Es. Scrivere in base $b=3$ il numero

242

Oss: $243 = 3^5 = 1\cdot3^5+0\cdot3^4+0\cdot3^3+0\cdot3^2+0\cdot3+0$

$[243]_{10} = [x]_3 = [100000]_3$

$[242]_{10} = [x]_3$? $= [22222]_3$

Oss: se $b=10$ $\quad 1000 = 1\cdot10^3+0\cdot10^2+0\cdot10+0$

$999 = 9\cdot10^2+9\cdot10+9$

$242 : 3 = 80$

-2

2

$242 = 80\cdot3+2 = (26\cdot3+2)\cdot3+2 =$

$80 : 3 = 26$

20

2

$= 26\cdot3^2+2\cdot3+2$

$= (8\cdot3+2)\cdot3^2+2\cdot3+2 =$

$80 = 26\cdot3+2$

$8\cdot3^3+2\cdot3^2+2\cdot3+2$

$26 = 8\cdot3+2$

$= (2\cdot3+2)\cdot3^3+2\cdot3^2+2\cdot3+2$

$8 = 2\cdot3+2$

$= 2\cdot3^4+2\cdot3^3+2\cdot3^2+2\cdot3+2$

$\rightarrow [22222]_3$

OSS: perché $b \geq 2$?

$b = 1 \rightarrow b^k = 1 \quad \forall k \in \mathbb{N}$

I coefficienti a_j dovrebbero verificare

$0 \leq a_j \leq b-1 \rightarrow a_j = 0 \quad \forall j$!!!

Non è possibile

Come si possono eseguire le addizioni in base $b \neq 10$?

In base 10:

$$\begin{array}{r} {\scriptstyle (1)\,(1)} \\ 347 \\ +\ 598 \\ \hline 945 \end{array}$$

$15 = (1) \cdot 10 + (5)$

$14 = 1 \cdot 10 + (4)$

$9 = 0 \cdot 10 + (9)$

In un'altra base (es. $b = 5$)

(1) $[321]_5 + [123]_5 =$

$= (3 \cdot 5^2 + 2 \cdot 5 + 1) + (1 \cdot 5^2 + 2 \cdot 5 + 3)$

$= (3+1)5^2 + (2+2) \cdot 5 + (1+3) =$

$= \underset{<5}{4} \cdot 5^2 + \underset{<5}{4} \cdot 5 + \underset{<5}{4}$

$\rightarrow [321]_5 + [123]_5 = [444]_5$

② $[321]_5 + [444]_5$

$(3 \cdot 5^2 + 2 \cdot 5 + 1) + (4 \cdot 5^2 + 4 \cdot 5 + 4) =$

$= (3+4) \cdot 5^2 + (2+4) \cdot 5 + (1+4) =$

$= \underset{\geq 5}{7} \cdot 5^2 + \underset{\geq 5}{6} \cdot 5 + \underset{\geq 5}{5}$

$\rightarrow [765]_5$? NO

i coefficienti devono essere ≤ 4

$(3+4) \cdot 5^2 + (2+4) \cdot 5 + (1+4)$

$= 7 \cdot 5^2 + 6 \cdot 5 + 5 =$

$= 7 \cdot 5^2 + 6 \cdot 5 + (1 \cdot 5 + 0)$

$= 7 \cdot 5^2 + (6+1) \cdot 5 + 0$

$= 7 \cdot 5^2 + 7 \cdot 5 + 0$

$= 7 \cdot 5^2 + (1 \cdot 5 + 2) \cdot 5 + 0$

$= 7 \cdot 5^2 + 1 \cdot 5^2 + 2 \cdot 5 + 0$

$= 8 \cdot 5^2 + 2 \cdot 5 + 0 =$

$= (1 \cdot 5 + 3) \cdot 5^2 + 2 \cdot 5 + 0$

$= 1 \cdot 5^3 + 3 \cdot 5^2 + 2 \cdot 5 + 0$

$\leq 4 \quad \leq 4 \quad \leq 4 \quad \leq 4$

$\rightarrow [321]_5 + [444]_5 = [1320]_5$

Anche in colonna

$$\begin{array}{r} {\scriptstyle 1\,1\,1} \\ 321 \\ +\ 444 \\ \hline 1320 \end{array}$$

$4+1=5=1\cdot5+0$

$4+2+1=7=1\cdot5+2$

$4+3+1=8=1\cdot5+3$

$1=0\cdot5+1$

Abbiamo utilizzato le classi di resti modulo 5

Vogliamo ora verificare il calcolo in base 10: trasformiamo tutto in base 10 e facciamo la somma in base 10: viene la stessa cosa?

