TN1 - Introduzione alla teoria dei numeri - A.A. 2006/2007
Valutazione "in itinere" - I Prova

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

esercizio	1, a	1, b	2, a	2, b	3	4, a	4, b	5, a	5, b	5, c	5, d	5, e
punteggio max	3	6	3	7	7	3	4	3	4	4	6	8
punteggio assegnato												
totale												

ESERCIZIO 1. (a) Dimostrare che per ogni intero $m \geq 2$ e per ogni intero $a \in \mathbb{Z}$ tale che $\mathrm{MCD}(a, m) = 1$ si ha:

$$a^m \equiv a^{m-\varphi(m)} \pmod{m}.$$

(b) Se n è un intero positivo pari allora mostrare che $\varphi(2n) = 2\varphi(n)$.

ESERCIZIO 2.

(a) Sia $f(X) \equiv 0 \pmod{2 \cdot m}$ una congruenza polinomiale. Si assuma che:
   (1) $f(X) \equiv 0 \pmod 2$ ha come soluzioni $0, 1 \pmod 2$;
   (2) $f(X) \equiv 0 \pmod m$ ha come soluzioni $\{x_1, x_2, \ldots, x_s\} \pmod m$;
   (3) m è un intero dispari.

   Dimostrare che le soluzioni di $f(X) \equiv 0 \pmod{2 \cdot m}$ sono in numero di $2 \cdot s$ e sono date da $\{x_1, x_2, \ldots, x_s,\ x_1 + m, x_2 + m, \ldots, x_s + m\}$.

(b) Determinare tutte le (eventuali) soluzioni della congruenza polinomiale:

$$f(X) := X^4 + 3X^3 + 2X - 44 \equiv 0 \pmod{50}\,.$$

ESERCIZIO 3. Determinare, al variare di λ e di μ, con $0 \leq \lambda \leq 2$ e $0 \leq \mu \leq 1$, tutte le (eventuali) soluzioni del seguente sistema di congruenze lineari in due indeterminate:

$$\begin{cases} 2\lambda X - 2Y \equiv 2 \pmod{17} \\ 8X + 9Y \equiv 5\mu \pmod{17}\,. \end{cases}$$

ESERCIZIO 4. Si consideri la seguente equazione diofantea in due indeterminate

$$3X + (8\lambda + 1)Y = 5\,.$$

(a) Determinare per quali $\lambda \in \mathbb{Z}$ l'equazione è risolubile.
(b) Determinare tutte le soluzioni dell'equazione data per il più piccolo $\lambda \geq 0$ per cui l'equazione è risolubile.

ESERCIZIO 5. Per ogni intero $n \geq 1$ sia

$$F(n) := \prod_{d|n} d.$$

(a) Mostrare che F non è una funzione moltiplicativa.
(b) Determinare $F(10)$ e $F^{-1}(10)$.
(c) Sia f la funzione aritmetica tale che $F = \sigma_f$. Determinare $f(10)$.
(d) Sia $n = p^k$ con p primo e $k \in \mathbb{N}$. Dimostrare che $F(n) = n^{\frac{\tau(n)}{2}}$.
(e) Dimostrare la formula in (d) per ogni intero $n \geq 2$.
(Attenzione: F non è moltiplicativa)

Soluzioni

1. (a) Si osservi che $m \geq \varphi(m)$ e quindi, per il Teorema di Euler-Fermat,

$$a^m = a^{m-\varphi(m)}a^{\varphi(m)} \equiv a^{m-\varphi(m)} \cdot 1 = a^{m-\varphi(m)} \pmod{m}.$$

(b) Sia $n = 2^k n'$, con n' dispari e $k \geq 1$. E' facile vedere che $\varphi(2^k) = 2^{k-1}$. Quindi $\varphi(2n) = \varphi(2 \cdot 2^k n') = \varphi(2^{k+1}n') = \varphi(2^{k+1})\varphi(n') = 2^k\varphi(n') = 2 \cdot 2^{k-1}\varphi(n') = 2\varphi(2^k)\varphi(n') = 2\varphi(2^k n') = 2\varphi(n)$.

2. (a) Qualunque intero (mod 2) è soluzione di $f(X) \equiv 0 \pmod 2$. In particolare, qualunque elemento di $\{x_1, x_2, \ldots, x_s, x_1+m, x_2+m, \ldots, x_s+m, \}$ è soluzione di $f(X) \equiv 0 \pmod 2$. Si noti che gli elementi di tale insieme a due a due non congrui (mod $2 \cdot m$).

Per il Teorema Cinese dei resti, le soluzioni $f(X) \equiv 0 \pmod{2 \cdot m}$ devono essere in numero di $2 \cdot s$, allora si conclude facilmente che $\{x_1, x_2, \ldots, x_s,\ x_1 + m, x_2 + m, \ldots, x_s + m, \}$ è l'insieme completo delle soluzioni di $f(X) \equiv 0 \pmod{2 \cdot m}$.

