TN1 - Introduzione alla teoria dei numeri - A.A. 2001/2002

Esame: Appello A

MATRICOLA (O ALTRO IDENTIFICATIVO): .....

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

ESERCIZIO 1. Sia p un primo della forma $8t+3$, con $t>0$, e si supponga che $q := \frac{p-1}{2}$ sia anch'esso un numero primo.

(a) Dimostrare che se a è relativamente primo con p, allora $\mathrm{ord}_p(a) = 2, q, 2q$.

(b) Dimostrare che $2^q \equiv 1 \pmod p$ se e soltanto se $(\frac{2}{p}) = 1$.

(c) Mostrare che 2 è una radice primitiva di p.

(d) Determinare almeno due radici primitive distinte di 27.

ESERCIZIO 2. Trovare tutte le eventuali soluzioni della congruenza

$$9X^2 - 12X\lambda + 4\lambda^2 + 4 - \lambda \equiv 0 \pmod{13},$$

al variare di λ, $0 \leq \lambda \leq 12$.

ESERCIZIO 3. Per ogni intero $n > 1$, sia:

$$F(n) := \sum_{d|n} \mu(d)\sigma(d).$$

(a) Dimostrare che $F = \mu\sigma * \mathbf{1}$ (dove $(\mu\sigma)(n) := \mu(n)\sigma(n)$, per ogni $n \in \mathbb{N}^+$) è una funzione moltiplicativa.

(b) Sia $n = p_1^{e_1}p_2^{e_2}\cdot\ldots\cdot p_r^{e_r}$ la fattorizzazione in primi distinti di un intero positivo $n > 1$. Mostrare che $F(n) = (-1)^r p_1 p_2 \cdot \ldots \cdot p_r$.

(c) Calcolare $F(630)$.

(d) Determinare tramite la formula di inversione di Möbius, la funzione moltiplicativa f tale che $F = \sigma_f$. Calcolare $f(12)$.

ESERCIZIO 4. Sia p un numero primo dispari, m un intero positivo ed a un intero tale che $p \nmid a$. Sia $d := \mathrm{MCD}(m, p-1)$. Dimostrare la validità del seguente Criterio di Euler:

la congruenza $X^m \equiv a \pmod p$ *è risolubile se, e soltanto se,*

$$a^{\frac{p-1}{d}} \equiv 1 \pmod p .$$

ESERCIZIO 5. Trovare tutte le eventuali soluzioni del sistema seguente, al variare del parametro $\lambda, 0 \leq \lambda \leq 6$:

$$\begin{cases} 3X + 2\lambda Y \equiv 3 + \lambda \pmod 7 \\ X + 4Y \equiv 0 \pmod 7, \end{cases}$$

ESERCIZIO 1: Soluzione. **(a)** Poiché $p-1 = 2q$, con q primo, $\mathrm{ord}_p(a) = 2, q, 2q$, dato che in generale $\mathrm{ord}_p(a) \mid p-1$.

(b) $2^q \equiv 1 \pmod p$ se e soltanto se $(\frac{2}{p}) = 1$ (Criterio di Eulero, vedere appunti).

(c) $\mathrm{ord}_p(2) \neq 2$ perché $4 \not\equiv 1 \pmod p$ $(p > 3)$. Inoltre, $\mathrm{ord}_p(2) \neq q$ perché $2^q \not\equiv 1 \pmod p$, essendo $(\frac{2}{p}) = -1$ in quanto $p \equiv 3 \pmod 8$. Dunque, necessariamente, $\mathrm{ord}_p(2) = 2q$ e quindi 2 è una radice primitiva di p.

(d) Se $p = 27$, $q = 13$. In tal caso 2 è una radice primitiva di 27. Le altre radici primitive sono date da 2^k, al variare di k, con MCD$(k,\ 26) = 1$ e $1 \leq k \leq 26$.

ESERCIZIO 2: Soluzione. Basta risolvere la congruenza $Y^2 \equiv \lambda - 4 \pmod{13}$, dove $Y := 3X - 2\lambda$. Questa congruenza è risolubile per $\lambda = 0, 1, 3, 4, 5, 7, 8$ e le soluzioni rispettive per questi valori di λ sono $y_1 = 3, 6, 8, 0, 1, 4, 2$ e $y_2 = 10, 7, 5, 0, 12, 9, 11$. Dunque, le soluzioni della congruenza data sono le seguenti:

Per $\lambda = 0 \ \rightarrow \ x = 1,\ 12$;
Per $\lambda = 1 \ \rightarrow \ x = 3,\ 7$;
Per $\lambda = 3 \ \rightarrow \ x = 8,\ 9$;
Per $\lambda = 4 \ \rightarrow \ x = 7$;
Per $\lambda = 5 \ \rightarrow \ x = 3,\ 8$;
Per $\lambda = 7 \ \rightarrow \ x = 6,\ 12$;
Per $\lambda = 8 \ \rightarrow \ x = 6,\ 9$.

ESERCIZIO 3: Soluzione.

(a) Essendo $F = \mu\sigma * \mathbf{1}$, F è una funzione moltiplicativa, perché prodotto di Dirichlet di due funzioni moltiplicative (si noti che $\mu\sigma$ è una funzione moltiplicativa).

(b) $F(p^e) = 1 + \mu(p)\sigma(p) = 1 - (1 + p) = -p$.

(c) Poiché $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$, segue che $F(630) = (-1)^4 \cdot 2 \cdot 3 \cdot 5 \cdot 7 = 210$.

(d) E' immediato che $f = \mu\sigma$, essendo $F = \mu\sigma * \mathbf{1}$ e, quindi, $f = F * \mu = \mu\sigma$. Pertanto, $f(12) = \mu(12)\sigma(12) = 0$.

ESERCIZIO 4: Soluzione. Vedere gli appunti del corso.

ESERCIZIO 5: Soluzione.

Si ha che $\Delta_\lambda := 12 - 2\lambda \equiv 5 + 5\lambda \pmod 7$, $\alpha_\lambda := 5 + 4\lambda$ e $\beta_\lambda := 4 + 6\lambda \pmod 7$.

Inoltre MCD$(\Delta_\lambda, 7) = 1$ se e soltanto se $\Delta_\lambda \not\equiv 0 \pmod 7$, cosa che avviene se e solo se $\lambda \not\equiv 6 \pmod 7$.

In questi casi il sistema dato ammette un'unica soluzione:

$\lambda = 0,\ \ (x, y) = (1, 5)$;
$\lambda = 1,\ \ (x, y) = (3, 1)$;
$\lambda = 2,\ \ (x, y) = (6, 2)$;
$\lambda = 3,\ \ (x, y) = (4, 6)$;
$\lambda = 4,\ \ (x, y) = (0, 0)$;
$\lambda = 5,\ \ (x, y) = (2, 3)$;

Se, invece, $\lambda \equiv 6 \pmod 7$, il sistema non è risolubile.