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

Esame: Appello B

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

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

ESERCIZIO 1. Siano p un primo dispari, $a \geq 1$ con $\mathrm{MCD}(a,p) = 1$ e $S(a) := \{k \cdot a : 1 \leq k \leq (p-1)/2\}$. Si ponga $\nu(a) :=$ numero degli elementi k tali che $(p+1)/2 \leq k \cdot a \leq p-1$.
(1) In tale situazione, determinare quale tra le seguenti condizioni è equivalente alla risolubilità della congruenza $X^2 \equiv a \pmod{p}$:
(a) $\nu(a) = 1$.
(b) $\nu(a)$ è pari.
(c) $\nu(a)$ è dispari.
(d) $\nu(a) = \mathrm{ord}_p(a)$.
(2) Dare una dimostrazione completa di quanto enunciato in **(1)** .

ESERCIZIO 2. Determinare in funzione di λ, con $0 \leq \lambda \leq 10$, quando la congruenza quadratica

$$X^2 + 4X + 7\lambda \equiv 0 \pmod{11}$$

è risolubile.

Per ciascun valore di λ, con $0 \leq \lambda \leq 10$, per il quale la congruenza è risolubile determinare tutte le sue soluzioni.

ESERCIZIO 3. Risolvere le seguenti congruenze:
(1) $X^6 \equiv 1 \pmod{14}$;
(2) $3X^5 + 31X^4 + 17X^3 + 4X^2 + 2X + 9 \equiv 0 \pmod{54}$.

ESERCIZIO 4. 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) un intero positivo n pari è differenza di due quadrati se e soltanto se 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 5. Determinare tutte le (eventuali) soluzioni (mod 42) della congruenza:

$$5^X \equiv 4X^4 \pmod{7}\,.$$

ESERCIZIO 1: Soluzione. (1): (b); (2): Vedere gli appunti del corso.

ESERCIZIO 2: Soluzione. Basta ricondursi ad una congruenza del tipo $Y^2 \equiv \Delta_\lambda \pmod{11}$. Questa congruenza è risolubile per $\lambda = 0, 2, 3, 4, 8, 10$. Le soluzioni della congruenza data sono le seguenti:

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

ESERCIZIO 3: Soluzione.

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

(2)
Mod 2 $\rightarrow x = 1$;
Mod 3 $\rightarrow x = 0, 1$;
Mod 9 $\rightarrow x = 0, 4$;
Mod 27 $\rightarrow x = 4, 9$;
Mod 54 $\rightarrow x = 9, 31$.

ESERCIZIO 4: 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 $a^2 \equiv 0, 1, 3 \pmod 4$, da cui $a^2 - b^2 \equiv 0, 1 \pmod 4$; segue che $n \not\equiv 2 \pmod 4$, cioè che n non è della forma $4k + 2$.

ESERCIZIO 5: Soluzione. Le soluzioni sono date da $x \equiv 4, 8, 10, 12, 20, 30 \pmod{7 \cdot 6}$.