Esercizi di Strutture Discrete

Alberto Carraro

04/05/2006

Classi resto

Esercizio 1. *Si dica*

a) quanti e quali elementi ha l'insieme $\mathbb{Z}/\equiv_0$

b) quanti e quali elementi ha l'insieme $\mathbb{Z}/\equiv_1$

Soluzione

a) $\mathbb{Z}/\equiv_0 = \{[a]_{\equiv_0} \mid a \in \mathbb{Z}\} = \{\{z\} \mid z \in \mathbb{Z}\}$.
$\mathbb{Z}/\equiv_0$ è equipotente a $\mathbb{Z}$ ma non è uguale ad esso.

b) $\mathbb{Z}/\equiv_1 = \{[a]_{\equiv_1} \mid a \in \mathbb{Z}\} = \{[0]_{\equiv_1}\} = \{\mathbb{Z}\}$.
$\mathbb{Z}/\equiv_1$ non è uguale a $\mathbb{Z}$ e ha cardinalità 1.

Esercizio 2. *Siano* $n \geq 1$ *e* k *numeri interi fissati. Si consideri l'applicazione* $f : \mathbb{Z}/\equiv_n \to \mathbb{Z}/\equiv_n$ *definita da* $f([a]) = [ka]$ *per ogni* $a \in \mathbb{Z}$. *Si dimostri che*

a) l'applicazione f *è ben definita, cioè che se* $a, b \in \mathbb{Z}$ *e* $[a] = [b]$, *allora* $f([a]) = [ka] = [kb] = f([b])$

b) f *è iniettiva sse* n *e* k *sono primi tra loro*

c) f *è suriettiva sse l'equazione* $kx \equiv_n b$ *ha una soluzione in* $\mathbb{Z}$ *per ogni* $b \in \mathbb{Z}$

d) l'equazione $kx \equiv_n b$ *ha una soluzione in* $\mathbb{Z}$ *per ogni* $b \in \mathbb{Z}$ *sse* n *e* k *sono primi tra loro*

Soluzione

a) Assumiamo $[a] = [b]$.
$a \equiv_n b$
$nq = (a - b)$
$n(kq) = ka - kb$
$ka \equiv_n kb$
$[ka] = [kb]$

b) **(⇒)** Assumiamo f iniettiva. Supponiamo, per assurdo, che $MCD(n, k) \neq 1$. Allora $\exists q \in \mathbb{Z}.(q \mid n \ \wedge \ q \mid k \ \wedge \ q > 1)$, da cui $xq = n$ e $yq = k$. Si

noti inoltre che dovrà valere che $n, k > 1$. Dimostriamo che f non è iniettiva. Siano $a, b \in \mathbb{Z}$ tali che $[ka] = [kb]$.

$$
\begin{array}{ll}
n \mid k(a-b) & \\
xq \mid yq(a-b) & \text{(con } y \text{ ed } x \text{ primi tra loro)} \\
xq \nmid y & (x \nmid y \text{ e } q \nmid y \text{ perché } q = (n,k)) \\
xq \mid q(a-b) & \\
x \mid (a-b) & \text{(con } 0 < x < n)
\end{array}
$$

Consideriamo allora $[x]$ e $[0]$. Nonostante $[x] \neq [0]$, vediamo che $f([x]) = [kx] = [0] = f([0])$ perché $n \mid k(x-0)$ dato che $xq \mid yqx$.

($\Leftarrow$) Assumiamo n e k primi tra loro. Siano $[a], [b] \in \mathbb{Z}/\equiv_n$ tali che $[ka] = [kb]$. Allora $n \mid k(a-b)$. Ma $n \nmid k$, quindi deve essere $n \mid (a-b)$. Quindi $[a] = [b]$.

c) ($\Rightarrow$) Assumiamo f suriettiva. Sia $b \in \mathbb{Z}$.

$$
\begin{array}{ll}
\exists [a] \in \mathbb{Z}/\equiv_n .(b \in [a]) & \text{(la relazione } \equiv_n \text{ partiziona } \mathbb{Z}) \\
\exists a \in \mathbb{Z}.(n \mid (b-a)) & \\
n \mid (a-b) & \\
\exists [x] \in \mathbb{Z}/\equiv_n .([a] = [kx]) & (f \text{ suriettiva}) \\
n \mid (a-kx) & \\
n \mid (kx-a) & \\
n \mid (kx-a) + (a-b) & \\
n \mid (kx-b) &
\end{array}
$$

Quindi dato un qualsiasi $b \in \mathbb{Z}$, esiste una soluzione $x \in \mathbb{Z}$ per l'equazione data.

