Compitino di Matematica Discreta
19 dicembre 2013. Soluzioni

Cognome e nome: .....

Numero di matricola: ..... Corso e Aula: .....

IMPORTANTE: Non si possono consultare libri e appunti. Non si possono usare calcolatrici, computer o altri dispositivi elettronici. Non si può scrivere con il lapis. Motivare in modo chiaro le risposte. I testi degli esercizi sono su fogli separati su cui vanno scritte le rispettive soluzioni: **scrivere il nome su ciascun foglio**. Mettere entro un riquadro bene evidenziato la soluzione, e nel resto del foglio lo svolgimento.

Esercizio 1.
a) Trovare tutte le soluzioni della congruenza $22x \equiv 29 \bmod 39$.
b) Trovare tutte le soluzioni del sistema di congruenze

$$\begin{cases} 146^{2403} \equiv x \bmod 19 \\ 22x \equiv 29 \bmod 39 \end{cases}$$

Soluzione: Affinché la seconda congruenza del sistema abbia soluzione deve valere $MCD(22, 39)|29$. Calcolando trovo $MCD(22, 39) = 1$, quindi la congruenza ha soluzione. Per Bezout il massimo comun divisore si può scrivere come combinazione lineare dei due numeri. Nel nostro caso (applicando l'algoritmo di Bezout) ottengo $1 = 22 \cdot 16 - 39 \cdot 9$. Quindi l'inverso di 22 modulo 39 è 16. Moltiplicando entrambi i membri della seconda congruenza per 16 ottengo la congruenza equivalente $x \equiv 29 \cdot 16 \bmod 39$, ovvero $x \equiv 35 \bmod 39$. Le soluzioni della congruenza $22x \equiv 29 \bmod 39$ sono dunque tutti e soli i numeri interi della forma $35 + 39k$ al variare di k in $\mathbb{Z}$.

Consideriamo ora la prima congruenza del sistema. Poiché 146 è congruo a 13 modulo 19, la possiamo riscrivere come $13^{2403} \equiv x \bmod 19$. Poiché 19 è primo e $MCD(13, 19) = 1$, dal piccolo teorema di Fermat sappiamo che $13^{18} \equiv 1 \bmod 19$. Quindi nel calcolare 13^{2403} modulo 19 possiamo sostituire 2403 con il suo resto modulo 18, che è 9. La prima congruenza equivale dunque a $13^9 \equiv x \bmod 19$. Per calcolare 13^9 modulo 19 osserviamo che $13 \equiv -6 \bmod 19$ e quindi $13^2 \equiv 36 \equiv -2 \bmod 19$, da cui $13^9 \equiv (13^2)^4 \cdot 13 \equiv (-2)^4(-6) \equiv (-3)(-6) \equiv -1 \bmod 19$. Ne segue che la soluzione della prima congruenza del sistema è $x \equiv -1 \bmod 19$, o equivalentemente $x \equiv 18 \bmod 19$.

Il sistema assegnato equivale quindi a

$$\begin{cases} x \equiv 18 \bmod 19 \\ x \equiv 35 \bmod 39 \end{cases}$$

Poiché i due moduli 19 e 39 sono relativamente primi il sistema ha soluzione e le soluzioni si ottengono sommando ad una soluzione particolare x_0 un multiplo di $19 \cdot 39 = 741$. Per trovare una soluzione particolare sostituiamo alla x della prima congruenza la soluzione generica $x = 35 + k39$ della seconda congruenza, ottenendo $35 + k39 \equiv 18 \bmod 19$, che equivale a $16 + k \equiv 18 \bmod 19$, ovvero $k \equiv 2 \bmod 19$. Sostituendo $k = 2$ in $x = 35 + k39$ otteniamo la soluzione particolare $x_0 = 35 + 2 \cdot 39 = 113$ del sistema. La soluzione generale del sistema si ottiene sommandogli un multiplo di 741 ottenendo $x = 113 + m741$, ovvero $x \equiv 113 \bmod 741$. □

Cognome e nome: .....

Numero di matricola: ..... Corso e Aula: .....

Esercizio 2. Sia $\mathbb{N}_{28} = \{1, 2, ..., 28\}$.
a) Quanti sono i sottoinsiemi di $\mathbb{N}_{28}$?
b) Quanti sono i sottoinsiemi di A di $\mathbb{N}_{28}$ tali che $A \cap \{1, 2\} \neq \emptyset$?
c) Quanti sono i sottoinsiemi di $\mathbb{N}_{28}$ che contengono esattamente cinque numeri pari e almeno un numero dispari?
d) Quante sono le coppie di sottoinsiemi A, B di $\mathbb{N}_{28}$ tali che $A \cup B = \mathbb{N}_{28}$, $|A| = 3|A \cap B|$ e $|B| = 2|A \cap B|$?

