Laboratorio di Matematica 2016 — 1^o esonero — Roma, 23 novembre 2016, 14:00–16:00.

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

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare, sintetiche e complete.* NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI.

1. Siano dati gli insiemi $A = \{x, y, z, u\}$ e $B = \{1, 2, 3, 4\}$. Calcolare il numero di elementi delle seguenti famiglie di funzioni, spiegando i ragionamenti usati:

$$\{f : A \to B\}, \quad \{f : A \to B \mid f(x) \neq f(y)\}, \quad \{f : A \to B \mid \text{iniettive}\}, \quad \{f : A \to B \mid f(x) = f(y) = 1\}.$$

Soluzione:
Una funzione $f : A \to B$ è completamente determinata quando sono assegnate le immagini dei punti del dominio $f(x)$, $f(y)$, $f(z)$, $f(u)$: ad esempio $f(x) = 2$, $f(y) = 4$, $f(z) = 4$ ed $f(u) = 1$, oppure $f(x) = 2$, $f(y) = 1$, $f(z) = 3$ ed $f(u) = 4$.

(1) Per $f(x)$ ci sono 4 scelte, per $f(y)$ 4 scelte, per $f(z)$ 4 scelte e per $f(u)$ 4 scelte. Tutte queste scelte sono indipendenti! In totale ci sono $4 \cdot 4 \cdot 4 \cdot 4 = 256$ funzioni.

(2) Per $f(x)$ ci sono 4 scelte, per $f(y)$ 3 scelte (perché deve essere diversa da $f(x)$), per $f(z)$ 4 scelte e per $f(u)$ 4 scelte. Tutte queste scelte sono indipendenti! In totale ci sono $4 \cdot 3 \cdot 4 \cdot 4 = 192$ funzioni con $f(x) \neq f(y)$.

(3) Per $f(x)$ ci sono 4 scelte, per $f(y)$ 3 scelte (perché deve essere diversa da $f(x)$), per $f(z)$ 2 scelte (perché deve essere diversa da $f(x)$ e da $f(y)$), per $f(u)$ 1 scelta (perché deve essere diversa da $f(x)$, da $f(y)$ e da $f(z)$). Tutte queste scelte sono indipendenti! In totale ci sono $4 \cdot 3 \cdot 2 \cdot 1 = 24$ funzioni iniettive.

(4) Per $f(x)$ ed $f(y)$ c'è una scelta sola: $f(x) = f(y) = 1$. Per $f(z)$ ci sono 4 scelte e 4 sclete per $f(u)$. Tutte queste scelte sono indipendenti! In totale ci sono $4 \cdot 4 = 16$ funzioni con $f(x) = f(y) = 1$.

2. Determinare l'insieme A di tutti gli $x \in \mathbf{R}$ che soddisfano la disuguaglianza

$$3^{\frac{x-1}{x-4}} < 1.$$

Sia $B = [0, 2] \cup [3, +\infty[$. Calcolare $A \cap B$.

Soluzione: Poiché $3 > 1$, la funzione $\mathbf{R} \to \mathbf{R}$, $z \mapsto 3^z$ è strettamente crescente e vale 1 per $z = 0$. Dunque disequazione è soddisfatta se e solo se

$$\frac{x-1}{x-4} < 0,$$

ossia se e solo se

$$\begin{cases} x - 1 < 0 \\ x - 4 > 0 \end{cases} \quad \text{oppure} \quad \begin{cases} x - 1 > 0 \\ x - 4 < 0 \end{cases}.$$

Il primo sistema non ha soluzioni, mentre le soluzioni del secondo sono i numeri reali $1 < x < 4$.
Conclusione

$$A =]1, 4[\qquad A \cap B =]1, 2] \cup [3, 4[.$$

3. Sia assegnata la seguente corrispondenza tra lettere e numeri:

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*z*
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20

e si scrivano i messaggi in blocchi da 3 cifre.
3.a) Decifrare il seguente messaggio, che è stato cifrato con il cifrario di Cesare di chiave 351:

411 169 441 151

Soluzione: Il messaggio è stato cifrato tramite la funzione $\mathbf{Z}_{1000} \to \mathbf{Z}_{1000}$, definita da $\overline{m} \mapsto \overline{c} = \overline{m} + \overline{351}$. Conoscendo il messaggio cifrato $\overline{c}$, si recupera il messaggio in chiaro $\overline{m}$ mediante l'uguaglianza $\overline{m} = \overline{c} - \overline{351}$. Notiamo che, in $\mathbf{Z}_{1000}$, si ha che $-\overline{351} = \overline{1000} - \overline{351} = \overline{1000 - 351} = \overline{649}$; dunque, la funzione per decifrare è $\overline{c} \mapsto \overline{m} = \overline{c} + \overline{649}$.