($\Leftarrow$) Assumiamo che l'equazione $kx \equiv_n b$ ha una soluzione in $\mathbb{Z}$ per ogni $b \in \mathbb{Z}$.

$$
\begin{array}{ll}
\forall b \in \mathbb{Z}.\exists x \in \mathbb{Z}.([kx] = b) & \text{(per ipotesi)} \\
\forall [b] \in \mathbb{Z}/\equiv_n .\exists x \in \mathbb{Z}.([kx] = b) & \\
\forall [b] \in \mathbb{Z}/\equiv_n .\exists [x] \in \mathbb{Z}/\equiv_n .(f([x]) = b) &
\end{array}
$$

d) ($\Rightarrow$) Assumiamo che l'equazione $kx \equiv_n b$ ha una soluzione in $\mathbb{Z}$ per ogni $b \in \mathbb{Z}$

$$
\begin{array}{l}
\forall b \in \mathbb{Z}.\exists x \in \mathbb{Z}.(n \mid kx - b) \\
\forall b \in \mathbb{Z}.\exists x \in \mathbb{Z}.(n \mid b - kx) \\
\forall b \in \mathbb{Z}.\exists x, q \in \mathbb{Z}.(nq = b - kx) \\
\forall b \in \mathbb{Z}.\exists x, q \in \mathbb{Z}.(nq + kx = b)
\end{array}
$$

Quindi, in particolare, l'enunciato sarà vero per $b = 1$. Così otteniamo che $\exists x, q \in \mathbb{Z}.(nq + kx = 1)$. Per il Corollario 4.5 a pag 30 del Facchini, si ha che $MCD(n,k) = 1$.

($\Leftarrow$) Assumiamo che n e k siano primi tra loro. Per il Corollario 4.5 a pag 30 del Facchini, si ha che $\exists \alpha, \beta \in \mathbb{Z}.(\alpha n + \beta k = 1)$. Sia $b \in \mathbb{Z}$. Allora

$$
\begin{array}{l}
\alpha n b + \beta k b = b \\
(\alpha b)n + (\beta b)k = b \\
(\alpha b)n = b - (\beta b)k
\end{array}
$$

Quindi esiste $x = (\beta b)$ tale che $n \mid (b - kx)$.

Esercizio 3. *Sia $n \geq 1$ un numero intero fissato. Si consideri l'applicazione $f : \mathbb{Z} \to \mathbb{Z}$ definita, per ogni $x \in \mathbb{Z}$, da $f(x) =$"resto della divisione di x per n". Si dimostri che:*

a) la relazione $\sim_f$ associata all'applicazione r è la congruenza modulo n ($\equiv_n$).

b) se $y \in \{0, 1, \cdots, n-1\}$, allora $f^{-1}(y) = [y]_{\equiv_n}$.

Soluzione Ricordiamo che se si dividono x e y per n si ha che $x = qn + r$, $y = q'n + r'$, $0 \leq r < n$ e $0 \leq r' < n$ per opportuni $q, r, q', r' \in \mathbb{Z}$.

a) Dobbiamo dimostrare che per ogni $x, y \in \mathbb{Z}$, $x \sim_f y$ sse $x \equiv_n y$.

(⇒) Assumiamo $x \sim_f y$. Allora

$$\begin{aligned} &f(x) = f(y) = r \\ &x - y = (qn + r) - (q'n + r) = (q - q')n \end{aligned}$$

Quindi $x \equiv_n y$.

(⇐) Assumiamo $x \equiv_n y$. Siano $r(x) = r$ e $r(y) = r'$. Allora

$$\begin{aligned} &(x - y) = (qn + r) - (q'n + r) = (q - q')n + (r - r') \\ &n \mid (q - q')n + (r - r') \\ &n \mid (q - q')n \\ &n \mid (r - r') \end{aligned}$$

Poiché $0 \leq r < n$ e $0 \leq r' < n$, si ha $-n < r - r' < n$. Quindi $r - r' = 0$.

b) Sia $y \in \{0, 1, \cdots, n-1\}$.

$$\begin{aligned} f^{-1}(y) &= \{x \in \mathbb{Z} \mid f(x) = y\} \\ &= \{x \in \mathbb{Z} \mid x = nq + y, q \in \mathbb{Z}\} \\ &= \{x \in \mathbb{Z} \mid x - y = nq, q \in \mathbb{Z}\} \\ &= \{x \in \mathbb{Z} \mid n \mid (x - y)\} \\ &= \{x \in \mathbb{Z} \mid x \equiv_n y)\} \\ &= [y]_{\equiv_n} \end{aligned}$$