TN1 - Introduzione alla teoria dei numeri - A.A. 2009/2010

Appello A

ESERCIZIO 1. Determinare in funzione di λ, con $0 \leq \lambda \leq 12$, quando la congruenza quadratica

$$X^2 + 4X - 5\lambda \equiv 0 \pmod{13}$$

è risolubile.

Per ciascun valore di λ, con $0 \leq \lambda \leq 12$, per il quale la congruenza è risolubile determinare tutte le sue soluzioni.

ESERCIZIO 2. Dimostrare che:

(1) un intero positivo n è differenza di due quadrati se e soltanto se n è prodotto di due fattori interi entrambi pari o entrambi dispari;

(2) se un intero positivo n pari è differenza di due quadrati allora n è divisibile per 4;

(3) se un intero positivo n è differenza di due quadrati, allora n *non* è della forma $4k + 2$.

ESERCIZIO 3. **(1)** Dimostrare il seguente Teorema di Lagrange:
Sia p un numero primo e sia

$$f(X) := a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 \in \mathbb{Z}[X] \;\; \textit{con } p \nmid a_n \,,$$

allora la congruenza $f(X) \equiv 0 \pmod{p}$ ha al più n soluzioni (incongrue) mod p.

(2) Determinare le condizioni sotto le quali la congruenza

$$X^d - 1 \equiv 0 \pmod{p}$$

ha *esattamente* d soluzioni (incongrue) mod p.

ESERCIZIO 4. Risolvere le seguenti congruenze:

(1) $X^6 + 13 \equiv 0 \pmod{14}$;

(2) $X^5 + 11X^4 + 17X^3 + 4X^2 + 2X + 5 \equiv 0 \pmod{54}$.

ESERCIZIO 5. Si consideri il seguente sistema di congruenze lineari in due indeterminate:

$$\begin{cases} 2X + \lambda Y \equiv 3 \pmod{13} \\ 3X + 5Y \equiv 7 \pmod{13}\,. \end{cases}$$

(1) Determinare, al variare di λ, con $0 \leq \lambda \leq 12$, quando e quali tra i seguenti casi si verificano (mod 13): il sistema è risolubile ed ammette un'unica soluzione; il sistema è risolubile ed ammette più di una soluzione; il sistema non è risolubile.

(2) Determinare esplicitamente le eventuali soluzioni del sistema precedente per $\lambda = 11$ e $\lambda = 12$.

ESERCIZIO 6. Sia φ la funzione di Euler e sia μ la funzione di Möbius.
(1) Dimostare che, per ogni $n \geq 1$,

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d} .$$

(2) Se $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$, allora dimostrare che

$$\sum_{d|n} \mu(d)\varphi(d) = (2 - p_1)(2 - p_2) \cdot \ldots \cdot (2 - p_r) .$$

ESERCIZIO 7.
(1) 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,*

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

(2) Determinare per quali valori di a, con $0 \leq a \leq 10$, la congruenza

$$X^6 \equiv a \pmod{11}$$

è risolubile e per ciascun valore di a, con $0 \leq a \leq 10$, per il quale la congruenza è risolubile, determinare tutte le sue soluzioni (mod 11).

ESERCIZIO 1: Soluzione. Basta ricondursi ad una congruenza del tipo $Y^2 \equiv d_\lambda := 12 + 7\lambda \pmod{13}$ (con $Y = 2X + 4$). Tale congruenza è risolubile per $\lambda = 0, 1, 2, 5, 7, 9, 12$. Le soluzioni della congruenza data sono le seguenti:

Per $\lambda = 0 \quad \rightsquigarrow \quad x = 0,\ 9$;
Per $\lambda = 1 \quad \rightsquigarrow \quad x = 1,\ 8$;
Per $\lambda = 2 \quad \rightsquigarrow \quad x = 10,\ 12$;
Per $\lambda = 5 \quad \rightsquigarrow \quad x = 2,\ 7$;
Per $\lambda = 7 \quad \rightsquigarrow \quad x = 11$;
Per $\lambda = 9 \quad \rightsquigarrow \quad x = 4,\ 5$;
Per $\lambda = 12 \quad \rightsquigarrow \quad x = 3,\ 6$.

ESERCIZIO 2: Soluzione.

(1) Basta osservare che se $n = a^2 - b^2$, allora $n = (a + b)(a - b)$, che sono entrambi pari (se a e b sono entrambi pari o entrambi dispari) o dispari (se a e b sono uno pari e l'altro dispari).