Applicando la funzione per decifrare al messaggio assegnato, si trova (scrivo il rappresentante con tre cifre, perchè il messaggio è stato scritto in blocchi di 3 cifre):
$\overline{411} \mapsto \overline{411} + \overline{649} = \overline{060}$
$\overline{169} \mapsto \overline{169} + \overline{649} = \overline{818}$
$\overline{441} \mapsto \overline{441} + \overline{649} = \overline{090}$
$\overline{151} \mapsto \overline{151} + \overline{649} = \overline{800}$
Poichè sappiamo che il messaggio è stato cifrato a blocchi, riuniamo in un solo numero complessivo i numeri ottenuti decifrando: 060818090800. Scomponiamo il numero trovato in blocchi da 2 cifre (ciascuno dei quali corrisponde a una lettera) e recuperiamo il messaggio in chiaro:

06	08	18	09	08	00
g	*i*	*u*	*l*	*i*	*a*

3.b) Cifrare il seguente messaggio, utilizzando il cifrario affine di chiave (9,234): *uva*

Soluzione: Il messaggio defe essere cifrato a blocchi di 3 cifre. Calcolo quindi la corrispondenza tra le lettere nel messaggio 'uva' e le coppie di cifre:

u	*v*	*a*
18	19	00

Unisco le cifre ottenute in un unico numero complessivo 181900 che poi scompongo in blocchi da 3 cifre, ottenendo: 181 900.
Ora siamo pronti per cifrare con il cifrario affine. La funzione per cifrare $\mathbf{Z}_{1000} \to \mathbf{Z}_{1000}$ è definita da $\overline{m} \mapsto \overline{c} = \overline{9}\overline{m} + \overline{234}$ (in base alla chiave assegnata); otteniamo:
$\overline{811} \mapsto \overline{9811} + \overline{234} = \overline{863}$
$\overline{900} \mapsto \overline{9900} + \overline{234} = \overline{334}$
Il messaggio cifrato è dunque: 863 334.

4. Si consideri la funzione $f : \mathbf{Z}_{1000} \to \mathbf{Z}_{1000}$ definita da $f(\overline{m}) = \overline{7}\,\overline{m}$. Determinare l'inversa di f.

Soluzione: La funzione inversa $g : \mathbf{Z}_{1000} \to \mathbf{Z}_{1000}$ esiste se e solo se la classe $\overline{7}$ ammette inverso $(\overline{7})^{-1}$; in tal caso, la funzione inversa g è definita da $g(\overline{m}) = (\overline{7})^{-1}\,\overline{m}$.
Iniziamo verificando se $\overline{7}$ ammette inverso; in base alla teoria generale, ciò accade se e solo se $MCD(1000, 7) = 1$. Applichiamo il metodo di Euclide per il calcolo del massimo comun divisore $MCD(1000, 7)$:
$1000 = 7 \cdot 142 + 6$
$7 = 6 \cdot 1 + 1$
$6 = 1 \cdot 6 + 0$
L'ultimo resto non nullo, 1, coincide con $MCD(1000, 7)$. Poichè $MCD(1000, 7) = 1$, la classe resto $\overline{7}$ ammette inverso $(\overline{7})^{-1}$. Ora cerchiamo di individuare in modo esplicito la classe resto $(\overline{7})^{-1}$. Riprendiamo le divisioni svolte (con resto non nullo) per il calcolo di MCD, mettendo in evidenza i resti:
$6 = 1000 - 7 \cdot 142$
$1 = 7 - 6 \cdot 1$
Nell'ultima equazione, sostituisco l'espressione di 6 ottenuta dalla relazione precedente e poi raccolgo:

$$1 = 7 - 6 \cdot 1 = 7 - 6 = 7 - (1000 - 7 \cdot 142) = -1000 - 7 \cdot 141$$

Dunque $1 = -1000 + 7 \cdot (-141)$. Passando alle classi resto modulo 1000, si ricava che

$$\overline{1} = -\overline{1000} + \overline{7} \cdot \overline{(-141)} = \overline{7} \cdot \overline{(-141)}.$$

In particolare, $(\overline{7})^{-1} = \overline{(-141)} = \overline{(1000 - 141)} = \overline{(859)}$.