Esercizi di Strutture Discrete

Alberto Carraro

27/04/2006

MCD, mcm, congruenze

Esercizio 1. *Quali sono il quoto e il resto della divisione di -202 per 20?*

Soluzione $-202 = 20 \cdot (-10) + (-2)$

Esercizio 2. *Sia* $a \in \mathbb{Z}$*. Si dimostri che* $0 \mid a$ *sse* $a = 0$*.*

Soluzione

($\Rightarrow$) Assumiamo $0 \mid a$. Allora esiste $c \in \mathbb{Z}$ tale che $a = 0 \cdot c$. Ma per ogni $c \in \mathbb{Z}$ si ha $0 = 0 \cdot c$, quindi $a = 0$.

($\Leftarrow$) Assumiamo $a = 0$. Come già detto per ogni $c \in \mathbb{Z}$ si ha $0 = 0 \cdot c$. Quindi $0 \mid 0$.

Esercizio 3. *Si dimostri che per ogni* $a \in \mathbb{Z}$

a) $a \mid 0$

b) $1 \mid a$

Soluzione

a) Bisogna verificare che esiste $c \in \mathbb{Z}$ tale che $0 = ac$. Basta prendere $c = 0$.

b) Bisogna verificare che esiste $c \in \mathbb{Z}$ tale che $a = 1 \cdot c$. Basta prendere $c = a$.

Esercizio 4. *Si dimostri che* $a \mid 1$ *sse* $a = 1$ *oppure* $a = -1$*.*

Soluzione

($\Rightarrow$) Assumiamo $a \mid 1$. Allora esiste $c \in \mathbb{Z}$ tale che $1 = ac$. Gli unici casi possibili in $\mathbb{Z}$ sono: $c = a = 1$ oppure $c = a = -1$.

($\Leftarrow$) Assumiamo $a = 1$. Allora esiste $c \in \mathbb{Z}$ tale che $1 = ac$. Basta prendere $c = 1$. Ora assumiamo $a = -1$. Allora esiste $c \in \mathbb{Z}$ tale che $1 = ac$. Basta prendere $c = -1$.

Esercizio 5. *Qual è la classe di equivalenza di 24 nella relazione* $\equiv_9$ *in* $\mathbb{Z}$*, cioè cos'è* $[24]_{\equiv_9}$*?*

Soluzione Sono tutti i numeri interi a tali che $9 \mid (24 - a)$: cioè è l'insieme $\{\ldots, -21, -12, -3, 6, 15, 24, \ldots\}$.

Esercizio 6. *Siano a, b, m, n numeri interi, $m, n \geq 1$, e sia $[m, n]$ il mcm positivo di m ed n. Si dimostri che $a \equiv_m b$ e $a \equiv_n b$ sse $a \equiv_{[m,n]} b$.*

Soluzione

(⇒) Assumiamo $a \equiv_m b$ e $a \equiv_n b$.

$m \mid (a-b)$	(def di congruenza)
$n \mid (a-b)$	(def di congruenza)
$(m \mid (a-b) \wedge m \mid (a-b)) \Rightarrow [m,n] \mid (a-b)$	(def di mcm)

Quindi $a \equiv_{[m,n]} b$.

(⇐) Assumiamo $a \equiv_{[m,n]} b$.

$[m,n] \mid (a-b)$	(def di congruenza)
$\exists c \in \mathbb{Z}.([m,n]c = (a-b))$	(def di divisibilità)
$\exists k \in \mathbb{Z}.(mk = [m,n])$	(def di mcm)
$\exists h \in \mathbb{Z}.(nh = [m,n])$	(def di mcm)
$m(kc) = (a-b)$	
$n(hc) = (a-b)$	

Quindi $a \equiv_m b$ e $a \equiv_n b$.

Esercizio 7. *Si dimostri che per ogni numero naturale n si ha $7^n \equiv_8 1$ se n è pari, e $7^n \equiv_8 7$ se n è dispari.*

Soluzione

a) Assumiamo n pari. Allora $n = 2k$ con $k \in \mathbb{N}$. Possiamo procedere per induzione su k.

(Caso base: $k = 0$**)** $7^0 = 1$. $1 \equiv_8 1$ è vero perché $8 \mid 0$.

(Caso ind: $k > 0$**)** Supponiamo $8 \mid (7^{2k} - 1)$ e verifichiamo l'asserto per $n = 2(k+1)$.

$\exists c \in \mathbb{Z}.((7^{2k} - 1) = 8c)$	(ipotesi induttiva)
$7^{2k} = 8c + 1$	
$7^{2k+2} = 49(8c + 1)$	
$7^{2(k+1)} - 1 = 49 \cdot 8c + 48)$	
$7^{2(k+1)} - 1 = 8(49c + 6)$	
$8 \mid (7^{2(k+1)} - 1)$	

b) Assumiamo n dispari. Allora $n = 2k + 1$ con $k \in \mathbb{N}$. Possiamo procedere per induzione su k.

(Caso base: $k = 0$**)** $7^1 = 7$. $7 \equiv_8 7$ è vero perché $8 \mid 0$.

(Caso ind: $k > 0$**)** Supponiamo $8 \mid (7^{2k+1} - 7)$ e verifichiamo l'asserto per $n = 2(k+1) + 1$.

$\exists c \in \mathbb{Z}.((7^{2k+1} - 7) = 8c)$	(ipotesi induttiva)
$7^{2k+1} = 8c + 7$	
$7^{2k+2+1} = 49(8c + 7)$	
$7^{2(k+1)+1} - 7 = 49 \cdot 8c + 7 \cdot 48$	
$7^{2(k+1)+1} - 7 = 8(49c + 42)$	
$8 \mid (7^{2(k+1)+1} - 7)$	