(b) $f(X) \equiv 0 \pmod 2$ ha due soluzioni $y_{1,1} \equiv 0 \pmod 2$ e $y_{1,2} \equiv 1 \pmod 2$.

$f(X) \equiv 0 \pmod 5$ ha una soluzione $y_{2,1} \equiv 2 \pmod 5$.

$f(X) \equiv 0 \pmod{5^2}$ ha cinque soluzioni $\{2, 7, 12, 17, 22\} \pmod{5^2}$.

Da cui, tenendo presente (a) (oppure il Teorema Cinese dei Resti), si ricava che: $f(X) \equiv 0 \pmod{50}$ ha 10 $(= 2 \cdot 5)$ soluzioni $\{2, 7, 12, 17, 22, 27, 32, 37, 42, 47\} \pmod{50}$.

3. $\Delta_\lambda = 18\lambda + 16$. Si vede che $\Delta_\lambda \equiv 0 \pmod{17}$ se e soltanto se $\lambda \equiv 1 \pmod{17}$.

Per $(\lambda, \mu) = (0, 0)$ il sistema ha un'unica soluzione $(x, y) = (16, 16) \pmod{17}$.

Per $(\lambda, \mu) = (0, 1)$ il sistema ha un'unica soluzione $(x, y) = (6, 16) \pmod{17}$.

Per $(\lambda, \mu) = (2, 0)$ il sistema ha un'unica soluzione $(x, y) = (1, 1) \pmod{17}$.

Per $(\lambda, \mu) = (2, 1)$ il sistema ha un'unica soluzione $(x, y) = (11, 4) \pmod{17}$.

Per $\lambda = 1$ e $\mu = 0, 1$ il sistema non ammette soluzioni (mod 17).

4. (a) L'equazione ha soluzione se e soltanto se $\text{MCD}(3, 8\lambda + 1)|5$, quindi se e soltanto se $\text{MCD}(3, 8\lambda + 1)) = 1$, ovvero se e soltanto se $8\lambda + 1 \not\equiv 0 \pmod 3$.

Ne segue che l'equazione ha soluzione se e soltanto se $\lambda \not\equiv 1 \pmod 3$.

(b) Per $\lambda = 0$, le soluzioni sono (x_t, y_t) dove $x_t = t$, $y_t = 5 - 3t$, $\forall\ t \in \mathbb{Z}$.

5. (a) $F(2) = 2, F(3) = 3$, ma $F(6) = 36$.

(b) $F(10) = 100$. Per calcolare $F^{-1}(10)$, notiamo che $0 = F * F^{-1}(10) = F(1)F^{-1}(10) + F(2)F^{-1}(5) + F(5)F^{-1}(2) + F(10)F^{-1}(1)$. Dato che si verifica facilmente che $F(1) = F^{-1}(1) = 1$, $F(p) = p$ e $F^{-1}(p) = -p$ per un primo p e $F(10) = 100$ otteniamo che $0 = F * F^{-1}(10) = F^{-1}(10) - 20 + 100$ e quindi $F^{-1}(10) = -80$.

(c) Dal fatto che $f = F * \mu$ si ricava che$f(10) = 94$.

(d) $F(p^k) = p \cdot p^2 \ldots p^k = p^{1+2+\ldots+k} = p^{\frac{k\cdot(k+1)}{2}} = (p^k)^{\frac{k+1}{2}} = n^{\frac{\tau(n)}{2}}$ (utilizzando il fatto che $\tau(p^k) = k + 1$)).

(e) Sia $\{d_1, d_2, \ldots, d_k\}$ l'insieme dei divisori positivi di n minori di $\sqrt{n}$.

Supponiamo ora che n non sia un quadrato. Si osserva facilmente che l'insieme dei divisori positivi di n è $\{d_1, d_2, \ldots, d_k, \frac{n}{d_k}, \ldots, \frac{n}{d_1}\}$. Pertanto $\tau(n) = 2k$. Allora $F(n) = d_1\frac{n}{d_1} \cdot d_2\frac{n}{d_2} \cdot \ldots \cdot d_k\frac{n}{d_k} = n^k = n^{\frac{\tau(n)}{2}}$.

Se invece n è un quadrato l'insieme dei divisori è $\{d_1, d_2, \ldots, d_k, \frac{n}{d_k}, \ldots, \frac{n}{d_1}, \sqrt{n}\}$. Pertanto $\tau(n) = 2k + 1$. Allora $F(n) = d_1\frac{n}{d_1} \cdot d_2\frac{n}{d_2} \cdot \ldots \cdot d_k\frac{n}{d_k} \cdot \sqrt{n} = n^k n^{1/2} = n^{k+\frac{1}{2}} = n^{\frac{2k+1}{2}} = n^{\frac{\tau(n)}{2}}$.

Si noti che ovviamente si poteva procedere in questo modo anche per risolvere il punto (d).