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

Prova di Esame, Appello X, Settembre 2010

MATRICOLA (o, altro identificativo personale): ....

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

ESERCIZIO 1. **(a)** Determinare per quali valori di a, con $0 \leq a \leq 16$, la seguente congruenza esponenziale (in una indeterminata X)

$$4^X \equiv a \pmod{17}$$

è risolubile.

(b) Per ciascuno dei valori di a, con $0 \leq a \leq 16$, per i quali la congruenza precedente è risolubile determinare tutte le soluzioni $\pmod{16}$.

ESERCIZIO 2. **(a)** Dare una dimostrazione completa del seguente Criterio di Euler (utilizzando l'esistenza di una radice primitiva): *Sia* a *un intero non nullo e sia* p *un intero primo dispari tale che* $\mathrm{MCD}(a, p) = 1$. *Allora,* a *è un residuo quadratico modulo* p *se e soltanto se* $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(b) Utilizzando **(a)**, determinare tutti i residui quadratici (mod 17).

(c) Trovare tutte le eventuali soluzioni della congruenza $X^2 \equiv 13$ (mod 17).

ESERCIZIO 3. Determinare tutte le eventuali soluzioni della congruenza polinomiale:

$$X^5 + 3X^3 + X^2 - 93 \equiv 0 \pmod{120\ (= 2^3 \cdot 3 \cdot 5)}.$$

ESERCIZIO 4. **(a)** Dimostrare che *un intero primo dispari* p *si può scrivere come somma di due quadrati di interi se e soltanto se* $p \equiv 1 \pmod{4}$.

(b) Determinare (spiegando il metodo seguito) tutti gli eventuali interi positivi $a,\ b$ tali che

$$61 = a^2 + b^2.$$

ESERCIZIO 5. **(a)** 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.

(b) Determinare per quali valori di d, $1 \leq d \leq 22$

$$X^d - 1 \equiv 0 \pmod{23}$$

ha *esattamente* d soluzioni (incongrue) mod 23.

(c) Determinare esplicitamente le soluzioni di $X^d - 1 \equiv 0 \pmod{23}$, per $d = 10$ e $d = 11$.

ESERCIZIO 6. **(a)** Dimostrare per ogni $n \geq 1$ la seguente formula:

$$n = \sum_{d|n} \sigma(d) \cdot \mu\left(\frac{n}{d}\right).$$

(b) Calcolare il valore di

$$\sum_{1 \leq k \leq 6} \sigma(k)$$

(spiegando il metodo utilizzato).

Soluzioni

ESERCIZIO 1

Per i seguenti valori di $0 \leq a \leq 16$ la congruenza è risolubile ed ha le soluzioni sotto indicate:
per $a = 1$, le soluzioni (mod 16) sono date da $x = 0, 4, 8, 12$;
per $a = 4$, le soluzioni (mod 16) sono date da $x = 1, 5, 9, 13$;
per $a = 16$, le soluzioni (mod 16) sono date da $x = 2, 6, 10, 14$;
per $a = 13$, le soluzioni (mod 16) sono date da $x = 3, 7, 11, 15$.

ESERCIZIO 2

(b) $a =, 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$.
(c) $x = 8, 9 \pmod{17}$.

ESERCIZIO 3

$x = 3, 23, 33, 53, 63, 83, 93, 113 \pmod{120}$.

ESERCIZIO 4

(b) $(a, b) = (5, 6), (6, 5)$.

ESERCIZIO 5

(b) $d = 1, 2, 11, 22 \pmod{23}$.
(c) Per ciascun valore di d sopra elencato vengono date sotto le soluzioni:
$d = 1 \mapsto x = 1$;
$d = 2 \mapsto x = 1, 22$;
$d = 11 \mapsto x = 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$;
$d = 22 \mapsto 1 \leq x \leq 22$.

ESERCIZIO 6

(b) 33.

Lo svolgimento degli "esercizi teorici" è contenuto nelle dispense.