Soluzione: a) I sottoinsiemi di $\mathbb{N}_{28}$ sono 2^{28}.

b) Dobbiamo togliere dal totale dei sottoinsiemi di $\mathbb{N}_{28}$, che sono 2^{28}, quelli che hanno una intersezione vuota con $\{1, 2\}$, che sono 2^{26}. La soluzione è dunque $2^{28} - 2^{26} = 2^{26}(2 + 1) = 3 \cdot 2^{26}$.

c) Vi sono $\binom{14}{5}$ modi di scegliere 5 numeri pari dall'insieme $\mathbb{N}_{28}$. Dobbiamo calcolare il numero di modi di scegliere un sottoinsiemi non vuoto dei dispari. I sottoinsiemi dei dispari sono 2^{14}, ma dobbiamo togliere l'insieme vuoto. Dunque vi sono $2^{14} - 1$ modi di scegliere un sottoinsieme non vuoto dei dispari. La soluzione si ottiene moltiplicando: $\binom{14}{5}(2^{14} - 1)$.

d) La formula di inclusione-esclusione ci dice che

$$|A \cap B = |A| + |B| - |A \cap B|.$$

Visto che $|A| = 3|A \cap B|$ e $|B| = 2|A \cap B|$, sostituendo i dati del problema abbiamo

$$28 = 3|A \cap B| + 2|A \cap B| - |A \cap B|,$$

e quindi $|A \cap B| = 28/4 = 7$, $|A| = 3 \cdot 7 = 21, |B| = 2 \cdot 7 = 14$.

Il problema equivale dunque a chiedersi quante siano le coppie di sottoinsiemi (A, B) di $\mathbb{N}_{28}$ con $|A \cap B| = 7$, $|A| = 21$ e $|B| = 14$. Ci sono $\binom{28}{7}$ modi di scegliere gli elementi da mettere in $A \cap B$, $\binom{28-7}{21-7} = \binom{21}{14}$ modi di scegliere i rimanenti elementi di A. I sette elementi rimanenti appartengono solo a B. La risposta è dunque $\binom{28}{7}\binom{21}{14}$. □

Cognome e nome: .....

Numero di matricola: ..... Corso e Aula: .....

Esercizio 3.
a) Trovare una formula non ricorsiva per il termine a_n della successione definita da $a_0 = 3, a_1 = -2$ e, per $n \geq 2$:

$$a_n = 4a_{n-2}$$

b) Si determini, dato n, la massima potenza di 2 che divide a_n.

Soluzione: a) Cerco una successione della forma $a_n = \alpha^n$ che verifichi l'equazione di ricorrenza, senza per il momento preoccuparmi delle condizioni iniziali. Sostituendo otteniamo $\alpha^n = 4\alpha^{n-2}$, o equivalentemente (dividendo per α^{n-2}) $\alpha^2 = 4$. Le soluzioni sono $\alpha = 2$ ed $\alpha = -2$ e quindi sia $a_n = 2^n$ che $a_n = (-2)^n$ verificano l'equazione di ricorrenza, così come anche le loro combinazioni lineari $a_n = A2^n + B(-2)^n$ (ciò segue dalla teoria generale, ma in ogni caso potete verificare facilmente sostituendo). Devo trovare A e B in modo che siano verificate anche le condizioni iniziali $a_0 = 3, a_1 = -2$. Sostituendo ottengo il sistema $3 = A + B$, $-2 = 2A - 2B$, che ha soluzione $A = 1, B = 2$. La soluzione del punto a) è dunque $a_n = 2^n + 2(-2)^n$. (Alternativamente si poteva risolvere l'esercizio considerando separatamente gli n pari e gli n dispari.)

b) La massima potenza di 2 che divide $a_n = 2^n + 2(-2)^n$ è 2^n. Infatti sicuramente 2^n divide $2^n + 2(-2)^n$, e rimane dunque solo da mostrare che 2^{n+1} non lo divide. Ma questo è chiaro in quanto se divido a_n per 2^n ottengo un numero intero dispari: $\frac{a_n}{2^n} = 1 + 2\frac{(-2)^n}{2^n} = 1 + 2(-1)^n$. □