(2) Dal punto **(1)**, n è prodotto di due interi entrambi pari o entrambi dispari. Poiché n è pari, questi due interi devono essere entrambi pari (cioè divisibili entrambi per 2) e quindi n è divisibile per 4.

(3) Sia a un intero qualsiasi, allora è noto che $a^2 \equiv 0, 1 \pmod 4$, da cui $a^2 - b^2 \equiv 0, 1, 3 \pmod 4$; segue che $n \not\equiv 2 \pmod 4$, cioè che n *non* è della forma $4k + 2$.

ESERCIZIO 3: Soluzione. Vedere gli appunti del corso.

ESERCIZIO 4: Soluzione.

(1)
Mod 2 $\quad \rightsquigarrow \quad x = 1$;
Mod 7 $\quad \rightsquigarrow \quad x = 1, 2, 3, 4, 5, 6$;
Mod 14 $\quad \rightsquigarrow \quad x = 1, 3, 5, 9, 11, 13$.

(2)
Mod 2 $\quad \rightsquigarrow \quad x = 1$;
Mod 3 $\quad \rightsquigarrow \quad x = 2$;
Mod 9 $\quad \rightsquigarrow \quad x = 2, 5, 8$;
Mod 27 $\quad \rightsquigarrow \quad x = 8, 17, 26$;
Mod 54 $\quad \rightsquigarrow \quad x = 17, 35, 53$.

ESERCIZIO 5: Soluzione.

(1) Abbiamo che $\Delta \equiv 10 - 3\lambda \pmod{13}$. Il sistema ammette un'unica soluzione per $\Delta \not\equiv 0 \pmod{13}$ ovvero per $\lambda \not\equiv 12 \pmod{13}$. Mentre per $\lambda \equiv 12 \pmod{13}$ il sistema non è risolubile.

(2)
Per $\lambda = 0 \quad \rightsquigarrow \quad (x, y) = (8, 7)$;
Per $\lambda = 1 \quad \rightsquigarrow \quad (x, y) = (3, 10)$;
Per $\lambda = 2 \quad \rightsquigarrow \quad (x, y) = (10, 11)$;
Per $\lambda = 3 \quad \rightsquigarrow \quad (x, y) = (7, 5)$;
Per $\lambda = 4 \quad \rightsquigarrow \quad (x, y) = (0, 4)$;
Per $\lambda = 5 \quad \rightsquigarrow \quad (x, y) = (4, 12)$;
Per $\lambda = 6 \quad \rightsquigarrow \quad (x, y) = (5, 1)$;
Per $\lambda = 7 \quad \rightsquigarrow \quad (x, y) = (9, 9)$;
Per $\lambda = 8 \quad \rightsquigarrow \quad (x, y) = (2, 8)$;

Per $\lambda = 9 \quad \rightsquigarrow \quad (x, y) = (12, 2)$;
Per $\lambda = 10 \quad \rightsquigarrow \quad (x, y) = (6, 3)$;
Per $\lambda = 11 \quad \rightsquigarrow \quad (x, y) = (1, 6)$.

ESERCIZIO 6: Soluzione.

(1) Dalla teoria delle funzioni aritmetiche moltiplicative, sappiamo che $e = \varphi * \mathbf{1}$. Quindi, per la formula di inversione di Möbius, $e * \mu = \varphi$.

La funzione $f(n) := \mu(n) \cdot \varphi(n)$ è moltiplicativa, quindi anche $F := f * \mathbf{1}$ è moltiplicativa. Inoltre, è subito visto che $F(p^e) = 2 - p$, per ogni primo p e per ogni $e \geq 1$.

ESERCIZIO 7: Soluzione.

(1) Vedere gli appunti delle lezioni.

(2) Non è risolubile per $a = 2, 6, 7, 8, 10$. Mentre,
$a = 0 \quad \rightsquigarrow \quad x = 0$;
$a = 1 \quad \rightsquigarrow \quad x = 1, 10$;
$a = 3 \quad \rightsquigarrow \quad x = 3, 8$;
$a = 4 \quad \rightsquigarrow \quad x = 4, 7$;
$a = 5 \quad \rightsquigarrow \quad x = 5, 6$;
$a = 9 \quad \rightsquigarrow \quad x = 2, 9$.