11 \cdot 2 \equiv 3 \pmod{19}$ [dove 11 è l'inverso aritmetico di 7 (mod 19)]. Questa ha un'unica soluzione: $14 \pmod{19}$ [ottenuta dalla congruenza $7Y \equiv 13 \pmod{18}$ (dove 13 è l'indice di 3, rispetto alla radice primitiva $r = 2$), la quale ha come soluzione $7 \pmod{18}$, dove $\mathrm{ind}_2(14) = 7$].

(c) Le soluzioni si ottengono dalle soluzioni della congruenza $16X \equiv 8 \pmod{18}$ e che sono $5, 14 \pmod{18}$.

ESERCIZIO 4: Soluzione. E' risolubile per $\lambda = 0, 2, 4, 12, 16, 18$ ed ha come soluzioni, rispettivamente i seguenti insiemi: $\{0, 2, 11, 13\}$, $\{5, 8, 16, 19\}$, $\{4, 9, 15, 20\}$, $\{6, 7, 17, 18\}$, $\{1, 12\}$, $\{3, 10, 14, 21\}$.

ESERCIZIO 5: Soluzione.

(a) Si calcola agevolmente che
$\left(\frac{1}{2}\right) = 1$, $\left(\frac{1}{7}\right) = 1$, $\left(\frac{1}{14}\right) = 1$ ◀ .
$\left(\frac{3}{2}\right) = 1$, $\left(\frac{3}{7}\right) = -1$, $\left(\frac{3}{14}\right) = -1$.
$\left(\frac{5}{2}\right) = 1$, $\left(\frac{5}{7}\right) = -1$, $\left(\frac{5}{14}\right) = -1$.
$\left(\frac{9}{2}\right) = 1$, $\left(\frac{9}{7}\right) = 1$, $\left(\frac{9}{14}\right) = 1$ ◀ .
$\left(\frac{11}{2}\right) = 1$, $\left(\frac{11}{7}\right) = 1$, $\left(\frac{11}{14}\right) = 1$ ◀ .
$\left(\frac{13}{2}\right) = 1$, $\left(\frac{13}{7}\right) = -1$, $\left(\frac{13}{14}\right) = -1$.

(b) Se $1 \leq a \leq 13$ e $\mathrm{MCD}(a, 14) = 1$, da quanto sopra si ricava che $X^2 - a \equiv 0 \pmod{14}$ è risolubile se e soltanto se $a = 1, 9, 11 \pmod{14}$.

Per $a = 1$, l'insieme delle soluzioni (mod 14) è dato da $\{1, 13\}$.

Per $a = 9$, l'insieme delle soluzioni (mod 14) è dato da $\{3, 11\}$.

Per $a = 11$, l'insieme delle soluzioni (mod 14) è dato da $\{5, 9\}$.

Si noti anche che la congruenza $X^2 - a \equiv 0 \pmod{14}$ è anche risolubile per altri valori di a non relativamente primi con 14.

Per $a = 0$, l'insieme delle soluzioni (mod 14) è dato da $\{0\}$.

Per $a = 2$, l'insieme delle soluzioni (mod 14) è dato da $\{4, 10\}$.

Per $a = 4$, l'insieme delle soluzioni (mod 14) è dato da $\{2, 12\}$.
Per $a = 8$, l'insieme delle soluzioni (mod 14) è dato da $\{6, 8\}$.

ESERCIZIO 6: Soluzione. (b) Basta osservare che, per ogni intero fissato $k \geq 1$, l'applicazione $f : \ d \mapsto d^k$ è una funzione moltiplicativa. Poi applicare (a).