TN01 - Introduzione alla teoria dei numeri - A.A. 2002/2003
Appello B

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

ESERCIZIO 1. Data la congruenza:

$$X^2 + 3X + 2 + \lambda \equiv 0 \pmod{13},$$

(1) (**5pt**) dire per quali valori di λ, $0 \leq \lambda \leq 12$, la congruenza data è risolubile;
(2) (**2pt**) per il più piccolo valore di λ per il quale la congruenza è risolubile, trovare le soluzioni.

ESERCIZIO 2. (**7pt**) Determinare tutte le (eventuali) soluzioni della congruenza polinomiale:

$$X^4 + 47X^3 + 57X^2 + 77X + 36 \equiv 0 \pmod{135}.$$

ESERCIZIO 3. (**7pt**) Trovare tutte le soluzioni dell'equazione diofantea:

$$6^X - 8X^5 + 21Y = 0.$$

ESERCIZIO 4. (**4pt**) Mostrare che 3 è un non residuo quadratico per ogni primo p della forma $4^n + 1$.

ESERCIZIO 5.

(1) (**2pt**) Sia $f : \mathbb{N}^+ \to \mathbb{C}$ una funzione moltiplicativa. Dimostrare che σ_f è moltiplicativa.
(2) (**1pt**) Dimostrare che se f è totalmente moltiplicativa, allora σ_f non è in generale totalmente moltiplicativa.
(3) (**2pt**) Sia φ la funzione di Eulero, calcolare $\varphi^{-1}(84)$.

SOLUZIONI

Soluzione Esercizio 1.

(1) La congruenza data è equivalente alla congruenza
$$4X^2 + 12X + 9 + 4\lambda - 1 \equiv 0 \pmod{13},$$
(basta moltiplicare tutto per 4 ed aggiungere e sottrarre 9). Quindi, ponendo $Y := 2X + 3$, ci si riduce a studiare la congruenza $Y^2 \equiv 1 - 4\lambda \pmod{13}$. Per la risolubilità si studi il simbolo di Legendre $(\frac{1-4\lambda}{13})$, con $0 \leq \lambda \leq 12$. La congruenza è risolubile per $\lambda \equiv 0, 1, 6, 7, 9, 10, 11$.

(2) Per $\lambda = 0$ le soluzioni sono $y \equiv \pm 1 \pmod{13}$, da cui segue che $2X + 3 \equiv \pm 1 \pmod{13}$ e, quindi, $x \equiv 11, 12 \pmod{13}$.

Soluzione Esercizio 2. Sia $f(X) := X^4 + 47X^3 + 57X^2 + 77X + 36$. Allora:
$f(X) \equiv 0$ (mod 5) ha soluzione: $2, 3, 4$;
$f(X) \equiv 0$ (mod 3) ha soluzioni: $0, 2$;
$f(X) \equiv 0$ (mod 9) ha soluzioni: 0, 2;
$f(X) \equiv 0$ (mod 27) ha soluzioni: 2, 9;
$f(X) \equiv 0$ (mod 54) ha soluzioni: $2, 9, 29, 63, 83, 117$.

Soluzione Esercizio 3.
Si studia la congruenza $6^X \equiv 8X^5 \pmod{21}$. Ci si riduce a studiare le due congruenze $6^X \equiv 8X^5 \pmod{3}$ e $6^X \equiv 8X^5 \pmod{7}$.

La congruenza $6^X \equiv 8X^5 \pmod{3}$ ha come soluzione $x \equiv 0 \pmod{3}$ con $x \neq 0$!

Per la risoluzione della congruenza $6^X \equiv 8X^5 \pmod{7}$ si consideri la radice primitiva di 7, $r = 3$. Applicando la teoria degli indici si ottiene che deve essere $3X \equiv 5\,\mathrm{ind}_3(X) \pmod{6}$. Quest'ultima congruenza è risolubile se e solo se $3 \mid \mathrm{ind}_3(X)$ e questo avviene se e solo se $x \equiv 1, 6 \pmod{7}$. Quindi si risolvono i sistemi
$$\begin{cases} X \equiv 6 \pmod{7} \\ 3X \equiv 5 \cdot 3 \pmod{6}\,. \end{cases}$$
$$\begin{cases} X \equiv 1 \pmod{7} \\ 3X \equiv 5 \cdot 6 \pmod{6}\,. \end{cases}$$
da cui si ricavano le soluzioni $x \equiv 13, 8 \pmod{14}$.

Mettendo a sistema queste soluzioni con $x \equiv 0 \pmod{3}$ si ottengono le soluzioni della congruenza iniziale $6^X \equiv 8X^5 \pmod{21}$, che sono $x \equiv 27, 36 \pmod{42}$.

A questo punto le soluzioni dell'equazione diofantea data sono le seguenti:
$(27 + 42h, \frac{8(27+42h)^5 - 6^{(27+42h)}}{21})$ con $h \in \mathbb{Z}$, e $(36 + 42k, \frac{8(36+42k)^5 - 6^{(36+42k)}}{21})$ con $k \in \mathbb{Z}$.

Soluzione Esercizio 4. Si osservi che poiché $4^n + 1$ deve essere primo, allora $n \geq 1$. Adesso, $4^n + 1 \equiv 1 \pmod{4}$ quindi, applicando la LQR, abbiamo che $(\frac{3}{4^n+1}) = (\frac{4^n+1}{3}) = (\frac{2}{3}) = -1$. La tesi segue.

Soluzione Esercizio 5.

(1) Vedere le dispense del corso.

(2) Basta prendere la funzione $\tau = \sigma_{\mathbf{1}}$ che non è totalmente moltiplicativa mentre **1** lo è .

(3) Per ogni $n \geq 2$ si ha che $\varphi^{-1}(n) = \prod_{p|n}(1-p)$. Dunque $\varphi^{-1}(84) = (1-2)(1-3)(1-7) = -12$.