

Terza Esercitazione di Elementi di Matematica (Matematica discreta)

3 febbraio 2010

COGNOME _____

NOME _____ MATRICOLA _____

Indicare la risposta corretta con una crocetta

1 Si consideri l'equazione

$$[p^{883x}]_{(p-1)h} = [1]_{(p-1)h}$$

nell'incognita x positiva dove p è un numero primo. Allora

- a) ogni x positivo è soluzione se e solo se h è pari
- b) ammette soluzione se h è un numero primo diverso da p ;
- 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 p .

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

Allora

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

3. Siano A e B insiemi rispettivamente di cardinalità r e s . Allora le funzioni suriettive da A a B sono

- a) 0 se $r < s$;
- b) s^r
- c) r^s .
- d) $\binom{r}{s}$ per $r \geq s$.

4. Sia D l'insieme $\{2, 3, 4, 6, 18, 24\}$ ordinato rispetto alla divisibilità. Sia poi $C = \{2, 4, 6\}$. Allora

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

5. Dato l'anello $\mathbb{Z}_{p^r q^s}$ con p e q primi distinti con r e s interi positivi

- a) ci sono esattamente $p^r q^s - 1 - (p^{r-1} q^{s-1})(p-1)(q-1)$ divisori dello zero (diversi da zero);
- b) ci sono esattamente $(p^r - p^{r-1})(q^s - q^{s-1})$ divisori dello zero (diversi da zero);

2

- c) $[p]_{p^r q^s}$ è invertibile;
- d) non ci sono divisori dello zero.

6. Dato un anello A con unità, quale delle seguenti affermazioni è vera:

- a) se $a \in A$ è invertibile, allora a non è divisore dello zero;
- b) se $a \in A$ non è divisore dello zero allora a è invertibile;
- c) $a \in A$ è invertibile se e solo se a non è divisore dello zero
- d) nessuna delle precedenti.

7.. Si consideri la congruenza lineare

$$ax \equiv b \pmod{n}$$

con a, b e n in \mathbb{Z} , $n > 1$ e $a \neq 0$, allora

- a) ha soluzioni comunque si scelgano a, b e n ;
- b) posto $\text{M.C.D}(a, n) = d$, se d divide b la congruenza ha d soluzioni a due a due non congrue mod n ;
- c) ha una e una sola soluzione se $\text{M.C.D}(a, n) \neq 1$;
- d) ha una e una sola soluzione se $\text{M.C.D}(a, n) = 1$.

8.

- (1) Si dia la definizione di anello con unità;
- (2) si dia la definizione di elemento neutro per un'operazione;
- (3) si determinino gli elementi invertibili in \mathbb{Z}
- (4) si dia un esempio, se esiste, di sottoinsieme di \mathbb{Z} che sia un gruppo rispetto al prodotto.

Si svolga il seguente esercizio, dando una piena giustificazione

9. Si consideri il sistema crittografico RSA con la chiave pubblica data dalla coppia $(26, 5)$; ricevete il messaggio $a = 23$ (si suppone di avere identificato le lettere dell'alfabeto inglese ordinatamente con i numeri naturali da 1 a 26)

- 1) Decifrate il messaggio;(suggerimento $23^2 \equiv 9 \pmod{26}$);
- 2) giustificate dal punto di vista teorico quanto fatto nel punto 1).