$[321]_5 = 3\cdot5^2+2\cdot5+1 = 86$

$[444]_5 = 4\cdot5^2+4\cdot5+4 = 124$

$$\begin{array}{r} {\scriptstyle 1\,\overset{\uparrow}{8}\,6} \\ +\ 124 \\ \hline 210 \end{array}$$

$86+124=210$

$[1320]_5 = 1\cdot5^3+3\cdot5^2+2\cdot5+0 =$

$125+75+10 = \boxed{210}$ ok!

Torniamo agli esercizi lasciati:

① Sia X un insieme $X \neq \emptyset$ e sia R una relazione di equivalenza. Siano poi $x, y \in X$ e $[x]$, $[y]$ le loro classi di equivalenza. Allora si verifica una sola delle due possibilità

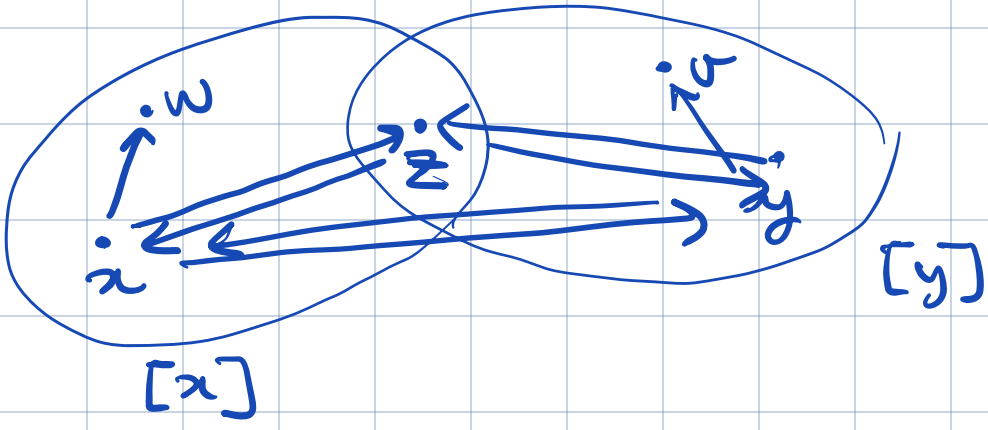
1) $[x] \cap [y] = \emptyset$

2) $[x] = [y]$.

dim: Supponiamo che $[x] \cap [y] \neq \emptyset$ e mostriamo che allora $[x] = [y]$ cioè $[x] \subseteq [y]$ e $[y] \subseteq [x]$.

Mostriamo dapprima che $x \in [y]$ e $y \in [x]$.

Sia $z \in [x] \cap [y]$, cioè
xRz e yRz



So che xRx, yRy (Riflessiva)
e poiché xRz anche zRx
yRz anche zRy (simmetria)

Mostro che xRy e yRx:
infatti $xRz, zRy \rightarrow xRy$
Transitiva

e $yRz, zRx \rightarrow yRx$
transitiva

$\rightarrow x \in [y], \quad y \in [x]$

Mostriamo ora che $[x] \subseteq [y]$:
Sia $w \in [x]$ cioè xRw, ma

allora $yRx,\ xRw \longrightarrow yRw$
(transitività)

cioè $w \in [y]$

Analogamente mostriamo che $[y] \subseteq [x]$
sia $v \in [y]$ cioè yRv

Allora $xRy,\ yRv \rightarrow xRv$
(transitività)

cioè $v \in [x]$. FINE

---

(2) sia $X = \mathbb{N} - \{0\}$
siano $n, m \in X$ e poniamo
$n R m$ se n è divisibile per m.
Mostrare che R è una relazione
d'ordine

(OSS: è una relazione d'ordine parziale)

Ricordo che n è divisibile per m

se $\exists q \in \mathbb{N}$ tale che $n = q m$

1) R è riflessiva?

