

Terzo compitino di Elementi di Matematica (Matematica discreta)B

12 febbraio 2010

COGNOME _____

NOME _____ MATRICOLA _____

Indicare la risposta corretta con una crocetta

1 Si consideri la congruenza

$$7^{6x} \equiv 1 \pmod{6h}$$

nell'incognita x positiva

- a) ogni x positivo è soluzione se e solo se h è pari
- b) ammette soluzione se h è un numero primo diverso da 7;
- c) comunque si scelga h positivo x è soluzione se e solo se x è primo;
- d) comunque si scelga h positivo x è soluzione se e solo se x è multiplo di 7.

2. Siano a e n due numeri interi positivi maggiori di 1.

Allora

- a) $(a + nh)^{\phi(n)} \equiv 1 \pmod{n}$ se e solo se $h = 0$;
- b) $(a + nh)^{\phi(n)} \equiv 1 \pmod{n}$ per ogni $h \in \mathbb{Z}$ se e solo se a e n sono primi tra loro (cioè $\text{M.C.D.}(a, n) = 1$);
- c) $(a + nh)^{\phi(n)} \equiv 1 \pmod{n}$ se $h = 0$;
- d) $(a + nh)^{\phi(n)} \equiv 1 \pmod{n}$ per ogni $h \in \mathbb{Z}$ se e solo se cioè $\text{M.C.D.}(a, n) \neq 1$.

3. Sia X un insieme, $X = A \cup B$ con $|X| = 9$, $|A| = 6$, $|B| = 3$, (quindi $A \cap B = \emptyset$).

Allora il numero di permutazioni f su X (cioè il numero di funzioni f biettive da X in se stesso) tali che $f(A) = A$ e $f(B) = B$ è:

- a) un numero maggiore di $3!6!$ e minore di $9!$;
- b) $9!$;
- c) $3!6!$;
- d) 0.

4. Sia D l'insieme $\{2, 5, 4, 10, 20, 30\}$ ordinato rispetto alla divisibilità. Sia poi $C = \{4, 5, 10\}$. Allora

- a) l'insieme D ammette massimo ma non minimo;
- b) l'insieme D ammette minimo ma non massimo;
- c) il sottoinsieme C (ordinato rispetto alla divisibilità) ha minimo;
- d) il sottoinsieme C (ordinato rispetto alla divisibilità) ha due elementi minimali.

5. Dato l'anello \mathbb{Z}_{pq} con p e q primi distinti

- a) ci sono esattamente $(p-1)(q-1)$ divisori dello zero;
- b) ci sono esattamente $p+q-2$ divisori dello zero (diversi da $[0]_{pq}$);
- c) $[q]_{pq}$ è invertibile;
- d) non ci sono divisori dello zero.

6. Si consideri in \mathbb{Z}_n l'elemento $[b]_n \neq [0]_n$, che sia un divisore dello zero. Allora

- a) $[a]_n[b]_n$ è un divisore dello zero per ogni $[a]_n \in \mathbb{Z}_n$ con $[a]_n \neq [0]_n$;
- b) $[a]_n[b]_n$ è invertibile per ogni $[a]_n \in \mathbb{Z}_n$, $[a]_n \neq [0]_n$
- c) $[a]_n[b]_n$ è invertibile per ogni $[a]_n \in \mathbb{Z}_n$, con $M.C.D(a, n) = 1$;
- d) nessuna delle precedenti.

7. Si consideri l'equazione in \mathbb{Z}_n

$$[a]_n[x]_n = [b]_n,$$

nell'incognita $[x]_n$, allora

- a) ha soluzioni comunque si scelgano $[a]_n$ e $[b]_n$;
- b) ha una e una sola soluzione se $M.C.D(b, n) = 1$;
- c) ha una e una sola soluzione se $M.C.D(a, n) = 1$;
- d) ha una e una sola soluzione se $M.C.D(b, a) = 1$.

8.

- (1) Si dia la definizione di gruppo;
- (2) si dia la definizione di campo;
- (3) si dia un esempio di un anello che non sia un campo.

Si svolga il seguente esercizio, dando una piena giustificazione

9. Si consideri il sistema crittografico RSA con la chiave pubblica data dalla coppia $(21, 5)$; ricevete il messaggio $a = 16$ (si suppone di avere identificato le lettere dell'alfabeto italiano ordinatamente con i numeri naturali da 1 a 21 (per esempio la lettera T è identificata con 18)).

- 1) Decifrate il messaggio (sugg: $16^2 \equiv 4 \pmod{21}$);
- 2) giustificate dal punto di vista teorico quanto fatto nel punto 1).