

## COMPITO DI ARITMETICA

7 luglio 2014

Cognome e nome: .....

Numero di matricola: .....

### Esercizio 1.

Sia  $X = \{1, 2, \dots, 100\}$ . Calcolare la cardinalità dei seguenti insiemi:

a)  $\{(A, B) \in \mathcal{P}(X)^2 \mid |A \cup B| = 40 \text{ e } |A| = 10\}$ ;

b)  $\{A \in \mathcal{P}(X) \mid |A| = 5 \text{ e } \prod_{x \in A} x \equiv 0 \pmod{9}\}$

### Esercizio 2.

Determinare i valori del parametro intero  $a$  per cui il seguente sistema di congruenze ha soluzione:

$$\begin{cases} 2^x \equiv 3^{x+a^2} \pmod{17} \\ 3x \equiv a^{23} \pmod{24} \end{cases}$$

### Esercizio 3.

Sia  $G$  un gruppo abeliano e sia  $H$  il suo sottoinsieme formato da tutti gli elementi di ordine finito.

a) Dimostrare che  $H$  è un sottogruppo di  $G$  e mostrare con un esempio che  $H$  può essere infinito.

b) Dimostrare che  $G/H$  è isomorfo a  $G$  se e solo se  $H$  è banale.

### Esercizio 4.

Sia  $p$  un primo dispari, e sia  $f(x) = x^6 + ax^3 + b \in \mathbb{F}_p[x]$ .

a) Dimostrare che il grado del campo di spezzamento di  $f(x)$  su  $\mathbb{F}_{p^2}$  può essere solo 1 o 3

b) Dimostrare che il grado del campo di spezzamento di  $f(x)$  su  $\mathbb{F}_p$  non può essere né 4 né 5.

c) Mostrare che se  $p \equiv 2 \pmod{3}$  il grado del campo di spezzamento di  $f(x)$  su  $\mathbb{F}_p$  non può essere 3.