Sia $n \in X$ $\quad nRn$? sì

perché $n = 1 \cdot n$
$\quad\quad\quad\quad\quad \overset{\shortparallel}{q}$

2) R è antisimmetrica? sì:

Siano $n, m \in X$ e supponiamo nRm e mRn, cioè

$\exists q_1 \in \mathbb{N}$ tale che $n = q_1 m$

$\exists q_2 \in \mathbb{N}$ tale che $m = q_2 n$

quindi $n = q_1 \cdot (q_2 n) =$
$= (q_1 q_2) \cdot n$

perché $\underline{\underline{n \neq 0}}$ per la legge di cancellazione del prodotto $1 = q_1 q_2$

e quindi $q_1 = q_2 = 1$ cioè

$n = m$.

3) R è Transitiva? sì:

Siano $n, m, p \in X$ e supponiamo nRm, mRp e mostriamo che allora nRp.

Supponiamo quindi che $\exists q_1, q_2 \in \mathbb{N}$ tali che

$n = q_1 m$

$m = q_2 p$

ma allora $n = q_1(q_2 p) = (q_1 q_2) \cdot p$

e quindi n è divisibile per p, cioè nRp.

DIVISORI e MASSIMO COMUNE DIVISORE

(Cazzola cap 4 pagg 16 e seguenti)

Ricordo la definizione

Definizione: Dati $a, b \in \mathbb{N}$, $b \neq 0$

diciamo che

- b è un divisore di a
- a è divisibile per b
- a è multiplo di b

- la divisione di a per b è esatta

se $\exists\, q \in \mathbb{N}$ tale che $a = qb$

e scriviamo $a : b = q$.

OSS:

① $a = 0$ è divisibile per ogni $b \neq 0$

Infatti $0 = 0 \cdot b \quad \forall b \neq 0$

② Se $a \neq 0$, si ha che a è divisibile per a: infatti

$a = 1 \cdot a$

③ $\forall a \in \mathbb{N}$ a è divisibile per 1:

$a = a \cdot 1$

④ Se $a \neq 0$ e

$a = q \cdot b \qquad q, b \neq 0$

$(a, b, q \in \mathbb{N})$

allora $q \leq a$ e $b \leq a$.

Infatti: Poiché $q, b \neq 0$ si ha

che $\exists\, n, m \in \mathbb{N}$: $q = n^+$

$b = m^+$

Allora

$$a = qb = q m^+ = qm + q$$

$qm \in \mathbb{N}$

↑ definizione di prodotto

cioè $q \leq a$

↑ era la definizione!!

analogamente

$$a = q \cdot b = bq = b m^+ = bm + b$$

$bm \in \mathbb{N}$

cioè $b \leq a$

Abbiamo mostrato che: tutti i divisori di un numero $a \in \mathbb{N}$, $a \neq 0$ sono minori o uguali al numero a stesso.

Problema: dati $a, b \in \mathbb{N}$ trovare tutti e soli i divisori comuni di a e b.

OSS: Se $a = b = 0$, allora $\forall\, q \in \mathbb{N}$, $q \neq 0$

q divide a e b.

Definizione: Dati $a, b \in \mathbb{N}$ non entrambi nulli, definiamo MASSIMO COMUNE DIVISORE di a e b e lo denotiamo $MCD(a,b)$ il più grande fra i divisori comuni di a e b.

OSS: (1) Se $a = b = 0$ non esiste $MCD(a,b)$ poichè $\forall q \in \mathbb{N}, q \neq 0$ q è un divisore comune.

