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

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

ESERCIZIO 1. (**7pt**)

$$\begin{cases} 11X - 2\lambda Y \equiv 6 \pmod{13} \\ 12X + 5Y \equiv 1 + 2\mu \pmod{13} . \end{cases}$$

(1) Studiare la risolubilità del sistema assegnato al variare di λ e μ, con $0 \leq \lambda, \mu \leq 12$ (cioè dire quando è risolubile e, nei casi in cui è risolubile, dire quante soluzioni ammette).
(2) Al variare di $7 \leq \lambda \leq 8$ e $0 \leq \mu \leq 1$, trovare tutte le (eventuali) soluzioni del sistema.

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

$$X^4 + 15X^3 + 95X^2 + 75X + 39 \equiv 0 \pmod{135}.$$

ESERCIZIO 3. (**6pt**) Determinare $(\bmod\, 4 \cdot 17)$ tutte le soluzioni della congruenza:

$$13^X \equiv 4X \pmod{17}.$$

ESERCIZIO 4.

(1) (**2pt**) Sia p un numero primo e siano a, b interi qualsiasi. Mostrare che se a è un residuo quadratico modulo p e $ab \equiv 1 \pmod{p}$, allora b è un residuo quadratico modulo p;
(2) (**4pt**) Siano p e q primi dispari tali che $q = 10p + 3$. Dimostrare che $(\frac{p}{q}) = (\frac{3}{p})$.

ESERCIZIO 5. Sia $*$ il prodotto di Dirichlet di funzioni aritmetiche e si ponga $F := \mu * \varphi\tau$.

(1) (**2pt**) Calcolare $F^{-1}(22)$.
(2) (**2pt**) Sia f la funzione aritmetica determinata dalla formula di inversione di Möbius. Calcolare $f(22)$.

SOLUZIONI

Soluzione Esercizio 1.

(1) Abbiamo che $\Delta \equiv 3 - 2\lambda \pmod{13}$. Il sistema ammette un'unica soluzione se e soltanto se $\Delta \not\equiv 0 \pmod{13}$, ovvero per $\lambda \not\equiv 8 \pmod{13}$, qualunque sia il valore assunto da $\mu \in \mathbb{Z}$.
Se $\lambda \equiv 8 \pmod{13}$ allora $\Delta \equiv 0 \pmod{13}$, quindi il sistema è risolubile se e soltanto se $\alpha \equiv 0 \pmod{13}$ e $\beta \equiv 0 \pmod{13}$. Adesso, $\alpha \equiv 2\lambda + 4\lambda\mu + 4 \pmod{13}$ e $\beta \equiv 4 - 4\mu \pmod{13}$. Se $\lambda \equiv 8 \pmod{13}$, allora $\alpha \equiv \beta \equiv 0 \pmod{13}$ se e soltanto se $\mu \equiv 1 \pmod{13}$.
Dunque se $\lambda \equiv 8 \pmod{13}$ e $\mu \equiv 1 \pmod{13}$ il sistema ammette 13 soluzioni distinte. Se $\lambda \equiv 8 \pmod{13}$ e $\mu \not\equiv 1 \pmod{13}$ il sistema non è risolubile.

(2) Se $\lambda = 7$ e $\mu = 20$, l'unica soluzione del sistema è $(9, 2)$.
Se $\lambda = 7$ e $\mu = 1$, l'unica soluzione del sistema è $(10, 0)$.
Se $\lambda = 8$ e $\mu = 0$ il sistema non è risolubile.
Se $\lambda = 8$ e $\mu = 1$ le due congruenze del sistema sono una multipla dell'altra, pertanto le soluzioni del sistema sono le soluzioni di una delle due congruenze del sistema. Il sistema ammette 13 soluzioni distinte che si possono esprimere brevemente attraverso la seguente forma parametrica: $(k, 8k-2)$, con $0 \leq k \leq 12$.

Soluzione Esercizio 2. Sia $f(X) := X^4 + 15X^3 + 95X^2 + 75X + 39$. Allora:
$f(X) \equiv 0 \pmod 5$ ha soluzione: $1, 2, 3, 4$;
$f(X) \equiv 0 \pmod 3$ ha soluzioni: $0, 1, 2$;
$f(X) \equiv 0 \pmod 9$ ha soluzioni: 1, 8;
$f(X) \equiv 0 \pmod{27}$ ha soluzioni: 8, 10;
$f(X) \equiv 0 \pmod{54}$ ha soluzioni: $8, 37, 62, 64, 89, 91, 116, 118$.

Soluzione Esercizio 3.
Scegliamo $r = 2$ come radice primitiva $\pmod{17}$. Le soluzioni della congruenza sono le soluzioni del sistema:

$$\begin{cases} X \equiv a \pmod{17} \\ 4X \equiv 12 + \mathrm{ind}_2(a) \pmod{16}. \end{cases}$$

La seconda equazione del sistema è risolubile se e soltanto se $\mathrm{ind}_2(a) \equiv 0 \pmod 4$. Questo avviene se e soltanto se $a \equiv 1, 4, 13, 16 \pmod{17}$. In corrispondenza di questi valori di a, le soluzioni della congruenza sono $x \equiv 33, 35, 38, 64 \pmod{68}$.

Soluzione Esercizio 4.

(1) Basta osservare che $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$. Quindi $(\frac{a}{p})(\frac{b}{p}) = (\frac{1}{p})$ e, poiché $(\frac{a}{p}) = 1$, deve essere anche $(\frac{b}{p}) = 1$.

(2) Poiché $q = 10p + 3$, allora $\frac{q-1}{2}$ è pari. Quindi $(\frac{p}{q}) = (\frac{q}{p}) = (\frac{10p+3}{p}) = (\frac{3}{p})$.

Soluzione Esercizio 5.

(1) $F(22) = \varphi(22)\tau(22) + \mu(2)\varphi(11)\tau(11) + \mu(11)\varphi(2)\tau(2) + \mu(22) = 10 \cdot 4 - 2 - 20 + 1 = 19$.
Per il calcolo di $F^{-1}(22)$, basta osservare che $F * F^{-1} = u$, da cui:
$F^{-1}(22)F(1) + F^{-1}(11)F(2) + F^{-1}(2)F(11) + F^{-1}(1)F(22) = u(22) = 0.$

Osserviamo anche che, per la validità della stessa formula di sopra, $F^{-1}(p) = -F(p)$, per ogni primo p. Quindi, $F^{-1}(2) = -F(2) = -1$ e $F^{-1}(11) = -F(11) = -19$. Risulta, allora, che $F^{-1}(22) = -19+19+19 = 19$.

(2) $f(28) = \mu(22)+F(2)\mu(11)+F(11)\mu(2)+F(22) = 1-F(2)-F(11)+F(22) = 1-1-19+19 = 0$.