(2) Se $a = 0$, $b \neq 0$
$MCD(0, b) = b$

Mostreremo che il problema di trovare tutti i divisori comuni di a e b è legato alla determinazione del $MCD(a,b)$

PROPOSIZIONE:

Dati $a, b \in \mathbb{N}$ non entrambi nulli, i divisori comuni di a e b sono tutti e soli i divisori del $MCD(a,b)$.

dim: Dobbiamo dimostrare che

1) Se $d \in \mathbb{N}$, $d \neq 0$ è un divisore comune di a e b, allora d divide $MCD(a,b)$
(segue dal teorema di BÉzout)

2) Se $d \in \mathbb{N}$, $d \neq 0$ divide $MCD(a,b)$ allora d è un divisore comune di a e b.

Dimostriamo 2)

Sia $d \in \mathbb{N}$, $d \neq 0$ un divisore di $MCD(a,b)$ cioè $\exists\, q \in \mathbb{N}$ tale che

$$MCD(a,b) = qd$$

Poiché $MCD(a,b)$ divide a e divide b, allora $\exists\, q_1, q_2 \in \mathbb{N}$ tali che

$a = q_1 \cdot MCD(a,b)$

$b = q_2 \cdot MCD(a,b)$

da cui $a = q_1 \cdot (qd) = (q_1 q) \cdot d$

$b = q_2 (qd) = (q_2 q) \cdot d$

cioè d divide a e b.

OSS: Per trovare i divisori comuni di a e b (non entrambi nulli) possiamo trovare $MCD(a,b)$ e i suoi divisori. Questo metodo è utile perché è possibile determinare $MCD(a,b)$ SENZA trovare i divisori comuni di a e b: METODO DELLE DIVISIONI SUCCESSIVE.

ESEMPIO:

Trovare $MCD(241, 148)$

$a = 241$

$b = 148$

$148 < 241$

$241 : 148 = 1$
$\quad 93$

$241 = 1 \cdot 148 + 93$

OSSERVAZIONE: i divisori comuni di 241 e 148 sono tutti e soli i divisori comuni di 148 e 93

Infatti se $d \in \mathbb{N}$, $d \neq 0$ divide 148 e 93 allora

$148 = q_1 d \qquad q_1, q_2 \in \mathbb{N}$
$93 = q_2 d$

e allora $241 = q_1 d + q_2 d =$
$= (\underbrace{q_1 + q_2}_{\in \mathbb{N}}) d$

d divide 241.

D'altra parte se d divide 241 e 148, allora d divide anche 93:

Infatti $241 = 148 + 93$

cioè $93 = 241 - 148$

ma $\exists\ q_1, q_2$: $241 = q_1 \cdot d$

$148 = q_2 \cdot d$

da cui $93 = q_1 d - q_2 d =$

$= (q_1 - q_2)\, d$

d divide 93.

Quindi $MCD(241, 148) = MCD(148, 93)$

ripartiamo:

$148 = 1 \cdot 93 + 55$

Come prima

$MCD(148, 93) = MCD(93, 55)$

$93 = 1 \cdot 55 + 38$

$MCD(93, 55) = MCD(55, 38)$

$55 = 1 \cdot 38 + 17$

$MCD(55, 38) = MCD(38, 17)$

$38 = 2 \cdot 17 + 4$

$MCD(38, 17) = MCD(17, 4)$

$17 = 4 \cdot 4 + 1$

$MCD(17, 4) = MCD(4, 1)$

$4 = 4 \cdot 1 + 0$

$1 = MCD(4, 1) = \dots = MCD(241, 148)$

Il $MCD(a, b)$ è l'ultimo resto nelle divisioni successive diverso da 0

Abbiamo sfruttato questa

Proposizione:

Siano $a, b \in \mathbb{N}$, $b \neq 0$ e siano $q, r \in \mathbb{N}$ $0 \leq r \leq b-1$ tali che

$$a = qb + r$$

I divisori comuni di a e b sono tutti e soli i divisori comuni di b e r e quindi.

$$MCD(a,b) = MCD(b,r)$$

(se $r \neq 0$; se $r = 0$ allora $MCD(a,b) = b$)

(Non la dimostriamo in generale: l'abbiamo fatta su un esempio)

ESERCIZIO: Determinare $MCD(220, 121)$

con il metodo delle divisioni successive

(risultato: $MCD(220, 121) = 11$)